PRILOG III

ZAHJTEVI ZA IZRADU, ISPITIVANJE, UGRADNJU, RAD I POPRAVAK PAMETNIH TAHOGRAFA I NJIHOVIH SASTANVIH DJELOVA (PRILOG I.C)

I. Definicije:

1) **„digitalni tahograf"** ili **„tahograf prve generacije"** znači digitalni tahograf koji nije pametni tahograf;
2) **„spoljni uređaj GNSS-a"** znači uređaj koji sadrži prijemnik GNSS-a kad jedinica u vozilu nije samostalna te ostale sastavne dijelove potrebne za zaštitu prenosa podataka o položaju ostatku jedinice u vozilu;
3) **"opisna mapa"** znači cjelokupna mapa, u elektroničkom ili fizičkom obliku, koja sadrži sve informacije koje je proizvođač ili njegov zastupnik dostavio homologacijskom tijelu u svrhu homologacije tahografa ili nekog njegovog sastavnog dijela, uključujući certifikate, obavljena ispitivanja definisana u Prilogu I.C te nacrte, fotografije i druge relevantne dokumente;
1) **„opisna dokumentacija"** znači opisna mapa, u elektronskom ili fizičkom obliku, kojoj su priloženi svi drugi dokumenti koje je homologacijsko tijelo dodalo opisnoj mapi tokom provođenja svojih djelatnosti, uključujući certifikat o EZ homologaciji tahografa ili nekog njegova sastavnog dijela;
2) **„legeda opisne dokumentacije"** znači dokument u kojem je naveden i brojevima označen sadržaj opisne dokumentacije te u kojem su utvrđeni svi relevantni dijelovi te dokumentacije. U formatu tog dokumenta razlikuju se uzastopni koraci u postupku EZ homologacije, uključujući datume svih revizija i ažuriranja opisne dokumentacije;
3) **„uređaj za rano otkrivanje na daljinu"** znači oprema jedinice u vozilu koja se upotrebljava za ssprovođenje ciljanih provjera na putu;
4) **„sastavni dio tahografa"** ili **„sastavni dio"** znači bilo koji od sljedećih elemenata: jedinica u vozilu, senzor kretanja, tahografska kartica, tahografski listić, spoljni uređaj GNSS-a i uređaj za rano otkrivanje na daljinu;
5) **„homologacijsko tijelo"** znači tijelo države članice nadležno za ssprovođenje homologacije tahografa ili njegovih sastavnih dijelova, postupka ovlaštenja, izdavanja i, prema potrebi, povlačenja certifikata o homologaciji, koje djeluje u svojstvu kontaktne točke za homologacijska tijela drugih država članica te osigurava da proizvođači ispunjuju svoje obveze u pogledu shodnosti sa zahtjevima iz ove Uredbe.
6) **‚pametni tahograf'** ili **‚tahograf druge generacije'** znači digitalni tahograf koji je izrađen shodno ovim pravilnikom i prilozima
7) **‚sastavni dio tahografa'** znači bilo koji od sljedećih elemenata: jedinica u vozilu, senzor kretanja, tahografski listić, spoljni uređaj GNSS-a i spoljni uređaj za rano otkrivanje na daljinu;";
8) **„homologacijsko tijelo"** znači tijelo države nadležno za sprovođenje homologacije tahografa ili njegovih sastavnih dijelova, postupka ovlaštenja, izdavanja i, prema potrebi, povlačenja certifikata o homologaciji, koje djeluje u svojstvu kontaktne tačke za homologacijska tijela drugih država članica te osigurava da proizvođači ispunjuju svoje obveze u pogledu shodnosti sa zahtjevima iz ove Uredbe.
9) **‚jedinica u vozilu'** znači tahograf bez senzora kretanja i kabla za spajanje senzora kretanja. To može biti jedna jedinica ili više jedinica raspoređenih u vozilu te uključuje procesorsku jedinicu, podatkovnu memoriju, funkciju mjerenja vremena, dva uređaja sa sučeljem za pametne kartice za vozača i suvozača, pisač, displej, priključke i uređaje za unose korisnika, prijemnik za GNSS i uređaj za komunikaciju na daljinu. Jedinica u vozilu može se sastojati od sljedećih komponenti koje podliježu homologaciji:
    - jedinica u vozilu kao zasebna komponenta (uključujući prijemnik GNSS-a i uređaj za komunikaciju na daljinu),
    - glavno kućište jedinice u vozilu (uključujući uređaj za komunikaciju na daljinu) i spoljni uređaj GNSS-a,
    - glavno kućište jedinice u vozilu (uključujući prijemnik GNSS-a) i spoljni uređaj za komunikaciju na daljinu,
    - glavno kućište jedinice u vozilu, spoljni uređaj GNSS-a i spoljni uređaj za komunikaciju na daljinu.

Ako se jedinica u vozilu sastoji od nekoliko jedinica raspoređenih u vozilu, glavno kućište jedinice u vozilu je jedinica koja sadrži procesorsku jedinicu, podatkovnu memoriju i funkciju mjerenja vremena.
‚jedinica u vozilu (VU)' upotrebljava se za ‚jedinicu u vozilu' ili ‚glavno kućište jedinice u vozilu'.";

II. Usluge koje se temelje na lokaciji

1. Proizvođači osiguravaju shodnost pametnih tahografa s uslugama pozicioniranja koje pružaju sistem Galileo i Evropski geostacionarni navigacijski sistem („EGNOS").

2. Uz sisteme navedene u stavu 1. proizvođači mogu odlučiti osigurati shodnost i s drugim satelitskim navigacijskim sistemima.

III. Postupci za homologaciju tahografa i sastavnih dijelova tahografa

1. Proizvođač ili njegov zastupnik predaje zahtjev za homologaciju tahografa ili njegovih sastavnih dijelova ili skupine sastavnih dijelova homologacijskim tijelima koja određuju države članice. Zahtjev se sastoji od opisne mape koja sadrži informacije o svakom predmetnom dijelu uključujući, prema potrebi, certifikate o homologaciji drugih sastavnih dijelova potrebnih za upotpunjivanje tahografa te sve druge relevantne dokumente.

2. Država članica odobrava homologaciju tahografu, njegovu sastavnom dijelu ili skupini sastavnih dijelova koji su usklađeni s administrativnim i tehničkim zahtjevima navedenima u članu 1. stavu 2. ili 3. kako je primjenjivo. U tom slučaju homologacijsko tijelo podvlasniku zahtjeva izdaje certifikat o homologaciji.

3. Homologacijsko tijelo može zatražiti od proizvođača ili njegova zastupnika da dostavi dodatne informacije.

4. Proizvođač ili njegov zastupnik homologacijskim tijelima i tijelima nadležnima za izdavanje certifikata stavlja na raspolaganje onoliko tahografa ili sastavnih dijelova tahografa koliko je potrebno za uspješnu ssprovođenje postupka homologacije.

5. Ako proizvođač ili njegov zastupnik zatraži homologaciju određenih sastavnih dijelova ili skupina sastavnih dijelova tahografa, homologacijskim tijelima dostavlja druge sastavne dijelove koji su već homologirani i druge dijelove potrebne za izradu potpunog tahografa, kako bi ta tijela mogla provesti potrebna ispitivanja.

IV. Izmjene homologacije

1. Proizvođač ili njegov zastupnik bez odlaganja izvješćuje homologacijska tijela koja su odobrila prvobitnu homologaciju o svim izmjenama softvera ili hardvera tahografa ili vrste materijala upotrijebljenih u njegovoj proizvodnji koje se unose u opisnu dokumentaciju te dostavlja zahtjev za izmjenu homologacije.

2. Homologacijska tijela mogu revidirati ili proširiti postojeću homologaciju ili izdati novu homologaciju u skladu s vrstom i značajkama izmjena.

„Revizija" se sprovodi ako homologacijsko tijelo smatra da su izmjene softvera ili hardvera tahografa ili vrste materijala upotrijebljenih u njegovoj proizvodnji neznatne. U tom slučaju homologacijsko tijelo izdaje revidirane dokumente iz opisne dokumentacije u kojima je navedena vrsta provedenih izmjena i datum njihova odobrenja. Ažurirana verzija opisne dokumentacije u pročišćenom obliku uz detaljne opise provedenih izmjena dovoljna je za ispunjenje tog zahtjeva.

„Proširenje" se sprovodi ako homologacijsko tijelo smatra da su izmjene softvera ili hardvera tahografa ili vrste materijala upotrijebljenih u njegovoj proizvodnji znatne. U tom slučaju može zatražiti sprovođenje novih ispitivanja i o tome izvijestiti proizvođača ili njegova zastupnika. Pokažu li se ta ispitivanja zadovoljavajućima, homologacijsko tijelo izdaje revidirani certifikat o homologaciji koji sadrži broj koji se odnosi na dodijeljeno proširenje. U certifikatu o homologaciji navodi se razlog proširenja i datum njegova izdavanja.

3. U kazalu opisne dokumentacije navodi se datum najnovijeg proširenja ili revizije homologacije ili datum najnovije konsolidacije ažurirane verzije homologacije.

4. Nova homologacija potrebna je ako bi zbog zatraženih izmjena homologovanog tahografa ili njegovih dijelova došlo do izdavanja novog certifikata o sigurnosti ili interoperabilnosti.

PIRLOG 1 C Zahtjevi u pogledu izrade, ispitivanja, ugradnje i pregleda

4.5.2 Identifikacija IC kartice
4.5.2.1 Identifikacija čipa
4.5.2.2 DIR (prisutan samo na tahografskim karticama druge generacije)
4.5.2.3 Podaci ATR-a (uvjetno, prisutno samo na tahografskim karticama druge generacije)
4.5.2.4 Podaci proširene veličine (uvjetno, prisutno samo na tahografskim karticama druge generacije)
4.5.3 Kartica vozača
4.5.3.1 Tahografska aplikacija (pristup jedinicama u vozilu prve i druge generacije)
4.5.3.1.1 Identifikacija aplikacije
4.5.3.1.2 Ključevi i certifikati
4.5.3.1.3 Identifikacija kartice
4.5.3.1.4 Identifikacija vlasnika kartice
4.5.3.1.5 Preuzimanje podataka s kartice
4.5.3.1.6 Podaci o vozačkoj dozvoli
4.5.3.1.7 Podaci o događajima
4.5.3.1.8 Podaci o kvarovima
4.5.3.1.9 Podaci o aktivnosti vozača
4.5.3.1.10 Podaci o upotrijebljenim vozilima
4.5.3.1.11 Mjesta početka i/ili završetka dnevnog radnog vremena
4.5.3.1.12 Podaci o upotrebi kartice
4.5.3.1.13 Podaci o aktivnostima nadzora
4.5.3.1.14 Podaci o posebnim stanjima
4.5.3.2 Tahografska aplikacija druge generacije (nije dostupno jedinici u vozilu prve generacije)
4.5.3.2.1 Identifikacija aplikacije
4.5.3.2.2 Ključevi i certifikati
4.5.3.2.3 Identifikacija kartice
4.5.3.2.4 Identifikacija vlasnika kartice
4.5.3.2.5 Preuzimanje podataka s kartice
4.5.3.2.6 Podaci o vozačkoj dozvoli
4.5.3.2.7 Podaci o događajima
4.5.3.2.8 Podaci o kvarovima
4.5.3.2.9 Podaci o aktivnosti vozača
4.5.3.2.10 Podaci o upotrijebljenim vozilima
4.5.3.2.11 Mjesta i položaji početka i/ili završetka dnevnog radnog vremena
4.5.3.2.12 Podaci o upotrebi kartice
4.5.3.2.13 Podaci o aktivnostima nadzora
4.5.3.2.14 Podaci o posebnim stanjima
4.5.3.2.15 Podaci o upotrijebljenoj jedinici u vozilu
4.5.3.2.16 Podaci o mjestima na kojima se dostižu tri sata akumulisane vožnje
4.5.4 Kartica radionice
4.5.4.1 Tahografska aplikacija (pristup jedinicama u vozilu prve i druge generacije)
4.5.4.1.1 Identifikacija aplikacije
4.5.4.1.2 Ključevi i certifikati
4.5.4.1.3 Identifikacija kartice
4.5.4.1.4 Identifikacija vlasnika kartice
4.5.4.1.5 Preuzimanje podataka s kartice

4.5.4.1.6 Podaci o kalibraciji i prilagođavanju vremena
4.5.4.1.7 Podaci o događajima i kvarovima
4.5.4.1.8 Podaci o aktivnosti vozača
4.5.4.1.9 Podaci o upotrijebljenim vozilima
4.5.4.1.10 Podaci o početku i/ili završetku dnevnog radnog vremena
4.5.4.1.11 Podaci o upotrebi kartice
4.5.4.1.12 Podaci o aktivnostima nadzora
4.5.4.1.13 Podaci o posebnim stanjima
4.5.4.2 Tahografska aplikacija druge generacije (nije dostupno jedinici u vozilu prve generacije)
4.5.4.2.1 Identifikacija aplikacije
4.5.4.2.2 Ključevi i certifikati
4.5.4.2.3 Identifikacija kartice
4.5.4.2.4 Identifikacija vlasnika kartice
4.5.4.2.5 Preuzimanje podataka s kartice
4.5.4.2.6 Podaci o kalibraciji i prilagođavanju vremena
4.5.4.2.7 Podaci o događajima i kvarovima
4.5.4.2.8 Podaci o aktivnosti vozača
4.5.4.2.9 Podaci o upotrijebljenim vozilima
4.5.4.2.10 Podaci o početku i/ili završetku dnevnog radnog vremena
4.5.4.2.11 Podaci o upotrebi kartice
4.5.4.2.12 Podaci o aktivnostima nadzora
4.5.4.2.13 Podaci o upotrijebljenoj jedinici u vozilu
4.5.4.2.14 Podaci o mjestima na kojima se dostižu tri sata akumulisane vožnje
4.5.4.2.15 Podaci o posebnim stanjima
4.5.5 Kontrolna kartica
4.5.5.1 Tahografska aplikacija (pristup jedinicama u vozilu prve i druge generacije)
4.5.5.1.1 Identifikacija aplikacije
4.5.5.1.2 Ključevi i certifikati
4.5.5.1.3 Identifikacija kartice
4.5.5.1.4 Identifikacija vlasnika kartice
4.5.5.1.5 Podaci o aktivnostima nadzora
4.5.5.2 Tahografska aplikacija druge generacije (nije dostupno jedinici u vozilu prve generacije)
4.5.5.2.1 Identifikacija aplikacije
4.5.5.2.2 Ključevi i certifikati
4.5.5.2.3 Identifikacija kartice
4.5.5.2.4 Identifikacija vlasnika kartice
4.5.5.2.5 Podaci o aktivnostima nadzora
4.5.6 Kartica preduzeća
4.5.6.1 Tahografska aplikacija (pristup jedinicama u vozilu prve i druge generacije)
4.5.6.1.1 Identifikacija aplikacije
4.5.6.1.2 Ključevi i certifikati
4.5.6.1.3 Identifikacija kartice
4.5.6.1.4 Identifikacija vlasnika kartice
4.5.6.1.5 Podaci o aktivnostima preduzeća
4.5.6.2 Tahografska aplikacija druge generacije (nije dostupno jedinici u vozilu prve generacije)
4.5.6.2.1 Identifikacija aplikacije

UVOD

Sistem digitalnog tahografa prve generacije upotrebljava se od 1. svibnja 2006. U prijevozu unutar zemlje može se upotrebljavati do isteka njegova životnog ciklusa. U međunarodnom prijevozu sva se vozila 15 godina nakon stepena na snagu ove Uredbe Komisije moraju opremiti drugom generacijom pametnih tahografa koja je u skladu s tahografima uvedenima ovom Uredbom.

Ovaj Prilog sadrži zahtjeve u pogledu uređaja za evidentiranje podataka i tahografskih kartica druge generacije. Od datuma njegova uvođenja u vozila koja se prvi put registriraju ugrađuju se uređaji za evidentiranje podataka druge generacije te se izdaju tahografske kartice druge generacije.

Kako bi se poticalo nesmetano uvođenje sistema tahografa druge generacije,

- tahografske kartice druge generacije osmišljene su tako da se mogu upotrebljavati i u jedinicama u vozilima prve generacije;
- zamjena važećiih tahografskih kartica prve generacije ne zahtijeva se na datum uvođenja.

Time će se vozačima omogućiti da zadrže vlastitu jedinstvenu karticu vozača te da je upotrebljavaju za oba sistema.

Međutim, uređaj za evidentiranje podataka druge generacije kalibrira se samo upotrebom kartica radionice druge generacije.

Ovaj Prilog sadrži sve zahtjeve koji se odnose na interoperabilnost sistema tahografa prve i druge generacije.

Dodatak 15. sadrži dodatne pojedinosti o načinu upravljanja supostojanjem dvaju sistema.

Popis dodataka

Dodatak 1.: RJEČNIK S PODACIMA

Dodatak 2.: SPECIFIKACIJE TAHOGRAFSKE KARTICE

Dodatak 3.: PIKTOGRAMI

1 DEFINICIJE

U ovom Prilogu:

a) „aktiviranje" znači: faza u kojoj je tahograf u potpunosti operativan i sprovodi sve funkcije, uključujući sigurnosne funkcije, upotrebom kartice radionice;

b) „autentifikacija" znači: funkcija namijenjena utvrđivanju i provjeri identiteta;

c) „autentičnost" znači: obilježje da informacija dolazi od izvora čiji je identitet moguće provjeriti;

d) „ugrađeno ispitivanje (BIT)" znači: ispitivanja koja se provode na zahtjev i koja aktivira operater ili se aktiviraju spoljnom opremom;

e) „kalendarski dan" znači: dan koji traje od 00:00 sati do 24:00 sata. Svi kalendarski dani odnose se na koordinirano svjetsko vrijeme (UTC);

f) „kalibracija" pametnog tahografa znači: ažuriranje ili potvrda parametara vozila koje treba sačuvati u memoriji podataka. Parametri vozila uključuju identifikaciju vozila (VIN, VRN i država registracije) i karakteristike vozila (w, k, l, veličina guma, podešavanje uređaja za ograničavanje brzine (prema potrebi), trenutno vrijeme po UTC-u, trenutno stanje na brojaču kilometara); tokom kalibracije uređaja za evidentiranje podataka u memoriji podataka arhiviraju se i tipovi i identifikatori svih postavljenih plombi koje su važne za homologaciju; svako ažuriranje ili potvrđivanje samo vremena po UTC-u smatra se prilagodbom vremena, a ne kalibracijom, pod uslovom da se time ne proturječi zahtjevu 409; za kalibriranje uređaja za evidentiranje podataka potrebna je kartica radionice;

g) „broj kartice" znači: broj od 16 alfanumeričkih znakova kojim se na jedinstven način identifikuje tahografska kartica unutar neke države članice. Broj kartice uključuje indeks rednog broja kartice (prema potrebi), indeks zamjene kartice i indeks obnavljanja kartice; kartica se tako na jedinstven način identifikuje oznakom države članice izdavateljice i brojem kartice;

h) „indeks rednog broja kartice" znači: 14. alfanumerički znak broja kartice koji se upotrebljava za razlikovanje različitih kartica izdatih poduzeću, radionici ili nadzornom tijelu koje ima pravo na više tahografskih kartica. Preduzeće, radionica ili nadzorno tijelo na jedinstven se način identifikuje s pomoću prvih 13 cifara broja kartice;

i) „indeks obnavljanja kartice" znači: 16. alfanumerički znak broja kartice koji se uvećava pri svakom obnavljanju tahografske kartice;

j) „indeks zamjene kartice" znači: 15. alfanumerički znak broja kartice koji se uvećava pri svakoj zamjeni tahografske kartice;

k) „karakteristični koeficijent vozila" znači: brojčana veličina koja navodi vrijednost izlaznog signala koji nastaje na priključnom mjestu uređaja za evidentiranje podataka i vozila (na mjenjaču ili osovini tačka) dok vozilo prelazi put od jednog kilometra u standardnim uslovima ispitivanja kako je definisano u zahtjevu 414. Karakteristični koeficijent izražava se u impulsima po kilometru (w = ⋯ imp/km);

l) „kartica preduzeća" znači: tahografska kartica koju ovlaštena tijela u državi članici izdaju prijevoznom poduzeću koje upravlja vozilima u koja je ugrađen tahograf, a koja služi za identifikaciju

prijevoznog preduzeća te omogućava prikazivanje, preuzimanje i ispisivanje podataka sačuvanih u tahografu koje je prijevozno preduzeće zaključalo; m) „konstanta uređaja za evidentiranje podataka" znači: brojčana veličina koja navodi vrijednost ulaznog signala potrebnog za pokazivanje i evidentiranje dužine prijeđenog puta od jednog kilometra; ta se konstanta izražava u impulsima po kilometru (k = ⋯ imp/km)

n) „neprekidno vrijeme vožnje" izračunava se u uređaju za evidentiranje podataka kao: neprekidno vrijeme vožnje izračunava se kao trenutno akumulisano vrijeme vožnje određenog vozača od završetka posljednjeg perioda DOSTUPNOSTI ili PAUZE/ODMORA ili NEPOZNATO u trajanju od najmanje 45 minuta. U navedenom se izračunu prema potrebi uzimaju u obzir prethodne aktivnosti sačuvane na kartici vozača. Ako vozač nije umetnuo svoju karticu, izračun se temelji na zapisima iz podatkovne memorije koji se odnose na tekuće period u kojem kartica nije bila umetnuta u odgovarajući otvor za kartice;

o) „kontrolna kartica" znači: tahografska kartica koju ovlaštena tijela u državi članici izdaju nacionalnom nadležnom nadzornom tijelu, a koja služi za identifikaciju nadzornog tijela i, prema potrebi, službenika za kontrolu te koja omogućava pristup podacima sačuvanima u memoriji podataka, kartici vozača ili, prema potrebi, karticama radionice, u svrhu njihova čitanja, ispisivanja i/ili preuzimanja. Osim toga, omogućava pristup funkciji provjere kalibracije na putu i podacima na čitaču komunikacije ranog otkrivanja na daljinu;

p) „kumulativno vrijeme pauze" izračunava se u uređaju za evidentiranje podataka kao: kumulativno vrijeme pauze od vremena vožnje izračunava se kao trenutno akumulisano vrijeme DOSTUPNOSTI ili PAUZE/ODMORA ili NEPOZNATO u trajanju od najmanje 15 minuta za pojedinog vozača, od završetka posljednjeg perioda njegove DOSTUPNOSTI ili PAUZE/ODMORA ili NEPOZNATO u trajanju od najmanje 45 minuta. U navedenom se izračunu prema potrebi uzimaju u obzir prethodne aktivnosti sačuvane na kartici vozača. Nepoznata perioda negativnog vremenskog izračuna (početak nepoznatog perioda vremenski je kasniji od završetka nepoznatog perioda) zbog vremenskih preklapanja između dvaju različitih uređaja za evidentiranje podataka ne uzimaju se u obzir za izračun. Ako vozač nije umetnuo svoju karticu, izračun se temelji na zapisima iz podatkovne memorije koji se odnose na tekuće period u kojem kartica nije bila umetnuta u odgovarajući otvor za kartice;

q) „podatkovna memorija" znači: elektroničko sredstvo za arhiviranje podataka ugrađeno u uređaj za evidentiranje podataka;

r) „digitalni potpis" znači: podaci stavljeni na blok podataka ili kriptografska pretvorba bloka podataka koja omogućava primatelju bloka podataka dokazivanje autentičnosti i integriteta bloka podataka;

s) „preuzimanje podataka" znači: kopiranje, zajedno s digitalnim potpisom, dijela ili čitavog skupa datoteka zabilježenih u memoriji podataka jedinice u vozilu ili u memoriji tahografske kartice pod uslovom da taj proces ne mijenja niti briše sačuvane podatke. Proizvođači jedinica pametnih tahografa u vozilu i proizvođači opreme oblikovane i namijenjene za preuzimanje datoteka moraju poduzeti sve razumne mjere da osiguraju da prijevozna preduzeća ili vozači mogu preuzeti te podatke uz minimalnu odgodu. Preuzimanje datoteke s detaljnim podacima o brzini ne mora biti potrebno za utvrđivanje, no može se upotrijebiti za druge potrebe, kao što je istraživanje nesreća;

t) „kartica vozača" znači: tahografska kartica koju ovlaštena tijela u državi članici izdaju pojedinom vozaču, a koja služi za identifikaciju vozača te omogućava čuvanje podataka o aktivnosti vozača;

u) „djelatni opseg tačka" znači: srednja vrijednost prijeđenog puta pogonskog tačka kod punog okretaja. Mjerenje tog puta mora se obavljati u standardnim uslovima ispitivanja, kako je definisano u zahtjevu 414, i izražava se u obliku „l = ⋯ mm". Proizvođači vozila mogu nadomjestiti mjerenje tog puta teoretskim izračunom u kojem se uzima u obzir raspored opterećenja po osovinama za nenatovareno vozilo u stanju spremnom za vožnju. Metode takvog teoretskog izračuna odobrava nadležno tijelo države članice i mogu se poduzeti samo prije aktivacije tahografa;

v) „događaj" znači: neuobičajeno djelovanje koje otkrije pametni tahograf, a koje može biti rezultat pokušaja prijevare;

w) „spoljni uređaj GNSS-a" znači: uređaj koji sadrži prijemnik GNSS-a kad jedinica u vozilu nije samostalna te ostale sastavne dijelove potrebne za zaštitu prenosa podataka o položaju drugim dijelovima jedinice u vozilu;

x) „kvar" znači: neuobičajeno djelovanje koje otkrije pametni tahograf, a koje može biti rezultat nepravilnosti ili greške na uređaju;

y) „prijemnik GNSS-a" znači: elektronički uređaj koji prima i digitalno obrađuje signale iz jednoga globalnog satelitskog navigacijskog sistema ili više njih (eng. *Global Navigation Satellite System*, GNSS) radi pružanja informacija o položaju, brzini i vremenu;

z) „ugradnja” znači: postavljanje tahografa u vozilo;

aa) „interoperabilnost” znači: sposobnost sistema i temeljnih poslovnih procesa da razmjenjuju podatke i dijele informacije;

bb) „sučelje” znači: veza između sistema koja im omogućava međusobno povezivanje i interakciju;

cc) „položaj” znači: geografske koordinate vozila u određenom trenutku;

dd) „senzor kretanja” znači: dio tahografa na kojem se prikazuje signalna oznaka brzine vozila i/ili dužine prijeđenoga puta vozila;

ee) „nevažeća kartica” znači: kartica za koju se otkrije da je neispravna ili čija početna autentifikacija nije uspjela ili čiji datum početka važenja još nije dosegnut ili čiji je datum isteka prošao;

ff) „otvorena norma” znači: norma iz dokumenta o specifikaciji normi koja je dostupna besplatno ili uz nominalnu naplatu i može se kopirati, dijeliti ili upotrebljavati bez naknade ili uz nominalnu naknadu;

gg) „izvan područja primjene” znači: okolnosti u kojima uređaj za evidentiranje podataka nije potrebno upotrebljavati.

hh) „prekoračenje brzine” znači: prekoračenje dopuštene brzine vozila koja se utvrđuje u bilo kojem periodu dužem od 60 sekundi, tokom kojeg izmjerena brzina vozila prelazi graničnu brzinu podešenu uređajem za ograničenje brzine;

ii) „periodični pregled” znači: skup postupaka koji se obavljaju za provjeru radi li tahograf pravilno, odgovaraju li njegove postavke parametrima vozila i jesu li uređaji za manipulaciju spojeni na tahograf;

jj) „pisač” znači: sastavni dio uređaja za evidentiranje podataka koji daje ispis sačuvanih podataka;

kk) „komunikacija ranog otkrivanja na daljinu” znači: komunikacija između uređaja za rano otkrivanje na daljinu i čitača komunikacije ranog otkrivanja na daljinu tokom ciljanih provjera na putu u cilju daljinskog otkrivanja moguće manipulacije ili zloupotrebe uređaja za evidentiranje podataka;

ll) ‚uređaj za komunikaciju na daljinu’ ili ‚uređaj za rano otkrivanje na daljinu’ znači: oprema jedinice u vozilu koja se upotrebljava za sprovođenje ciljanih provjera na putu;

mm) „čitač komunikacije ranog otkrivanja na daljinu” znači: sistem koji upotrebljavaju službenici za kontrolu za ciljane provjere na putu;

nn) „obnavljanje” znači: izdavanje nove tahografske kartice kad postojećoj kartici istekne važnost ili kad postane neispravna pa je vraćena tijelu koje ju je izdalo. Obnavljanje uvijek podrazumijeva sigurnost da ne postoje dvije važeće kartice;

oo) „popravak” znači: bilo kakav popravak senzora kretanja, jedinice u vozilu ili kabla koji zahtijeva isključivanje s napajanja ili isključivanje s drugih sastavnih dijelova tahografa ili otvaranje senzora kretanja ili jedinice u vozilu;

pp) „zamjena kartice” znači: izdavanje tahografske kartice kao zamjene za postojeću karticu čiji su gubitak, krađa ili neispravnost prijavljeni, a nije vraćena tijelu koje ju je izdalo. Zamjena uvijek podrazumijeva rizik da mogu istodobno postojati dvije važeće kartice;

qq) „sigurnosno certifikovanje” znači: postupak kojim certifikacijsko tijelo koje je primijenilo zajednička mjerila tokom certifikacije potvrđuje da uređaj za evidentiranje podataka (ili njegov sastavni dio) ili tahografska kartica koja se ispituje zadovoljava sigurnosne zahtjeve utvrđene u odgovarajućim profilima zaštite;

rr) „samoispitivanje” znači: ispitivanja koja uređaj za evidentiranje podataka sprovodi ciklički i automatski radi otkrivanja kvarova;

ss) „izmjereno vrijeme” znači: trajni digitalni zapis koordiniranog svjetskog datuma i vremena (UTC);

tt) ‚prilagođavanje vremena’ znači: prilagođavanje trenutnog vremena; ta prilagođavanje mogu biti automatska u redovnim vremenskim razmacima, korištenjem referentnog vremena koje pruža prijemnik GNSS-a, ili se može obaviti u načinu rada za kalibraciju;”;

uu) „veličina gume” znači: oznaka dimenzije guma (spoljnih pogonskih tačka);

vv) „identifikacija vozila” znači: brojevi kojima se identifikuje vozilo: registracijski broj vozila (eng. Vehicle Registration Number, VRN) s oznakom države članice u kojoj je vozilo registrirano i identifikacijski broj vozila (eng. Vehicle Identification Number, VIN);

ww) za potrebe izračunavanja u uređaju za evidentiranje podataka „tjedan” znači: period između 00:00 sati UTC u ponedjeljak i 24:00 sata UTC u nedjelju;

xx) „kartica radionice” znači: tahografska kartica koju su ovlaštena tijela u državi članici izdala ovlaštenom osoblju proizvođača tahografa, instalatera, proizvođača vozila ili radionice koje je država

članica odobrila, a koja služi za identifikaciju vlasnika kartice te omogućava ispitivanje, kalibraciju i aktiviranje tahografa i/ili preuzimanje podataka iz njih;

yy) „adapter" znači: uređaj koji stalno daje signal brzine vozila i/ili prijeđene udaljenosti, osim onoga koji se upotrebljava za nezavisno otkrivanje kretanja, te koji se:

- ugrađuje i upotrebljava samo u vozilima tipa M1 i N1;
- ugrađuje kada nije mehanički moguće ugraditi bilo kakvu drugu vrstu postojećeg senzora kretanja, koji je inače usklađen s odredbama ovog Priloga i njegovih dodataka od 1. do 15.,
- ugrađuje između jedinice u vozilu i ondje gdje ugrađeni senzori ili alternativna sučelja proizvode impulse brzine/udaljenosti.
- Gledano iz jedinice u vozilu, ponašanje adaptera jednako je kao da je senzor kretanja, sukladan odredbama ovog Priloga i njegovih dodataka od 1. do 16., spojen na jedinicu u vozilu.

Upotrebom takvog adaptera u prethodno opisanim vozilima omogućuju se ugradnja i ispravna upotreba jedinice u vozilu koja je u skladu sa svim zahtjevima ovog Priloga.

Za ta vozila, pametni tahograf sastavljen je od kabla, adaptera i jedinice u vozilu;

zz) „integritet podataka" znači: tačnost i dosljednost sačuvanih podataka, na koje upućuje nedostatak bilo kakvih promjena podataka između dvaju ažuriranja podatkovnog zapisa. Integritet podrazumijeva da su podaci tačna preslika izvorne verzije, npr. da nisu postali neispravni u procesu njihova zapisivanja na tahografsku karticu ili namjensku opremu ili njihova čitanja s nje, ili tokom prenosa bilo kakvim komunikacijskim kanalom;

aaa) „zaštita podataka" znači: ukupne tehničke mjere koje su poduzete kako bi se osiguralo ispravno sprovođenje načela;

bbb) „sistem pametnog tahografa" znači: uređaj za evidentiranje podataka, tahografske kartice i skup svih uređaja koji su s njima direktno ili nedirektno povezani tokom njihove izrade, ugradnje, upotrebe, ispitivanja i nadzora, kao što su kartice, čitač komunikacije na daljinu i svi ostali uređaji za preuzimanje podataka, analizu podataka, kalibraciju, generisanje sigurnosnih elemenata, upravljanje njima ili njihovo uvođenje itd.

ccc) „datum uvođenja" znači: 36 mjeseci nakon stepena na snagu detaljnih odredbi.

To je datum:

- nakon kojeg se u vozila koja se prvi put registriraju ugrađuje tahograf koji je povezan s uslugom pozicioniranja na temelju satelitskog navigacijskog sistema,
- nakon kojeg vozila koja se prvi put registriraju mogu dostavljati podatke za ciljane provjere na putu nadležnim nadzornim tijelima dok je vozilo u pokretu
- i nakon kojeg vozila koja se prvi put registriraju mogu biti opremljena standardizovanim sučeljima putem kojih podatke koje je tahograf zabilježio ili generisao može na operativan način upotrebljavati spoljni uređaj;

ddd) „profil zaštite" znači: dokument koji se upotrebljava kao dio postupka certificiranja u skladu sa zajedničkim mjerilima i omogućava ssprovođenje nezavisnih specifikacija zahtjeva u pogledu osiguravanja informatičke sigurnosti;

eee) „tačnost GNSS-a": u kontekstu bilježenja položaja na temelju globalnog satelitskog navigacijskog sistema (GNSS) tahografima, znači vrijednost horizontalnog slabljenja preciznosti (eng. *Horizontal Dilution of Precision*, HDOP) izračunanu kao minimalne vrijednosti HDOP prikupljene na raspoloživim sistemima GNSS-a.

„fff) ‚akumulisano vrijeme vožnje' znači: vrijednost koja predstavlja ukupan akumulirani broj minuta vožnje za pojedino vozilo. Vrijednost akumulisanog vremena vožnje je zbir svih minuta koje funkcija praćenja aktivnosti vožnje uređaja za evidentiranje smatra VOŽNJOM i koristi se samo da bi se pokrenulo evidentiranje položaja vozila svaki put kad se dosegne višestruke tri sata akumulisane vožnje. Akumulisano vrijeme započinje po aktivaciji uređaja za evidentiranje. Na njega ne utiču nikakvi drugi uslovi kao što je vožnja izvan područja primjene ili vožnja trajektom/vozom. Vrijednost akumulisanog vremena vožnje nije namijenjena prikazivanju, ispisivanju ili preuzimanju.

2 OPŠTA OBILJEŽJA I FUNKCIJE UREĐAJA ZA EVIDENTIRANJE PODATAKA

2.1 Opšta obilježja

Svrha uređaja za evidentiranje podataka je evidentiranje, arhiviranje, prikaz, ispis i generisanje podataka o aktivnostima vozača.

Vozilo opremljeno uređajem za evidentiranje podataka u skladu s odredbama ovog Priloga mora imati pokazivač brzine i brojač kilometara. Te funkcije mogu biti ugrađene u uređaj za evidentiranje podataka.

01) Uređaj za evidentiranje podataka sastoji se od kabla, senzora kretanja i jedinice u vozilu.

02) Sučelje između senzora kretanja i jedinica u vozilu u skladu je sa zahtjevima navedenima u Dodatku 11.

03) Jedinica u vozilu povezana je na globalni satelitski navigacijski sistem ili više njih, kako je određeno u Dodatku 12.

04) Jedinica u vozilu komunicira s čitačima komunikacije ranog otkrivanja na daljinu, kako je utvrđeno u Dodatku 14.

05) Jedinica u vozilu može uključivati sučelje ITS-a koje je određeno u Dodatku 13.

Uređaj za evidentiranje podataka može se spojiti na druge uređaje preko dodatnih sučelja i/ili preko neobaveznog sučelja ITS-a.

06) Nijednim priključivanjem ili spajanjem neke funkcije, jednog uređaja ili više njih, bili oni odobreni ili ne, na uređaj za evidentiranje podataka ne smije se ometati ili moći ometati pravilan i siguran rad uređaja za evidentiranje podataka i odredbi ove Uredbe.

Korisnici uređaja za evidentiranje podataka identifikujeju se s pomoću tahografskih kartica.

07) Uređajem za evidentiranje podataka daje se pravo selektivnog pristupa podacima i funkcijama u skladu s vrstom i/ili identitetom korisnika.

Uređaj za evidentiranje podataka bilježi i arhivira podatke u podatkovnu memoriju, uređaj za komunikaciju na daljinu i na tahografske kartice.

2.2 Funkcije

08) Uređaj za evidentiranje podataka osigurava sljedeće funkcije:

- praćenje umetanja i uklanjanja kartice,
- mjerenje brzine, prijeđenog puta i položaja,
- mjerenje vremena,
- praćenje aktivnosti vozača,
- praćenje statusa vožnje,
- ručne unose vozača:
- unos mjesta početka i/ili završetka dnevnog radnog vremena,
- ručni unos aktivnosti vozača,
- unos posebnih uslova,
- upravljanje blokadama preduzeća,
- praćenje aktivnosti nadzora,
- otkrivanje događaja i/ili kvarova,
- ugrađena ispitivanja i samoispitivanja,
- čitanje iz podatkovne memorije,
- evidentiranje i arhiviranje u memoriji podataka,
- čitanje s tahografskih kartica,
- evidentiranje i arhiviranje na tahografske kartice,
- prikaz,
- ispis,
- upozoravanje,
- preuzimanje podataka na vanjske medije,
- daljinsku komunikaciju za ciljane provjere na putu,
- izlaz podataka na dodatne uređaje,
- kalibraciju,
- provjeru kalibracije na putu,
- prilagodbu vremena.

2.3 Načini rada

09) Uređaj za evidentiranje podataka mora ima četiri načina rada:

- operativni način,
- kontrolni način,

- kalibracijski način,
- način rada preduzeća.

10) Uređaj za evidentiranje podataka prebacuje se na sljedeći način rada u skladu s umetnutim važećiim tahografskim karticama u uređaje s kartičnim sučeljem. Za određivanje načina rada nije važna generacija tahografske kartice ako je umetnuta kartica važećia. Kartica radionice prve generacije uvijek se smatra nevažećom ako je umetnuta u jedinicu u vozilu druge generacije.

Način rada		**Otvor vozača**				
		Bez kartice	**Kartica vozača**	**Kontrolna kartica**	**Kartica radionice**	**Kartica preduzeća**
Otvor suvozača	Bez kartice	Operativni	Operativni	Kontrolni	Kalibracijski	Preduzeće
	Kartica vozača	Operativni	Operativni	Kontrolni	Kalibracijski	Preduzeće
	Kontrolna kartica	Kontrolni	Kontrolni	Kontrolni (*1)	Operativni	Operativni
	Kartica radionice	Kalibracijski	Kalibracijski	Operativni	Kalibracijski (*1)	Operativni
	Kartica preduzeća	Preduzeće	Preduzeće	Operativni	Operativni	Preduzeće (*1)
(*1) U tim situacijama uređaj za evidentiranje podataka upotrebljava samo tahografsku karticu umetnutu u otvor vozača.						

11) Uređaj za evidentiranje podataka zanemaruje ubačene nevažeće kartice, osim prikaza, ispisa ili preuzimanja podataka s istekle kartice, što mora biti omogućeno.

12) Sve funkcije navedene pod točkom 2.2. moraju raditi u svim načinima rada, uz sljedeće iznimke:

- funkcija kalibracije dostupna je samo u kalibracijskom načinu rada,
- funkcija provjere kalibracije na putu dostupna je samo u kontrolnom načinu rada,
- funkcija upravljanja blokadama preduzeća dostupna je samo u načinu rada preduzeća,
- funkcija praćenja aktivnosti nadzora radi samo u kontrolnom načinu rada,
- funkcija preuzimanja podataka nije dostupna u operativnom načinu rada (osim kako je predviđeno u zahtjevu 193) osim preuzimanja podataka s kartice vozača kad nijedna druga kartica nije umetnuta u jedinicu u vozilu.

13) Uređaj za evidentiranje podataka može prenijeti sve podatke na displej, pisač ili vanjska sučelja uz sljedeće iznimke:

- u operativnom načinu rada svi lični identifikacijski podaci (prezime i ime(na)) koji ne odgovaraju umetnutoj tahografskoj kartici ostaju nevidljivi, a svaki broj kartice koji ne odgovara umetnutoj tahografskoj kartici ostaje djelomično nevidljiv (nevidljiva je svaka neparna znamenka slijeva nadesno),
- u načinu rada preduzeća, podaci o vozaču (zahtjevi 102, 105 i 108) mogu se prenijeti samo za perioda u kojima nema blokade ili za perioda koja nije blokiralo neko drugo preduzeće(koje se identifikuje s pomoću prvih 13 cifara broja kartice preduzeća),
- kad u uređaj za evidentiranje podataka nije umetnuta kartica, podaci o vozaču mogu se prenijeti samo za tekući dan i prethodnih osam kalendarskih dana,
- lični podaci iz jedinice u vozilu ne prenose se preko sučelja ITS-a jedinice u vozilu bez provjere pripauza vozača na kojeg se podaci odnose,
- jedinice u vozilu uz redovni rad imaju rok trajanja od 15 godina, počevši od datuma početka važenja certifikata za jedinice u vozilu, ali se jedinice u vozilu mogu upotrebljavati dodatna tri mjeseca samo u svrhu preuzimanja podataka.

2.4 Sigurnost

Cilj je sigurnosti sistema zaštititi memoriju podataka sprečavanjem neovlašćenog pristupa i manipulisanja podacima te otkrivanjem svakog takvog pokušaja, zaštititi integritet i autentičnost podataka koji se razmjenjuju između senzora kretanja i jedinice u vozilu, zaštititi integritet i autentičnost podataka koji se razmjenjuju između uređaja za evidentiranje podataka i tahografskih kartica, zaštititi integritet i autentičnost podataka koji se razmjenjuju između jedinice u vozilu i spoljnog uređaja GNSS-a, ako postoje, zaštititi povjerljivost, integritet i autentičnost podataka koji se razmjenjuju komunikacijom ranog otkrivanja na daljinu u svrhu nadzora te provjeriti integritet i autentičnost preuzetih podataka.

14) Kako bi se postigla sigurnost sistema, sljedeći sastavni dijelovi moraju zadovoljavati sigurnosne zahtjeve utvrđene u njihovim profilima zaštite, kako se zahtijeva u Dodatku 10.:

- jedinica u vozilu,
- tahografska kartica,
- senzor kretanja,

- spoljni uređaj GNSS-a (ovaj je profil nužan i primjenjiv samo za vanjsku verziju GNSS-a).

3 ZAHTJEVI U POGLEDU IZRADE I FUNKCIONALNOSTI UREĐAJA ZA EVIDENTIRANJE PODATAKA

3.1 Praćenje umetanja i uklanjanja kartica

15) Uređaj za evidentiranje podataka nadzire uređaje s kartičnim sučeljem tako da registrira umetanje i uklanjanje kartice.

16) Pri umetanju kartice uređaj za evidentiranje podataka otkriva je li umetnuta kartica važeća tahografska kartica i u tom slučaju identifikuje vrstu kartice i generaciju kartice.

Ako je u uređaj za evidentiranje podataka već umetnuta kartica s istim brojem kartice i većim indeksom obnavljanja, kartica se označava kao nevažeća.

Ako je u uređaj za evidentiranje podataka već umetnuta kartica s istim brojem kartice i indeksom ponovnog izdavanja, ali s većim indeksom zamjene kartice, kartica se označava kao nevažeća.

17) Uređaj za evidentiranje podataka tahografske kartice prve generacije smatra nevažećima nakon što radionica onemogući upotrebu tahografskih kartica prve generacije u skladu s Dodatkom 15. (zahtjev MIG003).

18) Kartice radionice prve generacije koje su ubačene u uređaj za evidentiranje podataka druge generacije smatraju se nevažećima.

19) Uređaj za evidentiranje podataka mora biti osmišljen tako da se tahografske kartice blokiraju u tom položaju pri pravilnom umetanju u uređaje s kartičnim sučeljem.

20) Tahografske kartice mogu se deblokirati samo kad je vozilo zaustavljeno i nakon što su odgovarajući podaci sačuvani na kartice. Za deblokiranje kartice potrebna je aktivnost korisnika.

3.2 Mjerenje brzine, položaja i prijeđenog puta

21) Senzor kretanja (koji može biti ugrađen u adapter) glavni je izvor za mjerenje brzine i prijeđenog puta.

22) Ta funkcija mora neprekidno mjeriti i dati stanje brojača kilometara koje odgovara ukupnoj udaljenosti koju je vozilo prešlo upotrebom impulsa koje šalje senzor kretanja.

23) Ta funkcija mora neprekidno mjeriti i dati brzinu vozila upotrebom impulsa koje šalje senzor kretanja.

24) Funkcija mjerenja brzine daje informaciju i kreće li se vozilo ili stoji. Smatra se da se vozilo kreće čim funkcija utvrdi više od 1 imp/sek u trajanju od najmanje 5 sekundi na senzoru kretanja; u protivnom se smatra da vozilo stoji.

25) Uređaji za prikaz brzine (brzinomjer) i ukupno prijeđene udaljenosti (brojač kilometara) ugrađeni na svako vozilo opremljeno uređajem za evidentiranje podataka koji je sukladan odredbama ove Uredbe moraju udovoljavati zahtjevima u pogledu najvećih dopuštenih odstepena (vidjeti točke 3.2.1. i 3.2.2.) utvrđenima u ovom Prilogu.

26) Za otkrivanje manipulacije podacima o kretanju vozila, podaci iz senzora kretanja potvrđuju se podacima o kretanju vozila iz prijemnika GNSS-a i, prema potrebi, iz drugih izvora koji su neovisni o senzoru kretanja.

27) Ta funkcija mjeri položaj vozila kako bi se omogućilo automatsko evidentiranje:

- položaja na kojima vozač i/ili suvozač počinju svoje dnevno radno vrijeme;
- položaje na kojima akumulisano vrijeme vožnje dostiže višesrtuko tri sata;
- položaja na kojima vozač i/ili suvozač završavaju svoje dnevno radno vrijeme.

3.2.1 *Mjerenje prijeđene udaljenosti*

28) Prijeđena udaljenost može se mjeriti:

- tako da se zbraja kretanje unaprijed i unatrag, ili
- samo pri kretanju vozila unaprijed.

29) Uređaj za evidentiranje podataka mjeri udaljenost od 0 do 9 999 999,9 km.

30) Udaljenost mora biti u granicama sljedećih odstepena (na najmanjoj udaljenosti od 1 000 m):

- ± 1 % prije ugradnje,
- ± 2 % pri ugradnji i periodičnom pregledu,
- ± 4 % tokom upotrebe.

31) Udaljenost mora imati rezoluciju jednaku ili veću od 0,1 km.

3.2.2 *Mjerenje brzine*

32) Uređaj za evidentiranje podataka mjeri brzinu od 0 do 220 km/h.

33) Kako bi se osiguralo najveće dopušteno odstepene prikazane brzine od ± 6 km/h tokom upotrebe, a s obzirom na:

- dopušteno odstepene od ± 2 km/h za ulazna odstepena (trošenje guma, …),
- dopušteno odstepene od ± 1 km/h za mjerenja izvršena tokom ugradnje ili periodičnih pregleda, za brzine između 20 i 180 km/h i za karakteristične koeficijente vozila između 4 000 i 25 000 imp/km uređaj za evidentiranje podataka mjeri brzinu uz dopušteno odstepene od ± 1 km/h (pri konstantnoj brzini).

Napomena: Rezoluciju arhiviranje podataka ima dodatno dopušteno odstepene od ± 0,5 km/h za brzinu koju arhivira uređaj za evidentiranje podataka.

34) Brzina se mora mjeriti ispravno unutar uobičajenih dopuštenih odstepena u roku od 2 sekunde od završetka promjene brzine kad se brzina mijenjala do 2 m/s^2.

35) Mjerenje brzine mora imati rezoluciju jednaku ili bolju od 1 km/h.

3.2.3 ***Mjerenje položaja***

36) Uređaj za evidentiranje podataka mjeri apsolutni položaj vozila upotrebom prijemnika GNSS-a.

37) Apsolutni položaj mjeri se u koordinatama geografske širine i dužine u stepenima i minutama, uz rezoluciju od 1/10 minute.

3.3 Mjerenje vremena

38) Funkcija mjerenja vremena mora trajno mjeriti i digitalno iskazivati datum i vrijeme po UTC-u.

39) Pri datiranju podataka u uređaju za evidentiranje podataka (zapisi, razmjena podataka) i za sve ispise navedene u Dodatku 4. „Ispisi" upotrebljavaju se datum i vrijeme po UTC-u.

40) Za prikaz lokalnog vremena mora biti moguće mijenjati prikaz razlike vremena u polusatnim koracima. Drugi pomaci, osim negativnih ili pozitivnih višestrukea pola sata, nisu dozvoljeni;

41) Odstepene vremena može biti unutar vrijednosti od ± 2 sekunde po danu u uslovima homologacije, ako nema prilagodbe vremena.

42) Vrijeme koje se mjeri mora imati rezoluciju bolju od 1 sekunde ili jednaku.

43) Na mjerenje vremena ne smije uticati prekid spoljnog napajanja kraći od 12 mjeseci u uslovima homologacije.

3.4 Praćenje aktivnosti vozača

44) Ova funkcija mora neprekidno i odvojeno pratiti aktivnosti jednog vozača i jednog suvozača.

45) Aktivnosti vozača su VOŽNJA, RAD, DOSTUPNOST ili PAUZA/ODMOR.

46) Vozač i/ili suvozač moraju imati mogućnost ručnog odabira RADA, DOSTUPNOSTI ili PAUZE/ODMORA.

47) Ako se vozilo kreće, za vozača se automatski odabire VOŽNJA, a za suvozača se automatski odabire DOSTUPNOST.

48) Kad se vozilo zaustavi, za vozača se automatski odabire RAD.

49) Pretpostavlja se da je prva promjena aktivnosti u PAUZA/ODMOR ili DOSTUPNOST koja nastaje u roku od 120 sekundi od automatske promjene aktivnosti u RAD zbog zaustavljanja vozila nastupila u trenutku kad se vozilo zaustavilo (čime se eventualno poništava promjena aktivnosti u RAD).

50) Ova funkcija mora bilježiti podatke o promjenama aktivnosti u rezolucijui od jedne minute.

51) Ako je u minuti neposredno prije određene kalendarske minute i u minuti neposredno nakon nje registrirana aktivnost VOŽNJA, ta se minuta u cijelosti smatra minutom VOŽNJE.

52) Određena kalendarska minuta, koja se prema zahtjevu 051 ne smatra minutom VOŽNJE, u cijelosti se smatra minutom one vrste aktivnosti koja je najduže neprekidno trajala u toj minuti (ili posljednja aktivnost od jednako dugih aktivnosti).

53) Ova funkcija mora i trajno pratiti neprekidno vrijeme vožnje i kumulativno vrijeme pauze vozača.

3.5 Praćenje statusa vožnje

54) Ova funkcija mora neprekidno i automatski pratiti status vožnje.

55) Status vožnje POSADA odabire se kad se dvije važeće kartice vozača umetnu u uređaj, a u svim se drugim slučajevima odabire status vožnje JEDAN VOZAČ.

3.6 Unosi vozača

3.6.1 ***Unos mjesta početka i/ili kraja dnevnog radnog vremena***

56) Ova funkcija omogućava unos mjesta početka i/ili završetka dnevnog radnog vremena vozača i/ili suvozača.

57) Mjesta se definišeju kao država te, dodatno i prema potrebi, kao regija, a unose se i potvrđuju ručno.

58) U trenutku uklanjanja kartice vozača uređaj za evidentiranje podataka mora potaknuti (su)vozača da unese „mjesto završetka dnevnog radnog vremena".

59) Vozač zatim unosi trenutno mjesto vozila, a taj se unos smatra privremenim.

Privremeni unos pri posljednjem uklanjanju kartice potvrđuje se (tj. preko njega se više ne piše) pod sljedećim uslovima:

- unos mjesta na kojem započinje trenutno dnevno radno vrijeme tokom ručnog unosa u skladu sa zahtjevom 61);
- sljedeći unos mjesta na kojem započinje trenutno dnevno radno vrijeme ako vlasnik kartice ne unese ni jedno mjesto na kojem započinje ili je završilo radno vrijeme tokom ručnog unosa u skladu sa zahtjevom 61).

Preko privremenog unosa pri posljednjem uklanjanju kartice prepisuje se nova vrijednost te se ona potvrđuje pod sljedećim uslovima:

- sljedeći unos mjesta na kojem završava trenutno dnevno radno vrijeme ako vlasnik kartice ne unese ni jedno mjesto na kojem započinje ili je završilo radno vrijeme tokom ručnog unosa u skladu sa zahtjevom 61).

60) S pomoću naredbi u meniju mora biti moguće unijeti mjesta početka i/ili završetka dnevnog radnog vremena. Ako se u jednoj kalendarskoj minuti dogodi više od jednog takvog unosa, bilježi se samo unos zadnjeg mjesta početka i unos zadnjeg mjesta završetka, izvršen u tom vremenu.

3.6.2 *Ručni unos aktivnosti vozača i saglasnost vozača u pogledu sučelja ITS-a*

61) Nakon umetanja kartice vozača (ili radionice), i samo tada, uređaj za evidentiranje podataka dopušta ručne unose aktivnosti. Ručni unosi aktivnosti izvode se upotrebom vrijednosti lokalnog vremena i datuma vremenske zone (odstepene UTC) koja je trenutno namještena u jedinici u vozilu.

Pri umetanju kartice vozača ili radionice vlasnika kartice podsjeća se na:

- datum i vrijeme njegova posljednjeg uklanjanja kartice;
- neobavezno: odstepene lokalnog vremena koji je trenutno namješten u jedinici u vozilu.

Pri prvom umetanju određene kartice vozača ili kartice radionice koja je trenutno nepoznata jedinici u vozilu, vlasnika kartice poziva se da dâ svoju saglasnost za prenos ličnih podataka iz tahografa preko neobaveznog sučelja ITS-a.

U svakom se trenutku saglasnost vozača (odnosno radionice) može omogućiti ili onemogućiti s pomoću naredbi u meniu ako je umetnuta kartica vozača (odnosno radionice).

Mora biti moguć unos aktivnosti sa sljedećim ograničenjima:

- vrste aktivnosti su RAD, DOSTUPNOST ili PAUZA/ODMOR;
- vremena početka i završetka svake aktivnosti mogu biti samo u okviru perioda od posljednjeg uklanjanja do trenutnog umetanja kartice;
- međusobno vremensko preklapanje aktivnosti nije dopušteno.

Prema potrebi ručni su unosi mogući pri prvom umetanju prethodno neupotrebljavane kartice vozača (ili radionice).

Postupak za ručni unos aktivnosti uključuje onoliko uzastopnih koraka koliko je potrebno za namještanje vrste, vremena početka i vremena završetka svake aktivnosti. Za bilo koji dio vremenskog perioda između posljednjeg uklanjanja i trenutnog umetanja kartice vlasnik kartice ima mogućnost ne prijaviti nikakvu aktivnost.

Za vrijeme ručnih unosa povezanih s umetanjem kartice, ako je primjenljivo, vlasnik kartice ima mogućnost unijeti:

- mjesto gdje je završilo prethodno dnevno radno vrijeme, povezano s odgovarajućim vremenom (što se zapisuje preko unosa zapisanog pri posljednjem uklanjanju kartice te se unos potvrđuje),
- mjesto gdje započinje trenutačno dnevno radno vrijeme, povezano s odgovarajućim vremenom (čime se potvrđuje privremeni unos zabilježen pri posljednjem uklanjanju kartice).

Ako vlasnik kartice ne unese mjesto početka ili završetka radnog vremena pri ručnim unosima povezanima s umetanjem kartice, to se smatra izjavom da se njegovo radno vrijeme nije promijenilo od posljednjeg uklanjanja kartice. Sljedeći unos mjesta gdje je završilo prethodno dnevno radno vrijeme zapisuje se preko privremenog unosa zapisanog pri posljednjem uklanjanju kartice.

Ako se unese mjesto, ono se bilježi na odgovarajuću tahografsku karticu.

Ručni se unosi prekidaju:

- ako se kartica ukloni, ili
- ako se vozilo kreće i kartica je u otvoru vozača.

Dozvoljeni su dodatni prekidi, npr. zbog isteka vremena nakon određenog perioda korisnikove neaktivnosti. Ako se ručni unosi prekinu, uređaj za evidentiranje podataka potvrđuje sva potpuno unesena mjesta i aktivnosti (koje imaju nedvosmisleno mjesto i vrijeme ili vrstu aktivnosti, vrijeme početka i vrijeme završetka).

Ako se za vrijeme ručnih unosa aktivnosti za prvu umetnutu karticu umetne kartica drugog vozača ili kartica radionice, prije početka ručnih unosa za drugu umetnutu karticu mora se omogućiti završetak ručnih unosa za prvu umetnutu karticu.

Vlasnik kartice ima mogućnost unijeti ručne unose prema sljedećem minimalnom postupku:

- ručni unos aktivnosti, hronološkim redom, za period od posljednjeg uklanjanja kartice do trenutnog umetanja kartice.
- vrijeme početka prve aktivnosti namješta se na vrijeme uklanjanja kartice. Za svaki sljedeći unos, vrijeme početka unaprijed se namješta tako da odmah slijedi vrijeme završetka ranijeg unosa. Za svaku se aktivnost izabere vrsta aktivnosti i vrijeme završetka.

Postupak završava kad je vrijeme završetka ručno unesene aktivnosti jednako vremenu umetanja kartice. Uređaj za evidentiranje podataka može po izboru vlasniku kartice omogućiti da do potvrde unosa posebnom naredbom izmijeni bilo koju ručno unesenu aktivnost. Nakon potvrde svaka je takva izmjena zabranjena.

3.6.3 *Unos posebnih stanja*

62) Uređaj za evidentiranje podataka mora vozaču dopustiti unos sljedećih dvaju posebnih stanja, u realnom vremenu:

- „IZVAN PODRUČJA PRIMJENE” (početak, završetak) i
- „VOŽNJA TRAJEKTOM/VOZOM” (početak, završetak)

Stanje „VOŽNJA TRAJEKTOM/VOZOM” ne može se pojaviti ako je započeto stanje „IZVAN PODRUČJA PRIMJENE”.

Započeto stanje „IZVAN PODRUČJA PRIMJENE” uređaj za evidentiranje podataka mora automatski zatvoriti ako se kartica vozača umeće ili uklanja.

Započeto stanje „IZVAN PODRUČJA PRIMJENE” sprečava sljedeće događaje i upozorenja:

- vožnju bez odgovarajuće kartice i
- upozorenja povezana s neprekidnim periodm vožnje.

Oznaka početka VOŽNJE TRAJEKTOM/VOZOM stavlja se prije gašenja motora na trajektu/vlaku.

Započeta VOŽNJA TRAJEKTOM/VOZOM mora završiti ako nastupi neka od sljedećih mogućnosti:

- vozač je ručno završio VOŽNJU TRAJEKTOM/VOZOM
- vozač je izbacio svoju karticu

Započeta VOŽNJA TRAJEKTOM/VOZOM završava ako više nije važećia na temelju odredaba Uredbe (EZ) br. 561/2006.

3.7 Upravljanje blokadama preduzeća

63) Ova funkcija omogućava upravljanje blokadama koje postavi preduzeće kako bi ograničilo pristup podacima preduzeća za sebe.

64) Blokade preduzeća sastoje se od datuma/vremena početka (zaključavanje blokade) i datuma/vremena završetka (otključavanje blokade) pridruženih identifikaciji preduzeća naznačenoj u broju kartice preduzeća (pri zaključavanju blokade).

65) Blokade se mogu zaključati odnosno otključati samo u realnom vremenu.

66) Otključavanje blokade može izvršiti samo preduzeće čija je blokada postavljena (što je određeno s pomoću prvih 13 cifara broja kartice preduzeća) ili

67) otključavanje blokade automatsko je kad drugo preduzeće izvrši zaključavanje blokade.

68) U slučaju zaključavanja blokade preduzeća kad je prethodna blokada bila za isto preduzeće, pretpostavlja se da prethodna blokada nije bila otključana te da je i dalje zaključana.

3.8 Praćenje aktivnosti nadzora

69) Ova funkcija prati aktivnosti PRIKAZA, ISPISA, jedinice u vozilu i PREUZIMANJA podataka s kartice te provjere KALIBRACIJE NA PUTU dok je u kontrolnom načinu.

70) Ova funkcija prati i aktivnosti KONTROLE PREKORAČENJA BRZINE dok je u kontrolnom načinu. Smatra se da je kontrola prekoračenja brzine nastala ako je u kontrolnom načinu ispis „prekoračenje brzine" poslan na pisač ili na displej ili ako su podaci o „događajima i kvarovima" preuzeti iz podatkovne memorije jedinice u vozilu.

3.9 Prepoznavanje događaja i/ili kvarova

71) Ova funkcija otkriva sljedeće događaje i/ili kvarove:

3.9.1 ***Događaj „umetanje nevažeće kartice"***

72) Ovaj se događaj aktivira umetanjem bilo koje nevažeće kartice, umetanjem kartice vozača koja je već zamijenjena i/ili ako istekne važnost ubačene važeće kartice.

3.9.2 ***Događaj „konflikt kartica"***

73) Ovaj se događaj aktivira ako se javi bilo koja kombinacija s važećiim karticama označena u tablici s X:

Konflikt kartica		**Otvor vozača**				
		Bez kartice	**Kartica vozača**	**Kontrolna kartica**	**Kartica radionice**	**Kartica preduzeća**
Otvor suvozača	Bez kartice					
	Kartica vozača				X	
	Kontrolna kartica			X	X	X
	Kartica radionice		X	X	X	X
	Kartica preduzeća			X	X	X

3.9.3 ***Događaj „vremensko preklapanje"***

74) Ovaj se događaj aktivira kad su datum/vrijeme posljednjeg uklanjanja kartice vozača, očitani s kartice, kasniji nego tekući datum/vrijeme uređaja za evidentiranje podataka u koji je umetnuta kartica.

3.9.4 ***Događaj „vožnja bez odgovarajuće kartice"***

75) Ovaj se događaj aktivira za bilo koju kombinaciju s važećiim tahografskim karticama označenu znakom X u sljedećoj tablici ako se aktivnost vozača promijeni na VOŽNJU ili ako dođe do promjene načina rada kada je aktivnost vozača VOŽNJA:

Vožnja bez odgovarajuće kartice		**Otvor vozača**				
		Bez (važeće) kartice	**Kartica vozača**	**Kontrolna kartica**	**Kartica radionice**	**Kartica preduzeća**
Otvor suvozača	Bez (važeće) kartice	X		X		X
	Kartica vozača	X		X	X	X
	Kontrolna kartica	X	X	X	X	X
	Kartica radionice	X	X	X		X
	Kartica preduzeća	X	X	X	X	X

3.9.5 ***Događaj „umetanje kartice tokom vožnje"***

76) Ovaj se događaj aktivira kad se tahografska kartica umetne u bilo koji otvor u vrijeme dok je aktivnost vozača VOŽNJA.

3.9.6 ***Događaj „neispravno zatvaranje posljednje razmjene podataka s karticom"***

77) Ovaj se događaj aktivira kad pri umetanju kartice uređaj za evidentiranje podataka utvrdi da unatoč odredbama utvrđenima u stavu 3. tački 1. prethodna razmjena podataka s karticom nije pravilno završena (kartica je uklonjena prije nego što su svi potrebni podaci spremljeni na karticu). Ovaj se događaj aktivira samo karticom vozača i karticom radionice.

3.9.7 ***Događaj „prekoračenje brzine"***

78) Ovaj se događaj aktivira pri svakom prekoračenju brzine.

3.9.8 ***Događaj „prekid napajanja"***

79) Ovaj se događaj aktivira izvan kalibracijskog ili kontrolnog načina pri svakom prekidu napajanja senzora kretanja i/ili jedinice u vozilu dužem od 200 milisekundi. Prag prekida utvrđuje proizvođač. Padom napajanja zbog pokretanja motora vozila ne aktivira se ovaj događaj.

3.9.9 ***Događaj „greška u komunikaciji s uređajem za komunikaciju na daljinu"***

80) Ovaj se događaj aktivira izvan kalibracijskog načina kad uređaj za komunikaciju na daljinu u više od tri pokušaja ne potvrdi uspješan primitak podataka prenesenih na daljinu iz jedinice u vozilu.

3.9.10 ***Događaj „izostanak podataka o položaju iz prijemnika GNSS-a"***

81) Ovaj se događaj aktivira **izvan kalibracijskog načina** u slučaju izopauza podataka o položaju iz prijemnika GNSS-a (unutrašnjeg ili spoljnog) dužeg od tri sata ukupnog vremena vožnje.

3.9.11 ***Događaj „greška u komunikaciji s spoljnim uređajem GNSS-a"***

82) Ovaj se događaj aktivira **izvan kalibracijskog načina** u slučaju prekida komunikacije između spoljnog uređaja GNSS-a i jedinice u vozilu dužeg od 20 uzastopnih minuta ako se vozilo kreće.

3.9.12 ***Događaj „greška u podacima o kretanju"***

83) Ovaj se događaj aktivira **izvan kalibracijskog načina** u slučaju prekida redovnog protoka podataka između senzora kretanja i jedinice u vozilu i/ili u slučaju greške u integritetu podataka ili greške u autentifikaciji podataka tokom razmjene podataka između senzora kretanja i jedinice u vozilu.

3.9.13 ***Događaj „konflikt u kretanju vozila"***

84) Ovaj se događaj aktivira **izvan kalibracijskog načina** ako su podaci o kretanju iz senzora o kretanju u suprotnosti s podacima o kretanju izračunatima iz unutrašnjeg prijemnika GNSS-a ili iz spoljnog uređaja GNSS-a, ili, prema potrebi, iz drugih nezavisnih izvora, kako je utvrđeno u Dodatku 12. Ovaj se događaj ne aktivira tokom vožnje trajektom/vozom, u uslovima IZVAN PODRUČJA PRIMJENE ili kad podaci o položaju iz prijemnika GNSS-a nisu raspoloživi.

3.9.14 ***Događaj „pokušaj povrede sigurnosti"***

85) Ovaj se događaj aktivira za sve ostale događaje koji utiču na sigurnost senzora kretanja i/ili jedinice u vozilu i/ili spoljnog uređaja GNSS-a, kako je navedeno u Dodatku 10., dok nisu u načinu kalibracije.

3.9.15 ***Događaj „vremenski konflikt"***

86) Ovaj se događaj aktivira izvan kalibracijskog načina kad jedinica u vozilu otkrije razliku od više od jedne minute između vremena funkcije mjerenja vremena jedinice u vozilu i vremena iz prijemnika GNSS-a. Taj se događaj bilježi zajedno sa stanjem unutrašnjeg sata jedinice u vozilu i izražava zajedno sa automatskim prilagođavanjem vremena. Nakon što se aktivira događaj vremenskog konflikta, jedinica u vozilu neće stvarati druge događaje vremenskog konflikta sljedećih 12 sati. Taj se događaj neće aktivirati ako prijamnik GNSS-a nije mogao otkriti važećii signal GNSS-a 30 ili više dana.

3.9.16 ***Kvar „kartica"***

87) Ovaj se kvar aktivira ako se tokom rada javi greška na tahografskoj kartici.

3.9.17 ***Kvar „uređaj za evidentiranje podataka"***

88) Ovaj se kvar aktivira za neku od sljedećih grešaka, dok uređaj nije u kalibracijskom načinu:

- unutarnji kvar jedinice u vozilu,
- kvar pisača,
- kvar displeja,
- kvar pri preuzimanju podataka,
- kvar senzora,
- kvar prijemnika GNSS-a ili spoljnog uređaja GNSS-a,
- kvar uređaja za komunikaciju na daljinu.
- kvar povezan s ITS sučeljem (ako je primjenjivo)

3.10 Ugrađena ispitivanja i samoispitivanja

89) Uređaj za evidentiranje podataka otkriva kvarove samoispitivanjima i ugrađenim ispitivanjima prema sljedećoj tablici:

Podsklop za ispitivanje	**Samoispitivanje**	**Ugrađeno ispitivanje**
Softver		Integritet
Podatkovna memorija	Pristup	Pristup, integritet podataka
Uređaji s kartičnim sučeljem	Pristup	Pristup

Tipkovnica		Ručna provjera
Pisač	(zavisi o proizvođaču)	Ispis
Prikaz		Vizualna provjera
Preuzimanje podataka (sprovodi se samo tokom preuzimanja podataka)	Ispravan rad	
Senzor	Ispravan rad	Ispravan rad
Uređaja za komunikaciju na daljinu	Ispravan rad	Ispravan rad
Uređaj GNSS-a	Ispravan rad	Ispravan rad
ITS sučelje (neobvezno)	Ispravan rad	

3.11 Čitanje iz memorije podataka

90) Uređaj za evidentiranje podataka mora moći očitati sve podatke sačuvane u svojoj memoriji podataka.

3.12 Evidentiranje i arhiviranje u memoriji podataka

Za potrebe ovog stava:

- „365 dana" definiše se kao 365 kalendarskih dana prosječne aktivnosti vozača u vozilu. Prosječna dnevna aktivnost u vozilu definiše se kao najmanje šest vozača ili suvozača, šest ciklusa umetanja i uklanjanja kartice i 256 promjena aktivnosti. „365 dana" stoga uključuje najmanje 2 190 (su)vozača, 2 190 ciklusa umetanja i uklanjanja kartice i 93 440 promjena aktivnosti,
- prosječan broj položaja u danu definiše se kao najmanje šest položaja početka dnevnog radnog vremena, šest položaja u kojima akumulisano vrijeme vožnje dostiže višestrukih tri sata te šest položaja završetka dnevnog radnog vremena, tako da ‚365 dana' uključuje najmanje 6570 položaja,
- vremena se bilježe uz rezoluciju od jedne minute, osim ako nije drukčije određeno,
- stanje brojača kilometara bilježi se uz rezoluciju od jednog kilometra,
- brzine se bilježe uz rezoluciju od 1 km/h,
- položaji (geografske širine i dužine) bilježe se u stepenima i minutama, uz rezoluciju od 1/10 minute te povezanu tačnost GNSS-a i vrijeme dobivanja podataka.

91) Na podatke sačuvane u memoriji podataka ne smije uticati nikakav spoljni prekid napajanja kraći od dvanaest mjeseci u uslovima homologacije. Osim toga, na podatke sačuvane u spoljnom uređaju za komunikaciju na daljinu, kako je definisan u Dodatku 14., ne smije uticati nikakav spoljni prekid napajanja kraći od 28 dana.

92) Uređaj za evidentiranje podataka mora moći bilježiti i sačuvati direktno ili nedirektno sljedeće podatke u svojoj memoriji podataka:

3.12.1 *Identifikacijski podaci o uređaju*

3.12.1.1 Identifikacijski podaci jedinice u vozilu

93) Uređaj za evidentiranje podataka mora moći u svojoj memoriji podataka sačuvati sljedeće identifikacijske podatke jedinice u vozilu:

- naziv proizvođača,
- adresu proizvođača,
- kataloški broj,
- serijski broj,
- generaciju jedinice u vozilu,
- mogućnost upotrebe tahografskih kartica prve generacije
- broj verzije softvera,
- datum ugradnje verzije softvera,
- godinu proizvodnje uređaja,
- homologacijski broj.

94) Identifikacijske podatke jedinice u vozilu bilježi i arhivira jednom zauvijek proizvođač jedinice u vozilu, osim podataka koji se odnose na softver i homologacijski broj, koji se mogu mijenjati u slučaju ažuriranja softvera te mogućnosti upotrebe tahografskih kartica prve generacije.

3.12.1.2 Identifikacijski podaci senzora kretanja

95) Senzor kretanja mora moći sačuvati u svojoj memoriji sljedeće identifikacijske podatke:

- naziv proizvođača,
- serijski broj,

- homologacijski broj.
- identifikator ugrađene sigurnosne komponente (npr. interni kataloški broj ugrađenog čipa/procesora),
- identifikator operativnog sistema (npr. broj verzije softvera).

96) Identifikacijske podatke senzora kretanja belježi i arhivira jednom zauvijek u senzoru kretanja proizvođač senzora kretanja.

97) Jedinica u vozilu mora moći bilježiti i sačuvati u svojoj memoriji podataka sljedeće podatke koji se odnose na zadnjih 20 uparivanja senzora kretanja (ako tokom jednog kalendarskog dana dođe do više uparivanja, arhiviraju se samo prvo i posljednje uparivanje):

Za svako od spomenutih uparivanja bilježe se sljedeći podaci:

- identifikacijski podaci senzora kretanja:
- serijski broj,
- homologacijski broj;
- podaci za povezivanje sa senzorom kretanja:
- datum uparivanja.

3.12.1.3 Identifikacijski podaci globalnih satelitskih navigacijskih sistema

98) Spoljni uređaj GNSS-a mora moći sačuvati u svojoj memoriji sljedeće identifikacijske podatke:

- naziv proizvođača,
- serijski broj,
- homologacijski broj.
- identifikator ugrađene sigurnosne komponente (npr. interni kataloški broj ugrađenog čipa/procesora),
- identifikator operativnog sistema (npr. broj verzije softvera).

99) Identifikacijske podatke belježi i arhivira jednom zauvijek u spoljnom uređaju GNSS-a proizvođač spoljnog uređaja GNSS-a.

100) Jedinica u vozilu mora moći bilježiti i sačuvati u svojoj memoriji podataka sljedeće podatke koji se odnose na zadnjih 20 povezivanja spoljnih uređaja GNSS-a (ako u toku jednog kalendarskog dana dođe do više povezivanja, arhiviraju se samo prvo i posljednje povezivanje):

Za svako od spomenutih povezivanja bilježe se sljedeći podaci:

- identifikacijski podaci spoljnog uređaja GNSS-a:
- serijski broj,
- homologacijski broj.
- podaci za povezivanje s spoljnim uređajem GNSS-a:
- datum povezivanja

3.12.2 *Ključevi i certifikati*

101) Uređaj za evidentiranje podataka mora moći sačuvati niz kriptografskih ključeva i certifikata, kako je određeno u Dodatku 11. dijelovima A i B.

3.12.3 *Podaci o umetanju i uklanjanju kartice vozača ili kartice radionice*

102) Za svaki ciklus umetanja i uklanjanja kartice vozača ili kartice radionice u uređaj ili iz njega, uređaj za evidentiranje podataka mora zabilježiti i sačuvati u svoju podatkovnu memoriju:

- prezime(na) i ime(na) vlasnika kartice arhivirana na kartici,
- broj kartice, državu članicu izdavanja i datum isteka sačuvane na kartici,
- generaciju kartice,
- datum i vrijeme umetanja,
- stanje brojača kilometara vozila pri umetanju kartice,
- otvor u koji je kartica umetnuta,
- datum i vrijeme uklanjanja,
- stanje brojača kilometara vozila pri uklanjanju kartice,
- sljedeće informacije sačuvane na kartici o prethodnom vozilu kojim se vozač koristio:
- VRN i državu članicu registracije,
- generaciju jedinice u vozilu (ako je dostupna),
- datum i vrijeme uklanjanja kartice,

- oznaku koja pokazuje je li pri umetanju kartice vlasnik kartice ručno unio aktivnosti.

103) Podatkovna memorija mora moći čuvati te podatke najmanje 365 dana.

104) Kad se iscrpi kapacitet za čuvanje, novim se podacima zamjenjuju najstariji podaci.

3.12.4 *Podaci o aktivnosti vozača*

105) Uređaj za evidentiranje podataka bilježi i arhivira u svoju podatkovnu memoriju svaku promjenu aktivnosti vozača i/ili suvozača i/ili svaku promjenu statusa vožnje i/ili svako umetanje ili uklanjanje kartice vozača ili kartice radionice:

- status vožnje (POSADA, JEDAN VOZAČ),
- otvor (VOZAČ, SUVOZAČ),
- status kartice u odgovarajućem otvoru (UMETNUTA, NIJE UMETNUTA),
- aktivnost (VOŽNJA, DOSTUPNOST, RAD, PAUZA/ODMOR),
- datum i vrijeme promjene.

UMETNUTA označava da je važeća kartica vozača ili kartica radionice umetnuta u otvor. NIJE UMETNUTA označava suprotno, tj. da važeća kartica vozača ili kartica radionice nije umetnuta u otvor (npr. da je umetnuta kartica preduzeća ili da nije umetnuta nikakva kartica).

Podaci o aktivnosti koje ručno unosi vozač ne bilježe se u memoriji podataka.

106) Podatkovna memorija mora moći čuvati podatke o aktivnosti vozača najmanje 365 dana.

107) Kad se iscrpi kapacitet za čuvanje, novim se podacima zamjenjuju najstariji podaci.

3.12.5. Mjesta i položaji početka i završetka dnevnog radnog vremena i/ili dostizanja tri sata akumulisanog vremena vožnje

108) Uređaj za bilježenje podataka bilježi i arhivira u svojoj memoriji podataka:

- mjesta i položaje na kojima vozač i/ili suvozač počinju svoje dnevno radno vrijeme;
- položaje na kojima akumulisano vrijeme vožnje dostiže višestrukih tri sata;
- mjesta i položaje na kojima vozač i/ili suvozač završavaju svoje dnevno radno vrijeme.

109) Ako u tom trenutku položaj vozila nije dostupan iz prijemnika GNSS-a, uređaj za evidentiranje podataka upotrebljava posljednji dostupni položaj te povezani datum i vrijeme.

110) Zajedno sa svakim mjestom ili položajem uređaj za evidentiranje podataka u svojoj memoriji podataka bilježi i arhivira:

- broj kartice (su)vozača i državu članicu izdavatelja kartice,
- generaciju kartice,
- datum i vrijeme unosa,
- vrstu unosa (početak, završetak ili tri sata akumulisanog vremena vožnje),
- povezanu tačnost GNSS-a, datum i vrijeme ako je primjenjivo;
- stanje brojača kilometara vozila.

111) Memorija podataka mora moći čuvati mjesta i položaje početka i završetka dnevnog radnog vremena i/ili dostizanja tri sata akumulisanog vremena vožnje najmanje 365 dana.

112) Kad se iscrpi kapacitet za čuvanje, novim se podacima zamjenjuju najstariji podaci.

3.12.6 *Stanje brojača prijeđenih kilometara*

113) Uređaj za evidentiranje podataka bilježi i arhivira u svoju podatkovnu memoriju stanje brojača prijeđenih kilometara i pripadajući datum u ponoć svakog kalendarskog dana.

114) Podatkovna memorija mora moći pohranjivati ponoćna stanja brojača kilometara najmanje 365 kalendarskih dana.

115) Kad se iscrpi kapacitet za čuvanje, novim se podacima zamjenjuju najstariji podaci.

3.12.7 *Detaljni podaci o brzini*

116) Uređaj za evidentiranje podataka bilježi i čuva u svoju memoriju podataka trenutnu brzinu vozila te pripadajući datum i vrijeme u svakoj sekundi tokom najmanje posljednja 24 sata kretanja vozila.

3.12.8 *Podaci o događajima*

Za potrebe ovog podstava vrijeme se bilježi uz rezoluciju od jedne sekunde.

117) Za svaki otkriveni događaj uređaj za evidentiranje podataka bilježi i arhivira u svoju podatkovnu memoriju sljedeće podatke prema sljedećim pravilima arhiviranje:

Događaj	Pravila arhiviranje	Podaci koje je potrebno bilježiti po događaju

Umetanje nevažeće kartice	— deset najnovijih događaja.	— datum i vrijeme događaja, — vrstu, broj, državu članicu izdavatelja kartice ili kartica i generaciju kartice kojom je stvoren događaj. — broj sličnih događaja tog dana
Konflikt kartica	— deset najnovijih događaja.	— datum i vrijeme početka događaja, — datum i vrijeme završetka događaja, — vrstu, broj, državu članicu izdavatelja kartice ili kartica i generaciju dviju kartica zbog kojih je nastao konflikt.
Vožnja bez odgovarajuće kartice	— najduži događaj za svaki od deset zadnjih dana pojave, — pet najdužih događaja u zadnjih 365 dana.	— datum i vrijeme početka događaja, — datum i vrijeme završetka događaja, — vrstu, broj, državu članicu koja je izdala karticu i generaciju bilo koje kartice ubačene na početku i/ili završetku događaja, — broj sličnih događaja tog dana.
Umetanje kartice tokom vožnje	— zadnji događaj za svaki od 10 zadnjih dana pojave,	— datum i vrijeme događaja, — vrstu i broj kartice, državu članicu koja je izdala karticu i generaciju kartice, — broj sličnih događaja tog dana.
Posljednja razmjena podataka s karticom koja nije ispravno zatvorena	— deset najnovijih događaja.	— datum i vrijeme umetanja kartice, — vrstu i broj kartice, državu članicu koje je izdala karticu i generaciju kartice, — posljednju razmjenu podataka očitanih s kartice: — datum i vrijeme umetanja kartice, — VRN, državu članicu registracije i generaciju jedinice u vozilu.
Prekoračenje brzine (1)	— najozbiljniji događaj za svaki od 10 zadnjih dana pojave (tj. događaj s najvećom prosječnom brzinom), — pet najozbiljnijih događaja u zadnjih 365 dana, — prvi događaj koji se dogodio nakon zadnje kalibracije.	— datum i vrijeme početka događaja, — datum i vrijeme završetka događaja, — najveću brzinu izmjerenu tokom događaja, — aritmetički prosjek brzine izmjerene tokom događaja, — vrstu, broj, državu članicu koja je izdala karticu i generaciju kartice vozača (ako je primjereno), — broj sličnih događaja tog dana.
Prekid napajanja (2)	— najduži događaj za svaki od deset zadnjih dana pojave, — pet najdužih događaja u zadnjih 365 dana.	— datum i vrijeme početka događaja, — datum i vrijeme završetka događaja, — vrstu, broj, državu članicu koja je izdala karticu i generaciju bilo koje kartice ubačene na početku i/ili završetku događaja, — broj sličnih događaja tog dana.
Greška u komunikaciji s uređajem za komunikaciju na daljinu	— najduži događaj za svaki od deset zadnjih dana pojave, — pet najdužih događaja u zadnjih 365 dana.	— datum i vrijeme početka događaja, — datum i vrijeme završetka događaja, — vrstu, broj, državu članicu koja je izdala karticu i generaciju bilo koje kartice ubačene na početku i/ili završetku događaja, — broj sličnih događaja tog dana.
Izostanak podataka o položaju iz prijemnika GNSS-a	— najduži događaj za svaki od deset zadnjih dana pojave, — pet najdužih događaja u zadnjih 365 dana.	— datum i vrijeme početka događaja, — datum i vrijeme završetka događaja, — vrstu, broj, državu članicu koja je izdala karticu i generaciju bilo koje kartice ubačene na početku i/ili završetku događaja, — broj sličnih događaja tog dana.
Greška u komunikaciji s spoljnim uređajem GNSS-a	— najduži događaj za svaki od deset posljednjih dana pojave, — pet najdužih događaja u zadnjih 365 dan	— datum i vrijeme početka događaja, — datum i vrijeme završetka događaja, — vrstu, broj, državu članicu koja je izdala karticu i generaciju bilo koje kartice ubačene na početku i/ili završetku događaja, — broj sličnih događaja tog dana.
Greška u podacima o kretanju	— najduži događaj za svaki od deset zadnjih dana pojave, — pet najdužih događaja u zadnjih 365 dana.	— datum i vrijeme početka događaja, — datum i vrijeme završetka događaja, — vrstu, broj, državu članicu koja je izdala karticu i generaciju bilo koje kartice ubačene na početku i/ili završetku događaja, — broj sličnih događaja tog dana.
Konflikt u kretanju vozila	— najduži događaj za svaki od deset zadnjih dana pojave, — pet najdužih događaja u zadnjih 365 dana.	— datum i vrijeme početka događaja, — datum i vrijeme završetka događaja, — vrstu, broj, državu članicu koja je izdala karticu i generaciju bilo koje kartice ubačene na početku i/ili završetku događaja, — broj sličnih događaja tog dana.
Pokušaji povrede sigurnosti	— deset najnovijih događaja po vrsti događaja.	— datum i vrijeme početka događaja, — datum i vrijeme završetka događaja (ako je potrebno), — vrstu, broj, državu članicu koja je izdala karticu i generaciju bilo koje kartice ubačene na početku i/ili završetku događaja, — vrstu događaja.

Vremenski konflikt	— najozbiljniji događaj za svaki od deset zadnjih dana pojave (tj. događaj s najvećom razlikom između datuma i vremena iz uređaja za bilježenje podataka i datuma i vremena iz GNSS-a). — pet najozbiljnijih događaja u zadnjih 365 dana.	— datum i vrijeme iz uređaja za bilježenje podataka, — datum i vrijeme iz GNSS-a, — vrstu, broj, državu članicu koja je izdala karticu i generaciju bilo koje kartice ubačene na početku i/ili završetku događaja, — broj sličnih događaja tog dana.”;

(1) Uređaj za evidentiranje podataka bilježi i arhivira u svojoj memoriji podataka i:

- datum i vrijeme posljednje KONTROLE PREKORAČENJA BRZINE,
- datum i vrijeme prvog prekoračenja nakon te KONTROLE PREKORAČENJA BRZINE i
- broj događaja prekoračenja nakon posljednje KONTROLE PREKORAČENJA BRZINE.

(2) Ti se podaci mogu bilježiti samo nakon ponovnog priključenja napajanja; vremena mogu biti poznata uz tačnost u minutu.

3.12.9 ***Podaci o kvarovima***

Za potrebe ovog podstava vrijeme se bilježi uz rezoluciju od jedne sekunde.

118) Za svaki otkriveni kvar uređaj za evidentiranje podataka mora pokušati zabilježiti i sačuvati u svoju memoriju podataka sljedeće podatke prema sljedećim pravilima arhiviranje:

Kvar	**Pravila arhiviranje**	**Podaci koje je potrebno bilježiti po kvaru**
Kvar kartice	— deset najnovijih kvarova kartice vozača.	— datum i vrijeme početka kvara, — datum i vrijeme završetka kvara, — vrstu i broj kartice, državu članicu koja je izdala karticu i generaciju kartice.
Kvar uređaja za evidentiranje podataka	— deset najnovijih kvarova po vrsti kvara. — prvi kvar koji se dogodio nakon zadnje kalibracije.	— datum i vrijeme početka kvara, — datum i vrijeme završetka kvara, — vrsta kvara, — vrstu, broj, državu članicu koja je izdala karticu i generaciju bilo koje kartice ubačene na početku i/ili završetku kvara.

3.12.10 ***Podaci o kalibraciji***

119) Uređaj za evidentiranje podataka bilježi i arhivira u svojoj memoriji podataka podatke od važnosti za:

- poznate parametre kalibracije u trenutku aktivacije,
- njegovu prvu kalibraciju nakon aktiviranja,
- njegovu prvu kalibraciju u trenutnom vozilu (koje se identifikuje VIN brojem),
- 20 posljednjih kalibracija (ako je tokom jednog kalendarskog dana izvršeno više kalibracija, arhiviraju se samo prva i posljednja izvršena tog dana).

120) Za svaku od spomenutih kalibracija bilježe se sljedeći podaci:

- svrha kalibracije (aktivacija, prva ugradnja, ugradnja, periodični pregled),
- naziv i adresa radionice,
- broj kartice radionice, država članica koja je izdala karticu i datum isteka važenja kartice,
- identifikacija vozila,
- parametri koji se ažuriraju ili potvrđuju: w, k, l, dimenzije guma, podešavanje uređaja za ograničavanje brzine, stanje brojača kilometara (nove i stare vrijednost), datum i vrijeme (nove i stare vrijednosti),
- tipovi i identifikatori svih postavljenih plombi.

121) Osim toga, uređaj za evidentiranje podataka bilježi i arhivira u svoju podatkovnu memoriju mogućnost upotrebe tahografskih kartica prve generacije (bez obzira na to jesu li još uvijek aktivirane).

122) Senzor kretanja bilježi i arhivira u svoju memoriju sljedeće podatke o ugradnji senzora kretanja:

- prvo uparivanje s jedinicom u vozilu (datum, vrijeme, homologacijski broj jedinice u vozilu, serijski broj jedinice u vozilu),
- posljednje uparivanje s jedinicom u vozilu (datum, vrijeme, homologacijski broj jedinice u vozilu, serijski broj jedinice u vozilu).

123) Spoljni uređaj GNSS-a bilježi i arhivira u svoju memoriju sljedeće podatke o ugradnji spoljnog uređaja GNSS-a:

- prvo povezivanje s jedinicom u vozilu (datum, vrijeme, homologacijski broj jedinice u vozilu, serijski broj jedinice u vozilu),

- posljednje povezivanje s jedinicom u vozilu (datum, vrijeme, homologacijski broj jedinice u vozilu, serijski broj jedinice u vozilu).

3.12.11 *Podaci o prilagođavanju vremena*

124) Uređaj za evidentiranje podataka belježi i arhivira u svojoj memoriji podataka podatke koji su važni za prilagodbu vremena izvršenu u kalibracijskom načinu rada izvan okvira redovne kalibracije (def. (f)):

- posljednju prilagodbu vremena,
- pet najvećih prilagođavanju vremena.

125) Za svaku od tih prilagođavanju vremena bilježe se sljedeći podaci:

- datum i vrijeme, stara vrijednost,
- datum i vrijeme, nova vrijednost,
- naziv i adresa radionice,
- broj kartice radionice, država članica koja je izdala karticu, generacija kartice i datum isteka važenja kartice.

3.12.12 *Podaci o aktivnostima nadzora*

126) Uređaj za evidentiranje podataka belježi i arhivira u svoju podatkovnu memoriju sljedeće podatke od važnosti za 20 posljednjih aktivnosti nadzora:

- datum i vrijeme nadzora,
- broj kontrolne kartice, državu članicu koja je izdala karticu i generaciju kartice,
- vrstu nadzora (prikaz i/ili ispis i/ili preuzimanje podataka s jedinice u vozilu i/ili preuzimanje podataka s kartice i/ili provjera kalibracije na putu).

127) U slučaju preuzimanja podataka bilježe se i datumi prvog i posljednjeg dana za koje se preuzimaju podaci.

3.12.13 *Podaci o blokadama preduzeća*

128) Uređaj za evidentiranje podataka belježi i arhivira u svoju podatkovnu memoriju sljedeće podatke od važnosti za 255 posljednjih blokada preduzeća:

- datum i vrijeme zaključavanja blokade,
- datum i vrijeme otključavanja blokade,
- broj kartice preduzeća, državu članicu koja je izdala karticu i generaciju kartice,
- naziv i adresa preduzeća.

Podaci koji su bili prethodno zaključani blokadom, koja je radi prethodno navedene granične vrijednosti uklonjena iz memorije, tretiraju se kao da nisu zaključani.

3.12.14 *Podaci o aktivnostima preuzimanja podataka*

129) Uređaj za evidentiranje podataka belježi i arhivira u svojoj memoriji podataka sljedeće podatke od važnosti za posljednje preuzimanje podataka iz podatkovne memorije na vanjske medije u načinu rada preduzeća ili kalibracije:

- datum i vrijeme preuzimanja podataka,
- broj kartice preduzeća ili radionice, državu članicu koja je izdala karticu i generaciju kartice,
- naziv preduzeća ili radionice.

3.12.15 *Podaci o posebnim stanjima*

130) Uređaj za evidentiranje podataka belježi u svoju podatkovnu memoriju sljedeće podatke od važnosti za posebna stanja:

- datum i vrijeme unosa,
- vrstu posebnog stanja.

131) Podatkovna memorija mora moći čuvati podatke o posebnim stanjima najmanje 365 dana (uz pretpostavu da se dnevno u prosjeku otvara i zatvara jedno stanje). Kad se iscrpi kapacitet za čuvanje, novim se podacima zamjenjuju najstariji podaci.

3.12.16 *Podaci o tahografskoj kartici*

132) Uređaj za evidentiranje podataka mora moći sačuvati sljedeće podatke koji se odnose na različite tahografske kartice koje su upotrijebljene u jedinici u vozilu:

- broj tahografske kartice i njezin serijski broj,
- proizvođača tahografske kartice,

- vrstu tahografske kartice,
- verziju tahografske kartice.

133) Uređaj za evidentiranje podataka mora moći sačuvati najmanje 88 takvih zapisa.

3.13 Očitavanje podataka s tahografskih kartica

134) Uređaj za evidentiranje podataka mora moći očitavati s tahografskih kartica prve i druge generacije, ako je primjereno, sljedeće potrebne podatke:

- identifikovati vrstu kartice, vlasnika kartice, prethodno upotrijebljeno vozilo, datum i vrijeme posljednjeg uklanjanja kartice i aktivnost odabranu u to vrijeme,
- provjeriti je li posljednja razmjena podataka s karticom ispravno zatvorena,
- izračunati neprekidno vrijeme vožnje vozača, kumulativno vrijeme pauze i kumulativno vrijeme vožnje u prethodnom i tekućem nedeljni,
- izraditi ispise prema podacima zabeleženima na kartici vozača,
- preuzeti podatke s kartice vozača na vanjske medije.

Taj se uvjet primjenjuje samo na tahografske kartice prve generacije ako radionica nije onemogućila njihovu upotrebu.

135) U slučaju greške pri čitanju, uređaj za evidentiranje podataka mora ponovo pokušati, najviše tri puta, istu naredbu očitavanja, a ako je očitavanje i tada neuspješno, karticu proglasiti neispravnom i nevažećom.

3.14 Evidentiranje i arhiviranje podataka na tahografske kartice

3.14.1 *Evidentiranje i arhiviranje podataka na tahografske kartice prve generacije*

136) Ako radionica nije onemogućila upotrebu tahografskih kartica prve generacije, uređaj za evidentiranje podataka bilježi i arhivira podatke na potpuno isti način kao što bi to učinio uređaj za evidentiranje podataka prve generacije.

137) Uređaj za evidentiranje podataka postavlja „podatke o razmjeni podataka s karticom” u karticu vozača ili karticu radionice odmah nakon umetanja kartice.

138) Uređaj za evidentiranje podataka ažurira podatke sačuvane na važećioj kartici vozača, radionice, preduzeća i/ili kontrolnoj kartici sa svim podacima koji su bitni za period u kojem je kartica umetnuta i koji se odnose na vlasnika kartice. Podaci sačuvani na tim karticama navedeni su u poglavlju 4.

139) Uređaj za evidentiranje podataka ažurira podatke o aktivnosti vozača i mjestima (kako je navedeno u tačkama 4.5.3.1.9. i 4.5.3.1.11.) sačuvane na važećiim karticama vozača i/ili karticama radionice s podacima o aktivnostima i mjestima koje je vlasnik kartice unio ručno.

140) Svi događaji koji nisu definisani za uređaje za evidentiranje podataka prve generacije ne arhiviraju se na kartice vozača ili radionice.

141) Ažuriranje tahografskih kartica mora biti takvo da se, prema potrebi i uzimajući u obzir stvarni kapacitet arhiviranje, najnovijim podacima zamjenjuju najstariji.

142) U slučaju greške u zapisu, uređaj za evidentiranje podataka mora pokušati ponovno, najviše tri puta, izvršiti istu naredbu zapisivanja, a ako je i dalje neuspješna, proglasiti karticu neispravnom i nevažećom.

143) Prije deblokiranja kartice vozača, a nakon što su svi potrebni podaci sačuvani na karticu, uređaj za evidentiranje podataka poništava „podatke o razmjeni podataka s karticom”.

3.14.2 *Evidentiranje i arhiviranje podataka na tahografske kartice druge generacije*

144) Tahografske kartice druge generacije moraju sadržiti dvije različite kartične aplikacije, od kojih je prva potpuno jednaka aplikaciji za tahografske kartice prve generacije TACHO, a druga je aplikacija „TACHO_G2”, kako je određeno u poglavlju 4. i Dodatku 2.

145) Uređaj za evidentiranje podataka postavlja „podatke o razmjeni podataka s karticom” u karticu vozača ili karticu radionice odmah nakon umetanja kartice.

146) Uređaj za evidentiranje podataka ažurira podatke sačuvane na dvije kartične aplikacije za važeće kartice vozača, radionice, preduzeća i/ili kontrolne kartice sa svim podacima koji su bitni za period u kojem je kartica umetnuta i koji se odnose na vlasnika kartice. Podaci sačuvani na tim karticama navedeni su u poglavlju 4.

147) Uređaj za evidentiranje podataka ažurira podatke o aktivnosti vozača i mjestima (kako je navedeno u tačkama 4.5.3.1.9., 4.5.3.1.11., 4.5.3.2.9. i 4.5.3.2.11.) sačuvane na važećiim karticama

vozača i/ili karticama radionice s podacima o aktivnostima i mjestima koje je vlasnik kartice unio ručno.

148) Ažuriranje tahografskih kartica mora biti takvo da se, prema potrebi i uzimajući u obzir stvarni kapacitet arhiviranje, najnovijim podacima zamjenjuju najstariji.

149) U slučaju greške u zapisu, uređaj za evidentiranje podataka mora pokušati ponovno, najviše tri puta, izvršiti istu naredbu zapisivanja, a ako je i dalje neuspješna, proglasiti karticu neispravnom i nevažećom.

150) Prije deblokiranja kartice vozača, a nakon što su svi potrebni podaci sačuvani na dvije kartične aplikacije za karticu, uređaj za evidentiranje podataka poništava podatke o razmjeni podataka s karticom.

3.15 Prikaz

151) Prikaz mora imati najmanje 20 znakova.

152) Najmanja veličina znaka je 5 mm u visinu i 3,5 mm u širinu.

153) Prikaz podržava znakove navedene u Dodatku 1. poglavlju 4. „Skupovi znakova". Displej može upotrebljavati pojednostavnjene znakove (npr. slovni znakovi s naglaskom mogu se prikazivati bez naglaska ili se mala slova mogu prikazivati kao velika slova).

154) Displej mora imati odgovarajuće neblješteće osvjetljenje.

155) Naznake moraju biti vidljive s vanjske strane uređaja za evidentiranje podataka.

156) Uređaj za evidentiranje podataka mora moći prikazati:

- standardne podatke,
- podatke povezane s upozorenjima,
- podatke povezane s pristupom meniu,
- ostale podatke koje korisnik zatraži.

Uređaj za evidentiranje podataka može prikazati dodatne informacije ako ih je moguće jasno razlikovati od prethodno navedenih podataka.

157) Displej uređaja za evidentiranje podataka upotrebljava piktograme ili kombinacije piktograma navedene u Dodatku 3. Na displeju se mogu prikazati i dodatni piktogrami ili kombinacije piktograma ako ih je moguće jasno razlikovati od ranije spomenutih piktograma ili kombinacija piktograma.

158) Displej mora biti uključen uvijek kad se vozilo kreće.

159) Uređaj za evidentiranje podataka može imati ručnu ili automatsku mogućnost isključivanja displeja kad se vozilo ne kreće.

Oblik prikaza naveden je u Dodatku 5.

3.15.1 *Standardni prikaz*

160) Kad nije potreban prikaz nikakvih drugih podataka, uređaj za evidentiranje podataka mora standardno prikazivati sljedeće informacije:

- lokalno vrijeme (kao rezultat vremena po UTC-u i odstepena koji namješta vozač),
- način rada,
- trenutačnu aktivnost vozača i trenutačnu aktivnost suvozača,
- informacije koje se odnose na vozača:
- ako je njegova trenutna aktivnost VOŽNJA, njegovo trenutno neprekidno vrijeme vožnje i njegovo trenutno kumulativno vrijeme pauze,
- ako njegova trenutna aktivnost nije VOŽNJA, trenutno trajanje te aktivnosti (od trenutka kada je odabrana) i njegovo trenutno kumulativno vrijeme pauze.

161) Prikaz podataka koji se odnose na svakog vozača mora biti jasan, jednostavan i nedvosmislen. U slučaju kad se informacije o vozaču i suvozaču ne mogu prikazati istodobno, uređaj za evidentiranje podataka mora standardno prikazivati podatke koji se odnose na vozača, a korisniku mora omogućiti da prikaže i podatke koji se odnose na suvozača.

162) U slučaju kad širina displeja ne omogućava standardno prikazivanje načina rada, uređaj za evidentiranje podataka mora nakratko prikazati novi način rada kad se on izmijeni.

163) Uređaj za evidentiranje podataka nakratko prikazuje ime vlasnika kartice pri umetanju kartice.

164) Ako je započelo stanje „IZVAN PODRUČJA PRIMJENE" ili VOŽNJA TRAJEKTOM/VOZOM, standardni displej mora, upotrebljavajući odgovarajući piktogram, prikazati da je takvo stanje započelo (prihvatljivo je da se tekuća aktivnost vozača ne mora prikazati istodobno).

3.15.2 *Prikaz upozorenja*

165) Uređaj za evidentiranje podataka prikazuje informacije upozorenja upotrebljavajući prvenstveno piktograme iz Dodatka 3., dopunjene prema potrebi dodatnim numerički kodiranim podacima. Može se dodati i tekstualni opis upozorenja na jeziku po odabiru vozača.

3.15.3 *Pristup meniju*

166) Uređaj za evidentiranje podataka mora osigurati potrebne naredbe putem odgovarajuće strukture menija.

3.15.4 *Ostali prikazi*

167) Na zahtjev se mora omogućiti odabir sljedećih prikaza:

- datum i vrijeme po UTC-u te odstepene lokalnog vremena,
- sadržaj bilo kojeg od šest ispisa u istom obliku kao što su sami ispisi,
- neprekidno vrijeme vožnje i kumulativno vrijeme pauze vozača,
- neprekidno vrijeme vožnje i kumulativno vrijeme pauze suvozača,
- kumulativno vrijeme vožnje vozača u prethodnom i tekućoj nedeljni,
- kumulativno vrijeme vožnje suvozača u prethodnom i tekućoj nedeljni,
- neobavezno:
- sadašnje trajanje aktivnosti suvozača (od trenutka kad je odabrana),
- kumulativno vrijeme vožnje vozača u tekućoj nedeljni,
- kumulativno vrijeme vožnje suvozača za tekuće dnevno radno vrijeme,
- kumulativno vrijeme vožnje vozača za tekuće dnevno radno vrijeme.

168) Prikaz sadržaja ispisa je u slijedu, redak po redak. Ako je širina displeja manja od 24 slovna znaka, korisniku se pruža potpuna informacija na primjeren način (nekoliko redaka, klizni prikaz teksta, …).

Linija ispisa koji se odnose na ručno unesene informacije mogu se izostaviti iz prikaza.

3.16 Ispis

169) Uređaj za evidentiranje podataka mora moći ispisati podatke iz svoje podatkovne memorije i/ili tahografskih kartica u obliku sljedećih sedam ispisa:

- dnevni ispis aktivnosti vozača s kartice,
- dnevni ispis aktivnosti vozača iz jedinice u vozilu,
- ispis događaja i kvarova s kartice,
- ispis događaja i kvarova iz jedinice u vozilu,
- ispis tehničkih podataka,
- ispis prekoračenja brzine,
- istorija podataka o tahografskoj kartici za određenu jedinicu u vozilu (vidjeti poglavlje 3.12.16.).

Pojedinosti o obliku i sadržaju ovih ispisa navedeni su u Dodatku 4.

Na kraju ispisa mogu se dati dodatni podaci.

Uređaj za evidentiranje podataka može omogućiti i druge ispise ako se oni jasno razlikuju od sedam prethodno spomenutih ispisa.

170) „Dnevni ispis aktivnosti vozača s kartice” i „ispis događaja i kvarova s kartice” moraju biti dostupni samo kad je kartica vozača ili kartica radionice umetnuta u uređaj za evidentiranje podataka. Prije početka ispisa uređaj za evidentiranje podataka mora ažurirati podatke sačuvane na odgovarajućoj kartici.

171) Kako bi se izradio „dnevni ispis aktivnosti vozača s kartice” ili „ispis događaja i kvarova s kartice”, uređaj za evidentiranje podataka mora:

- automatski odabrati karticu vozača ili karticu radionice ako je umetnuta samo jedna od navedenih kartica,
- ili omogućiti naredbu za odabir kartice ili izabrati karticu u otvoru vozača ako su obje kartice ubačene u uređaj za evidentiranje podataka.

172) Pisač mora moći ispisati 24 slovna znaka po retku.

173) Najmanja veličina znaka je 2,1 mm u visinu i 1,5 mm u širinu.

174) Pisač podržava znakove navedene u Dodatku 1. poglavlju 4. „Skupovi znakova”.

175) Pisači moraju biti tako izrađeni da daju ispise s takvom oštrinom da se izbjegne svaka nejasnoća pri njihovu čitanju.

176) Ispisi moraju zadržati svoje dimenzije i zapise pod uobičajenim uslovima vlažnosti (10 – 90 %) i temperature.

177) Homologirani papir za uređaj za evidentiranje podataka mora imati odgovarajuću oznaku homologacije i naznaku vrste (vrsta) uređaja za evidentiranje podataka u kojima se može upotrebljavati.

178) Ispisi moraju u normalnim uslovima arhiviranje, s obzirom na jakost svjetla, vlažnost i temperaturu, ostati jasno čitljivi i prepoznatljivi najmanje dvije godine.

179) Ispisi moraju biti u skladu barem sa specifikacijama ispitivanja utvrđenima u Dodatku 9.

180) Mora postojati i mogućnost da se u ove dokumente dodaju rukom pisane zabilješke, kao što je potpis vozača.

181) Događaje „nestanak papira" pri ispisu uređaj za evidentiranje podataka mora riješiti tako da nakon ponovnog umetanja papira ponovno počne ispis od početka ili da se ispis nastavi uz jasno upućivanje na prethodno ispisani dio.

3.17 Upozorenja

182) Uređaj za evidentiranje podataka upozorava vozača pri otkrivanju svakog događaja i/ili kvara.

183) Upozorenje o prekidu napajanja može se odgoditi do ponovnog uspostave napajanja.

184) Uređaj za evidentiranje podataka mora upozoriti vozača 15 minuta prije i u trenutku prekoračenja najvećeg dozvoljenog neprekidnog vremena vožnje.

185) Upozorenja moraju biti vizualna. Uz vizualna upozorenja može se osigurati i zvučni signal.

186) Vizualna upozorenja moraju biti korisniku jasno prepoznatljiva, moraju biti smještena u vidnom polju vozača te jasno čitljiva i danju i noću.

187) Prikaz vizualnih upozorenja može biti ugrađen u uređaj za evidentiranje podataka i/ili odvojen od uređaja za evidentiranje podataka.

188) U posljednjem slučaju označen je simbolom „T".

189) Upozorenja moraju trajati najmanje 30 sekundi, osim ako ih korisnik ne potvrdi prištampano na jednu specifičnu tipku uređaja za evidentiranje podataka ili više njih. Prva potvrda ne smije izbrisati prikaz uzroka upozorenja iz sljedećeg stava.

190) Uzrok upozorenja mora se prikazati na uređaju za evidentiranje podataka i ostati vidljiv dok ga korisnik ne potvrdi upotrebom posebne tipke ili naredbe u uređaju za evidentiranje podataka.

191) Dodatna upozorenja mogu se predvidjeti dokle god ona ne zbunjuju vozače u pogledu prethodno danih upozorenja.

3.18 Preuzimanje podataka na vanjske medije

192) Uređaj za evidentiranje podataka mora moći na zahtjev preuzeti podatke iz svoje podatkovne memorije ili s kartice vozača na vanjske medije za čuvanje preko priključka za kalibraciju / preuzimanje podataka. Prije početka preuzimanja podataka uređaj za evidentiranje podataka mora ažurirati podatke sačuvane na odgovarajućoj kartici.

193) Osim toga, kao neobavezna funkcija, uređaj za evidentiranje podataka može, u bilo kojem načinu rada, na bilo koji drugi način preuzimati podatke za preduzeće koje se identifikujelo preko tog kanala. U tom se slučaju na takvo preuzimanje podataka primjenjuju prava pristupa podacima u načinu rada preduzeća.

194) Preuzimanje podataka ne izmjenjuje ili briše niti jedan sačuvani podatak.

195) Elektronsko sučelje priključka za kalibraciju / preuzimanje podataka opisano je u Dodatku 6.

196) Protokoli preuzimanja podataka opisani su u Dodatku 7.

3.19 Komunikacija na daljinu za ciljane provjere na putu

197) Kad je vozilu dan kontakt, jedinica u vozilu u uređaju za komunikaciju na daljinu svakih 60 sekundi arhivira najnovije podatke potrebne u svrhu ciljanih provjera na putu. Ti se podaci šifriraju i potpisuju kako je određeno u Dodatku 11. i Dodatku 14.

198) Podaci koje je potrebno provjeriti na daljinu moraju biti dostupni čitačima komunikacije na daljinu bežično, kako je određeno u Dodatku 14.

199) Podaci potrebni u svrhu ciljanih provjera na putu odnose se na sljedeće:

- najnoviji pokušaj povrede sigurnosti,

- najduži prekid napajanja,
- kvar senzora,
- grešku u podacima o kretanju,
- konflikt u kretanju vozila,
- vožnju bez važeće kartice,
- umetanje kartice tokom vožnje,
- podatke o prilagođavanju vremena,
- podatke o kalibraciji, uključujući datume dvaju najnovijih sačuvanih zapisa o kalibraciji,
- registarski broj vozila,
- brzinu koju je tahograf zabeležio.

3.20 Izlazni podaci za dodatne vanjske uređaje

200) Uređaj za belježenje podataka može biti opremljen i standardizovanim sučeljima putem kojih podatke koje je tahograf zabilježio ili generisao može u operativnom ili kalibracijskom načinu rada upotrebljavati spoljni uređaj.

U Dodatku 13. određeno je i standardizirano neobvezno ITS sučelje. Uz njega mogu postojati i druga sučelja jedinica u vozilu ako su u potpunosti u skladu sa zahtjevima Dodatka 13. u smislu minimalnog popisa podataka, sigurnosti i saglasnosti vozača.

Saglasnost vozača ne primjenjuje se na podatke koje uređaj za belježenje prenosi mreži vozila. Ako su lični podaci poslani mreži vozila dalje obrađuju izvan mreže vozila, proizvođač vozila odgovoran je za usklađivanje tog postupka obrade ličnih podataka (‚Opšta uredba o zaštiti podataka').

Saglasnost vozača ne primjenjuje se ni na podatke tahografa koje preuzima udaljeno preduzeće (zahtjev 193)) jer se taj scenarij prati u okviru prava pristupa s pomoću kartice preduzeće.

Sljedeći se zahtjevi primjenjuju na podatke ITS-a koji su stavljeni na raspolaganje putem tog sučelja:

- ti su podaci skup odabranih postojećih podataka iz rečnika tahografskih podataka (Dodatak 1.),
- podskup tih odabranih podataka označen je kao ‚lični podaci',
- podskup ‚ličnih podataka' dostupan je samo ako je omogućena provjerljiva saglasnost vozača kojom vozač prihvaća da njegovi lični podaci mogu izaći iz mreže vozila,
- u svakom se trenutku saglasnost vozača može omogućiti ili onemogućiti uz pomoć naredbi u meniu, pod uslovom da je kartica vozača umetnuta,
- skup i podskup podataka šalje se bežičnim Bluetooth protokolom u radijusu kabine vozila, uz frekvenciju osvježavanja od 1 minute,
- uparivanje vanjskog uređaja s ITS sučeljem zaštitit će se namjenskim nasumičnim PIN-om od najmanje četiri karakteristik koji će se zabilježiti i biti dostupan na displeju svake jedinice u vozilu,
- prisutnošću ITS sučelja ni u kojim se okolnostima ne može narušiti ispravno funkcionisanje i sigurnost jedinice u vozilu, niti na njih utjecati.

Uz skup odabranih postojećih podataka, koji se smatra minimalnim popisom, mogu se osigurati i drugi podaci pod uslovom da se oni ne mogu smatrati ličnim podacima.

Uređaj za evidentiranje može prenijeti status saglasnosti vozača drugim platformama unutar mreže vozila.

Kad je uključen kontakt vozila, ti se podaci neprekidno šalju.

201) Tahografi mogu i dalje biti opremljeni serijskim sučeljem, radi obrnute kompatibilnosti. U svakom slučaju, saglasnost vozača i dalje je potrebna ako se prenose lični podaci.

3.21 Kalibracija

202) Funkcija kalibracije mora omogućavati:

- automatsko uparivanje senzora kretanja s jedinicom u vozilu,
- automatsko povezivanje spoljnog uređaja GNSS-a s jedinicom u vozilu ako je primjenjivo,
- digitalno prilagođavanje konstante uređaja za evidentiranje podataka (k) karakterističnom koeficijentu vozila (w),
- prilagodbu trenutnog vremena u okviru roka važenja ubačene kartice radionice,
- podešavanje trenutne vrijednosti brojača kilometara,
- ažuriranje identifikacijskih podataka senzora kretanja sačuvanih u memoriji podataka,
- ažuriranje identifikacijskih podataka spoljnog uređaja GNSS-a sačuvanih u memoriji podataka ako je primjenjivo,

- ažuriranje tipova i identifikatora svih postavljenih plombi,
- ažuriranje ili potvrdu ostalih parametara poznatih uređaju za evidentiranje podataka: identifikaciju vozila, w, l, veličinu guma i podešavanje uređaja za ograničavanje brzine ako je primjenjivo.

203) Osim toga, funkcija kalibracije mora omogućiti onemogućivanje upotrebe tahografskih kartice prve generacije u uređaju za evidentiranje podataka ako su ispunjeni uslovi određeni u Dodatku 15.

204) Uparivanje senzora kretanja s jedinicom u vozilu sastoji se barem od sljedećeg:

- ažuriranja instalacijskih podataka senzora kretanja koji se čuvaju u senzoru kretanja (prema potrebi),
- kopiranja iz senzora kretanja u podatkovnu memoriju jedinice u vozilu potrebnih identifikacijskih podataka senzora kretanja.

205) Povezivanje spoljnog uređaja GNSS-a s jedinicom u vozilu sastoji se barem od sljedećeg:

- ažuriranja podataka o ugradnji spoljnog uređaja GNSS-a koje čuva spoljni uređaj GNSS-a (prema potrebi),
- kopiranja s spoljnog uređaja GNSS-a u memoriju podataka jedinice u vozilu potrebnih identifikacijskih podataka o spoljnom uređaju GNSS-a, uključujući serijski broj spoljnog uređaja GNSS-a.

Nakon povezivanja sprovodi se provjera podataka o položaju GNSS-a.

206) Funkcija kalibriranja mora moći unijeti potrebne podatke preko priključka za kalibraciju/preuzimanje podataka u skladu s protokolom kalibracije utvrđenim u Dodatku 8. Funkcija kalibriranja može unositi potrebne podatke i na druge načine.

3.22 Provjera kalibracije na putu

207) Funkcija provjere kalibracije na putu mora omogućiti očitavanje serijskog broja senzora kretanja (koji može biti ugrađen u adapter) i serijskog broja spoljnog uređaja GNSS-a (ako je primjenjivo) priključenog na jedinicu u vozilu u trenutku zahtjeva.

208) To očitavanje mora biti moguće barem putem displeja jedinice u vozilu s pomoću naredbi u meniju.

209) Funkcija provjere kalibracije na putu mora omogućiti i izbor U/I načina rada kalibracijske U/I signalne linije određenog u Dodatku 6., preko sučelja K-linije. To se sprovodi preko ECUAdjustmentSession, kako je određeno u Dodatku 8., odjeljku 7. Upravljanje ispitnim impulsima – funkcionalna jedinica za upravljanje ulazom/izlazom.

3.23 Prilagođavanje vremena

210) Funkcija prilagodbe vremena mora omogućiti automatsku prilagodbu trenutnog vremena. Za prilagodbu vremena u uređaju za evidentiranje podataka upotrebljavaju se dva izvora vremena: 1) unutarnji sat jedinice u vozilu, 2) prijemnik GNSS-a.

211) Postavljanje vremena unutarnjeg sata jedinice u vozilu automatski se ponovno prilagođava u intervalima od 12 sati. Kad ta ponovna prilagodba nije moguća jer signal GNSS-a nije dostupan, vrijeme se postavlja čim jedinica u vozilu dobije pristup važećiom vremenu iz prijamnika GNSS-a, u skladu s uslovima paljenja vozila. Referentno vrijeme za automatsko postavljanje vremena unutarnjeg sata jedinice u vozilu preuzima se iz prijamnika GNSS-a.

212) Funkcija prilagodbe vremena mora u kalibracijskom načinu omogućavati aktiviranje prilagodbe trenutnog vremena.

3.24 Karakteristike radnog učinka

213) Jedinica u vozilu mora biti u potpunosti operativna u rasponu temperature od – 20 °C do 70 °C, spoljni uređaj GNSS-a u rasponu temperature od – 20 °C do 70 °C, a senzor kretanja u rasponu temperature od – 40 °C do 135 °C. Sadržaj podatkovne memorije mora se očuvati pri temperaturi do – 40 °C.

214) Tahograf mora biti u potpunosti spreman za rad pri rasponu vlažnosti od 10 % do 90 %.

215) Plombe upotrijebljene u pametnom tahografu moraju izdržati iste uslove kao sastavni dijelovi tahografa na koje su stavljene.

216) Uređaj za evidentiranje podataka mora biti zaštićen od prenapona, zamjene polariteta napajanja i kratkih spojeva.

217) Senzori kretanja:

- reagiraju na magnetsko polje koje ometa detekciju kretanja vozila. U takvim okolnostima jedinica u vozilu bilježi i arhivira kvar senzora (zahtjev 88) ili,

- imaju senzorski element zaštićen od magnetskih polja ili je na njih neosjetljiv.

218) Uređaj za evidentiranje podataka i spoljni uređaj GNSS-a moraju biti u skladu s međunarodnin pravilnikom UNECE-a R10 i zaštićeni od elektrostatičkih pražnjenja i prelaznih pojava.

3.25 Materijali

219) Svi sastavni dijelovi uređaja za evidentiranje podataka moraju biti izrađeni od materijala dostatne stabilnosti i mehaničke čvrstoće te stabilnih električnih i magnetskih osobina.

220) U normalnim uslovima upotrebe svi unutarnji dijelovi uređaja moraju biti zaštićeni od vlage i prašine.

221) Jedinica u vozilu i spoljni uređaj GNSS-a moraju zadovoljavati stepen zaštite IP 40, a senzor kretanja mora zadovoljavati stepen zaštite IP 64 prema normi IEC 60529:1989, uključujući A1:1999 i A2:2013.

222) Uređaj za evidentiranje podataka mora odgovarati važećim tehničkim specifikacijama u odnosu na ergonomsku izvedbu.

223) Uređaj za evidentiranje podataka mora biti zaštićen od slučajnog oštećenja.

3.26 Oznake

224) Ako uređaj za evidentiranje podataka prikazuje stanje brojača kilometara i brzinu vozila, na displeju se pojavljuju sljedeće pojedinosti:

- pokraj broja koji označava udaljenost, jedinicu mjere za udaljenost označenu kraticom „km”,
- pokraj broja koji pokazuje brzinu, oznaku „km/h”.

Uređaj za evidentiranje podataka može se prebaciti i na prikaz brzine u miljama na sat, a u tom se slučaju jedinica mjere za brzinu prikazuje kraticom „mph” . Uređaj za evidentiranje podataka može prebaciti i na prikaz udaljenosti u miljama, a u tom se slučaju jedinica mjere za udaljenost prikazuje kraticom „mi” .

225) Opisna pločica pričvršćuje se na svakom odvojenom sastavnom dijelu uređaja za bilježenje podataka i prikazuje sljedeće podatke:

- naziv i adresu proizvođača,
- kataloški broj proizvođača i godinu proizvodnje,
- serijski broj,
- oznaku homologacije.

226) Ako fizički prostor nije dostatan za prikaz svih prethodno navedenih podataka, opisna pločica prikazuje barem: naziv ili zaštitni znak proizvođača i kataloški broj.

4 ZAHTJEVI U POGLEDU IZRADE I FUNKCIONALNOSTI TAHOGRAFSKIH KARTICA

4.1 Vidljivi podaci

Prednja strana mora sadržiti:

227) riječi „kartica vozača” ili „kontrolna kartica” ili „kartica radionice” ili „kartica preduzeća” štampane velikim slovima na službenom jeziku ili jezicima države članice koja izdaje karticu, prema vrsti kartice;

228) ime države članice koja je izdala karticu (nije obvezno);

229) razlikovnu oznaku države članice koja izdaje karticu, tiskanu u negativu u plavom pravougaoniku i okruženu s 12 žutih zvijezda. Poznati znakovi sljedeći su:

B BG CZ CY	Belgija Bugarska Češka Cipar	LV L LT M	Latvija Luksemburg Litva Malta
DK	Danska	NL	Holandija
D EST	Njemačka Estonija	A PL	Austrija Poljska
GR	Grčka	P RO SK SLO	Portugal Rumunija Slovačka Slovenija
E	Španija	FIN	Finska
F HR H	Francuska Hrvatska Mađarska	S	Švedska
IRL	Irska	UK	Ujedinjena Kraljevina

I	Italija		

230) podatke karakteristične za izdatu karticu, označene kako slijedi:

	Kartica vozača	Kontrolna kartica	Kartica preduzeća ili radionice
1.	prezime vozača	naziv nadzornog tijela	naziv preduzeća ili radionice
2.	ime(na) vozača	prezime nadzornika (ako je primjenjivo)	prezime vlasnika kartice (ako je primjenjivo)
3.	datum rođenja vozača	ime(na) nadzornika (ako je primjenjivo)	ime(na) vlasnika kartice (ako je primjenjivo)
4.a	datum početka važenja kartice		
4.b	datum isteka važenja kartice		
4.c	naziv tijela koje je izdalo karticu (može se ispisati na stražnjoj strani)		
4.d	drukčiji broj od broja pod točkom 5., zbog administrativnih razloga (nije obvezno)		
5.a	broj vozačke dozvole (na datum izdavanja kartice vozača)	—	—
5.b	broj kartice		
6.	fotografija vozača	fotografija nadzornika (nije obvezno)	fotografija instalatera (nije obvezno)
7.	potpis vlasnika (nije obvezno)		
8.	uobičajeno boravište ili poštanska adresa vlasnika (nije obvezno).	poštanska adresa nadzornog tijela	poštanska adresa preduzeća ili radionice

231) datumi se pišu u obliku „dd/mm/gggg" ili „dd.mm.gggg." (dan, mjesec, godina).

Zadnja strana mora sadržiti:

232) objašnjenje navedenih stavki na prednjoj strani kartice;

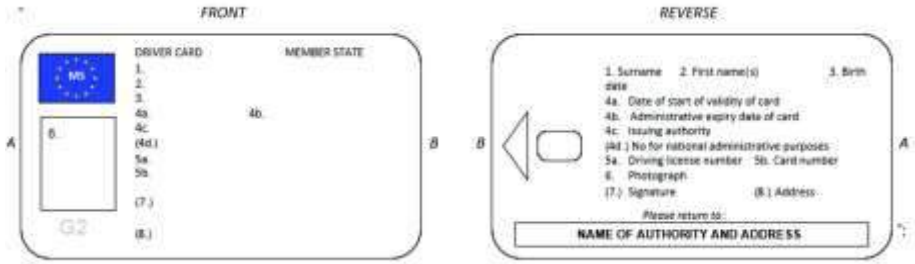
233) uz poseban pisani pristanak vlasnika mogu se dodati i informacije koje se ne odnose na vođenje kartice, pri čemu njihovo dodavanje ni na koji način neće izmijeniti upotrebu obrasca kao tahografske kartice.

234) Tahografske kartice moraju se štampati sa sljedećim prevladavajućim bojama pozadine:

- kartica vozača : bijela,
- kontrolna kartica : plava,
- kartica radionice : crvena,
- kartica preduzeća : žuta.

235) Tahografske kartice moraju imati barem sljedeća obilježja za zaštitu tijela kartice od krivotvorenja i neovlaštenog rukovanja:

- sigurnosnu podlogu s tankim guilloche uzorcima i štampano s duginim efektom (irisnim štampano),
- na prostoru za fotografiju, sigurnosno izvedena pozadina i fotografija moraju se preklapati,
- barem jednu dvobojnu liniju u mikrotisku.



236) Nakon dogovora s Komisijom države članice mogu dodavati boje i oznake kao što su nacionalni simboli i sigurnosna obilježja, ne dovodeći u pitanje druge odredbe ovog Priloga.

237) Privremene kartice iz člana 26. stava 4. Uredbe (EU) br. 165/2014 moraju biti u skladu s odredbama ovog Priloga.

4.2 Sigurnost

Sigurnost sistema ima za cilj zaštitu integriteta i autentičnosti podataka koji se razmjenjuju između kartica i uređaja za evidentiranje podataka, zaštitu integriteta i autentičnosti podataka koji se preuzimaju s kartica, omogućavanje određenih aktivnosti upisivanja na kartice samo uređaju za

evidentiranje podataka, dešifriranje određenih podataka, isključivanje svake mogućnosti krivotvorenja podataka sačuvanih na karticama, sprečavanje neovlaštenog rukovanja i otkrivanje svih pokušaja te vrste.

238) Kako bi se postigla sigurnost sistema, tahografske kartice moraju zadovoljavati sigurnosne zahtjeve utvrđene u dodacima 10. i 11.

239) Tahografske kartice moraju biti čitljive u drugoj opremi, kao što su osobna računala.

4.3 Norme

240) Tahografske kartice moraju zadovoljavati sljedeće norme:

- ISO/IEC 7810 Identification cards – Physical characteristics,
- ISO/IEC 7816 Identification cards – Integrated circuit cards:
- Part 1: Physical characteristics,
- Part 2: Dimensions and position of the contacts (ISO/IEC 7816-2:2007),
- Part 3: Electrical interface and transmission protocols (ISO/IEC 7816-3:2006),
- Part 4: Organisation, security and commands for interchange (ISO/IEC 7816-4:2013 + Cor 1:2014),
- Part 6: Interindustry data elements for interchange (ISO/IEC 7816-6:2004 + Cor 1:2006),
- Part 8: Commands for security operations (ISO/IEC 7816-8:2004).
- Tahografske kartice ispituju se u skladu s normom ISO/IEC 10373-3:2010 Identification cards – Test methods – *Part 3: Integrated circuit cards with contacts and related interface devices*.

4.4 Specifikacije okruženja i elektrotehničke specifikacije

241) Tahografske kartice moraju moći ispravno raditi u svim klimatskim uslovima uobičajenima na teritoriju Zajednice, pri temperaturnom rasponu od najmanje – 25 °C do + 70 °C s povremenim vršnim porastom do +85 °C, pri čemu „povremeno" označava ne duže od 4 sata svaki puta i ne više od 100 puta tokom vijeka trajanja kartice.

242) Tahografske kartice moraju moći ispravno raditi u rasponu vlažnosti između 10 % i 90 %.

243) Tahografske kartice moraju moći ispravno raditi tokom perioda od pet godina ako se upotrebljavaju u skladu sa specifikacijama okruženja i elektrotehničkim specifikacijama.

244) Tokom upotrebe tahografske kartice moraju biti u skladu s Pravilnikom UNECE-a R10 o elektromagnetskoj kompatibilnosti te moraju biti zaštićene od elektrostatskih pražnjenja.

4.5 Arhiviranje podataka

Za potrebe ovog stava

- vremena se bilježe uz rezoluciju od jedne minute, osim ako nije drukčije određeno,
- stanje brojača kilometara bilježi se uz rezoluciju od jednog kilometra,
- brzine se bilježe uz rezoluciju od 1 km/h,
- položaji (geografske širine i dužine) bilježe se u stepenima i minutama, uz rezoluciju od 1/10 minute.

Funkcije, naredbe i logičke strukture tahografskih kartica koje ispunjavaju zahtjeve u pogledu arhiviranje podataka navedene su u Dodatku 2.

Ako nije drukčije određeno, arhiviranje podataka na tahografske kartice organizira se tako da se novim podacima zamjenjuju najstariji sačuvani podaci ako je iscrpljena predviđena veličina memorije za određene zapise.

245) U ovom se stavu navodi minimalni kapacitet arhiviranje podataka za različite datoteke aplikacija. Tahografske kartice moraju moći prikazati uređaju za evidentiranje podataka stvarni kapacitet arhiviranje tih datoteka.

246) Svi dodatni podaci koji se mogu sačuvati na tahografskim karticama, a koji se odnose na druge podatke koji su možda sačuvani na kartici, arhiviraju se u skladu sa ovim pravilnikom.

247) Svaka glavna datoteka (eng. *Master File*, MF) tahografske kartice sadrži najviše pet elementarnih datoteka (eng. *Elementary File*, EF) za upravljanje karticama te identifikaciju aplikacija i čipova kao i dvije namjenske datoteke (eng. *Dedicated File*, DF):

- DF Tachograph koji sadrži aplikaciju kojoj mogu pristupiti jedinice u vozilu prve generacije i koja je prisutna i na tahografskim karticama prve generacije,
- DF Tachograph_G2 koji sadrži aplikaciju kojoj mogu pristupiti jedinice u vozilu druge generacije i koja je prisutna i na tahografskim karticama druge generacije.

Sve pojedinosti o strukturi tahografskih kartica određene su u Dodatku 2.

4.5.1 *Elementarne datoteke za identifikaciju i upravljanje karticama*

4.5.2 *Identifikacija IC kartice*

248) Tahografske kartice moraju moći sačuvati sljedeće identifikacijske podatke pametnih kartica:

- zaustavljanje sata,
- serijski broj kartice (s proizvodnim referencama),
- homologacijski broj kartice,
- identifikaciju (ID) personalizatora kartice,
- identifikaciju ugraditelja (ID),
- identifikator IC.

4.5.2.1 Identifikacija čipa

249) Tahografske kartice moraju moći sačuvati sljedeće identifikacijske podatke o integriranom krugu (IC):

- serijski broj IC,
- proizvodne reference IC.

4.5.2.2 DIR (prisutan samo na tahografskim karticama druge generacije)

250) Tahografske kartice moraju moći sačuvati objekte programskih identifikacijskih podataka određene u Dodatku 2.

4.5.2.3 Podaci ATR-a (uvjetno, prisutno samo na tahografskim karticama druge generacije)

251) Tahografske kartice moraju moći sačuvati sljedeći objekt podataka proširene veličine:

- ako tahografska kartica podržava polja proširene veličine, objekt podataka proširene veličine određen u Dodatku 2.

4.5.2.4 Podaci proširene veličine (uvjetno, prisutno samo na tahografskim karticama druge generacije)

252) Tahografske kartice moraju moći sačuvati sljedeće objekte podataka proširene veličine:

- ako tahografska kartica podržava polja proširene veličine, objekte podataka proširene veličine određene u Dodatku 2.

4.5.3 *Kartica vozača*

4.5.3.1 Tahografska aplikacija (pristup jedinicama u vozilu prve i druge generacije)

4.5.3.1.1 Identifikacija aplikacije

253) Kartica vozača mora moći sačuvati sljedeće programske identifikacijske podatke:

- identifikaciju tahografske aplikacije,
- identifikaciju vrste tahografske kartice.

4.5.3.1.2 Ključevi i certifikati

254) Kartica vozača mora moći sačuvati niz kriptografskih ključeva i certifikata, kako je određeno u Dodatku 11. dijelu A.

4.5.3.1.3 Identifikacija kartice

255) Kartica vozača mora moći sačuvati sljedeće identifikacijske podatke kartice:

- broj kartice,
- državu članicu izdavanja, naziv tijela koje izdaje karticu, datum izdavanja,
- datum početka i isteka važenja kartice.

4.5.3.1.4 Identifikacija vlasnika kartice

256) Kartica vozača mora moći sačuvati sljedeće identifikacijske podatke vlasnika kartice:

- prezime vlasnika,
- ime(na) vlasnika,
- datum rođenja,
- željeni jezik.

4.5.3.1.5 Preuzimanje podataka s kartice

257) Kartica vozača mora moći sačuvati sljedeće podatke koji se odnose na preuzimanje podataka s kartice:

- datum i vrijeme posljednjeg preuzimanja podataka s kartice (za sve potrebe osim nadzora).

258) Kartica vozača mora moći spremiti jedan takav zapis.

4.5.3.1.6 Podaci o vozačkoj dozvoli

259) Kartica vozača mora moći sačuvati sljedeće podatke o vozačkoj dozvoli:

- državu članicu izdavanja i naziv tijela koje je izdalo dozvolu,
- broj vozačke dozvole (na datum izdavanja kartice).

4.5.3.1.7 Podaci o događajima

Za potrebe ovog podstava vrijeme se bilježi uz rezoluciju od jedne sekunde.

260) Kartica vozača mora moći sačuvati podatke koji se odnose na sljedeće događaje koje je uređaj za evidentiranje podataka otkrio dok je bila umetnuta kartica:

- vremensko preklapanje (ako je navedena kartica uzrokovala događaj),
- umetanje kartice tokom vožnje (ako je navedena kartica predmet događaja),
- neispravan završetak posljednje razmjene podataka s karticom (ako je navedena kartica predmet događaja),
- prekid napajanja,
- grešku u podacima o kretanju,
- pokušaje povrede sigurnosti.

261) Kartica vozača mora moći sačuvati sljedeće podatke za navedene događaje:

- kod događaja,
- datum i vrijeme početka događaja (ili umetanja kartice ako je događaj u to vrijeme bio u toku),
- datum i vrijeme završetka događaja (ili uklanjanja kartice ako je događaj u to vrijeme bio u toku),
- VRN i državu članicu registracije vozila u kojem je nastao događaj.

Napomena: U slučaju događaja „vremensko preklapanje”:

- datum i vrijeme početka događaja moraju odgovarati datumu i vremenu uklanjanja kartice iz prethodnog vozila,
- datum i vrijeme završetka događaja moraju odgovarati datumu i vremenu umetanja kartice u aktualno vozilo,
- podaci o vozilu moraju se odnositi na aktualno vozilo, u kojemu je događaj nastupio.

Napomena: U slučaju događaja „neispravno zatvaranje posljednje razmjene podataka s karticom”:

- datum i vrijeme početka događaja moraju odgovarati datumu i vremenu umetanja kartice pri razmjeni podataka koja nije pravilno završena,
- datum i vrijeme završetka događaja moraju odgovarati datumu i vremenu umetanja kartice pri razmjeni podataka tokom koje je događaj otkriven (tekuća razmjena podataka),
- podaci o vozilu moraju se odnositi na vozilo u kojemu razmjena podataka nije pravilno završena.

262) Kartica vozača mora moći sačuvati podatke za šest posljednjih događaja za svaku vrstu (tj. 36 događaja).

4.5.3.1.8 Podaci o kvarovima

Za potrebe ovog podstava vrijeme se bilježi uz rezoluciju od jedne sekunde.

263) Kartica vozača mora moći sačuvati podatke koji se odnose na sljedeće kvarove koje je uređaj za evidentiranje podataka otkrio dok je kartica bila umetnuta:

- kvar kartice (kad je ta kartica predmet kvara),
- kvar uređaja za evidentiranje podataka.

264) Kartica vozača mora moći sačuvati sljedeće podatke za navedene kvarove:

- kod kvara,
- datum i vrijeme početka kvara (ili umetanja kartice ako je u tom trenutku kvar bio u toku),
- datum i vrijeme završetka kvara (ili uklanjanja kartice ako je u tom trenutku kvar bio u toku),
- VRN i državu članicu registracije vozila u kojemu je došlo do kvara.

265) Kartica vozača mora moći sačuvati podatke za dvanaest posljednjih kvarova za svaku vrstu (tj. 24 kvara).

4.5.3.1.9 Podaci o aktivnosti vozača

266) Kartica vozača mora moći sačuvati, za svaki kalendarski dan upotrebe kartice ili za koji je vozač ručno unio podatke, sljedeće podatke:

- datum,
- dnevni brojač prisustva (uvećan za jedan za svaki od navedenih kalendarskih dana),
- ukupnu udaljenost koju je vozač prešao u tom danu,
- status vozača u 00:00,
- kad god je vozač promijenio aktivnost i/ili status vožnje i/ili je umetnuo ili izvadio svoju karticu:
- status vožnje (POSADA, JEDAN VOZAČ),
- otvor (VOZAČ, SUVOZAČ),
- status kartice (UMETNUTA, NIJE UMETNUTA),
- aktivnost (VOŽNJA, DOSTUPNOST, RAD, PAUZA/ODMOR),
- vrijeme promjene.

267) Memorija kartice vozača mora moći zadržati podatke o aktivnosti vozača najmanje 28 dana (pri čemu se prosječna aktivnost vozača definiše kao 93 promjene aktivnosti dnevno).

268) Podaci navedeni u zahtjevima 261, 264 i 266 arhiviraju se na način koji omogućava učitavanje aktivnosti redoslijedom njihova pojavljivanja, čak i u slučaju vremenskog preklapanja.

4.5.3.1.10 Podaci o upotrijebljenim vozilima

269) Kartica vozača mora moći sačuvati sljedeće podatke za svaki kalendarski dan upotrebe kartice i za svako period upotrebe dotičnog vozila tog dana (periodm upotrebe obuhvaćeni su svi uzastopni ciklusi umetanja i uklanjanja kartice u tom vozilu s gledišta kartice):

- datum i vrijeme prve upotrebe vozila (tj. prvog umetanja kartice u navedenom periodu upotrebe vozila ili 00:00 ako je u to vrijeme vozilo već u upotrebi),
- stanje brojača kilometara vozila u to vrijeme,
- datum i vrijeme posljednje upotrebe vozila (tj. posljednjeg uklanjanja kartice u tom periodu upotrebe vozila ili 23:59 ako je u to vrijeme vozilo već u upotrebi),
- stanje brojača kilometara vozila u to vrijeme,
- VRN i državu članicu registracije vozila.

270) Kartica vozača mora moći sačuvati najmanje 84 takva zapisa.

4.5.3.1.11 Mjesta početka i/ili završetka dnevnog radnog vremena

271) Kartica vozača mora moći sačuvati sljedeće podatke koji se odnose na mjesto početka i/ili završetka dnevnog radnog vremena koje unese vozač:

- datum i vrijeme unosa (ili datum/vrijeme koje se odnosi na ručni unos),
- vrstu unosa (početak ili kraj, stanje unosa),
- državu i regiju ulaska,
- stanje brojača kilometara vozila.

272) Memorija kartice vozača mora moći sačuvati najmanje 42 para takvih zapisa.

4.5.3.1.12 Podaci o upotrebi kartice

273) Kartica vozača mora moći sačuvati podatke koji se odnose na vozilo u kojem je započela upotreba kartice:

- datum i vrijeme početka upotrebe (tj. umetanje kartice) uz rezoluciju od jedne sekunde,
- VRN i državu članicu registracije.

4.5.3.1.13 Podaci o aktivnostima nadzora

274) Kartica vozača mora moći sačuvati sljedeće podatke koji se odnose na aktivnosti nadzora:

- datum i vrijeme nadzora,
- broj kontrolne kartice i državu članicu koja je karticu izdala,
- vrsta nadzora (prikaz i/ili ispis i/ili preuzimanje podataka s jedinice vozila i/ili preuzimanje podataka s kartice (vidjeti napomenu)),
- period preuzimanja podataka (u slučaju preuzimanja podataka),
- VRN i državu članicu registracije vozila u kojoj je izvršen nadzor.

Napomena: preuzimanje podataka s kartice bilježi se samo ako je izvršeno preko uređaja za evidentiranje podataka.

275) Kartica vozača mora moći spremiti jedan takav zapis.

4.5.3.1.14 Podaci o posebnim stanjima

276) Kartica vozača mora moći sačuvati sljedeće podatke koji se odnose na posebna stanja koja su unesena dok je kartica bila umetnuta (bez obzira u koji otvor):

- datum i vrijeme unosa,
- vrstu posebnog stanja.

277) Kartica vozača mora moći sačuvati najmanje 56 takvih zapisa.

4.5.3.2 Tahografska aplikacija druge generacije (nije dostupno jedinici u vozilu prve generacije)

4.5.3.2.1 Identifikacija aplikacije

278) Kartica vozača mora moći sačuvati sljedeće programske identifikacijske podatke:

- identifikaciju tahografske aplikacije,
- identifikaciju vrste tahografske kartice.

4.5.3.2.2 Ključevi i certifikati

279) Kartica vozača mora moći sačuvati niz kriptografskih ključeva i certifikata, kako je određeno u Dodatku 11. dijelu B.

4.5.3.2.3 Identifikacija kartice

280) Kartica vozača mora moći sačuvati sljedeće identifikacijske podatke kartice:

- broj kartice,
- državu članicu izdavanja, naziv tijela koje izdaje karticu, datum izdavanja,
- datum početka i isteka važenja kartice.

4.5.3.2.4 Identifikacija vlasnika kartice

281) Kartica vozača mora moći sačuvati sljedeće identifikacijske podatke vlasnika kartice:

- prezime vlasnika,
- ime(na) vlasnika,
- datum rođenja,
- željeni jezik.

4.5.3.2.5 Preuzimanje podataka s kartice

282) Kartica vozača mora moći sačuvati sljedeće podatke koji se odnose na preuzimanje podataka s kartice:

- datum i vrijeme posljednjeg preuzimanja podataka s kartice (za sve potrebe osim nadzora).

283) Kartica vozača mora moći spremiti jedan takav zapis.

4.5.3.2.6 Podaci o vozačkoj dozvoli

284) Kartica vozača mora moći sačuvati sljedeće podatke o vozačkoj dozvoli:

- državu članicu izdavanja i naziv tijela koje je izdalo dozvolu,
- broj vozačke dozvole (na datum izdavanja kartice).

4.5.3.2.7 Podaci o događajima

Za potrebe ovog podstava vrijeme se bilježi uz rezoluciju od jedne sekunde.

285) Kartica vozača mora moći sačuvati podatke koji se odnose na sljedeće događaje koje je uređaj za evidentiranje podataka otkrio dok je bila umetnuta kartica:

- vremensko preklapanje (ako je navedena kartica uzrokovala događaj),
- umetanje kartice tokom vožnje (ako je navedena kartica predmet događaja),
- neispravan završetak posljednje razmjene podataka s karticom (ako je navedena kartica predmet događaja),
- prekid napajanja,
- grešku u komunikaciji s uređajem za komunikaciju na daljinu,
- događaj izopauza podataka o položaju iz prijemnika GNSS-a,
- grešku u komunikaciji s spoljnim uređajem GNSS-a
- grešku u podacima o kretanju,
- konflikt u kretanju vozila,
- pokušaje povrede sigurnosti,

- vremenski konflikt.

286) Kartica vozača mora moći sačuvati sljedeće podatke za navedene događaje:

- kod događaja,
- datum i vrijeme početka događaja (ili umetanja kartice ako je događaj u to vrijeme bio u toku),
- datum i vrijeme završetka događaja (ili uklanjanja kartice ako je događaj u to vrijeme bio u toku),
- VRN i državu članicu registracije vozila u kojem je nastao događaj.

Napomena: U slučaju događaja „vremensko preklapanje”:

- datum i vrijeme početka događaja moraju odgovarati datumu i vremenu uklanjanja kartice iz prethodnog vozila,
- datum i vrijeme završetka događaja moraju odgovarati datumu i vremenu umetanja kartice u aktualnom vozilu,
- podaci o vozilu moraju se odnositi na aktualno vozilo, u kojemu je događaj nastupio.

Napomena: U slučaju događaja „neispravno zatvaranje posljednje razmjene podataka s karticom”:

- datum i vrijeme početka događaja moraju odgovarati datumu i vremenu umetanja kartice pri razmjeni podataka koja nije pravilno završena,
- datum i vrijeme završetka događaja moraju odgovarati datumu i vremenu umetanja kartice pri razmjeni podataka tokom koje je događaj otkriven (tekuća razmjena podataka),
- podaci o vozilu moraju se odnositi na vozilo u kojemu razmjena podataka nije pravilno završena.

287) Kartica vozača mora moći sačuvati podatke za šest posljednjih događaja za svaku vrstu (tj. 66 događaja).

4.5.3.2.8 Podaci o kvarovima

Za potrebe ovog podstava vrijeme se bilježi uz rezoluciju od jedne sekunde.

288) Kartica vozača mora moći sačuvati podatke koji se odnose na sljedeće kvarove koje je uređaj za evidentiranje podataka otkrio dok je kartica bila umetnuta:

- kvar kartice (kad je ta kartica predmet kvara),
- kvar uređaja za evidentiranje podataka.

289) Kartica vozača mora moći sačuvati sljedeće podatke za navedene kvarove:

- kod kvara,
- datum i vrijeme početka kvara (ili umetanja kartice ako je u tom trenutku kvar bio u toku),
- datum i vrijeme završetka kvara (ili uklanjanja kartice ako je u tom trenutku kvar bio u toku),
- VRN i državu članicu registracije vozila u kojemu je došlo do kvara.

290) Kartica vozača mora moći sačuvati podatke za dvanaest posljednjih kvarova za svaku vrstu (tj. 24 kvara).

4.5.3.2.9 Podaci o aktivnosti vozača

291) Kartica vozača mora moći sačuvati, za svaki kalendarski dan upotrebe kartice ili za koji je vozač ručno unio podatke, sljedeće podatke:

- datum,
- dnevni brojač prisustva (uvećan za jedan za svaki od navedenih kalendarskih dana),
- ukupnu udaljenost koju je vozač prešao u tom danu,
- status vozača u 00:00,
- kad god je vozač promijenio aktivnost i/ili status vožnje i/ili je umetnuo ili izvadio svoju karticu:
- status vožnje (POSADA, JEDAN VOZAČ),
- otvor (VOZAČ, SUVOZAČ),
- status kartice (UMETNUTA, NIJE UMETNUTA),
- aktivnost (VOŽNJA, DOSTUPNOST, RAD, PAUZA/ODMOR).
- vrijeme promjene,

292) Memorija kartice vozača mora moći zadržati podatke o aktivnosti vozača najmanje 28 dana (pri čemu se prosječna aktivnost vozača definiše kao 93 promjene aktivnosti dnevno).

293) Podaci navedeni u zahtjevima 286, 289 i 291 arhiviraju se na način koji omogućava učitavanje aktivnosti redoslijedom njihova pojavljivanja, čak i u slučaju vremenskog preklapanja.

4.5.3.2.10 Podaci o upotrijebljenim vozilima

294) Kartica vozača mora moći sačuvati sljedeće podatke za svaki kalendarski dan upotrebe kartice i za svako period upotrebe dotičnog vozila tog dana (periodm upotrebe obuhvaćeni su svi uzastopni ciklusi umetanja i uklanjanja kartice u tom vozilu s gledišta kartice):

- datum i vrijeme prve upotrebe vozila (tj. prvog umetanja kartice u navedenom periodu upotrebe vozila ili 00:00 ako je u to vrijeme vozilo već u upotrebi),
- stanje brojača kilometara vozila u to vrijeme prve upotrebe,
- datum i vrijeme posljednje upotrebe vozila (tj. posljednjeg uklanjanja kartice u tom periodu upotrebe vozila ili 23:59 ako je kartica upotrijebljena u to vrijeme),
- stanje brojača kilometara vozila u to vrijeme zadnje upotrebe,
- VRN i državu članicu registracije vozila,
- VIN vozila.

295) Kartica vozača mora moći sačuvati najmanje 84 takva zapisa.

4.5.3.2.11 Mjesta i položaji početka i/ili završetka dnevnog radnog vremena

296) Kartica vozača mora moći sačuvati sljedeće podatke koji se odnose na mjesto početka i/ili završetka dnevnog radnog vremena koje unese vozač:

- datum i vrijeme unosa (ili datum/vrijeme koje se odnosi na ručni unos),
- vrstu unosa (početak ili kraj, stanje unosa),
- državu i regiju ulaska,
- stanje brojača kilometara vozila,
- položaj vozila,
- tačnost GNSS-a, datum i vrijeme kad je položaj utvrđen.

297) Memorija kartice vozača mora moći sačuvati najmanje 84 para takvih zapisa.

4.5.3.2.12 Podaci o upotrebi kartice

298) Kartica vozača mora moći sačuvati podatke koji se odnose na vozilo u kojem je započela upotreba kartice:

- datum i vrijeme početka upotrebe (tj. umetanje kartice) uz rezoluciju od jedne sekunde,
- VRN i državu članicu registracije.

4.5.3.2.13 Podaci o aktivnostima nadzora

299) Kartica vozača mora moći sačuvati sljedeće podatke koji se odnose na aktivnosti nadzora:

- datum i vrijeme nadzora,
- broj kontrolne kartice i državu članicu koja je karticu izdala,
- vrsta nadzora (prikaz i/ili ispis i/ili preuzimanje podataka s jedinice vozila i/ili preuzimanje podataka s kartice (vidjeti napomenu)),
- period preuzimanja podataka (u slučaju preuzimanja podataka),
- VRN i državu članicu registracije vozila u kojoj je izvršen nadzor.

Napomena: sigurnosnim zahtjevima podrazumijeva se da se preuzimanje podataka s kartice bilježi samo ako je izvršeno preko uređaja za evidentiranje podataka.

300) Kartica vozača mora moći spremiti jedan takav zapis.

4.5.3.2.14 Podaci o posebnim stanjima

301) Kartica vozača mora moći sačuvati sljedeće podatke koji se odnose na posebna stanja koja su unesena dok je kartica bila umetnuta (bez obzira u koji otvor):

- datum i vrijeme unosa,
- vrstu posebnog stanja.

302) Kartica vozača mora moći sačuvati najmanje 56 takvih zapisa.

4.5.3.2.15 Podaci o upotrijebljenoj jedinici u vozilu

303) Kartica vozača mora moći sačuvati sljedeće podatke koji se odnose na različite jedinice u vozilu u kojima je kartica upotrijebljena:

- datum i vrijeme početka perioda upotrebe jedinice u vozilu (tj. prvo umetanje kartice u jedinici u vozilu tokom perioda),
- proizvođača jedinice u vozilu,
- vrstu jedinice u vozilu,
- broj verzije softvera u jedinici u vozilu.

304) Kartica vozača mora moći sačuvati najmanje 84 takva zapisa.

4.5.3.2.16 Podaci o mjestima na kojima se dostižu tri sata akumulisane vožnje

305) Kartica vozača mora moći sačuvati sljedeće podatke koji se odnose na položaj vozila u kojem akumulisano vrijeme vožnje dostiže višekratnih tri sata:

- datum i vrijeme kad akumulisano vrijeme vožnje dostiže višekratnih tri sata,
- položaj vozila,
- tačnost GNSS-a, datum i vrijeme kad je položaj utvrđen,
- stanje brojača kilometara vozila.

306) Kartica vozača mora moći sačuvati najmanje 252 takva zapisa.

4.5.4 *Kartica radionice*

4.5.4.1 Tahografska aplikacija (pristup jedinicama u vozilu prve i druge generacije)

4.5.4.1.1 Identifikacija aplikacije

307) Kartica radionica mora moći sačuvati sljedeće programske identifikacijske podatke:

- identifikaciju tahografske aplikacije,
- identifikaciju vrste tahografske kartice.

4.5.4.1.2 Ključevi i certifikati

308) Kartica radionice mora moći sačuvati niz kriptografskih ključeva i certifikata, kako je određeno u Dodatku 11. dijelu A.

309) Kartica radionice mora moći sačuvati lični identifikacijski broj (PIN oznaku).

4.5.4.1.3 Identifikacija kartice

310) Kartica radionice mora moći sačuvati sljedeće identifikacijske podatke kartice:

- broj kartice,
- državu članicu izdavanja, naziv tijela koje izdaje karticu, datum izdavanja,
- datum početka i isteka važenja kartice.

4.5.4.1.4 Identifikacija vlasnika kartice

311) Kartica radionice mora moći sačuvati sljedeće identifikacijske podatke vlasnika kartice:

- naziv radionice,
- adresu radionice,
- prezime vlasnika,
- ime(na) vlasnika,
- željeni jezik.

4.5.4.1.5 Preuzimanje podataka s kartice

312) Kartica radionice mora moći sačuvati podatke o preuzimanju podataka s kartice na isti način kao i kartica vozača.

4.5.4.1.6 Podaci o kalibraciji i prilagođavanju vremena

313) Kartica radionice mora moći sačuvati zapise o kalibraciji i/ili prilagođavanjema vremena izvršenima dok je kartica bila umetnuta u uređaj za evidentiranje podataka.

314) Svaki zapis o kalibraciji mora sadržiti sljedeće podatke:

- svrhu kalibracije (aktiviranje, prva ugradnja, ugradnja, periodični pregled),
- identifikaciju vozila,
- parametre koji se ažuriraju ili potvrđuju (w, k, l, dimenzije guma, podešavanje uređaja za ograničavanje brzine, stanje brojača kilometara (novu i staru vrijednost), datum i vrijeme (novu i staru vrijednosti)),
- identifikaciju uređaja za evidentiranje podataka (kataloški broj jedinice u vozilu, serijski broj jedinice u vozilu, serijski broj senzora kretanja).

315) Kartica radionice mora moći sačuvati barem 88 takvih zapisa.

316) Kartica radionice mora sadržiti brojač za označivanje ukupnog broja kalibracija izvršenih s tom karticom.

317) Kartica radionice mora sadržiti brojač za označivanje broja kalibracija izvršenih nakon posljednjeg preuzimanja podataka s kartice.

4.5.4.1.7 Podaci o događajima i kvarovima

318) Kartica radionice mora moći sačuvati podatke o događajima i kvarovima na isti način kao i kartica vozača.

319) Kartica radionice mora moći sačuvati podatke za tri posljednja događaja svake vrste (tj. 18 događaja) i šest posljednjih kvarova svake vrste (tj. 12 kvarova).

4.5.4.1.8 Podaci o aktivnosti vozača

320) Kartica radionice mora moći sačuvati podatke o aktivnostima vozača na isti način kao i kartica vozača.

321) Kartica radionice mora moći čuvati podatke o aktivnostima vozača barem tokom jednog dana prosječne aktivnosti vozača.

4.5.4.1.9 Podaci o upotrijebljenim vozilima

322) Kartica radionice mora moći sačuvati podatke o upotrijebljenim vozilima na isti način kao i kartica vozača.

323) Kartica radionice mora moći sačuvati barem 4 takva zapisa.

4.5.4.1.10 Podaci o početku i/ili završetku dnevnog radnog vremena

324) Kartica radionice mora moći sačuvati podatke o početku i/ili završetku dnevnog radnog vremena na isti način kao i kartica vozača.

325) Kartica radionice mora moći čuvati najmanje tri para takvih zapisa.

4.5.4.1.11 Podaci o upotrebi kartice

326) Kartica radionice mora moći sačuvati podatke o upotrebi kartice na isti način kao i kartica vozača.

4.5.4.1.12 Podaci o aktivnostima nadzora

327) Kartica radionice mora moći sačuvati podatke o aktivnostima nadzora na isti način kao i kartica vozača.

4.5.4.1.13 Podaci o posebnim stanjima

328) Kartica radionice mora moći sačuvati podatke o posebnim uslovima na isti način kao i kartica vozača.

329) Kartica radionice mora moći sačuvati barem 2 takva zapisa.

4.5.4.2 Tahografska aplikacija druge generacije (nije dostupno jedinici u vozilu prve generacije)

4.5.4.2.1 Identifikacija aplikacije

330) Kartica radionica mora moći sačuvati sljedeće programske identifikacijske podatke:

- identifikaciju tahografske aplikacije,
- identifikaciju vrste tahografske kartice.

4.5.4.2.2 Ključevi i certifikati

331) Kartica radionice mora moći sačuvati niz kriptografskih ključeva i certifikata, kako je određeno u Dodatku 11. dijelu B.

332) Kartica radionice mora moći sačuvati lični identifikacijski broj (PIN oznaku).

4.5.4.2.3 Identifikacija kartice

333) Kartica radionice mora moći sačuvati sljedeće identifikacijske podatke kartice:

- broj kartice,
- državu članicu izdavanja, naziv tijela koje izdaje karticu, datum izdavanja,
- datum početka i isteka važenja kartice.

4.5.4.2.4 Identifikacija vlasnika kartice

334) Kartica radionice mora moći sačuvati sljedeće identifikacijske podatke vlasnika kartice:

- naziv radionice,
- adresu radionice,
- prezime vlasnika,
- ime(na) vlasnika,
- željeni jezik.

4.5.4.2.5 Preuzimanje podataka s kartice

335) Kartica radionice mora moći sačuvati podatke o preuzimanju podataka s kartice na isti način kao i kartica vozača.

4.5.4.2.6 Podaci o kalibraciji i prilagođavanju vremena

336) Kartica radionice mora moći sačuvati zapise o kalibraciji i/ili prilagođavanjema vremena izvršenima dok je kartica bila umetnuta u uređaj za evidentiranje podataka.

337) Svaki zapis o kalibraciji mora sadržiti sljedeće podatke:

- svrhu kalibracije (aktiviranje, prva ugradnja, ugradnja, periodični pregled),
- identifikaciju vozila,
- parametre koji se ažuriraju ili potvrđuju (w, k, l, dimenzije guma, postavke uređaja za ograničavanje brzine, stanje brojača kilometara (nove i stare vrijednosti), datum i vrijeme (nove i stare vrijednosti)),
- identifikaciju uređaja za evidentiranje podataka (kataloški broj jedinice u vozilu, serijski broj jedinice u vozilu, serijski broj senzora kretanja, serijski broj uređaja za komunikaciju na daljinu i serijski broj spoljnog uređaja GNSS-a, ako je primjenjivo),
- tip i identifikator svih postavljenih plombi,
- sposobnost jedinice u vozilu da upotrebljava tahografske kartice prve generacije (omogućeno ili ne).

338) Kartica radionice mora moći sačuvati barem 88 takvih zapisa.

339) Kartica radionice mora sadržiti brojač za označivanje ukupnog broja kalibracija izvršenih s tom karticom.

340) Kartica radionice mora sadržiti brojač za označivanje broja kalibracija izvršenih nakon posljednjeg preuzimanja podataka s kartice.

4.5.4.2.7 Podaci o događajima i kvarovima

341) Kartica radionice mora moći sačuvati podatke o događajima i kvarovima na isti način kao i kartica vozača.

342) Kartica radionice mora moći sačuvati podatke za tri posljednja događaja svake vrste (tj. 33 događaja) i šest posljednjih kvarova svake vrste (tj. 12 kvarova).

4.5.4.2.8 Podaci o aktivnosti vozača

343) Kartica radionice mora moći sačuvati podatke o aktivnostima vozača na isti način kao i kartica vozača.

344) Kartica radionice mora moći čuvati podatke o aktivnostima vozača barem tokom jednog dana prosječne aktivnosti vozača.

4.5.4.2.9 Podaci o upotrijebljenim vozilima

345) Kartica radionice mora moći sačuvati podatke o upotrijebljenim vozilima na isti način kao i kartica vozača.

346) Kartica radionice mora moći sačuvati barem 4 takva zapisa.

4.5.4.2.10 Podaci o početku i/ili završetku dnevnog radnog vremena

347) Kartica radionice mora moći sačuvati podatke o početku i/ili završetku dnevnog radnog vremena na isti način kao i kartica vozača.

348) Kartica radionice mora moći čuvati najmanje tri para takvih zapisa.

4.5.4.2.11 Podaci o upotrebi kartice

349) Kartica radionice mora moći sačuvati podatke o upotrebi kartice na isti način kao i kartica vozača.

4.5.4.2.12 Podaci o aktivnostima nadzora

350) Kartica radionice mora moći sačuvati podatke o aktivnostima nadzora na isti način kao i kartica vozača.

4.5.4.2.13 Podaci o upotrijebljenoj jedinici u vozilu

351) Kartica radionice mora moći sačuvati sljedeće podatke koji se odnose na različite jedinice u vozilu u kojima je kartica upotrijebljena:

- datum i vrijeme početka perioda upotrebe jedinice u vozilu (tj. prvo umetanje kartice u jedinicu u vozilu tokom perioda),
- proizvođača jedinice u vozilu,

- vrstu jedinice u vozilu,
- broj verzije softvera u jedinici u vozilu.

352) Kartica radionice mora moći sačuvati barem 4 takva zapisa.

4.5.4.2.14 Podaci o mjestima na kojima se dostižu tri sata akumulisane vožnje

353) Kartica radionice mora moći sačuvati sljedeće podatke koji se odnose na položaj vozila u kojem akumulisano vrijeme vožnje dostiže višekratnih tri sata:

- datum i vrijeme kad akumulisano vrijeme vožnje dostiže višekratnih tri sata,
- položaj vozila,
- tačnost GNSS-a, datum i vrijeme kad je položaj utvrđen,
- stanje brojača kilometara vozila.

354) Kartica radionice mora moći sačuvati barem 18 takvih zapisa

4.5.4.2.15 Podaci o posebnim stanjima

355) Kartica radionice mora moći sačuvati podatke o posebnim uslovima na isti način kao i kartica vozača.

356) Kartica radionice mora moći sačuvati barem 2 takva zapisa.

4.5.5 *Kontrolna kartica*

4.5.5.1 Tahografska aplikacija (pristup jedinicama u vozilu prve i druge generacije)

4.5.5.1.1 Identifikacija aplikacije

357) Kontrolna kartica mora moći sačuvati sljedeće programske identifikacijske podatke:

- identifikaciju tahografske aplikacije,
- identifikaciju vrste tahografske kartice.

4.5.5.1.2 Ključevi i certifikati

358) Kontrolna kartica mora moći sačuvati niz kriptografskih ključeva i certifikata, kako je određeno u Dodatku 11. dijelu A.

4.5.5.1.3 Identifikacija kartice

359) Kontrolna kartica mora moći sačuvati sljedeće identifikacijske podatke kartice:

- broj kartice,
- državu članicu izdavanja, naziv tijela koje izdaje karticu, datum izdavanja,
- datum početka i isteka važenja kartice (ako postoji).

4.5.5.1.4 Identifikacija vlasnika kartice

360) Kontrolna kartica mora moći sačuvati sljedeće identifikacijske podatke vlasnika kartice:

- naziv nadzornog tijela,
- adresu nadzornog tijela,
- prezime vlasnika,
- ime(na) vlasnika,
- željeni jezik.

4.5.5.1.5 Podaci o aktivnostima nadzora

361) Kontrolna kartica mora moći sačuvati sljedeće podatke o aktivnostima nadzora:

- datum i vrijeme nadzora,
- vrstu nadzora (prikaz i/ili ispis i/ili preuzimanje podataka s jedinice u vozilu i/ili preuzimanje podataka s kartice i/ili provjera kalibracije na putu).
- period preuzimanja podataka (ako postoji),
- VRN i tijelo države članice koje je registrovalo kontrolisano vozilo.
- broj kartice i državu članicu koja je izdala kontroliranu vozačku karticu.

362) Kartica mora moći spremiti najmanje 230 takvih zapisa.

4.5.5.2 Tahografska aplikacija druge generacije (nije dostupno jedinici u vozilu prve generacije)

4.5.5.2.1 Identifikacija aplikacije

363) Kontrolna kartica mora moći sačuvati sljedeće programske identifikacijske podatke:

- identifikaciju tahografske aplikacije,
- identifikaciju vrste tahografske kartice.

4.5.5.2.2 Ključevi i certifikati

364) Kontrolna kartica mora moći sačuvati niz kriptografskih ključeva i certifikata, kako je određeno u Dodatku 11. dijelu B.

4.5.5.2.3 Identifikacija kartice

365) Kontrolna kartica mora moći sačuvati sljedeće identifikacijske podatke kartice:

- broj kartice,
- državu članicu izdavanja, naziv tijela koje izdaje karticu, datum izdavanja,
- datum početka i isteka važenja kartice (ako postoji).

4.5.5.2.4 Identifikacija vlasnika kartice

366) Kontrolna kartica mora moći sačuvati sljedeće identifikacijske podatke vlasnika kartice:

- naziv nadzornog tijela,
- adresu nadzornog tijela,
- prezime vlasnika,
- ime(na) vlasnika,
- željeni jezik.

4.5.5.2.5 Podaci o aktivnostima nadzora

367) Kontrolna kartica mora moći sačuvati sljedeće podatke o aktivnostima nadzora:

- datum i vrijeme nadzora,
- vrsta nadzora (prikaz i/ili ispis i/ili preuzimanje podataka s jedinice u vozilu i/ili preuzimanje podataka s kartice i/ili provjera kalibracije na putu).
- period preuzimanja podataka (ako postoji),
- VRN i tijelo države članice koje je registrovalo kontrolirano vozilo,
- broj kartice i državu članicu koja je izdala kontroliranu vozačku karticu.

368) Kartica mora moći spremiti najmanje 230 takvih zapisa.

4.5.6 *Kartica preduzeća*

4.5.6.1 Tahografska aplikacija (pristup jedinicama u vozilu prve i druge generacije)

4.5.6.1.1 Identifikacija aplikacije

369) Kartica preduzeća mora moći sačuvati sljedeće programske identifikacijske podatke:

- identifikaciju tahografske aplikacije,
- identifikaciju vrste tahografske kartice.

4.5.6.1.2 Ključevi i certifikati

370) Kartica preduzeća mora moći sačuvati niz kriptografskih ključeva i certifikata, kako je određeno u Dodatku 11. dijelu A.

4.5.6.1.3 Identifikacija kartice

371) Kartica preduzeća mora moći sačuvati sljedeće identifikacijske podatke kartice:

- broj kartice,
- državu članicu izdavanja, naziv tijela koje izdaje karticu, datum izdavanja,
- datum početka i isteka važenja kartice (ako postoji).

4.5.6.1.4 Identifikacija vlasnika kartice

372) Kartica preduzeća mora moći sačuvati sljedeće identifikacijske podatke vlasnika kartice:

- naziv preduzeća,
- adresu preduzeća.

4.5.6.1.5 Podaci o aktivnostima preduzeća

373) Kartica preduzeća mora moći sačuvati sljedeće podatke o aktivnostima preduzeća:

- datum i vrijeme aktivnosti,
- vrstu aktivnosti (zaključavanje ili otključavanje blokade jedinice u vozilu, preuzimanje podataka s jedinice u vozilu i/ili s kartice),
- period preuzimanja podataka (ako postoji),
- VRN i tijelo koje je registrovalo vozilo u državi članici,
- broj kartice i državu članicu izdavanja kartice (u slučaju preuzimanja podataka s kartice).

374) Kartica preduzeća mora moći sačuvati barem 230 takvih zapisa.

4.5.6.2 Tahografska aplikacija druge generacije (nije dostupno jedinici u vozilu prve generacije)

4.5.6.2.1 Identifikacija aplikacije

375) Kartica preduzeća mora moći sačuvati sljedeće programske identifikacijske podatke:

- identifikaciju tahografske aplikacije,
- identifikaciju vrste tahografske kartice.

4.5.6.2.2 Ključevi i certifikati

376) Kartica preduzeća mora moći sačuvati niz kriptografskih ključeva i certifikata, kako je određeno u Dodatku 11. dijelu B.

4.5.6.2.3 Identifikacija kartice

377) Kartica preduzeća mora moći sačuvati sljedeće identifikacijske podatke kartice:

- broj kartice,
- državu članicu izdavanja, naziv tijela koje izdaje karticu, datum izdavanja,
- datum početka i isteka važenja kartice (ako postoji).

4.5.6.2.4 Identifikacija vlasnika kartice

378) Kartica preduzeća mora moći sačuvati sljedeće identifikacijske podatke vlasnika kartice:

- naziv preduzeća,
- adresu preduzeća.

4.5.6.2.5 Podaci o aktivnostima preduzeća

379) Kartica preduzeća mora moći sačuvati sljedeće podatke o aktivnostima preduzeća:

- datum i vrijeme aktivnosti,
- vrstu aktivnosti (zaključavanje ili otključavanje blokade jedinice u vozilu, preuzimanje podataka s jedinice u vozilu i/ili s kartice),
- period preuzimanja podataka (ako postoji),
- VRN i tijelo koje je registrovalo vozilo u državi članici,
- broj kartice i državu članicu izdavanja kartice (u slučaju preuzimanja podataka s kartice).

380) Kartica preduzeća mora moći sačuvati barem 230 takvih zapisa.

5 UGRADNJA UREĐAJA ZA EVIDENTIRANJE PODATAKA

5.1 Ugradnja

381) Novi se uređaj za evidentiranje podataka isporučuje neaktiviran instalaterima ili proizvođačima vozila sa svim parametrima za kalibraciju navedenima u poglavlju 3.21. podešenima na odgovarajuće i važeće osnovne vrijednosti. Ako neka određena vrijednost nije podešena, slovni parametri zamjenjuju se nizom znakova „?”, a numerički parametri postavljaju se na „0”. Dostava dijelova uređaja za evidentiranje podataka koji se odnose na sigurnost može se ograničiti ako se tako zahtijeva za vrijeme sigurnosnog certificiranja.

382) Prije aktivacije uređaj za evidentiranje podataka mora imati pristup funkciji kalibracije, čak i kada nije u kalibracijskom načinu rada.

383) Prije aktivacije uređaj za evidentiranje podataka ne smije zapisivati niti sačuvati podatke iz točaka 3.12.3., 3.12.9. i 3.12.12. do uključujući 3.12.15.

384) Tokom ugradnje proizvođači vozila moraju unaprijed podesiti sve poznate parametre.

385) Proizvođači vozila ili instalateri aktiviraju ugrađeni uređaj za evidentiranje podataka najkasnije prije upotrebe vozila u području primjene.

386) Aktiviranje uređaja za evidentiranje podataka vrši se automatski prvim umetanjem važeće kartice radionice u bilo koji uređaj kartičnog sučelja.

387) Posebne operacije uparivanja senzora kretanja i jedinice u vozilu, ako ih ima, vrše se automatski prije ili tokom aktiviranja.

388) Slično se posebne operacije povezivanja senzora kretanja i jedinice u vozilu, ako ih ima, vrše automatski prije ili tokom aktiviranja.

389) Nakon aktiviranja uređaj za evidentiranje podataka mora u potpunosti izvršavati funkcije i prava pristupa podacima.

390) Nakon aktiviranja uređaj za evidentiranje podataka uređaju za komunikaciju na daljinu prenosi sigurne podatke potrebne za ciljane provjere na daljinu.

391) Funkcije bilježenja i arhiviranje u uređaju za evidentiranje podataka postižu punu radnu sposobnost nakon njegova aktiviranja.

392) Nakon ugradnje slijedi kalibracija. Prva kalibracija ne mora nužno uključivati unos registracijskog broja vozila (VRN) ako ga ovlaštena radionica koja treba obaviti tu kalibraciju ne zna. Samo u tim okolnostima vlasnik vozila samo jednom može unijeti VRN koristeći se svojom karticom preduzeća prije upotrebe vozila u području primjene (npr. koristeći se naredbama putem odgovarajuće strukture menija sučelja čovjek-stroj jedinice u vozilu). Svako ažuriranje ili potvrda tog unosa moguća je samo karticom radionice.

393) Za ugradnju spoljnog uređaja GNSS-a potrebno je povezivanje s spoljnom jedinicom u vozilu i naknadna provjera podataka GNSS-a o položaju.

394) Uređaj za evidentiranje podataka mora biti smješten u vozilu tako da omogući vozaču pristup potrebnim funkcijama iz njegova sjedala.

5.2 Tipska naljepnica

395) Nakon provjere uređaja za evidentiranje podataka pri ugradnji na njega se pričvršćuje jasno vidljiva i lako dostupna tipska naljepnica, koja je trajno ugravirana ili tiskana. Ako to nije moguće, naljepnica se pričvršćuje na stup „B" vozila tako da je jasno vidljiva. Za vozila koja nemaju stup „B" tipska se naljepnica pričvršćuje na okvir vrata na vozačevoj strani vozila i jasno je vidljiva u svim slučajevima.

Poslije svakog pregleda kod ovlaštenog instalatera ili u ovlaštenoj radionici na mjesto prethodne postavlja se nova naljepnica.

396) Na naljepnicu moraju biti navedeni najmanje sljedeći podaci:

- naziv, adresa ili trgovački naziv ovlaštenog instalatera ili radionice,
- karakteristični koeficijent vozila u obliku ‚w = … imp/km',
- konstanta uređaja za bilježenje podataka u obliku ‚k = … imp/km',
- djelatni opseg guma tačka u obliku ‚l = … mm',
- veličina guma,
- datum mjerenja karakterističnog koeficijenta vozila i efikasnog obima guma tačka,
- identifikacijska oznaka vozila,
- prisutnost (ili neprisutnost) vanjskog uređaja GNSS-a,
- serijski broj vanjskog uređaja GNSS-a, ako je primjenjivo,
- serijski broj uređaja za komunikaciju na daljinu, ako postoji,
- serijski broj svih postavljenih plombi,
- dio vozila na koji se ugrađuje adapter, ako postoji,
- dio vozila na koji se ugrađuje senzor kretanja, ako nije priključen na mjenjač ili ako se ne upotrebljava adapter,
- opis boje kabla između adaptera i onog dijela vozila iz kojeg prima ulazne impulse,
- serijski broj ugrađenog senzora kretanja adaptera.

397) Samo za vozila M1 i N1 koja su opremljena adapterom u skladu s Uredbom Komisije (EZ) br. 68/2009 ([16]), kako je zadnje izmijenjena, a kad nije moguće uključiti sve potrebne informacije

opisane u zahtjevu 396, može se upotrijebiti druga, dodatna naljepnica. U takvim slučajevima dodatna naljepnica sadrži najmanje zadnje četiri alineje opisane u zahtjevu 396.

Ako se upotrebljava druga, dodatna naljepnica, pričvršćuje se pored ili uz prvu primarnu naljepnicu, opisanu u zahtjevu 396, i ima ist nivo zaštite. Nadalje, na dodatnoj naljepnici je naveden i naziv, adresa ili trgovački naziv ovlaštenog instalatera ili radionice koja je izvršila ugradnju te datum ugradnje.

5.3 Plombiranje

398) Sljedeći dijelovi moraju se zaštititi plombom:

- svaki spoj čije bi razdvajanje uzrokovalo izmjene ili gubitak podataka koje ne bi bilo moguće otkriti (to se može, na primjer, primijeniti na postavljanje senzora kretanja na mjenjač, adapter za vozila M1/N1, vezu s spoljnim GNSS-om ili jedinicu u vozilu);
- tipska naljepnica, osim ako je pričvršćena na takav način da ju je nemoguće ukloniti bez uništavanja oznaka na njoj.

398a) Gore spomenute plombe certifikuju se u skladu sa normom EN 16882:2016.

399) Prethodno navedene plombe mogu se ukloniti:

- u vanrednom slučaju,
- pri ugradnji, podešavanju ili popravku uređaja za ograničenje brzine ili nekog drugog uređaja koji pridonosi sigurnosti na putu, pod uslovom da uređaj za evidentiranje podataka nastavi raditi pouzdano i ispravno te da ovlašćeni instalater ili radionica ponovno postavi plombe (u skladu s poglavljem 6.) odmah nakon postavljanja uređaja za ograničenje brzine ili nekog drugog uređaja koji pridonosi sigurnosti na cestama ili u roku od sedam dana u drugim slučajevima.

400) Svaki put kad se te plombe skidaju, sastavlja se pisana izjava u kojoj se navode razlozi zbog kojih je to učinjeno i koja mora biti dostupna nadležnom tijelu.

401) Plombe moraju imati identifikacijski broj koji im je odredio proizvođač.

Taj broj mora biti jedinstven i mora se razlikovati od svih drugih brojeva plombi koje su odredili drugi proizvođači plombi.

Taj jedinstveni identifikacijski broj definira se na sljedeći način: MMNNNNNNNN oznakom koja se ne može ukloniti, pri čemu je MM jedinstvena identifikacija proizvođača (upis baze podataka vodit će EK), a NNNNNNNN alfanumerički broj plombe koji je jedinstven u domeni proizvođača.

402) Na plombama mora postojati slobodan prostor na kojem ovlašćeni instalateri, radionice ili proizvođači vozila mogu dodati posebnu oznaku u skladu sa ovim pravilnikom.

Ta oznaka ne smije prekriti identifikacijski broj plombe.

403) Proizvođači plombi moraju se upisati u posebnu bazu podataka kad certifikuju model plombe u skladu s normom EN 16882:2016 i objaviti svoje identifikacijske brojeve plombi u okviru postupka koji će utvrditi Evropski komisija.

404) ovlašćene radionice i proizvođači vozila smiju upotrebljavati plombe certifikovane u skladu s normom EN 16882:2016 samo onih proizvođača plombi koji su navedeni u prethodno navedenoj bazi podataka.

405) Proizvođači plombi i njihovi distributeri vode zapise o punoj sljedivosti prodanih plombi koje će se upotrebljavati u okviru ovog pravilnika te ih moraju biti spremni predati nadležnim nacionalnim tijelima kad god je potrebno.

406) Jedinstveni identifikacijski brojevi plombi moraju biti vidljivi na tipskoj pločici.

6 PROVJERE, PREGLEDI I POPRAVKE

Zahtjevi u pogledu okolnosti u kojima se plombe mogu ukloniti u utvrđeni su u poglavlju 5.3. ovog Priloga.

6.1 Ovlaštenje instalatera, radionica i proizvođača vozila

Države članice ovlašćuju, redovito nadziru i potvrđuju tijela koja obavljaju:

- ugradnju,
- provjere,
- preglede,
- popravke.

Osim ako ne postoji važećio opravdanje, kartice radionice izdaju se samo instalaterima i/ili radionicama koji su ovlašćeni za aktiviranje i/ili kalibraciju uređaja za evidentiranje podataka u skladu s ovim Prilogom i:

- koji nemaju pravo na karticu preduzeća
- i čija druga poslovna djelatnost ne dovodi u pitanje sveukupnu sigurnost sistema kako se zahtjeva u Dodatku 10.

6.2 Provjera novih ili popravljenih uređaja

407) Svaki pojedini uređaj, nov ili popravljen, provjerava se kalibracijom u pogledu ispravnog rada te tačnosti očitavanja i zapisa, u granicama utvrđenima u poglavljima 3.2.1., 3.2.2., 3.2.3. i 3.3.

6.3 Pregled pri ugradnji

408) Pri postavljanju u vozilo, čitava instalacija (uključujući i uređaj za bilježenje podataka) mora udovoljiti odredbama koje se odnose na najveća dopuštena odstepena utvrđena u poglavljima 3.2.1., 3.2.2., 3.2.3. i 3.3. Čitava instalacija zaštićuje se plombom u skladu s poglavljem 5.3. i uključuje kalibraciju.

6.4 Periodični pregledi

409) Periodični pregledi uređaja za evidentiranje podataka u vozilu obavljaju se nakon svakog popravka uređaja ili nakon svake izmjene karakterističnog koeficijenta vozila ili efikasnog obima guma ili nakon pogreške vremena po UTC-u u uređaju veće od 20 minuta, ili pri promjeni registracijske oznake vozila, te barem jednom svake dvije godine (24 mjeseca) nakon posljednjeg pregleda.

410) Ti pregledi obuhvaćaju sljedeće provjere:

- da uređaj za evidentiranje podataka radi ispravno, uključujući funkciju arhiviranje podataka na tahografske kartice i komunikaciju s čitačima komunikacije na daljinu,
- da je osigurana shodnost s odredbama poglavlja 3.2.1. i 3.2.2. o najvećem odstupanju pri ugradnji,
- da je osigurana shodnost s odredbama poglavlja 3.2.3. i 3.3.,
- ima li uređaj za evidentiranje podataka homologacijsku oznaku,
- da su ugrađene tipska pločica, kako je definisana u zahtjevu 396, i opisna pločica, kako je definisana u zahtjevu 225,
- kolika je veličina gume i stvarni opseg guma,
- da uređaju nisu dodani uređaji za manipulaciju,
- da su plombe ispravno postavljene, u dobrom stanju, da su njihovi identifikacijski brojevi važećii (ovlašćeni proizvođač plombi u bazi podataka EK-a) i da njihovi identifikacijski brojevi odgovaraju oznakama tipskih pločica (vidjeti zahtjev 401).

411) Ako se ustanovi da se nakon posljednjeg pregleda dogodio jedan od događaja navedenih u poglavlju 3.9. (Otkrivanje događaja i/ili kvarova) i proizvođači tahografa i/ili nacionalna tijela smatraju da on potencijalno dovodi u opasnost sigurnost uređaja, radionica tada:

a. upoređuje identifikacijske podatke senzora kretanja, koji je priključen na mjenjač, s podacima povezanog senzora kretanja registriranog u jedinici u vozilu;

b. provjerava podudaraju li se informacije zabilježene na tipskoj pločici s informacijama koje sadrži zapis jedinice u vozilu;

c. provjerava podudara li se serijski broj i homologacijski broj senzora kretanja, ako je ispisan na tijelu senzora kretanja, s informacijama koje sadrži zapis jedinice u vozilu;

d. upoređuje identifikacijske podatke označene na opisnoj pločici spoljnog uređaja GNSS-a, ako postoje, s podacima sačuvanima u memoriji podataka jedinice u vozilu.

412) Radionice u svojim izvješćima o pregledu zapisuju sva saznanja o slomljenim plombama ili uređajima za manipulaciju. Radionice ta izvješća čuvaju najmanje dvije godine i stavljaju ih na raspolaganje na zahtjev nadležnih tijela.

413) Ti pregledi moraju uključivati kalibraciju i preventivnu zamjenu plombi za čije su postavljanje odgovorne radionice.

6.5 Mjerenje grešaka

414) Mjerenje grešaka kod ugradnje i tokom upotrebe obavlja se pod sljedećim uslovima koji se smatraju standardnim uslovima ispitivanja:

- nenatovareno vozilo u stanju spremnom za vožnju,
- pritisak u gumama prema uputama proizvođača,
- istrošenost guma u okviru zakonski dopuštenih granica,
- kretanje vozila:
- vozilo se mora kretati snagom vlastitog motora, pravolinijski na ravnoj površini brzinom od 50 ± 5 km/h. Mjerna udaljenost iznosi najmanje 1 000 m.
- Ako im je tačnost uporediva, za provjeru se mogu koristiti i alternativne metode kao što je ispitivanje na odgovarajućem ispitnom stolu.

6.6 Popravke

415) Radionice moraju moći preuzeti podatke s uređaja za evidentiranje podataka kako bi ih mogli dostaviti odgovarajućem prevozniku.

416) Ovlaštene radionice izdaju prevoznicima potvrdu o nemogućnosti preuzimanja podataka kada neispravnost uređaja za evidentiranje podataka sprečava preuzimanje prethodno zabeleženih podataka, čak i nakon popravka u radionici. Radionice čuvaju presliku svake izdate potvrde u trajanju od najmanje dvije godine.

7 IZDAVANJE KARTICA

Postupci izdavanja kartica ustrojeni u državama članicama moraju biti u skladu sa sljedećim:

417) broj kartice prvog izdavanja tahografske kartice tražiocu mora imati redni indeks (ako je primjereno) i indeks zamjene te indeks ponovnog izdavanja postavljen na „0".

418) Brojevi kartica svih nepersonalizovanih tahografskih kartica koje se izdaju jednom nadzornom tijelu ili jednoj radionici ili jednom prevozniku moraju imati prvih 13 istih cifara, te različit redni indeks.

419) Tahografska kartica koja se izdaje kao zamjena za postojeću tahografsku karticu mora imati isti broj kartice kao i kartica koju zamjenjuje, osim indeksa zamjene koji se uvećava za „1" (redoslijedom 0, …, 9, A, …, Z).

420) Tahografska kartica koja se izdaje kao zamjena za postojeću tahografsku karticu mora imati isti datum isteka važenja kartice kao i kartica koju zamjenjuje.

421) Tahografska kartica koja se izdaje zbog obnavljanja postojeće tahografske kartice mora imati isti broj kartice kao i kartica koja se obnavlja, osim indeksa zamjene koji se ponovno vraća na nulu i indeksa ponovnog izdavanja koji se uvećava za „1" (redoslijedom 0, …, 9, A, …, Z).

422) Zamjena postojeće kartice tahografa radi izmjene administrativnih podataka slijedi pravila obnavljanja ako se obavlja unutar iste države članice odnosno pravila prvog izdavanja ako istu obavlja druga država članica.

423) „Prezime vlasnika kartice" za nepersonalizirane kartice radionice ili kontrolne kartice popunjava se nazivom radionice ili nadzornog tijela ili imenom instalatera ili službenika za kontrolu ako države članice tako odluče.

424) Države članice elektronski razmjenjuju podatke kako bi osigurale jedinstvenost tahografske kartice vozača koju izdaju u skladu sa ovim pravilnikom.

8 HOMOLOGACIJA UREĐAJA ZA EVIDENTIRANJE PODATAKA I TAHOGRAFSKIH KARTICA

8.1 Opšti zahtjevi

Za potrebe ovog poglavlja, riječi ‚uređaj za evidentiranje podataka' znače ‚uređaj za evidentiranje podataka ili njegovi sastavni dijelovi'. Homologacija nije potrebna za kablove koji povezuju senzor kretanja s jedinicom u vozilu, vanjski uređaj GNSS-a s jedinicom u vozilu ili vanjski uređaj za komunikaciju na daljinu s jedinicom u vozilu. Papir koji se upotrebljava u uređaju za evidentiranje podataka smatra se sastavnim dijelom uređaja za evidentiranje podataka.

Bilo koji proizvođač može zatražiti homologaciju sastavnih dijelova uređaja za evidentiranje podataka s bilo kojim drugim sastavnim dijelovima uređaja za evidentiranje podataka pod uslovom da je svaki sastavni dio u skladu sa zahtjevima iz ovog Priloga. U suprotnom, proizvođači mogu zatražiti i homologaciju uređaja za evidentiranje podataka.

Kao što je opisano u definiciji 10) u članu 2. ove Uredbe, jedinice u vozilu imaju više varijanti sklopova sastavnih dijelova. Bez obzira na sklop sastavnih dijelova jedinice u vozilu, vanjska antena i (ako je primjenjivo) antenski razdjelnik povezan s prijamnikom GNSS-a ili uređajem za komunikaciju na daljinu nisu dio homologacije jedinice u vozilu.

Bez obzira na to, proizvođači koji su dobili homologaciju za uređaj za evidentiranje podataka moraju održavati javno dostupan popis kompatibilnih antena i razdjelnika sa svakom homologovanom jedinicom u vozilu, vanjski uređaj GNSS-a i vanjski uređaj za komunikaciju na daljinu.

425) Uređaj za evidentiranje podataka podnosi se za homologaciju zajedno sa svim integrisanim dodatnim uređajima.

426) Homologacija uređaja za evidentiranje podataka i tahografskih kartica mora uključivati sigurnosna ispitivanja, ispitivanja funkcionalnosti i interoperabilnosti. Pozitivni rezultati svih ovih ispitivanja utvrđuju se u odgovarajućoj potvrdi.

427) Tijela država članica zadužena za homologaciju neće izdati certifikat o homologaciji ako nemaju:

- certifikat o sigurnosti (ako je to zatraženo u ovom Prilogu),
- certifikat o ispravnosti
- i certifikat o interoperabilnosti (ako je to zatraženo u ovom Prilogu)

za uređaj za bilježenje podataka ili tahografsku karticu koja je predmet zahtjeva za homologaciju.";

428) O svakoj izmjeni u softveru ili hardveru uređaja ili u naravi materijala upotrijebljenih u njegovoj proizvodnji mora se, prije nego što se primijeni, obavještenjeiti nadležno tijelo koje je odobrilo homologaciju za uređaj. To tijelo proizvođaču potvrđuje produženje homologacije ili može zahtijevati ažuriranje ili potvrdu relevantnih certifikata o ispravnosti, sigurnosti i/ili o interoperabilnosti.

429) Postupke softverske nadogradnje uređaja za evidentiranje podataka na licu mjesta odobrava tijelo koje je odobrilo homologaciju uređaja za evidentiranje podataka. Nadogradnja softvera ne smije mijenjati ili brisati niti jedan podatak o aktivnosti vozača sačuvan u uređaju za evidentiranje podataka. Softver se može nadograđivati samo pod odgovornosti proizvođača uređaja.

430) Homologacija izmjena softvera koje se odnose na nadogradnju prethodno homologovanog uređaja za evidentiranje podataka ne može se odbiti ako se te izmjene primjenjuju samo na funkcije koje nisu određene u Prilogu. Nadogradnja softvera uređaja za evidentiranje podataka može isključiti uvođenje novih skupova znakova ako to nije tehnički izvedivo.

8.2 Certifikat o sigurnosti

431) Certifikat o sigurnosti izdaje se u skladu s odredbama Dodatka 10. ovom Prilogu. Sastavni dijelovi uređaja za evidentiranje podataka koje je potrebno certificirati su jedinica u vozilu, senzor kretanja, spoljni uređaj GNSS-a i tahografske kartice.

432) U iznimnim okolnostima, kad tijela za sigurnosno certifikovanje odbijaju certificirati novu opremu radi zastarjelosti sigurnosnih mehanizama, homologacija se nastavlja izdavati u skladu s Uredbom samo u tim specifičnim i iznimnim okolnostima te kad ne postoji alternativno rješenje koje je u skladu s Uredbom.

433) U tim okolnostima, dotična država članica bez odgode obavještava Evropsku komisiju, koja u roku od dvanaest kalendarskih mjeseci od dodjele homologacije pokreće postupak kojim osigurava da se ponovno uspostavi prvobitni novo sigurnosti.

8.3 Certifikat o ispravnosti

434) Svaki kandidat za homologaciju mora dostaviti tijelu države članice odgovornom za homologaciju sve materijale i dokumente koje tijelo smatra potrebnima.

435) Proizvođači u roku od mjesec dana od datuma zahtjeva osiguravaju odgovarajuće uzorke proizvoda podnesenog za homologaciju i s tim povezanu dokumentaciju, koju zahtijevaju laboratorijai imenovani za obavljanje funkcionalnih ispitivanja. Sve troškove koji nastanu zbog tog zahtjeva snosi podvlasnik zahtjeva. Laboratorijai povjerljivo postupaju sa svim poslovno osjetljivim informacijama.

436) Certifikat o ispravnosti izdaje se proizvođaču tek nakon uspješnog okončanja najmanje onih ispitivanja funkcionalnosti koja su navedena u Dodatku 9.

437) Tijelo za homologaciju izdaje certifikat o ispravnosti. Osim naziva korisnika i identifikacije modela, u toj se potvrdi detaljno opisuju izvršena ispitivanja i postignuti rezultati.

438) U certifikatu o ispravnosti bilo kojeg sastavnog dijela uređaja za evidentiranje podataka navedeni su i homologacijski brojevi svih drugih homologovanih kompatibilnih sastavnih dijelova uređaja za evidentiranje podataka koji su ispitani tokom certificiranja tog dijela.

439) U certifikatu o ispravnosti svih sastavnih dijelova uređaja za evidentiranje podataka navodi se i norma ISO ili CEN u odnosu na koju je funkcionalno sučelje certificikovano.

8.4 Certifikat o interoperabilnosti

440) Ispitivanje interoperabilnosti sprovodi se u jednom od laboratorijaa pod nadležnošću i odgovornosti Evropske komisije.

441) Laboratorija mora upisati zahtjeve za ispitivanje interoperabilnosti koje podnose proizvođači hronološkim redom njihova pristizanja.

442) Zahtjevi se službeno upisuju samo kad laboratorija dođe u posjed:

- cjelokupnog niza materijala i dokumenata potrebnih za takva ispitivanja interoperabilnosti,
- odgovarajućeg certifikata o sigurnosti,
- odgovarajućeg certifikata o ispravnosti,

Datum upisa zahtjeva prijavljuje se proizvođaču.

443) Laboratorija ne obavlja nikakva ispitivanja interoperabilnosti za uređaj za evidentiranje podataka ili tahografske kartice koji nisu dobili sigurnosni certifikat i funkcionalni certifikat, osim u iznimnim okolnostima opisanima u zahtjevu 432.

444) Svaki proizvođač koji traži ispitivanje interoperabilnosti mora se obvezati da će laboratorijau zaduženom za takva ispitivanja ostaviti cjelokupan skup materijala i dokumenata koje je pribavio radi provedbe ispitivanja.

445) Ispitivanja interoperabilnosti moraju se izvesti u skladu s odredbama Dodatka 9. ovom Prilogu, na svim vrstama uređaja za evidentiranje podataka odnosno tahografskih kartica:

- za koje homologacija još vrijedi, ili
- za koje je homologacija u toku i koji imaju važeći certifikat o interoperabilnosti.

446) Ispitivanja interoperabilnosti moraju uključivati sve generacije uređaja za evidentiranje podataka ili tahografskih kartica koje se još uvijek upotrebljavaju.

447) Certifikat o interoperabilnosti laboratorija izdaje proizvođaču tek nakon uspješnog prolaska svih ispitivanja interoperabilnosti.

448) Ako ispitivanja interoperabilnosti na jednom uređaju za evidentiranje podataka ili više njih ili jednoj tahografskoj kartici ili više njih nisu bila uspješna, certifikat o interoperabilnosti ne smije se izdati prije nego proizvođač koji je podnio zahtjev ne izvrši potrebne izmjene i prođe ispitivanje interoperabilnosti. Laboratorija uz pomoć proizvođača na koje se odnosi ta pogreška interoperabilnosti utvrđuje uzrok problema te pokušava pomoći proizvođaču podvlasniku zahtjeva da pronađe tehničko rješenje. Ako je proizvođač izmijenio svoj proizvod, odgovornost je proizvođača da kod nadležnih tijela utvrdi vrijede li još uvijek certifikat o sigurnosti i certifikat o ispravnosti.

449) Certifikat o interoperabilnosti vrijedi šest mjeseci. Na kraju tog perioda on se opoziva ako proizvođač nije dobio odgovarajući certifikat o homologaciji. Proizvođač ga dostavlja tijelu države članice ovlaštenom za homologaciju koje je izdalo potvrdu o ispravnosti.

450) Nijedan element koji bi mogao biti ishodište neuspjeha provjere interoperabilnosti ne smije se upotrebljavati za ostvarivanje dobiti ili za preuzimanje vodećeg položaja.

8.5 Certifikat o homologaciji

451) Tijelo države članice ovlašteno za homologaciju može izdati certifikat o homologaciji čim zaprimi tri potrebna certifikata.

452) U certifikatu o homologaciji bilo kojeg dijela uređaja za evidentiranje podataka navedeni su i homologacijski brojevi svih drugih homologovanih kompatibilnih uređaja za evidentiranje podataka.

453) Tijelo ovlašteno za homologaciju certifikat o homologaciji mora istodobno dostaviti laboratorijau zaduženom za ispitivanje interoperabilnosti i proizvođaču.

454) Laboratorija nadležan za ispitivanje interoperabilnosti mora imati javne internetske stranice na kojima će se ažurirati popis modela uređaja za evidentiranje podataka ili tahografskih kartica:

- za koje je upisan zahtjev za ispitivanje interoperabilnosti,
- kojima je izdat certifikat o interoperabilnosti (čak i privremeni),
- kojima je izdat certifikat o homologaciji.

8.6 Izvanredni postupak: prvi certifikati o interoperabilnosti za uređaje za evidentiranje podataka i tahografske kartice druge generacije

455) Do isteka četiri mjeseca od izdavanja certifikata o interoperabilnosti za prvi par uređaja za evidentiranje podataka druge generacije i tahografskih kartica druge generacije (kartica vozača,

kartica radionice, kontrolna kartica i kartica preduzeća), svaki izdati certifikat (uključujući i prvi) u pogledu zahtjeva upisanih u tom periodu smatra se privremenim.

456) Ako na kraju tog perioda svi predmetni proizvodi budu međusobno interoperabilni, svi odgovarajući certifikati o interoperabilnosti postaju konačni.

457) Ako se tokom tog perioda utvrde pogreške interoperabilnosti, laboratorija zadužen za ispitivanje interoperabilnosti mora uz pomoć svih uključenih proizvođača utvrditi uzroke problema te ih mora pozvati da izvrše potrebne izmjene.

458) Ako se po isteku tog perioda problemi interoperabilnosti nastave, laboratorija zadužen za ispitivanje interoperabilnosti, u suradnji sa svim zainteresiranim proizvođačima i tijelima ovlašćenima za homologaciju koja su izdala odgovarajuće certifikate o ispravnosti, mora pronaći uzrok pogrešaka interoperabilnosti i utvrditi koje izmjene svaki od dotičnih proizvođača treba izvršiti. Traženje tehničkih rješenja traje najduže dva mjeseca, nakon čega Komisija, ako se ne pronađe nikakvo zajedničko rješenje i nakon dogovora s laboratorijaem zaduženim za ispitivanje interoperabilnosti, odlučuje koji će uređaj(i) za evidentiranje podataka i kartice dobiti konačni certifikat o interoperabilnosti te navesti razloge za tu odluku.

459) Svaki zahtjev za ispitivanje interoperabilnosti koji laboratorija upiše između kraja četveromjesečnog perioda nakon izdavanja prvog privremenog certifikata o interoperabilnosti i datuma odluke Komisije iz zahtjeva 455 mora se odgoditi dok se ne riješe prvi problemi interoperabilnosti. Takvi se zahtjevi potom obrađuju hronološkim redom njihova upisivanja.

Dodatak 1

RJEČNIK S PODACIMA

SADRŽAJ

2.44. CertificateRequestID
2.45. CertificationAuthorityKID
2.46. CompanyActivityData
2.47. CompanyActivityType
2.48. CompanyCardApplicationIdentification
2.49. CompanyCardHolderIdentification
2.50. ControlCardApplicationIdentification
2.51. ControlCardControlActivityData
2.52. ControlCardHolderIdentification
2.53. ControlType
2.54. CurrentDateTime
2.55. CurrentDateTimeRecordArray
2.56. DailyPresenceCounter
2.57. Datef
2.58. DateOfDayDownloaded
2.59. DateOfDayDownloadedRecordArray
2.60. Distance
2.61. DriverCardApplicationIdentification
2.62. DriverCardHolderIdentification
2.63. Rezervisano za buduću upotrebu
2.64. EGFCertificate
2.65. EmbedderIcAssemblerId
2.66. EntryTypeDailyWorkPeriod
2.67. EquipmentType
2.68. EuropeanPublicKey
2.69. EventFaultRecordPurpose
2.70. EventFaultType
2.71. ExtendedSealIdentifier
2.72. ExtendedSerialNumber
2.73. FullCardNumber
2.74. FullCardNumberAndGeneration
2.75. Generation
2.76. GeoCoordinates
2.77. GNSSAccuracy
2.78. GNSSAccumulatedDriving
2.79. GNSSAccumulatedDrivingRecord
2.80. GNSSPlaceRecord
2.81. HighResOdometer
2.82. HighResTripDistance
2.83. HolderName
2.84. InternalGNSSReceiver
2.85. K-ConstantOfRecordingEquipment
2.86. KeyIdentifier
2.87. KMWCKey
2.88. Language
2.89. LastCardDownload
2.90. LinkCertificate
2.91. L-TyreCircumference
2.92. MAC
2.93. ManualInputFlag

2.94. ManufacturerCode
2.95. ManufacturerSpecificEventFaultData
2.96. MemberStateCertificate
2.97. MemberStateCertificateRecordArray
2.98. MemberStatePublicKey
2.99. Name
2.100. NationAlpha
2.101. NationNumeric
2.102. NoOfCalibrationRecords
2.103. NoOfCalibrationsSinceDownload
2.104. NoOfCardPlaceRecords
2.105. NoOfCardVehicleRecords
2.106. NoOfCardVehicleUnitRecords
2.107. NoOfCompanyActivityRecords
2.108. NoOfControlActivityRecords
2.109. NoOfEventsPerType
2.110. NoOfFaultsPerType
2.111. NoOfGNSSADRecords
2.112. NoOfSpecificConditionRecords
2.113. OdometerShort
2.114. OdometerValueMidnight
2.115. OdometerValueMidnightRecordArray
2.116. OverspeedNumber
2.117. PlaceRecord
2.118. PreviousVehicleInfo
2.119. PublicKey
2.120. RecordType
2.121. RegionAlpha
2.122. RegionNumeric
2.123. RemoteCommunicationModuleSerialNumber
2.124. RSAKeyModulus
2.125. RSAKeyPrivateExponent
2.126. RSAKeyPublicExponent
2.127. RtmData
2.128. SealDataCard
2.129. SealDataVu
2.130. SealRecord
2.131. SensorApprovalNumber
2.132. SensorExternalGNSSApprovalNumber
2.133. SensorExternalGNSSCoupledRecord
2.134. SensorExternalGNSSIdentification
2.135. SensorExternalGNSSInstallation
2.136. SensorExternalGNSSOSIdentifier
2.137. SensorExternalGNSSSCIdentifier
2.138. SensorGNSSCouplingDate
2.139. SensorGNSSSerialNumber
2.140. SensorIdentification
2.141. SensorInstallation
2.142. SensorInstallationSecData
2.143. SensorOSIdentifier

2.144. SensorPaired
2.145. SensorPairedRecord
2.146. SensorPairingDate
2.147. SensorSCIdentifier
2.148. SensorSerialNumber
2.149. Signature
2.150. SignatureRecordArray
2.151. SimilarEventsNumber
2.152. SpecificConditionRecord
2.153. SpecificConditions
2.154. SpecificConditionType
2.155. Speed
2.156. SpeedAuthorised
2.157. SpeedAverage
2.158. SpeedMax
2.159. TachographPayload
2.160. Rezervisano za buduću upotrebu
2.161. TDesSessionKey
2.162. TimeReal
2.163. TyreSize
2.164. VehicleIdentificationNumber
2.165. VehicleIdentificationNumberRecordArray
2.166. VehicleRegistrationIdentification
2.167. VehicleRegistrationNumber
2.168. VehicleRegistrationNumberRecordArray
2.169. VuAbility
2.170. VuActivityDailyData
2.171. VuActivityDailyRecordArray
2.172. VuApprovalNumber
2.173. VuCalibrationData
2.174. VuCalibrationRecord
2.175. VuCalibrationRecordArray
2.176. VuCardIWData
2.177. VuCardIWRecord
2.178. VuCardIWRecordArray
2.179. VuCardRecord
2.180. VuCardRecordArray
2.181. VuCertificate
2.182. VuCertificateRecordArray
2.183. VuCompanyLocksData
2.184. VuCompanyLocksRecord
2.185. VuCompanyLocksRecordArray
2.186. VuControlActivityData
2.187. VuControlActivityRecord
2.188. VuControlActivityRecordArray
2.189. VuDataBlockCounter
2.190. VuDetailedSpeedBlock
2.191. VuDetailedSpeedBlockRecordArray
2.192. VuDetailedSpeedData
2.193. VuDownloadablePeriod

2.194. VuDownloadablePeriodRecordArray
2.195. VuDownloadActivityData
2.196. VuDownloadActivityDataRecordArray
2.197. VuEventData
2.198. VuEventRecord
2.199. VuEventRecordArray
2.200. VuFaultData
2.201. VuFaultRecord
2.202. VuFaultRecordArray
2.203. VuGNSSADRecord
2.204. VuGNSSADRecordArray
2.205. VuIdentification
2.206. VuIdentificationRecordArray
2.207. VuITSConsentRecord
2.208. VuITSConsentRecordArray
2.209. VuManufacturerAddress
2.210. VuManufacturerName
2.211. VuManufacturingDate
2.212. VuOverSpeedingControlData
2.213. VuOverSpeedingControlDataRecordArray
2.214. VuOverSpeedingEventData
2.215. VuOverSpeedingEventRecord
2.216. VuOverSpeedingEventRecordArray
2.217. VuPartNumber
2.218. VuPlaceDailyWorkPeriodData
2.219. VuPlaceDailyWorkPeriodRecord
2.220. VuPlaceDailyWorkPeriodRecordArray
2.221. VuPrivateKey
2.222. VuPublicKey
2.223. VuSerialNumber
2.224. VuSoftInstallationDate
2.225. VuSoftwareIdentification
2.226. VuSoftwareVersion
2.227. VuSpecificConditionData
2.228. VuSpecificConditionRecordArray
2.229. VuTimeAdjustmentData
2.230. Rezervisano za buduću upotrebu
2.231. Rezervisano za buduću upotrebu
2.232. VuTimeAdjustmentRecord
2.233. VuTimeAdjustmentRecordArray
2.234. WorkshopCardApplicationIdentification
2.235. WorkshopCardCalibrationData
2.236. WorkshopCardCalibrationRecord
2.237. WorkshopCardHolderIdentification
2.238. WorkshopCardPIN
2.239. W-VehicleCharacteristicConstant
2.240. VuPowerSupplyInterruptionRecord
2.241. VuPowerSupplyInterruptionRecordArray
2.242. VuSensorExternalGNSSCoupledRecordArray
2.243. VuSensorPairedRecordArray

1. UVOD

U ovom su dodatku navedeni formati podataka, podatkovni elementi i strukture podataka za upotrebu u uređajima za evidentiranje podataka i tahografskim karticama.

1.1. Pristup definisanju vrsta podataka

U ovom se dodatku za definisanje vrsta podataka upotrebljava *Abstract Syntax Notation One* (ASN.1). Time se omogućava definisanje jednostavnih i strukturiranih podataka bez impliciranja posebne sintakse prenosa (pravila u pogledu kodiranja) koji će zavisiti o primjeni i okolini.

Konvencije o nazivlju tipa ASN.1 u skladu su s normom ISO/IEC 8824-1. To znači sljedeće:

- ako je to moguće, značenje vrste podataka naslućuje se iz odabranih naziva,
- ako je vrsta podataka sastavljena od drugih vrsta podataka, naziv vrste podataka svejedno se sastoji od jednog slijeda abecednih znakova koji započinje velikim početnim slovom, ali se u nazivu upotrebljavaju velika slova kako bi se naglasilo odgovarajuće značenje,
- nazivi vrsta podataka uopšteno su povezani s nazivom vrsta podataka iz kojih su izvedeni, uređajem u kojem su podaci sačuvani i funkcijom u vezi s podacima.

Ako je vrsta podataka po ASN.1 već definisana kao dio neke druge norme, a važno je upotrijebiti je u uređaju za evidentiranje podataka, ta ASN.1 vrsta podataka bit će definisana u ovome dodatku.

Kako bi se omogućilo više vrsta pravila u pogledu kodiranja, neke su vrste ASN.1 u ovome dodatku ograničene identifikatorima raspona vrijednosti. Identifikatori raspona vrijednosti definisani su u stavu 3. i Dodatku 2.

1.2. Literatura

U ovome su Dodatku upotrijebljeni sljedeći izvori:

ISO 639 Code for the representation of names of languages. Prvo izdatje: 1988.

ISO 3166 Codes for the representation of names of countries and their subdivisions – Part 1: Country codes, 2013.

ISO 3779 Road vehicles – Vehicle identification number (VIN) – Content and structure. 2009.

ISO/IEC 7816-5 Identification cards – Integrated circuit cards – Part 5: Registration of application providers. Drugo izdatje: 2004.

ISO/IEC 7816-6 Identification cards – Integrated circuit cards – Part 6: Interindustry data elements for interchange, 2004 + Technical Corrigendum 1: 2006.

ISO/IEC 8824-1 Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation. 2008 + Technical Corrigendum 1: 2012 and Technical Corrigendum 2: 2014.

ISO/IEC 8825-2 Information technology – ASN.1 encoding rules: Specification of Packed Encoding Rules (PER). 2008.

ISO/IEC 8859-1 Information technology – 8 bit single-byte coded graphic character sets – Part 1: Latin alphabet No.1. Prvo izdatje: 1998.

ISO/IEC 8859-7 Information technology – 8 bit single-byte coded graphic character sets – Part 7: Latin/Greek alphabet. 2003.

ISO 16844-3 Road vehicles – Tachograph systems – Motion Sensor Interface. 2004 + Technical Corrigendum 1: 2006.

TR-03110-3 BSI / ANSSI Technical Guideline TR-03110-3, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 3 Common Specifications, verzija 2.20, 3. februar 2015.

2. DEFINICIJE VRSTA PODATAKA

Za sve vrste podataka navedene u nastavu zadana vrijednost za sadržaj „nepoznato" ili „nije primjenjivo" sastoji se od popunjavanja podatkovnog elementa bajtovima „FF". Sve se vrste podataka upotrebljavaju za aplikacije prve i druge generacije, osim ako nije navedeno drukčije.

Za vrste podataka na kartici koje se upotrebljavaju za aplikacije prve i druge generacije, veličina određena u ovom Dodatku je ona za aplikacije druge generacije. Čitaoc bi već trebao biti upoznat s veličinom za aplikacije prve generacije. Brojevi zahtjeva navedenih u Prilogu I.C povezani s takvim vrstama podataka odnose se na aplikacije prve i druge generacije.

2.1. ActivityChangeInfo

Tom se vrstom podataka omogućava kodiranje, u okviru dvobajtne riječi, statusa otvora u 00:00 sati i/ili stanja vožnje u 00:00 sati i/ili promjena aktivnosti i/ili promjena stanja vožnje i/ili promjena statusa kartice vozača ili suvozača. Ta se vrsta podataka odnosi na zahtjeve 105, 266, 291, 320, 321, 343 i 344 iz Priloga 1.C.

```
ActivityChangeInfo ::= OCTET STRING (SIZE(2))
```

Dodjela vrijednosti – oktetno poravnavanje: 'scpaatttttttttt' B (16 bitova)

Za zapise u memoriji podataka (ili status otvora):

's'B Otvor:
'0'B: VOZAČ,
'1'B: SUVOZAČ,

‘c’B Stanje vožnje:
‘0’B: JEDAN VOZAČ,
‘1’B: POSADA,
‘p’B Status kartice vozača (ili radionice) u odgovarajućem otvoru:
‘0’B: UMETNUTA, kartica je umetnuta,
‘1’B: NIJE UMETNUTA, kartica nije umetnuta (ili je kartica uklonjena),
‘aa’B Aktivnost:
‘00’B: PAUZA/ODMOR,
‘01’B: PRIPRAVNOST,
‘10’B: RAD,
‘11’B: VOŽNJA,
‘ttttttttttt’B Vrijeme promjene: broj minuta od 00:00 h određenog dana.

Za zapise na kartici vozača (ili radionice) (i stanje vožnje):

‘s’B Otvor (nije relevantno ako je ‘p’ = 1, osim prema napomeni navedenoj u nastavu):
‘0’B: VOZAČ,
‘1’B: SUVOZAČ,
‘c’B Stanje vožnje (ako je ‘p’ = 0) ili
Sljedeće stanje aktivnosti (ako je ‘p’ = 1):
‘0’B: JEDAN VOZAČ,
‘0’B: NEPOZNATO
‘1’B: POSADA,
‘1’B: POZNATO (= ručni unos)
‘p’B Status kartice:
‘0’B: UMETNUTA, kartica je umetnuta u uređaj za evidentiranje podataka,
‘1’B: NIJE UMETNUTA, kartica nije umetnuta (ili je kartica uklonjena),
‘aa’B Aktivnost (nije relevantno ako je ‘p’ = 1 i ‘c’ = 0, osim prema napomeni navedenoj u nastavu):
‘00’B: PAUZA/ODMOR,
‘01’B: PRIPRAVNOST,
‘10’B: RAD,
‘11’B: VOŽNJA,
‘ttttttttttt’B Vrijeme promjene: broj minuta od 00:00 h određenog dana.

Napomena u slučaju „uklanjanja kartice”:

Kad je kartica uklonjena:
— bit ‘s’ je relevantan i označava otvor iz kojeg je kartica uklonjena,
— bit ‘c’ mora biti postavljen na 0,
— bit ‘p’ mora biti postavljen na 1,
— bitom ‘aa’ mora se kodirati trenutna aktivnost odabrana u tom trenutku.

Kao rezultat ručnog unosa, kasnije se može pisati preko bitova ‘c’ i ‘aa’ riječi (sačuvanih u kartici) kako bi se odrazio unos.

2.2. Address

Adresa.

```
Address ::= SEQUENCE {
   codePage                    INTEGER (0..255),
   address                     OCTET STRING (SIZE(35))
}
```

codePage označava skup znakova definisan u poglavlju 4.,
address je adresa kodirana s pomoću posebnog skupa znakova.

2.3. AESKey

Druga generacija:

AES ključ dužine 128, 192 ili 256 bitova.

```
AESKey ::= CHOICE {
   aes128Key                   AES128Key,
   aes192Key                   AES192Key,
   aes256Key                   AES256Key
}
```

Dodjela vrijednosti: nije dodatno utvrđena.

2.4. AES128Key

Druga generacija:

AES128 ključ.

```
AES128Key ::= SEQUENCE {
   length                      INTEGER(0..255),
   aes128Key                   OCTET STRING (SIZE(16))
}
```

dužina označava dužinu AES128 ključa u oktetima.
aes128Key je AES ključ dužine 128 bitova.

Dodjela vrijednosti:

Dužina ima vrijednost 16.

2.5. AES192Key

Druga generacija:

AES192 ključ.

```
AES192Key ::= SEQUENCE {
   length                          INTEGER(0..255),
   aes192Key                       OCTET STRING (SIZE(24))
}
```

dužina označava dužinu AES192 ključa u oktetima.
aes192Key je AES ključ dužine 192 bita.
Dodjela vrijednosti:
Dužina ima vrijednost 24.

2.6. AES256Key

Druga generacija:
AES256 ključ.

```
AES256Key ::= SEQUENCE {
   length                          INTEGER(0..255),
   aes256Key                       OCTET STRING (SIZE(32))
}
```

dužina označava dužinu AES256 ključa u oktetima.
aes256Key je AES ključ dužine 256 bitova.
Dodjela vrijednosti:
Dužina ima vrijednost 32.

2.7. BCDString

BCDString primjenjuje se za prikaz binarno kodiranih decimalnih brojeva (BCD). Ta se vrsta podataka upotrebljava za prikaz jednodecimalne karakteristik u jednom poluoktetu (4 bita). BCDString temelji se na normi ISO/IEC 8824-1 'CharacterStringType'

```
BCDString ::= CHARACTER STRING (WITH COMPONENTS {
   identification ( WITH COMPONENTS {
   fixed PRESENT }) })
```

BCDString upotrebljava zapis „hstring". Krajnja lijeva heksadecimalna znamenka najvažniji je poluoktet prvog okteta. Višestruke okteta tvori se tako da se umetne poluoktet sa završnim nulama, prema potrebi, od mjesta krajnjeg lijevog poluokteta u prvom oktetu.
Dopuštene su karakteristik sljedeće: 0, 1, … 9.

2.8. CalibrationPurpose

Kod kojim se pojašnjava zašto je zabilježen niz parametara kalibriranja. Ta se vrsta podataka odnosi na zahtjeve 097 i 098 iz Priloga 1.B te na zahtjev 119 iz Priloga 1.C.

```
CalibrationPurpose ::= OCTET STRING (SIZE(1))
```

Dodjela vrijednosti:
Prva generacija:
'00'H rezervisana vrijednost,
'01'H aktivacija: evidentiranje poznatih parametara kalibriranja u trenutku aktivacije jedinice u vozilu,
'02'H prva ugradnja: prvo kalibriranje jedinice u vozilu nakon njezine aktivacije,
'03'H ugradnja: prvo kalibriranje jedinice u vozilu u sadašnjem vozilu,
'04'H periodični pregled.
Druga generacija:
Uz vrijednosti navedene za prvu generaciju upotrebljavaju se i sljedeće:
'05'H preduzeće unosi registracijski broj vozila (VRN),
'06'H podešavanje vremena bez kalibriranja,
'07'H do '7F'H RFU,
'80'H do 'FF'H specifično za proizvođača.

2.9. CardActivityDailyRecord

Informacije sačuvane na kartici koje se odnose na aktivnosti vozača na određeni kalendarski dan. Ta se vrsta podataka odnosi na zahtjeve 266, 291, 320 i 343 iz Priloga 1.C.

```
CardActivityDailyRecord ::= SEQUENCE {
   activityPreviousRecordLength        INTEGER(0..CardActivityLengthRange),
   activityRecordLength                INTEGER(0..CardActivityLengthRange),
   activityRecordDate                  TimeReal,
   activityDailyPresenceCounter        DailyPresenceCounter,
   activityDayDistance                 Distance,
   activityChangeInfo                  SET SIZE(1..1440) OF ActivityChangeInfo
}
```

activityPreviousRecordLength je ukupna dužina u bajtovima zapisa od prethodnog dana. Najveća vrijednost iskazana je dužinom oktetnog niza (OCTET STRING) koji sadrži te zapise (vidjeti CardActivityLengthRange u Dodatku 2. stavu 4.). Kad je taj zapis najstariji dnevni zapis, vrijednost activityPreviousRecordLength mora biti postavljena na 0.
activityRecordLength je ukupna dužina u bajtovima tog zapisa. Najveća vrijednost iskazana je dužinom OCTET STRING koji sadrži te zapise.
activityRecordDate je datum zapisa.
activityDailyPresenceCounter je brojač dnevne prisutnosti za određenu karticu za taj dan.
activityDayDistance je ukupna udaljenost prijeđena tog dana.

activityChangeInfo je skup ActivityChangeInfo podataka za vozača za taj dan. Smije sadržiti najviše 1440 vrijednosti (jedna promjena aktivnosti u minuti). U taj je skup uvijek uključen activityChangeInfo kojim se kodira stanje vožnje u 00:00 h.

2.10. CardActivityLengthRange

Broj bajtova na kartici vozača ili kartici radionice raspoloživih za arhiviranje zapisa o aktivnosti vozača.

```
CardActivityLengthRange ::= INTEGER(0..2^16-1)
```

Dodjela vrijednosti: vidjeti Dodatak 2.

2.11. CardApprovalNumber

Homologacijski broj kartice.

```
CardApprovalNumber ::= IA5String(SIZE(8))
```

Dodjela vrijednosti:

Homologacijski broj daje se u skladu s onime objavljenim na odgovarajućoj internetskoj stranici Evropske komisije, odnosno, na primjer, uključujući spojnice ako postoje. Homologacijski broj mora biti lijevo poravnat.

2.12. CardCertificate

Prva generacija:

Certifikat javnog ključa kartice.

```
CardCertificate ::= Certificate
```

2.13. CardChipIdentification

Informacije sačuvane na kartici koje se odnose na identifikaciju integriranog kruga (IC) kartice (zahtjev 249 iz Priloga 1.C). icSerialNumber i icManufacturingReferences zajedno čine jedinstvenu identifikaciju čipa kartice. icSerialNumber sâm za sebe ne čini jedinstvenu identifikaciju kartice.

```
CardChipIdentification ::= SEQUENCE {
  icSerialNumber                OCTET STRING (SIZE(4)),
  icManufacturingReferences     OCTET STRING (SIZE(4))
}
```

icSerialNumber je serijski broj IC-a.

icManufacturingReferences je posebni identifikator proizvođača IC-a.

2.14. CardConsecutiveIndex

Redni indeks kartice (definicija h)).

```
CardConsecutiveIndex ::= IA5String(SIZE(1))
```

Dodjela vrijednosti: (vidjeti poglavlje VII. Priloga 1.C)

Redoslijed povećavanja: '0, ⋯, 9, A, ⋯, Z, a, ⋯, z'

2.15. CardControlActivityDataRecord

Informacije sačuvane na kartici vozača ili kartici radionice koje se odnose na posljednju kontrolu kojoj je bio podvrgnut vozač (zahtjevi 274, 299, 327 i 350 iz Priloga 1.C).

```
CardControlActivityDataRecord ::= SEQUENCE {
  controlType                   ControlType,
  controlTime                   TimeReal,
  controlCardNumber             FullCardNumber,
  controlVehicleRegistration    VehicleRegistrationIdentification,
  controlDownloadPeriodBegin    TimeReal,
  controlDownloadPeriodEnd      TimeReal
}
```

controlType je vrsta kontrole.

controlTime je datum i vrijeme kontrole.

controlCardNumber je FullCardNumber službenika za kontrolu koji je sproveo kontrolu.

controlVehicleRegistration je VRN i država članica registracije vozila u kojem je provedena kontrola.

controlDownloadPeriodBegin i **controlDownloadPeriodEnd** su perioda za koja su preuzeti podaci, u slučaju preuzimanja podataka.

2.16. CardCurrentUse

Informacije o stvarnoj upotrebi kartice (zahtjevi 273, 298, 326 i 349 iz Priloga 1.C).

```
CardCurrentUse ::= SEQUENCE {
  sessionOpenTime               TimeReal,
  sessionOpenVehicle            VehicleRegistrationIdentification
}
```

sessionOpenTime je trenutak umetanja kartice radi trenutne upotrebe. Taj se element pri uklanjanju kartice postavlja na nulu.

sessionOpenVehicle je identifikacija vozila koje se trenutno upotrebljava, postavljena pri umetanju kartice. Taj se element pri uklanjanju kartice postavlja na nulu.

2.17. CardDriverActivity

Informacije sačuvane na kartici vozača ili radionice koje se odnose na aktivnosti vozača (zahtjevi 267, 268, 292, 293, 321 i 344 iz Priloga 1.C).

```
CardDriverActivity ::= SEQUENCE {
  activityPointerOldestDayRecord    INTEGER(0.. CardActivityLengthRange-1),
  activityPointerNewestRecord       INTEGER(0.. CardActivityLengthRange-1),
  activityDailyRecords              OCTET STRING
                                    (SIZE(CardActivityLengthRange))
}
```

activityPointerOldestDayRecord je određivanje početka prostora za čuvanje (broj bajtova od početka niza) najstarijeg zapisa za puni dan u nizu activityDailyRecords. Najveća vrijednost iskazana je dužinom niza.

activityPointerNewestRecord je određivanje početka prostora za čuvanje (broj bajtova od početka niza) najnovijeg zapisa za puni dan u nizu activityDailyRecords. Najveća vrijednost iskazana je dužinom niza.
activityDailyRecords je prostor raspoloživ za čuvanje podataka o aktivnosti vozača (struktura podataka: CardActivityDailyRecord) za svaki kalendarski dan kad je upotrebljavana kartica.
Dodjela vrijednosti: ovaj se oktetni niz ciklično popunjava zapisima CardActivityDailyRecord. Pri prvoj upotrebi arhiviranje započinje s prvim bajtom niza. Svi se novi zapisi dodaju na kraj prethodnog zapisa. Kad je niz pun, arhiviranje se nastavlja u prvi bajt niza nezavisno o prekidu u podatkovnom elementu. Prije postavljanja novih podataka o aktivnostima u niz (povećanje postojećeg activityDailyRecord ili postavljanje novog activityDailyRecord) kojima se zamjenjuju stariji podaci o aktivnostima, mora se ažurirati activityPointerOldestDayRecord kako bi se odrazilo novo mjesto najstarijeg zapisa za puni dan, a activityPreviousRecordLength tog (novog) najstarijeg zapisa za puni dan mora se ponovno postaviti na 0.

2.18. CardDrivingLicenceInformation

Informacije sačuvane na kartici vozača koje se odnose na podatke o vozačkoj dozvoli vlasnika kartice (zahtjevi 259 i 284 iz Priloga 1.C).

```
CardDrivingLicenceInformation ::= SEQUENCE {
   drivingLicenceIssuingAuthority      Name,
   drivingLicenceIssuingNation         NationNumeric,
   drivingLicenceNumber                IA5String(SIZE(16))
}
```

drivingLicenceIssuingAuthority je tijelo nadležno za izdavanje vozačke dozvole.
drivingLicenceIssuingNation je državna pripadnost tijela koje je izdalo vozačku dozvolu.
drivingLicenceNumber je broj vozačke dozvole.

2.19. CardEventData

Prva generacija:
informacije arhivirane na kartici vozača ili radionice koje se odnose na događaje povezane s vlasnikom kartice (zahtjevi 260) i 318) iz Priloga I.C).

```
CardEventData ::= SEQUENCE SIZE(6) OF
   cardEventRecords                    SET SIZE(NoOfEventsPerType) OF
                                       CardEventRecord
```

CardEventData je slijed poredan prema uzlaznoj vrijednosti EventFaultType za cardEventRecords (osim u slučaju zapisa povezanih s pokušajima probijanja zaštite koji su sakupljeni u posljednjem nizu slijeda).
cardEventRecords je niz zapisa o događajima određene vrste događaja (ili kategorije, u slučaju pokušaja probijanja zaštite).
Druga generacija:
informacije arhivirane na kartici vozača ili radionice koje se odnose na događaje povezane s vlasnikom kartice (zahtjevi 285) i 341) iz Priloga I.C).

```
CardEventData ::= SEQUENCE SIZE(11) OF
   cardEventRecords                    SET SIZE(NoOfEventsPerType) OF
                                       CardEventRecord
```

CardEventData je slijed poredan prema uzlaznoj vrijednosti EventFaultType za cardEventRecords (osim u slučaju zapisa povezanih s pokušajima probijanja zaštite koji su sakupljeni u posljednjem nizu slijeda).
cardEventRecords je niz zapisa o događajima određene vrste događaja (ili kategorije, u slučaju pokušaja probijanja zaštite).

2.20. CardEventRecord

Informacije sačuvane na kartici vozača ili radionice koje se odnose na određeni događaj povezan s vlasnikom kartice (zahtjevi 261, 286, 318 i 341 iz Priloga 1.C).

```
CardEventRecord ::= SEQUENCE {
   eventType                           EventFaultType,
   eventBeginTime                      TimeReal,
   eventEndTime                        TimeReal,
   eventVehicleRegistration            VehicleRegistrationIdentification
}
```

eventType je vrsta događaja.
eventBeginTime je datum i vrijeme početka događaja.
eventEndTime je datum i vrijeme završetka događaja.
eventVehicleRegistration je VRN i država članica registracije vozila u kojem je došlo do događaja.

2.21. CardFaultData

Informacije sačuvane na kartici vozača ili radionice koje se odnose na kvarove povezane s vlasnikom kartice (zahtjevi 263, 288, 318 i 341 iz Priloga 1.C).

```
CardFaultData ::= SEQUENCE SIZE(2) OF {
   cardFaultRecords                    SET SIZE(NoOfFaultsPerType) OF
                                       CardFaultRecord
}
```

CardFaultData je niz zapisa o kvarovima uređaja za evidentiranje podataka nakon kojih slijedi niz zapisa o kvarovima kartice.
cardFaultRecords je niz zapisa o kvarovima u okviru određene kategorije kvara (uređaj za evidentiranje podataka ili kartica).

2.22. CardFaultRecord

Informacije sačuvane na kartici vozača ili radionice koje se odnose na određeni kvar povezan s vlasnikom kartice (zahtjevi 264, 289, 318 i 341 iz Priloga 1.C).

```
CardFaultRecord ::= SEQUENCE {
   faultType                  EventFaultType,
   faultBeginTime             TimeReal,
   faultEndTime               TimeReal,
   faultVehicleRegistration   VehicleRegistrationIdentification
}
```

faultType je vrsta kvara.
faultBeginTime je datum i vrijeme početka kvara.
faultEndTime je datum i vrijeme završetka kvara..
faultVehicleRegistration je VRN i država članica registracije vozila u kojem je došlo do kvara.

2.23. CardIccIdentification

Informacije sačuvane na kartici koje se odnose na identifikaciju integriranog kruga (IC) kartice (zahtjev 248 iz Priloga 1.C).

```
CardIccIdentification ::= SEQUENCE {
   clockStop                  OCTET STRING (SIZE(1)),
   cardExtendedSerialNumber   ExtendedSerialNumber,
   cardApprovalNumber         CardApprovalNumber,
   cardPersonaliserID         ManufacturerCode,
   embedderIcAssemblerId      EmbedderIcAssemblerId,
   icIdentifier               OCTET STRING (SIZE(2))
}
```

clockStop je način rada „Clockstop" kako je definisan u Dodatku 2.
cardExtendedSerialNumber je jedinstveni IC serijski broj kartice kako je dodatno određeno vrstom podataka ExtendedSerialNumber.
cardApprovalNumber je homologacijski broj kartice.
cardPersonaliserID je identifikacijski broj personalizatora kartice kodiran kao ManufacturerCode.
embedderIcAssemblerId pruža informacije o ugraditelju/sastavljaču IC-a.
icIdentifier je identifikator IC-a na kartici i proizvođača IC-a kako je definisano u normi ISO/IEC 7816-6.

2.24. CardIdentification

Informacije sačuvane na kartici koje se odnose na identifikaciju kartice (zahtjevi 255, 280, 310, 333, 359, 365, 371 i 377 iz Priloga 1.C).

```
CardIdentification ::= SEQUENCE {
   cardIssuingMemberState     NationNumeric,
   cardNumber                 CardNumber,
   cardIssuingAuthorityName   Name,
   cardIssueDate              TimeReal,
   cardValidityBegin          TimeReal,
   cardExpiryDate             TimeReal
}
```

cardIssuingMemberState je kod države članice koja izdaje karticu.
cardNumber je broj kartice.
cardIssuingAuthorityName je naziv tijela koje je izdalo karticu.
cardIssueDate je datum izdavanja kartice sadašnjem vlasniku.
cardValidityBegin je datum početka važenja kartice.
cardExpiryDate je datum isteka važenja kartice.

2.25. CardMACertificate

Druga generacija:
Certifikat javnog ključa kartice za uzajamnu autentifikaciju s jedinicom u vozilu. Struktura tog certifikata utvrđena je u Dodatku 11.

```
CardMACertificate ::= Certificate
```

2.26. CardNumber

Broj kartice kako je definisan definicijom (g).

```
CardNumber ::= CHOICE {
   SEQUENCE {
      driverIdentification       IA5String(SIZE(14)),
      cardReplacementIndex       CardReplacementIndex,
      cardRenewalIndex           CardRenewalIndex
   },
   SEQUENCE {
      ownerIdentification        IA5String(SIZE(13)),
      cardConsecutiveIndex       CardConsecutiveIndex,
      cardReplacementIndex       CardReplacementIndex,
      cardRenewalIndex           CardRenewalIndex
   }
}
```

driverIdentification je jedinstvena identifikacija vozača u državi članici.
ownerIdentification je jedinstvena identifikacija preduzeća ili radionice ili nadzornog tijela u državi članici.
cardConsecutiveIndex je indeks rednog broja kartice.
cardReplacementIndex je indeks zamjene kartice.
cardRenewalIndex je indeks obnavljanja kartice.

Prvi slijed izbora prikladan je za kodiranje broja kartice vozača, drugi slijed izbora prikladan je za kodiranje brojeva kartice radionice, nadzornog tijela i preduzeća.

2.27. CardPlaceDailyWorkPeriod

Informacije sačuvane na kartici vozača ili radionice koje se odnose na mjesta na kojima počinju i/ili završavaju perioda dnevnog rada (zahtjevi 272, 297, 325 i 348 iz Priloga 1.C).

```
CardPlaceDailyWorkPeriod ::= SEQUENCE {
   placePointerNewestRecord    INTEGER(0 .. NoOfCardPlaceRecords-1),
   placeRecords                SET SIZE(NoOfCardPlaceRecords) OF PlaceRecord
}
```

placePointerNewestRecord je indeks posljednjeg ažuriranog zapisa o mjestu.

Dodjela vrijednosti: Broj koji odgovara brojniku zapisa o mjestu, a započinje s „0" za prvu pojavu zapisâ o mjestu u strukturi.

placeRecords je niz zapisa koji sadrže informacije povezane s unesenim mjestima.

2.28. CardPrivateKey

Prva generacija:

Privatni ključ kartice.

```
CardPrivateKey ::= RSAKeyPrivateExponent
```

2.29. CardPublicKey

Javni ključ kartice.

```
CardPublicKey ::= PublicKey
```

„2.30. CardRenewalIndex

Indeks obnavljanja kartice (definicija i)).

```
CardRenewalIndex::= IA5String(SIZE(1))
```

Dodjela vrijednosti: (vidjeti poglavlje 7. ovog Priloga).

‚0' Prvo izdavanje.

Redoslijed povećavanja: ‚0, …, 9, A, …, Z' ";

2.31. CardReplacementIndex

Indeks zamjene kartice (definicija (j)).

```
CardReplacementIndex ::= IA5String(SIZE(1))
```

Dodjela vrijednosti: (vidjeti poglavlje VII. ovog Priloga).

'0' Izvorna kartica.

Redoslijed povećavanja: '0, ⋯, 9, A, ⋯, Z'

2.32. CardSignCertificate

Druga generacija:

Certifikat javnog ključa kartice za potpis. Struktura tog certifikata utvrđena je u Dodatku 11.

```
CardSignCertificate ::= Certificate
```

2.33. CardSlotNumber

Kod namijenjen razlikovanju dvaju otvora u jedinici u vozilu.

```
CardSlotNumber ::= INTEGER {
   driverSlot                    (0),
   co-driverSlot                 (1)
}
```

Dodjela vrijednosti: nije dodatno utvrđena.

2.34. CardSlotsStatus

Kod koji označava vrstu kartica umetnutih u dva otvora u jedinici u vozilu.

```
CardSlotsStatus ::= OCTET STRING (SIZE(1))
```

Dodjela vrijednosti – oktetno poravnavanje: 'ccccdddd' B

'cccc'B identifikacija vrste kartice ubačene u otvor suvozača,

'dddd'B identifikacija vrste kartice ubačene u otvor vozača,

sa sljedećim identifikacijskim kodovima:

'0000'B nije umetnuta kartica,

'0001'B umetnuta je kartica vozača,

'0010'B umetnuta je kartica radionice,

'0011'B umetnuta je kontrolna kartica,

'0100'B umetnuta je kartica preduzeća.

2.35. CardSlotsStatusRecordArray

Druga generacija:

CardSlotsStatus i meta podaci kako se upotrebljavaju u postupku preuzimanja.

```
CardSlotsStatusRecordArray ::= SEQUENCE {
   recordType                    RecordType,
   recordSize                    INTEGER(1..65535),
   noOfRecords                   INTEGER(0..65535),
   records                       SET SIZE(noOfRecords) OF CardSlotsStatus
}
```

recordType označava vrstu zapisa (CardSlotsStatus). **Dodjela vrijednosti**: Vidjeti RecordType

recordSize je veličina podatka CardSlotsStatus u bajtovima.

noOfRecords je broj zapisâ u nizu zapisa.

records je niz zapisa CardSlotsStatus.

2.36. CardStructureVersion

Kod koji označava verziju strukture upotrijebljene u tahografskoj kartici.

```
CardStructureVersion ::= OCTET STRING (SIZE(2))
```

Dodjela vrijednosti: 'aabb' H:

'aa'H Indeks izmjena strukture
'00'H za aplikacije prve generacije
'01'H za aplikacije druge generacije

'bb'H Indeks izmjena u pogledu upotrebe podatkovnih elemenata definisanih za strukturu prikazanu gornjim bajtom.
'00'H za ovu verziju aplikacija prve generacije
'00'H za ovu verziju aplikacija druge generacije

2.37. CardVehicleRecord

Informacije sačuvane na kartici vozača ili radionice koje se odnose na period upotrebe vozila tokom kalendarskog dana (zahtjevi 269, 294, 322 i 345 iz Priloga 1.C).

Prva generacija:

```
CardVehicleRecord ::= SEQUENCE {
   vehicleOdometerBegin                OdometerShort,
   vehicleOdometerEnd                  OdometerShort,
   vehicleFirstUse                     TimeReal,
   vehicleLastUse                      TimeReal,
   vehicleRegistration                 VehicleRegistrationIdentification,
   vuDataBlockCounter                  VuDataBlockCounter
}
```

vehicleOdometerBegin je vrijednost na brojaču kilometara vozila na početku perioda upotrebe vozila.
vehicleOdometerEnd je vrijednost na brojaču kilometara vozila na završetku perioda upotrebe vozila.
vehicleFirstUse je datum i vrijeme početka perioda upotrebe vozila.
vehicleLastUse je datum i vrijeme završetka perioda upotrebe vozila.
vehicleRegistration je VRN i država članica registracije vozila.
vuDataBlockCounter je vrijednost VuDataBlockCounter pri posljednjem preuzimanju podataka o periodu upotrebe vozila.

Druga generacija:

```
CardVehicleRecord ::= SEQUENCE {
   vehicleOdometerBegin                OdometerShort,
   vehicleOdometerEnd                  OdometerShort,
   vehicleFirstUse                     TimeReal,
   vehicleLastUse                      TimeReal,
   vehicleRegistration                 VehicleRegistrationIdentification,
   vuDataBlockCounter                  VuDataBlockCounter,
   vehicleIdentificationNumber         VehicleIdentificationNumber
}
```

Uz podatkovne elemente navedene za prvu generaciju upotrebljava se i sljedeći:
VehicleIdentificationNumber je identifikacijski broj vozila koji se odnosi na vozilo kao cjelinu.

2.38. CardVehiclesUsed

Informacije sačuvane na kartici vozača ili radionice koje se odnose na vozila kojima se koristi vlasnik kartice (zahtjevi 270, 295, 323 i 346 iz Priloga 1.C).

```
CardVehiclesUsed ::= SEQUENCE {
   vehiclePointerNewestRecord          INTEGER(0..NoOfCardVehicleRecords-1),
   cardVehicleRecords                  SET SIZE(NoOfCardVehicleRecords) OF
                                       CardVehicleRecord
}
```

vehiclePointerNewestRecord je indeks posljednjeg ažuriranog zapisa o vozilu.
Dodjela vrijednosti: Broj koji odgovara brojniku zapisa o vozilu, a započinje s „0" za prvu pojavu zapisâ o vozilu u strukturi.
cardVehicleRecords je niz zapisa koji sadržiju informacije o upotrijebljenim vozilima.

2.39. CardVehicleUnitRecord

Druga generacija:

Informacije sačuvane na kartici vozača ili radionice koje se odnose na upotrijebljenu jedinicu u vozilu (zahtjevi 303 i 351 iz Priloga 1.C).

```
CardVehicleUnitRecord ::= SEQUENCE {
   timeStamp                           TimeReal,
   manufacturerCode                    ManufacturerCode,
   deviceID                            INTEGER(0..255),
   vuSoftwareVersion                   VuSoftwareVersion
}
```

timeStamp je početak perioda upotrebe jedinice u vozilu (tj. prvo umetanje kartice u jedinicu u vozilu za taj period).
manufacturerCode označava proizvođača jedinice u vozilu.
deviceID označava vrstu jedinice u vozilu proizvođača. Vrijednost je specifična za proizvođača.
vuSoftwareVersion je broj verzije softvera jedinice u vozilu.

2.40. CardVehicleUnitsUsed

Druga generacija:
Informacije sačuvane na kartici vozača ili radionice koje se odnose na jedinice u vozilu kojima se koristi vlasnik kartice (zahtjevi 306 i 352 iz Priloga 1.C).

```
CardVehicleUnitsUsed ::= SEQUENCE {
   vehicleUnitPointerNewestRecord      INTEGER(0..NoOfCardVehicleUnitRecords-1),
   cardVehicleUnitRecords              SET SIZE(NoOfCardVehicleUnitRecords) OF
                                       CardVehicleUnitRecord
}
```

vehicleUnitPointerNewestRecord je indeks posljednjeg ažuriranog zapisa o jedinici u vozilu.
Dodjela vrijednosti: Broj koji odgovara brojniku zapisa o jedinici u vozilu, a započinje s „0" za prvu pojavu zapisâ o jedinici u vozilu u strukturi.
cardVehicleUnitRecords je niz zapisa koji sadržiju informacije o upotrijebljenim jedinicama u vozilima.

2.41. Certificate

Certifikat javnog ključa koji je izdalo certifikacijsko tijelo.
Prva generacija:

```
Certificate ::= OCTET STRING (SIZE(194))
```

Dodjela vrijednosti: digitalni potpis s djelomičnom obnovom CertificateContent u skladu s Dodatkom 11, „Zajednički sigurnosni mehanizmi": Potpis (128 bajtova) || preostali dio javnog ključa (58 bajtova) || oznaka certifikacijskog tijela (8 bajtova).
Druga generacija:

```
Certificate ::= OCTET STRING (SIZE(204..341))
```

Dodjela vrijednosti: Vidjeti Dodatak 11.

2.42. CertificateContent

Prva generacija:
(Jasni) sadržaj certifikata javnog ključa u skladu s Dodatkom 11, „Zajednički sigurnosni mehanizmi".

```
CertificateContent ::= SEQUENCE {
   certificateProfileIdentifier        INTEGER(0..255),
   certificationAuthorityReference     KeyIdentifier,
   certificateHolderAuthorisation      CertificateHolderAuthorisation,
   certificateEndOfValidity            TimeReal,
   certificateHolderReference          KeyIdentifier,
   publicKey                           PublicKey
}
```

certificateProfileIdentifier je verzija odgovarajućeg certifikata.
Dodjela vrijednosti: '01h' za ovu verziju.
certificationAuthorityReference označava certifikacijsko tijelo koje izdaje certifikat. Označava i javni ključ tog certifikacijskog tijela.
certificateHolderAuthorisation označava prava vlasnika certifikata.
certificateEndOfValidity je datum administrativnog isteka važenja certifikata.
certificateHolderReference označava vlasnika certifikata. Označava i njegov javni ključ.
publicKey je javni ključ potvrđen tim certifikatom.

2.43. CertificateHolderAuthorisation

Označava prava vlasnika certifikata.

```
CertificateHolderAuthorisation ::= SEQUENCE {
   tachographApplicationID             OCTET STRING(SIZE(6))
   equipmentType                       EquipmentType
}
```

Prva generacija:
tachographApplicationID je identifikator aplikacije za tahograf.
Dodjela vrijednosti: 'FFh' '54h' '41h' '43h' '48h' '4Fh'. Taj je AID vlasnički neregistrirani identifikator aplikacije u skladu s normom ISO/IEC 7816-5.
equipmentType je identifikacija vrste opreme za koju je namijenjen certifikat.
Dodjela vrijednosti: u skladu s vrstom podataka EquipmentType. Vrijednost je **0** ako je certifikat izdala država članica.
Druga generacija:
tachographApplicationID označava šest najvažnijih bajtova identifikatora aplikacije (AID) tahografske kartice druge generacije. AID za aplikaciju tahografske kartice naveden je u poglavlju 6.2.
Dodjela vrijednosti:'FF 53 4D 52 44 54'
equipmentType je identifikacija vrste opreme utvrđene za drugu generaciju za koju je namijenjen certifikat.
Dodjela vrijednosti: u skladu s vrstom podataka EquipmentType.

2.44. CertificateRequestID

Jedinstvena identifikacija zahtjeva za certifikat. Može se upotrebljavati i kao identifikacij a javnog ključa jedinice u vozilu ako serijski broj jedinice u vozilu za koju je ključ namijenjen nije poznat u trenutku generisanja certifikata.

```
CertificateRequestID ::= SEQUENCE{
   requestSerialNumber                 INTEGER(0..2^32-1),
   requestMonthYear                    BCDString(SIZE(2)),
   crIdentifier                        OCTET STRING(SIZE(1)),
   manufacturerCode                    ManufacturerCode
}
```

requestSerialNumber je serijski broj zahtjeva za certifikat, jedinstven za proizvođača i mjesec naveden u nastavu.
requestMonthYear je identifikacija mjeseca i godine zahtjeva za certifikat.
Dodjela vrijednosti: BCD kodiranje mjeseca (dvije karakteristik) i godine (zadnje dvije karakteristik).
crIdentifier je identifikator kojim se razlikuje zahtjev za certifikat od proširenog serijskog broja.
Dodjela vrijednosti: 'FFh'.
manufacturerCode je numerički kod proizvođača koji zahtijeva certifikat.

2.45. CertificationAuthorityKID

Identifikator javnog ključa certifikacijskog tijela (država članica ili evropsko certifikacijsko tijelo).

```
CertificationAuthorityKID ::= SEQUENCE{
    nationNumeric                   NationNumeric,
    nationAlpha                     NationAlpha,
    keySerialNumber                 INTEGER(0..255),
    additionalInfo                  OCTET STRING(SIZE(2)),
    caIdentifier                    OCTET STRING(SIZE(1))
}
```

nationNumeric je nacionalni brojčani kod certifikacijskog tijela.
nationAlpha je nacionalni alfanumerički kod certifikacijskog tijela.
keySerialNumber je serijski broj kojim se razlikuju različiti ključevi certifikacijskog tijela u slučaju promjene ključeva.
additionalInfo je dvobajtno polje za dodatne kodove (specifično za certifikacijsko tijelo).
caIdentifier je identifikator za razlikovanje identifikatora ključa certifikacijskog tijela od drugih identifikatora ključa.
Dodjela vrijednosti: '01h'.

2.46. CompanyActivityData

Informacije sačuvane na kartici preduzeća koje se odnose na aktivnosti izvršene s karticom (zahtjevi 373 i 379 iz Priloga 1.C).

```
CompanyActivityData ::= SEQUENCE {
    companyPointerNewestRecord      INTEGER(0..NoOfCompanyActivityRecords-1),
    companyActivityRecords          SET SIZE(NoOfCompanyActivityRecords) OF
      companyActivityRecord           SEQUENCE {
        companyActivityType             CompanyActivityType,
        companyActivityTime             TimeReal,
        cardNumberInformation           FullCardNumber,
        vehicleRegistrationInformation  VehicleRegistrationIdentification,
        downloadPeriodBegin             TimeReal,
        downloadPeriodEnd               TimeReal
      }
}
```

companyPointerNewestRecord je indeks posljednjeg ažuriranog zapisa companyActivityRecord.
Dodjela vrijednosti: Broj koji odgovara brojniku zapisa o aktivnosti preduzeća, a započinje s „0" za prvu pojavu zapisâ o aktivnosti preduzeća u strukturi.
companyActivityRecords je niz svih zapisa o aktivnosti preduzeća.
companyActivityRecord je niz informacija povezanih s jednom aktivnošću preduzeća.
companyActivityType je vrsta aktivnosti preduzeća.
companyActivityTime je datum i vrijeme provođenja aktivnosti preduzeća.
cardNumberInformation je broj kartice i država članica koja je izdala karticu s koje se preuzimaju podaci, ako postoji.
vehicleRegistrationInformation je VRN i država članica registracije vozila u kojemu je izvršeno preuzimanje podataka odnosno postavljanje ili uklanjanje blokade.
downloadPeriodBegin i **downloadPeriodEnd** su period za koje su preuzeti podaci iz jedinice u vozilu, ako postoje.

2.47. CompanyActivityType

Kod koji označava aktivnost koju sprovodi preduzeće upotrebom svoje kartice preduzeća.

```
CompanyActivityType ::= INTEGER {
    card downloading                (1),
    VU downloading                  (2),
    VU lock-in                      (3),
    VU lock-out                     (4)
}
```

2.48. CompanyCardApplicationIdentification

Informacije sačuvane na kartici preduzeća koje se odnose na identifikaciju primjene kartice (zahtjevi 369 i 375 iz Priloga 1.C).

```
CompanyCardApplicationIdentification ::= SEQUENCE {
    typeOfTachographCardId          EquipmentType,
    cardStructureVersion            CardStructureVersion,
    noOfCompanyActivityRecords      NoOfCompanyActivityRecords
}
```

typeOfTachographCardId označava vrstu upotrijebljene kartice.

cardStructureVersion utvrđuje verziju strukture koja je primijenjena na kartici.
noOfCompanyActivityRecords je broj zapisa o aktivnostima preduzeća koji se najviše može sačuvati na kartici.

2.49. CompanyCardHolderIdentification

Informacije sačuvane na kartici preduzeća koje se odnose na identifikaciju vlasnika kartice (zahtjevi 372 i 378 iz Priloga 1.C).

```
CompanyCardHolderIdentification ::= SEQUENCE {
   companyName                          Name,
   companyAddress                       Address,
   cardHolderPreferredLanguage          Language
}
```

companyName je naziv preduzeća vlasnika.
companyAddress je adresa preduzeća vlasnika.
cardHolderPreferredLanguage je odabrani jezik vlasnika kartice.

2.50. ControlCardApplicationIdentification

Informacije sačuvane na kontrolnoj kartici koje se odnose na identifikaciju primjene kartice (zahtjevi 357 i 363 iz Priloga 1.C).

```
ControlCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId               EquipmentType,
   cardStructureVersion                 CardStructureVersion,
   noOfControlActivityRecords           NoOfControlActivityRecords
}
```

typeOfTachographCardId označava vrstu upotrijebljene kartice.
cardStructureVersion utvrđuje verziju strukture koja je primijenjena na kartici.
noOfControlActivityRecords je broj zapisa o nadzornim aktivnostima koji se najviše može sačuvati na kartici.

2.51. ControlCardControlActivityData

Informacije sačuvane na kontrolnoj kartici koje se odnose na nadzorne aktivnosti izvršene s karticom (zahtjevi 361 i 367 iz Priloga 1.C).

```
ControlCardControlActivityData ::= SEQUENCE {
   controlPointerNewestRecord       INTEGER(0.. NoOfControlActivityRecords-1),
   controlActivityRecords           SET SIZE(NoOfControlActivityRecords) OF
    controlActivityRecord            SEQUENCE {
     controlType                      ControlType,
     controlTime                      TimeReal,
     controlledCardNumber             FullCardNumber,
     controlledVehicleRegistration    VehicleRegistrationIdentification,
     controlDownloadPeriodBegin       TimeReal,
     controlDownloadPeriodEnd         TimeReal
    }
}
```

controlPointerNewestRecord je indeks posljednjeg ažuriranog zapisa o nadzornim aktivnostima.
Dodjela vrijednosti: Broj koji odgovara brojniku zapisa o nadzornoj aktivnosti, a započinje s „0" za prvu pojavu zapisâ o nadzornoj aktivnosti u strukturi.
controlActivityRecords je niz svih zapisa o nadzornim aktivnostima.
controlActivityRecord jeniz informacija povezanih s jednom kontrolom.
controlType je vrsta kontrole.
controlTime je datum i vrijeme kontrole.
controlledCardNumber je broj kartice i država članica koja je izdala karticu koju se kontrolira.
controlledVehicleRegistration je VRN i država članica registracije vozila u kojem je provedena kontrola.
controlDownloadPeriodBegin i **controlDownloadPeriodEnd** su period za koje su eventualno preuzeti podaci.

2.52. ControlCardHolderIdentification

Informacije sačuvane na kontrolnoj kartici koje se odnose na identifikaciju vlasnika kartice (zahtjevi 360 i 366 iz Priloga 1.C).

```
ControlCardHolderIdentification ::= SEQUENCE {
   controlBodyName                      Name,
   controlBodyAddress                   Address,
   cardHolderName                       HolderName,
   cardHolderPreferredLanguage          Language
}
```

controlBodyName je naziv nadzornog tijela vlasnika kartice.
controlBodyAddress je adresa nadzornog tijela vlasnika kartice.
cardHolderName je prezime i ime (imena) vlasnika kontrolne kartice.
cardHolderPreferredLanguage je odabrani jezik vlasnika kartice.

2.53. ControlType

Kod koji označava aktivnosti sprovedene tokom kontrole. Ta se vrsta podataka odnosi na zahtjeve 126, 274, 299, 327 i 350 iz Priloga 1.C.

```
ControlType ::= OCTET STRING (SIZE(1))
```

Prva generacija:
Dodjela vrijednosti – oktetno poravnavanje: 'cvpdxxxx'B (8 bitova)

‘c’B preuzimanje podataka s kartice:
‘0’B: tokom ove nadzorne aktivnosti nisu preuzeti podaci s kartice,
‘1’B: tokom ove nadzorne aktivnosti preuzeti su podaci s kartice
‘v’B preuzimanje podataka s jedinice u vozilu:
‘0’B: tokom ove nadzorne aktivnosti nisu preuzeti podaci s jedinice u vozilu
‘1’B: tokom ove nadzorne aktivnosti preuzeti su podaci s jedinice u vozilu
‘p’B ispis:
‘0’B: tokom ove nadzorne aktivnosti nije bilo ispisa,
‘1’B: tokom ove nadzorne aktivnosti ispisani su podaci
‘d’B displej:
‘0’B: tokom ove nadzorne aktivnosti nije upotrijebljen displej,
‘1’B: tokom ove nadzorne aktivnosti upotrijebljen je displej
‘xxxx’B ne upotrebljava se.

Druga generacija:

Dodjela vrijednosti – oktetno poravnavanje: ‘cvpdexxx’B (8 bitova)

‘c’B preuzimanje podataka s kartice:
‘0’B: tokom ove nadzorne aktivnosti nisu preuzeti podaci s kartice,
‘1’B: tokom ove nadzorne aktivnosti preuzeti su podaci s kartice
‘v’B preuzimanje podataka s jedinice u vozilu:
‘0’B: tokom ove nadzorne aktivnosti nisu preuzeti podaci s jedinice u vozilu
‘1’B: tokom ove nadzorne aktivnosti preuzeti su podaci s jedinice u vozilu
‘p’B ispis:
‘0’B: tokom ove nadzorne aktivnosti nije bilo ispisa,
‘1’B: tokom ove nadzorne aktivnosti ispisani su podaci
‘d’B displej:
‘0’B: tokom ove nadzorne aktivnosti nije upotrijebljen displej,
‘1’B: tokom ove nadzorne aktivnosti upotrijebljen je displej
‘e’B provjera kalibriranja uz cestu:
‘0’B: tokom ove nadzorne aktivnosti nisu provjereni parametri kalibriranja,
‘1’B: tokom ove nadzorne aktivnosti provjereni su parametri kalibriranja
‘xxx’B RFU.

2.54. CurrentDateTime

Trenutni datum i vrijeme na uređaju za evidentiranje podataka.

```
CurrentDateTime ::= TimeReal
```

Dodjela vrijednosti: nije dodatno utvrđena.

2.55. CurrentDateTimeRecordArray

Druga generacija:

Trenutni datum i vrijeme te meta podaci kako se upotrebljavaju u postupku preuzimanja.

```
CurrentDateTimeRecordArray ::= SEQUENCE {
    recordType                  RecordType,
    recordSize                  INTEGER(1..65535),
    noOfRecords                 INTEGER(0..65535),
    records                     SET SIZE(noOfRecords) OF CurrentDateTime
}
```

recordType označava vrstu zapisa (CurrentDateTime). **Dodjela vrijednosti**: Vidjeti RecordType
recordSize je veličina podatka CurrentDateTime u bajtovima.
noOfRecords je broj zapisâ u nizu zapisa.
records je niz zapisa o trenutnom datumu i vremenu.

2.56. DailyPresenceCounter

Brojač pohranjen na kartici vozača ili radionice, uvećan za jedan za svaki kalendarski dan tokom kojeg je kartica bila umetnuta u jedinicu u vozilu. Ta se vrsta podataka odnosi na zahtjeve 266, 299, 320 i 343 iz Priloga 1.C.

```
DailyPresenceCounter ::= BCDString(SIZE(2))
```

Dodjela vrijednosti: Redni brojevi s najvećom vrijednošću = 9 999, zatim ponovno od 0. U trenutku prvog izdavanja kartice, broj je postavljen na 0.

2.57. Datef

Datum iskazan u brojčanom obliku spremnom za ispis.

```
Datef ::= SEQUENCE {
    year        BCDString(SIZE(2)),
    month       BCDString(SIZE(1)),
    day         BCDString(SIZE(1))
}
```

Dodjela vrijednosti:

gggg godina
mm mjesec
dd dan
‘00000000’H izričito označava da nema datuma.

2.58. DateOfDayDownloaded

Druga generacija:

Datum i vrijeme preuzimanja.

```
DateOfDayDownloaded ::= TimeReal
```

Dodjela vrijednosti: nije dodatno utvrđena.

2.59. DateOfDayDownloadedRecordArray

Druga generacija:

Datum i vrijeme preuzimanja te meta podaci kako se upotrebljavaju u postupku preuzimanja.

```
DateOfDayDownloadedRecordArray ::= SEQUENCE {
   recordType                    RecordType,
   recordSize                    INTEGER(1..65535),
   noOfRecords                   INTEGER(0..65535),
   records                       SET SIZE(noOfRecords) OF
                                 DateOfDayDownloaded
}
```

recordType označava vrstu zapisa (DateOfDayDownloaded). **Dodjela vrijednosti**: Vidjeti RecordType

recordSize je veličina podatka CurrentDateTime u bajtovima.

noOfRecords je broj zapisa u nizu zapisa.

records je niz zapisa o datumu i vremenu preuzimanja.

2.60. Distance

Prijeđena udaljenost (rezultat izračuna razlike između dviju vrijednosti na brojaču u vozilu, u kilometrima).

```
Distance ::= INTEGER(0..2^16-1)
```

Dodjela vrijednosti: Nepotpisani binarni broj. Vrijednost u kilometrima u radnom rasponu od 0 do 9 999 km

2.61. DriverCardApplicationIdentification

Informacije sačuvane na kartici vozača koje se odnose na identifikaciju primjene kartice (zahtjevi 253 i 278 iz Priloga 1.C).

Prva generacija:

```
DriverCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfEventsPerType                   NoOfEventsPerType,
   noOfFaultsPerType                   NoOfFaultsPerType,
   activityStructureLength             CardActivityLengthRange,
   noOfCardVehicleRecords              NoOfCardVehicleRecords,
   noOfCardPlaceRecords                NoOfCardPlaceRecords
}
```

typeOfTachographCardId označava vrstu upotrijebljene kartice.

cardStructureVersion utvrđuje verziju strukture koja je primijenjena na kartici.

noOfEventsPerType je broj događaja po vrsti događaja koji se najviše može sačuvati na kartici.

noOfFaultsPerType je broj kvarova po vrsti kvara koji se najviše može sačuvati na kartici.

activityStructureLength označava broj bajtova dostupnih za arhiviranje zapisa o aktivnostima.

noOfCardVehicleRecords je broj zapisa o vozilu koji se najviše može sačuvati na kartici.

noOfCardPlaceRecords je broj zapisa o mjestima koji se najviše može sačuvati na kartici.

Druga generacija:

„

```
DriverCardApplicationIdentification ::= SEQUENCE {
typeOfTachographCardId          EquipmentType,
cardStructureVersion            CardStructureVersion,
noOfEventsPerType               NoOfEventsPerType,
noOfFaultsPerType               NoOfFaultsPerType,
activityStructureLength         CardActivityLengthRange,
noOfCardVehicleRecords          NoOfCardVehicleRecords,
noOfCardPlaceRecords            NoOfCardPlaceRecords,
noOfGNSSADRecords               NoOfGNSSADRecords,
noOfSpecificConditionRecords    NoOfSpecificConditionRecords
noOfCardVehicleUnitRecords      NoOfCardVehicleUnitRecords
}
```

"

Uz podatkovne elemente navedene za prvu generaciju upotrebljavaju se i sljedeći:

noOfGNSSADRecords je broj zapisa GNSS-a o akumulisanom vremenu vožnje koji se najviše može arhivirati na kartici.

noOfSpecificConditionRecords je broj zapisa o posebnim uslovima koji se najviše može arhivirati na kartici.

n**oOfCardVehicleUnitRecords** je broj zapisa o korištenim jedinicama u vozilu koji se najviše može arhivirati na kartici."

2.62. DriverCardHolderIdentification

Informacije sačuvane na kartici vozača koje se odnose na identifikaciju vlasnika kartice (zahtjevi 256 i 281 iz Priloga 1.C).

```
DriverCardHolderIdentification ::= SEQUENCE {
   cardHolderName                  HolderName,
   cardHolderBirthDate             Datef,
   cardHolderPreferredLanguage     Language
}
```

cardHolderName je prezime i ime (imena) vlasnika kartice vozača.

cardHolderBirthDate je datum rođenja vlasnika kartice vozača.

cardHolderPreferredLanguage je odabrani jezik vlasnika kartice.

2.63. Rezervisano za buduću uporebu

Druga generacija:
Informacije u običnom tekstu i MAC koji je potrebno prenijeti s pomoću DSRC-a iz tahografa u uređaj za daljinsko ispitivanje (RI), više pojedinosti u Dodatku 11. dijelu B poglavlju 13.

```
DSRCSecurityData ::= SEQUENCE {
   tagLenthPlainText                    OCTET STRING(SIZE(2)),
   currentDateTime                      CurrentDateTime,
   counter                              INTEGER(0..2^4-1),
   vuSerialNumber                       VuSerialNumber,
   dSRCMKVersionNumber                  INTEGER(SIZE(1)),
   tagLengthMac                         OCTET STRING(SIZE(2)),
   mac                                  MAC
}
```

tagLength je dio koda DER-TLV, postavlja se na „81 10" (vidjeti Dodatak 11. dio B poglavlje 13.).
currentDateTime je trenutni datum i vrijeme jedinice u vozilu.
counter označava RTM poruke.
vuSerialNumber je serijski broj jedinice u vozilu.
dSRCMKVersionNumber je broj verzije DSRC glavnog ključa iz kojeg su dobiveni DSRC ključevi specifični za jedinicu u vozilu.
tagLengthMac je oznaka i dužina podatkovnog objekta MAC kao dio koda DER-TLV. Oznaka se postavlja na '8E', a dužinom se kodira dužina MAC-a u oktetima (vidjeti Dodatak 11. dio B. poglavlje 13.).
mac je MAC izračunan s pomoću RTM poruke (vidjeti Dodatak 11. dio B poglavlje 13.).

2.64. EGFCertificate

Druga generacija:
Certifikat javnog ključa spoljnog uređaja GNSS-a za uzajamnu autentifikaciju s jedinicom u vozilu. Struktura tog certifikata utvrđena je u Dodatku 11.

```
EGFCertificate ::= Certificate
```

2.65. EmbedderIcAssemblerId

Daje informacije o ugraditelju IC-a.

```
EmbedderIcAssemblerId ::= SEQUENCE{
   countryCode                          IA5String(SIZE(2)),
   moduleEmbedder                       BCDString(SIZE(2)),
   manufacturerInformation              OCTET STRING(SIZE(1))
}
```

countryCode je kod zemlje ugrađivača modula, a sastoji se od dva slova u skladu s normom ISO 3166.
moduleEmbedder označava ugrađivača modula.
manufacturerInformation za internu upotrebu proizvođača

2.66. EntryTypeDailyWorkPeriod

Kod za razlikovanje početka i kraja unosa mjesta dnevnog rada te uslova unosa.
Prva generacija

```
EntryTypeDailyWorkPeriod ::= INTEGER {
   Begin,  related time = card insertion time or time of entry          (0),
   End,    related time = card withdrawal time or time of entry        (1),
   Begin,  related time manually entered (start time)                  (2),
   End,    related time manually entered (end of work period)          (3),
   Begin,  related time assumed by VU                                  (4),
   End,    related time assumed by VU                                  (5)
}
```

Dodjela vrijednosti: u skladu s normom ISO/IEC8824-1.
Druga generacija

```
EntryTypeDailyWorkPeriod ::= INTEGER {
   Begin,  related time = card insertion time or time of entry          (0),
   End,    related time = card withdrawal time or time of entry        (1),
   Begin,  related time manually entered (start time)                  (2),
   End,    related time manually entered (end of work period)          (3),
   Begin,  related time assumed by VU                                  (4),
   End,    related time assumed by VU                                  (5),
   Begin,  related time based on GNSS data                             (6),
   End     related time based on GNSS data                             (7)
}
```

Dodjela vrijednosti: u skladu s normom ISO/IEC8824-1.

2.67. EquipmentType

Kod za razlikovanje različitih vrsta opreme za aplikaciju tahografa.

```
EquipmentType ::= INTEGER(0..255)
```

Prva generacija:

```
--Reserved                           (0),
--Driver Card                        (1),
--Workshop Card                      (2),
--Control Card                       (3),
--Company Card                       (4),
--Manufacturing Card                 (5),
--Vehicle Unit                       (6),
--Motion Sensor                      (7),
--RFU                                (8..255)
```

Dodjela vrijednosti: U skladu s normom ISO/IEC8824-1.
Vrijednost 0 rezervisana je za označivanje države članice ili Europe u certifikacijskom polju CHA.

Druga generacija:
Upotrebljavaju se jednake vrijednosti kao i u prvoj generaciji, uz sljedeće dodane vrijednosti:

```
--GNSS Facility                 (8),
--Remote Communication Module   (9),
--ITS Interface module          (10),
--Plague                        (11),--may be used in SealRecord
--M1/M1 Adapter                 (12),--may be used in SealRecord
--European Root CA (ERCA)       (13),
--Member State CA (MSCA)        (14),
--External GNSS connection      (15),--may be used in SealRecord
--Unused                        (16),--used in SealDataVu
--Driver Card (Sign)            (17),--only to be used in the CHA
                                field of a signing certificate
--Workshop Card (Sign)          (18), --only to be used in the CHA
                                field of a signing certificate
--Vehicle Unit (Sign)           (19), --only to be used in the CHA
                                field of a signing certificate
--RFU                           (20..255)
```

Napomena 1.: vrijednosti druge generacije koje se odnose na pločicu, adapter i priključak vanjskog GNSS-a, kao i vrijednosti prve generacije koje se odnose na jedinicu u vozilu i senzor kretanja mogu se upotrijebiti u SealRecord, ako je to primjenljivo.
Napomena 2.: u polju CardHolderAuthorisation (CHA) certifikata druge generacije vrijednosti (1), (2) i (6) tumače se na način da označavaju certifikat za uzajamnu autentifikaciju pripadajuće vrste opreme. Za označavanje pripadajućeg certifikata za stvaranje digitalnog potpisa moraju se koristiti vrijednosti (17), (18) ili (19).

2.68. EuropeanPublicKey

Prva generacija:
Evropski javni ključ.

```
EuropeanPublicKey ::= PublicKey
```

2.69. EventFaultRecordPurpose

Kod kojim se objašnjava zašto je zapisan određeni događaj ili kvar.

```
EventFaultRecordPurpose ::= OCTET STRING (SIZE(1))
```

Dodjela vrijednosti:

'00'H	jedan od deset najnovijih (ili posljednjih) događaja ili kvarova
'01'H	najduži događaj za deset zadnjih dana pojave
'02'H	jedan od pet najdužih događaja u zadnjih 365 dana
'03'H	zadnji događaj za deset zadnjih dana pojave
'04'H	najozbiljniji događaj za deset zadnjih dana pojave
'05'H	jedan od pet najozbiljnijih događaja u zadnjih 365 dana
'06'H	prvi događaj ili kvar do kojeg je došlo nakon zadnjeg kalibriranja
'07'H	aktivni/tekući događaj ili kvar
'08'H to '7F'H	RFU
'80'H to 'FF'H	specifično za proizvođača

2.70. EventFaultType

Kod kojim se određuje događaj ili kvar.

```
EventFaultType ::= OCTET STRING (SIZE(1))
```

Dodjela vrijednosti:

Prva generacija:

'0x'H	opšti događaji,
'00'H	nema podrobnijih podataka,
'01'H	umetanje nevažeće kartice,
'02'H	konflikt kartica,
'03'H	vremensko preklapanje,
'04'H	vožnja bez odgovarajuće kartice,
'05'H	umetanje kartice tokom vožnje,
'06'H	posljednja sesija rada s karticom nije ispravno zaključena,
'07'H	prekoračenje brzine,
'08'H	prekid napajanja,
'09'H	pogreška u podacima o kretanju,
'0A'H	proturječnost u kretanju vozila,
'0B' to '0F'H	RFU

'1x'H '10'H '11'H '12'H '13'H '14'H '15'H '16'H '17'H '18'H '19'H to '1F'H	događaji koji označuju pokušaje probijanja zaštite povezani s jedinicom u vozilu, nema podrobnijih podataka, neuspjela autentifikacija senzora kretanja, neuspjela autentifikacija tahografske kartice, neovlaštena promjena senzora kretanja, pogreška u integritetu podataka sačuvanih na kartici, pogreška u integritetu sačuvanih korisničkih podataka, pogreška pri unutarnjem prenosu podataka, neovlašteno otvaranje kućišta. neovlaštene preinake hardvera, RFU
'2x'H '20'H '21'H '22'H '23'H '24'H '25'H '26'H to '2F'H	događaji koji označuju pokušaje probijanja zaštite povezani sa senzorom nema podrobnijih podataka, neuspješna autentifikacija, pogreška u integritetu sačuvanih podataka, pogreška pri unutarnjem prenosu podataka, neovlašteno otvaranje kućišta. neovlaštene preinake hardvera, RFU
'3x'H '30'H '31'H '32'H '33'H '34'H '35'H '36'H to '3F'H	kvarovi uređaja za evidentiranje podataka, nema podrobnijih podataka, interni kvar jedinice u vozilu kvar pisača, kvar displeja, kvar pri preuzimanju, kvar senzora, RFU
'4x'H '40'H '41'H to '4F'H	kvarovi kartice, nema podrobnijih podataka, RFU
'50'H to '7F'H	RFU
'80'H to 'FF'H	specifično za proizvođača

Druga generacija:

'0x'H '00'H '01'H '02'H '03'H '04'H '05'H '06'H '07'H '08'H '09'H '0A'H '0B'H '0C'H '0D'H '0E'H '0F'H	opći događaji, nema podrobnijih podataka, umetanje nevažeće kartice, konflikt kartica, vremensko preklapanje, vožnja bez odgovarajuće kartice, umetanje kartice tokom vožnje, posljednja razmjena podataka s karticom koja nije ispravno zatvorena, prekoračenje brzine, prekid napajanja, greška u podacima o kretanju, konflikt u kretanju vozila, vremenski konflikt (GNSS u odnosu na unutarnji sat jedinice u vozilu), greška u komunikaciji s uređajem za komunikaciju na daljinu, izostanak podataka o položaju iz prijamnika GNSS-a, greška u komunikaciji s vanjskim uređajem GNSS-a, RFU,

'1x'H '10'H '11'H '12'H '13'H '14'H '15'H '16'H '17'H '18'H '19'H '1A'H '1B'H '1C'H to '1F'H	događaji koji označuju pokušaje probijanja zaštite povezani s jedinicom u vozilu, nema podrobnijih podataka, neuspjela autentifikacija senzora kretanja, neuspjela autentifikacija tahografske kartice, neovlaštena promjena senzora kretanja, pogreška u integritetu podataka arhivirani na kartici, pogreška u integritetu arhivirani korisničkih podataka, pogreška unutarnjeg prenosa podataka, neovlašteno otvaranje kućišta, neovlaštene preinake hardvera, otkrivanje neovlaštenog zahvata na GNSS-u, istekla je autentifikacija vanjskog uređaja GNSS-a, istekla je važnost certifikata vanjskog uređaja GNSS-a, RFU,
'2x'H '20'H '21'H '22'H '23'H '24'H '25'H '26'H to '2F'H	događaji koji označuju pokušaje probijanja zaštite povezani sa senzorom, nema podrobnijih podataka, neuspješna autentifikacija, pogreška u integritetu arhivirani podataka, pogreška unutarnjeg prenosa podataka, neovlašteno otvaranje kućišta, neovlaštene preinake hardvera, RFU,
'3x'H '30'H '31'H '32'H '33'H '34'H '35'H '36'H '37'H '38'H '39'H '3A'H to '3F'H	kvarovi uređaja za bilježenje podataka, nema podrobnijih podataka, interni kvar jedinice u vozilu, kvar pisača, kvar zaslona, kvar pri preuzimanju podataka, kvar senzora, unutarnji prijamnik GNSS-a, vanjski uređaj GNSS-a, uređaj za komunikaciju na daljinu, ITS sučelje, RFU,
'4x'H '40'H '41'H to '4F'H	kvarovi kartice, nema podrobnijih podataka, RFU,
'5x'H to '7F'H	RFU,
'80'H to 'FF'H	specifično za proizvođača.";

2.71. ExtendedSealIdentifier

Druga generacija:

proširenim identifikatorom plombe moguće je jedinstveno identifikovati plombu (zahtjev 401) iz Priloga I.C).

```
ExtendedSealIdentifier ::= SEQUENCE{
   manufacturerCode              OCTET STRING (SIZE(2)),
   sealIdentifier                OCTET STRING (SIZE(8))
}
```

manufacturerCode je kôd proizvođača plombe.

sealIdentifier je identifikator plombe jedinstven za proizvođača.

2.72. ExtendedSerialNumber

Jedinstvena identifikacija opreme. Može se upotrebljavati i kao identifikacija javnog ključa opreme.

Prva generacija:

```
ExtendedSerialNumber ::= SEQUENCE{
   serialNumber                  INTEGER(0..2^^-1),
   monthYear                     BCDString(SIZE(2)),
   type                          OCTET STRING(SIZE(1)),
   manufacturerCode              ManufacturerCode
}
```

serialNumber je serijski broj opreme, jedinstven za proizvođača, vrstu opreme te mjesec i godinu navedene u nastavu.

monthYear je identifikacija mjeseca i godine proizvodnje (ili dodjele serijskog broja).
Dodjela vrijednosti: BCD kodiranje mjeseca (dvije karakteristik) i godine (zadnje dvije karakteristik).
type je identifikator vrste opreme.
Dodjela vrijednosti: specifična za proizvođača, s rezervisanom vrijednošću „FFh"
manufacturerCode: numerički kod koji označava proizvođača homologirane opreme.
Druga generacija:

```
ExtendedSerialNumber ::= SEQUENCE{
   serialNumber                    INTEGER(0..2^32-1),
   monthYear                       BCDString(SIZE(2)),
   type                            EquipmentType,
   manufacturerCode                ManufacturerCode
}
```

serialNumber vidjeti prvu generaciju
monthYear vidjeti prvu generaciju
type označava vrstu opreme
manufacturerCode: vidjeti prvu generaciju.

2.73. FullCardNumber

Kod kojim se u potpunosti identifikuje tahografska kartica.

```
FullCardNumber ::= SEQUENCE {
   cardType                        EquipmentType,
   cardIssuingMemberState          NationNumeric,
   cardNumber                      CardNumber
}
```

cardType je vrsta tahografske kartice.
cardIssuingMemberState je kod države članice koja je izdala karticu.
cardNumber je broj kartice.

2.74. FullCardNumberAndGeneration

Druga generacija:
Kod kojim se u potpunosti identifikujeju tahografska kartica i njezina generacija.

```
FullCardNumberAndGeneration ::= SEQUENCE {
   fullCardNumber                  FullCardNumber,
   generation                      Generation
}
```

fullcardNumber označava tahografsku karticu.
generacija označava generaciju tahografske kartice koja se upotrebljava.

2.75. Generation

Druga generacija:
Označava generaciju tahografa koji se upotrebljava.

```
Generation ::= INTEGER(0..255)
```

Dodjela vrijednosti:
'00'H RFU
'01'H Prva generacija
'02'H Druga generacija
'03'H .. 'FF'H RFU

2.76. GeoCoordinates

Druga generacija:
Geografske koordinate kodirane su kao cijeli brojevi. Ti su cijeli brojevi višekratnici koda ±DDMM.M za zemljopisnu širinu i koda ±DDDMM.M za zemljopisnu dužinu. Ovdje ±DD odnosno ±DDD označava stupnjeve, a MM.M minute.

```
GeoCoordinates ::= SEQUENCE {
   latitude                        INTEGER(-90000..90001),
   longitude                       INTEGER(-180000..180001)
}
```

latitude je kodiran kao višestruke (faktor 10) prikaza ±DDMM.M.
longitude je kodiran kao višestruke (faktor 10) prikaza ±DDDMM.M.

2.77. GNSSAccuracy

Druga generacija:
Tačnost podataka o GNSS poziciji (definicija (eee)). Ta je tačnost kodirana kao cijeli broj i višestruke je (faktor 10) vrijednosti X.Y dobivene iz NMEA-ine rečenice GSA.

```
GNSSAccuracy ::= INTEGER(1..100)
```

2.78. GNSSAccumulatedDriving

Druga generacija:
informacije arhivirane na kartici vozača ili radionice koje se odnose na položaj vozila prema GNSS-u ako akumuliran period vožnje dostigne višekratnih tri sata (zahtjevi 306) i 354) iz Priloga I.C).

```
GNSSAccumulatedDriving ::= SEQUENCE {
   gnssADRecordNewestRecord        INTEGER(0..NoOfGNSSADRecords-1),
   gnssAccumulatedDrivingRecords   SET SIZE(NoOfGNSSADRecords) OF
                                   GNSSAccumulatedDrivingRecord
}
```

gnssADPointerNewestRecord je indeks posljednjeg ažuriranog zapisa GNSS-a o akumulisanom periodu vožnje.
Dodjela vrijednosti je broj koji odgovara brojniku zapisa GNSS-a o akumulisanom periodu vožnje, a započinje s ‚0' za prvu pojavu zapisâ GNSS-a o akumulisanom periodu vožnje u strukturi.
gnssAccumulatedDrivingRecords je niz zapisa koji sadržiju datum i vrijeme kada akumulisano periodu vožnje dostigne višekratnih tri sata te informacije o položaju vozila.

2.79. GNSSAccumulatedDrivingRecord

Druga generacija:
informacije arhivirane na kartici vozača ili radionice koje se odnose na položaj vozila prema GNSS-u ako akumulisano period vožnje dostigne višekratnik tri sata (zahtjevi 305) i 353) iz Priloga I.C)

```
GNSSAccumulatedDrivingRecord ::= SEQUENCE {
  timeStamp                 TimeReal,
  gnssPlaceRecord           GNSSPlaceRecord,
  vehicleOdometerValue      OdometerShort
}
```

timeStamp je datum i vrijeme kad akumulisano vrijeme vožnje dostiže višekratnik tri sata.
gnssPlaceRecord sadrži informacije o položaju vozila.
vehicleOdometerValue je stanje brojača kilometara kad akumulisano vrijeme vožnje dostiže višekratnih tri sata.

2.80. GNSSPlaceRecord

Druga generacija:
Informacije o GNSS poziciji vozila (zahtjevi 108, 109, 110, 296, 305, 347 i 353 iz Priloga 1.C).

```
GNSSPlaceRecord ::= SEQUENCE {
  timeStamp                 TimeReal,
  gnssAccuracy              GNSSAccuracy,
  geoCoordinates            GeoCoordinates
}
```

timeStamp je datum i vrijeme utvrđivanja GNSS pozicije vozila.
gnssAccuracy je tačnost podataka o GNSS poziciji.
geoCoordinates je lokacija zabilježena s pomoću GNSS-a.

2.81. HighResOdometer

Vrijednost na brojaču kilometara vozila: Ukupna udaljenost koju je vozilo prošlo za vrijeme rada.

```
HighResOdometer ::= INTEGER(0..2^32-1)
```

Dodjela vrijednosti: Nepotpisani binarni broj. Vrijednost u 1/200 km u radnom rasponu od 0 do 21 055 406 km

2.82. HighResTripDistance

Udaljenost prijeđena tokom cijelog putovanja ili nekog dijela putovanja.

```
HighResTripDistance ::= INTEGER(0..2^32-1)
```

Dodjela vrijednosti: Nepotpisani binarni broj. Vrijednost u 1/200 km u radnom rasponu od 0 do 21 055 406 km

2.83. HolderName

Prezime i ime(na) vlasnika kartice.

```
HolderName ::= SEQUENCE {
  holderSurname             Name,
  holderFirstNames          Name
}
```

holderSurname je prezime vlasnika. U prezime se ne uključuju titule.
Dodjela vrijednosti: Ako se ne radi o osobnoj kartici, holderSurname sadrži jednake informacije sadržane u companyName ili workshopName ili controlBodyName.
holderFirstNames su ime (imena) i inicijali vlasnika.

2.84. InternalGNSSReceiver

Druga generacija:
Informacija o tome je li GNSS prijemnik unutarnji ili spoljni u odnosu na jedinicu u vozilu. TRUE znači da je GNSS prijemnik unutarnji u odnosu na jedinicu u vozilu. FALSE znači da je GNSS prijemnik spoljni.

```
InternalGNSSReceiver ::= BOOLEAN
```

2.85. K-ConstantOfRecordingEquipment

Konstanta uređaja za evidentiranje podataka (definicija (m)).

```
K-ConstantOfRecordingEquipment ::= INTEGER(0..2^16-1)
```

Dodjela vrijednosti: Broj impulsa po kilometru u radnom rasponu od 0 do 64 255 impulsa/km.

2.86. KeyIdentifier

Jedinstveni identifikator javnog ključa koji se upotrebljava pri navođenju i izboru ključa. Takođe identifikuje i nosioca ključa.

```
KeyIdentifier ::= CHOICE {
   extendedSerialNumber         ExtendedSerialNumber,
   certificateRequestID         CertificateRequestID,
   certificationAuthorityKID    CertificationAuthorityKID
}
```

Prvi izbor prikladan je za navođenje javnog ključa jedinice u vozilu, tahografske kartice ili vanjskog uređaja GNSS-a.
Drugi izbor prikladan je za navođenje javnog ključa jedinice u vozilu (u slučajevima u kojima u trenutku generisanja certifikata nije poznat serijski broj jedinice u vozilu).
Treći izbor prikladan je za navođenje javnog ključa države članice.

2.87. KMWCKey

Druga generacija:

AES ključ i verzija ključa povezana s njime koja se upotrebljava za uparivanje jedinice u vozilu i senzora kretanja. Više pojedinosti u Dodatku 11.

```
KMWCKey ::= SEQUENCE {
   kMWCKey                          AESKey,
   keyVersion                       INTEGER (SIZE(1))
}
```

kMWCKey je dužina AES ključa spojena s ključem koji se upotrebljava za uparivanje jedinice u vozilu i senzora kretanja.
keyVersion označava verziju AES ključa.

2.88. Language

Kod koji označava jezik.

```
Language ::= IA5String(SIZE(2))
```

Dodjela vrijednosti: Kodiranje s dva mala slova u skladu s normom ISO 639.

2.89. LastCardDownload

Datum i vrijeme posljednjeg preuzimanja podataka s kartice, sačuvani na kartici vozača (u svrhe drukčije od kontrole), zahtjevi 257 i 282 iz Priloga 1.C. Taj je datum moguće ažurirati s pomoću jedinice u vozilu ili bilo kojeg čitača kartica.

```
LastCardDownload ::= TimeReal
```

Dodjela vrijednosti: nije dodatno utvrđena.

2.90. LinkCertificate

Druga generacija:
Certifikat kojim se povezuju parovi ključeva glavnog evropskog certifikacijskog tijela.

```
LinkCertificate ::= Certificate
```

2.91. L-TyreCircumference

Djelatni opseg guma tačka (definicija (u)).

```
L-TyreCircumference ::= INTEGER(0..2^15-1)
```

Dodjela vrijednosti: Nepotpisan binarni broj, vrijednost u 1/8 mm u radnom rasponu od 0 do 8 031 mm.

„2.92. MAC

Druga generacija:
kriptografski kontrolni zbir dužine 8, 12 ili 16 bajtova koji odgovara sljedovima šifri utvrđenima u Dodatku 11.

```
MAC ::= CHOICE {
   Mac8                 OCTET STRING (SIZE(8)),
   Mac12                OCTET STRING (SIZE(12)),
   Mac16                OCTET STRING (SIZE(16)),
}
```

2.93. ManualInputFlag

Kod koji označava je li vlasnik kartice ručno unio aktivnosti vozača pri umetanju kartice ili nije (zahtjev 081 iz Priloga 1.B i zahtjev 102 iz Priloga 1.C).

```
ManualInputFlag ::= INTEGER {
   noEntry                          (0)
   manualEntries                    (1)
}
```

Dodjela vrijednosti: nije dodatno utvrđena.

2.94. ManufacturerCode

Kod koji označava proizvođača homologirane opreme.

```
ManufacturerCode ::= INTEGER(0..255)
```

Laboratorija nadležan za ispitivanja interoperabilnosti vodi i objavljuje popis šifri proizvođača na svojoj internetskoj stranici (zahtjev 454 iz Priloga 1.C).
ManufacturerCodes se privremeno dodjeljuju proizvođačima tahografske opreme na temelju zahtjeva upućenog laboratorijau nadležnom za ispitivanje interoperabilnosti.

2.95. ManufacturerSpecificEventFaultData

Druga generacija:
Kodovi pogrešaka specifični za proizvođača pojednostavnjuju analizu pogrešaka i održavanje jedinica u vozilu.

```
ManufacturerSpecificEventFaultData ::= SEQUENCE {
   manufacturerCode                 ManufacturerCode,
   manufacturerSpecificErrorCode    OCTET STRING(SIZE(3))
}
```

manufacturerCode označava proizvođača jedinice u vozilu.
manufacturerSpecificErrorCode je kod pogreške specifičan za proizvođača.

2.96. MemberStateCertificate

Certifikat javnog ključa države članice koji izdaje evropsko certifikacijsko tijelo.

```
MemberStateCertificate ::= Certificate
```

2.97. MemberStateCertificateRecordArray

Druga generacija:
Certifikat države članice i meta podaci kako se upotrebljavaju u postupku preuzimanja.

```
MemberStateCertificateRecordArray ::= SEQUENCE {
   recordType                       RecordType,
   recordSize                       INTEGER(1..65535),
   noOfRecords                      INTEGER(0..65535),
   records                          SET SIZE(noOfRecords) OF
                                    MemberStateCertificate
}
```

recordType označava vrstu zapisa (MemberStateCertificate). **Dodjela vrijednosti**: Vidjeti RecordType

recordSize je veličina podatka MemberStateCertificate u bajtovima.
noOfRecords je broj zapisâ u nizu zapisa. Vrijednost se postavlja na 1 jer certifikati mogu biti različitih dužina.
records je niz zapisa o certifikatima države članice.

2.98. MemberStatePublicKey

Prva generacija:
Javni ključ države članice.

```
MemberStatePublicKey ::= PublicKey
```

2.99. Name

Naziv.

```
Name ::= SEQUENCE {
   codePage                              INTEGER (0..255),
   name                                  OCTET STRING (SIZE(35))
}
```

codePage označava skup znakova definisanih u poglavlju 4.,
name je naziv kodiran s pomoću posebnog skupa znakova.

2.100. NationAlpha

Abecedna oznaka države mora biti u skladu s poznatim oznakama koje se upotrebljavaju na vozilima u međunarodnom prometu (Bečka konvencija Ujedinjenih naroda o drumskom prometu, 1968.)

```
NationAlpha ::= IA5String(SIZE(3))
```

Kodovi Nation Alpha i numerički (Numeric) kodovi održavaju se na popisu na internetskoj stranici laboratorijaa imenovanog za ispitivanje interoperabilnosti, kako je utvrđeno u zahtjevu 440 u Prilogu 1.C.

2.101. NationNumeric

Brojčana oznaka države.

```
NationNumeric ::= INTEGER(0 .. 255)
```

Dodjela vrijednosti: vidjeti vrstu podatka 2.100 (NationAlpha).
Specifikaciju Nation Alpha ili Numeric, opisanu u prethodnom stavu, može se izmijeniti ili ažurirati samo nakon što je imenovani laboratorija dobio stajališta proizvođača homologovanih digitalnih i pametnih tahografa (jedinice u vozilu).

2.102. NoOfCalibrationRecords

Broj zapisa o kalibriranju koji se najviše može sačuvati na kartici radionice.
Prva generacija:

```
NoOfCalibrationRecords ::= INTEGER(0..255)
```

Dodjela vrijednosti: vidjeti Dodatak 2.
Druga generacija:

```
NoOfCalibrationRecords ::= INTEGER(0..2^16-1)
```

Dodjela vrijednosti: vidjeti Dodatak 2.

2.103. NoOfCalibrationsSinceDownload

Brojač koji označava broj kalibriranja provedenih s karticom radionice od posljednjeg preuzimanja podataka s nje (zahtjevi 317 i 340 u Prilogu 1.C).

```
NoOfCalibrationsSinceDownload ::= INTEGER(0..2^16-1)
```

Dodjela vrijednosti: nije dodatno utvrđena.

2.104. NoOfCardPlaceRecords

Broj zapisa o mjestu koji se najviše može sačuvati na kartici vozača ili radionice.
Prva generacija:

```
NoOfCardPlaceRecords ::= INTEGER(0..255)
```

Dodjela vrijednosti: vidjeti Dodatak 2.
Druga generacija:

```
NoOfCardPlaceRecords ::= INTEGER(0..2^16-1)
```

Dodjela vrijednosti: vidjeti Dodatak 2.

2.105. NoOfCardVehicleRecords

Broj zapisa o korištenim vozilima koji se najviše može sačuvati na kartici vozača ili radionice.

```
NoOfCardVehicleRecords ::= INTEGER(0.. 2^16-1)
```

Dodjela vrijednosti: vidjeti Dodatak 2.

2.106. NoOfCardVehicleUnitRecords

Druga generacija:
Broj zapisa o korištenim jedinicama u vozilu koji se najviše može sačuvati na kartici vozača ili radionice.

```
NoOfCardVehicleUnitRecords ::= INTEGER(0.. 2^16-1)
```

Dodjela vrijednosti: vidjeti Dodatak 2.

2.107. NoOfCompanyActivityRecords

Broj zapisa o aktivnostima preduzeća koji se najviše može sačuvati na kartici preduzeća.

```
NoOfCompanyActivityRecords ::= INTEGER(0.. 2^16-1)
```

Dodjela vrijednosti: vidjeti Dodatak 2.

2.108. NoOfControlActivityRecords

Broj zapisa o nadzornim aktivnostima koji se najviše može sačuvati na kontrolnoj kartici.

```
NoOfControlActivityRecords ::= INTEGER(0.. 2^16-1)
```

Dodjela vrijednosti: vidjeti Dodatak 2.

2.109. NoOfEventsPerType

Broj događaja po vrsti događaja koji se najviše može sačuvati na kartici.

```
NoOfEventsPerType ::= INTEGER(0..255)
```

Dodjela vrijednosti: vidjeti Dodatak 2.

2.110. NoOfFaultsPerType

Broj kvarova po vrsti kvara koji se najviše može sačuvati na kartici.

```
NoOfFaultsPerType ::= INTEGER(0..255)
```

Dodjela vrijednosti: vidjeti Dodatak 2.

2.111. NoOfGNSSADRecords

Druga generacija:

broj zapisa GNSS-a o akumulisanom periodu vožnje koji se najviše može arhivirati na kartici.

```
NoOfGNSSADRecords ::= INTEGER (0..2^16-1)
```

Dodjela vrijednosti: vidjeti Dodatak 2.

2.112. NoOfSpecificConditionRecords

Druga generacija:

Broj zapisa o posebnim uslovima koji se najviše može sačuvati na kartici.

```
NoOfSpecificConditionRecords ::= INTEGER(0..2^16-1)
```

Dodjela vrijednosti: vidjeti Dodatak 2.

2.113. OdometerShort

Vrijednost na brojaču kilometara vozila u kratkom obliku.

```
OdometerShort ::= INTEGER(0..2^24-1)
```

Dodjela vrijednosti: Nepotpisani binarni broj. Vrijednost u kilometrima u radnom rasponu od 0 do 9 999 999 km

2.114. OdometerValueMidnight

Vrijednost na brojaču kilometara vozila u ponoć na određeni dan (zahtjev 090 iz Priloga 1.B i zahtjev 113 iz Priloga 1.C).

```
OdometerValueMidnight ::= OdometerShort
```

Dodjela vrijednosti: nije dodatno utvrđena.

2.115. OdometerValueMidnightRecordArray

Druga generacija:

OdometerValueMidnight i meta podaci koji se upotrebljavaju u postupku preuzimanja.

```
OdometerValueMidnightRecordArray ::= SEQUENCE {
  recordType                      RecordType,
  recordSize                      INTEGER(1..65535),
  noOfRecords                     INTEGER(0..65535),
  records                         SET SIZE(noOfRecords) OF
                                  OdometerValueMidnight
}
```

recordType označava vrstu zapisa (OdometerValueMidnight). **Dodjela vrijednosti**: Vidjeti RecordType

recordSize je veličina podatka OdometerValueMidnight u bajtovima.

noOfRecords je broj zapisâ u nizu zapisa.

records je niz zapisa OdometerValueMidnight.

2.116. OverspeedNumber

Broj događaja prekoračenja brzine od posljednje kontrole u pogledu prekoračenja brzine.

```
OverspeedNumber ::= INTEGER(0..255)
```

Dodjela vrijednosti: Vrijednost 0 znači da od posljednje kontrole u pogledu prekoračenja brzine nije zabilježen nijedan događaj prekoračenja brzine, vrijednost 1 znači da je od posljednje kontrole u pogledu prekoračenja brzine zabilježen jedan događaj prekoračenja brzine, ⋯, vrijednost 255 znači da je od posljednje kontrole u pogledu prekoračenja brzine zabilježeno 255 ili više događaja prekoračenja brzine.

2.117. PlaceRecord

Informacije povezane s mjestom na kojem počinje ili završava period dnevnog rada (zahtjevi 108, 271, 296, 324 i 347 iz Priloga 1.C).

Prva generacija:

```
PlaceRecord ::= SEQUENCE {
  entryTime                       TimeReal,
  entryTypeDailyWorkPeriod        EntryTypeDailyWorkPeriod,
  dailyWorkPeriodCountry          NationNumeric,
  dailyWorkPeriodRegion           RegionNumeric,
  vehicleOdometerValue            OdometerShort
}
```

entryTime je datum i vrijeme povezani s unosom.

entryTypeDailyWorkPeriod je vrsta unosa.

dailyWorkPeriodCountry je unesena zemlja.

dailyWorkPeriodRegion je unesena regija.

vehicleOdometerValue je vrijednost na brojaču kilometara u trenutku unosa mjesta.

Druga generacija:

```
PlaceRecord ::= SEQUENCE {
  entryTime                       TimeReal,
  entryTypeDailyWorkPeriod        EntryTypeDailyWorkPeriod,
  dailyWorkPeriodCountry          NationNumeric,
  dailyWorkPeriodRegion           RegionNumeric,
  vehicleOdometerValue            OdometerShort,
  entryGNSSPlaceRecord            GNSSPlaceRecord
}
```

Uz one navedene za prvu generaciju upotrebljava se i sljedeća komponenta:

entryGNSSPlaceRecord je zabilježena lokacija i vrijeme.

2.118. PreviousVehicleInfo

Informacije koje se odnose na vozilo koje je vozač prethodno upotrebljavao pri umetanju kartice u jedinicu u vozilu (zahtjev 081 iz Priloga 1.B i zahtjev 102 iz Priloga 1.C).

Prva generacija:

```
PreviousVehicleInfo ::= SEQUENCE {
   vehicleRegistrationIdentification      VehicleRegistrationIdentification,
   cardWithdrawalTime                     TimeReal
}
```

vehicleRegistrationIdentification je VRN i država članica registracije vozila.

cardWithdrawalTime je datum i vrijeme uklanjanja kartice.

Druga generacija:

```
PreviousVehicleInfo ::= SEQUENCE {
   vehicleRegistrationIdentification      VehicleRegistrationIdentification,
   cardWithdrawalTime                     TimeReal,
   vuGeneration                           Generation
}
```

Uz podatkovne elemente navedene za prvu generaciju upotrebljava se i sljedeći:

vuGeneration označava generaciju jedinice u vozilu.

2.119. PublicKey

Prva generacija:

Javni RSA ključ.

```
PublicKey ::= SEQUENCE {
   rsaKeyModulus                          RSAKeyModulus,
   rsaKeyPublicExponent                   RSAKeyPublicExponent
}
```

rsaKeyModulus je modul para ključeva.

rsaKeyPublicExponent je javni eksponent para ključeva.

2.120. RecordType

Druga generacija:

Upućivanje na vrstu zapisa. Ta se vrsta podataka upotrebljava za RecordArrays.

```
RecordType ::= OCTET STRING(SIZE(1))
```

Dodjela vrijednosti:

'01'H	ActivityChangeInfo,
'02'H	CardSlotsStatus,
'03'H	CurrentDateTime,
'04'H	MemberStateCertificate,
'05'H	OdometerValueMidnight,
'06'H	DateOfDayDownloaded,
'07'H	SensorPaired,
'08'H	Signature,
'09'H	SpecificConditionRecord,
'0A'H	VehicleIdentificationNumber,
'0B'H	VehicleRegistrationNumber,
'0C'H	VuCalibrationRecord,
'0D'H	VuCardIWRecord,
'0E'H	VuCardRecord,
'0F'H	VuCertificate,
'10'H	VuCompanyLocksRecord,
'11'H	VuControlActivityRecord,
'12'H	VuDetailedSpeedBlock,
'13'H	VuDownloadablePeriod,
'14'H	VuDownloadActivityData,
'15'H	VuEventRecord,
'16'H	VuGNSSCDRecord,
'17'H	VuITSConsentRecord,
'18'H	VuFaultRecord,
'19'H	VuIdentification,
'1A'H	VuOverSpeedingEventRecord
'1B'H	VuPlaceDailyWorkPeriodRecord,
'1C'H	VuTimeAdjustmentGNSSRecord,
'1D'H	VuTimeAdjustmentRecord,
'1E'H	VuPowerSupplyInterruptionRecord,
'1F'H	SensorPairedRecord,
'20'H	SensorExternalGNSSCoupledRecord,
'21'H	RFU
'22'H to '7F'H	specifično za proizvođača
'80'H to 'FF'H	

2.121. RegionAlpha

Abecedna oznaka regije u određenoj zemlji.

```
RegionAlpha ::= IA5STRING(SIZE(3))
```

Prva generacija:

Dodjela vrijednosti:

```
'  '        No information available,
Spain:
'AN '       Andalucía,
'AR '       Aragón,
'AST'       Asturias,
'C  '       Cantabria,
'CAT'       Cataluña,
'CL '       Castilla-León,
'CM '       Castilla-La-Mancha,
'CV '       Valencia,
'EXT'       Extremadura,
'G  '       Galicia,
'IB '       Baleares,
'IC '       Canarias,
'LR '       La Rioja,
'M  '       Madrid,
'MU '       Murcia,
'NA '       Navarra,
'PV '       Pais Vasco
```

Druga generacija:
Kodovi RegionAlpha održavaju se na popisu na internetskoj stranici laboratorijaa imenovanog za ispitivanje interoperabilnosti.

2.122. RegionNumeric

Brojčana oznaka regije u određenoj zemlji.

```
RegionNumeric ::= OCTET STRING (SIZE(1))
```

Prva generacija:

Dodjela vrijednosti:

```
'00'H       No information available,
Spain:
'01'H       Andalucía,
'02'H       Aragón,
'03'H       Asturias,
'04'H       Cantabria,
'05'H       Cataluña,
'06'H       Castilla-León,
'07'H       Castilla-La-Mancha,
'08'H       Valencia,
'09'H       Extremadura,
'0A'H       Galicia,
'0B'H       Baleares,
'0C'H       Canarias,
'0D'H       La Rioja,
'0E'H       Madrid,
'0F'H       Murcia,
'10'H       Navarra,
'11'H       Pais Vasco
```

Druga generacija:
Kodovi RegionNumeric održavaju se na popisu na internetskoj stranici laboratorijaa imenovanog za ispitivanje interoperabilnosti.

2.123. RemoteCommunicationModuleSerialNumber

Druga generacija:
Serijski broj modula za komunikaciju na daljinu.

```
RemoteCommunicationModuleSerialNumber ::= ExtendedSerialNumber
```

2.124. RSAKeyModulus

Prva generacija:
Modul RSA para ključeva.

```
RSAKeyModulus ::= OCTET STRING (SIZE(128))
```

Dodjela vrijednosti: Neodređeno.

2.125. RSAKeyPrivateExponent

Prva generacija:
Privatni eksponent RSA para ključeva.

```
RSAKeyPrivateExponent ::= OCTET STRING (SIZE(128))
```

Dodjela vrijednosti: Neodređeno.

2.126. RSAKeyPublicExponent

Prva generacija:
Javni eksponent RSA para ključeva.

```
RSAKeyPublicExponent ::= OCTET STRING (SIZE(8))
```

Dodjela vrijednosti: Neodređeno.

2.127. RtmData

Druga generacija:
Za definiciju ove vrste podataka vidjeti Dodatak 14.

2.128. SealDataCard

Druga generacija:
U ovoj su vrsti podataka sačuvane informacije o plombama stavljenima na različite sastavne dijelove vozila i namijenjene pohranjivanju na kartici. Ova se vrsta podataka odnosi na zahtjev 337 iz Priloga 1.C.

```
SealDataCard ::= SEQUENCE {
   noOfSealRecords                  INTEGER(1..5),
   sealRecords                      SET SIZE(noOfSealRecords) OF SealRecord
}
```

noOfSealRecords je broj zapisâ u sealRecords.
sealRecords je niz zapisa o plombi.

2.129. SealDataVu

Druga generacija:
U ovoj su vrsti podataka sačuvane informacije o plombama stavljenima na različite sastavne dijelove vozila i namijenjene pohranjivanju u jedinici u vozilu.

```
SealDataVu ::= SEQUENCE SIZE(5) OF {
   sealRecords                      SealRecord
}
```

sealRecords je niz zapisa o plombi. Ako je dostupno manje od pet plombi, vrijednost EquipmentType svih neiskorištenih sealRecords postavlja se na 16, odnosno na Unused (neiskorišteno).

2.130. SealRecord

Druga generacija:
U ovoj se vrsti podataka arhiviraju informacije o plombi koja se stavlja na određeni sastavni dio. Ova se vrsta podataka odnosi na zahtjev 337 iz Priloga 1.C.

```
SealRecord ::= SEQUENCE {
   equipmentType                    EquipmentType,
   extendedSealIdentifier           ExtendedSealIdentifier
}
```

equipmentType označava vrstu opreme na koju je stavljena plomba.
extendedSealIdentifier je identifikator plombe stavljene na opremu.

2.131. SensorApprovalNumber

Homologacijski broj senzora.
Prva generacija:

```
SensorApprovalNumber ::= IA5String(SIZE(8))
```

Dodjela vrijednosti: Neodređeno.
Druga generacija:

```
SensorApprovalNumber ::= IA5String(SIZE(16))
```

Dodjela vrijednosti:
Homologacijski broj daje se u skladu s onime objavljenim na odgovarajućoj internetskoj stranici Evropske komisije, odnosno, na primjer, uključujući spojnice ako postoje. Homologacijski broj mora biti lijevo poravnat.

2.132. SensorExternalGNSSApprovalNumber

Druga generacija:
Homologacijski broj spoljnog uređaja GNSS-a.

```
SensorExternalGNSSApprovalNumber ::= IA5String(SIZE(16))
```

Dodjela vrijednosti:
Homologacijski broj daje se u skladu s onime objavljenim na odgovarajućoj internetskoj stranici Evropske komisije, odnosno, na primjer, uključujući spojnice ako postoje. Homologacijski broj mora biti lijevo poravnat.

2.133. SensorExternalGNSSCoupledRecord

Druga generacija:
Informacije sačuvane u jedinici u vozilu koje se odnose na identifikaciju spoljnog uređaja GNSS-a uparenog s jedinicom u vozilu (zahtjev 100 iz Priloga 1.C).

```
SensorExternalGNSSCoupledRecord ::= SEQUENCE {
   sensorSerialNumber               SensorGNSSSerialNumber,
   sensorApprovalNumber             SensorExternalGNSSApprovalNumber,
   sensorCouplingDate               SensorGNSSCouplingDate
}
```

sensorSerialNumber je serijski broj spoljnog uređaja GNSS-a uparenog s jedinicom u vozilu.
sensorApprovalNumber je homologacijski broj tog spoljnog uređaja GNSS-a.
sensorCouplingDate je datum uparivanja tog spoljnog uređaja GNSS-a s jedinicom u vozilu.

2.134. SensorExternalGNSSIdentification

Druga generacija:
Informacije koje se odnose na identifikaciju spoljnog uređaja GNSS-a (zahtjev 98 iz Priloga 1.C).

```
SensorExternalGNSSIdentification ::= SEQUENCE {
   sensorSerialNumber               SensorGNSSSerialNumber,
   sensorApprovalNumber             SensorExternalGNSSApprovalNumber,
   sensorSCIdentifier               SensorExternalGNSSSCIdentifier,
   sensorOSIdentifier               SensorExternalGNSSOSIdentifier
}
```

sensorSerialNumber je proširen serijski broj spoljnog uređaja GNSS-a.
sensorApprovalNumber je homologacijski broj spoljnog uređaja GNSS-a.
sensorSCIdentifier je identifikator sigurnosne komponente spoljnog uređaja GNSS-a.
sensorOSIdentifier je identifikator operativnog sistema spoljnog uređaja GNSS-a.

2.135. SensorExternalGNSSInstallation

Druga generacija:
Informacije sačuvane u spoljnom uređaju GNSS-a koje se odnose na ugradnju senzora spoljnog uređaja GNSS-a (zahtjev 123 iz Priloga 1.C).

```
SensorExternalGNSSInstallation ::= SEQUENCE {
   sensorCouplingDateFirst              SensorGNSSCouplingDate,
   firstVuApprovalNumber                VuApprovalNumber,
   firstVuSerialNumber                  VuSerialNumber,
   sensorCouplingDateCurrent            SensorGNSSCouplingDate,
   currentVuApprovalNumber              VuApprovalNumber,
   currentVUSerialNumber                VuSerialNumber
}
```

sensorCouplingDateFirst je datum prvog uparivanja spoljnog uređaja GNSS-a s jedinicom u vozilu.
firstVuApprovalNumber je homologacijski broj prve jedinice u vozilu uparene s spoljnim uređajem GNSS-a.
firstVuSerialNumber je serijski broj prve jedinice u vozilu uparene s spoljnim uređajem GNSS-a.
sensorCouplingDateCurrent je datum trenutnog uparivanja spoljnog uređaja GNSS-a s jedinicom u vozilu.
currentVuApprovalNumber jehomologacijski broj jedinice u vozilu koja je trenutno uparena s spoljnim uređajem GNSS-a.
currentVuSerialNumber je serijski broj jedinice u vozilu koja je trenutno uparena s spoljnim uređajem GNSS-a.

2.136. SensorExternalGNSSOSIdentifier

Druga generacija:
Identifikator operativnog sistema spoljnog uređaja GNSS-a.

```
SensorOSIdentifier ::= IA5String(SIZE(2))
```

Dodjela vrijednosti: specifična za proizvođača.

2.137. SensorExternalGNSSSCIdentifier

Druga generacija:
Ova se vrsta upotrebljava, na primjer, za identifikaciju kriptografskog modula spoljnog uređaja GNSS-a.
Identifikator sigurnosne komponente spoljnog uređaja GNSS-a.

```
SensorExternalGNSSSCIdentifier ::= IA5String(SIZE(8))
```

Dodjela vrijednosti: specifična za proizvođača komponente.

2.138. SensorGNSSCouplingDate

Druga generacija:
Datum uparivanja spoljnog uređaja GNSS-a s jedinicom u vozilu.

```
SensorGNSSCouplingDate ::= TimeReal
```

Dodjela vrijednosti: Neodređeno.

2.139. SensorGNSSSerialNumber

Druga generacija:
Ova se vrsta upotrebljava za arhiviranje serijskog broja prijemnika GNSS-a i kad je u jedinici u vozilu i kad je izvan jedinice u vozilu.
Serijski broj prijemnika GNSS-a.

```
SensorGNSSSerialNumber ::= ExtendedSerialNumber
```

2.140. SensorIdentification

Informacije sačuvane u senzoru kretanja koje se odnose na identifikaciju senzora kretanja (zahtjev 077 iz Priloga 1.B i zahtjev 95 iz Priloga 1.C).

```
SensorIdentification ::= SEQUENCE {
   sensorSerialNumber                   SensorSerialNumber,
   sensorApprovalNumber                 SensorApprovalNumber,
   sensorSCIdentifier                   SensorSCIdentifier,
   sensorOSIdentifier                   SensorOSIdentifier
}
```

sensorSerialNumber je proširena serijski broj senzora kretanja (uključuje kataloški broj i šifru proizvođača).
sensorApprovalNumber je homologacijski broj senzora kretanja.
sensorSCIdentifier je identifikator sigurnosne komponente senzora kretanja.
sensorOSIdentifier je identifikator operativnog sistema senzora kretanja.

2.141. SensorInstallation

Informacije sačuvane u senzoru kretanja koje se odnose na ugradnju senzora kretanja (zahtjev 099 iz Priloga 1.B i zahtjev 122 iz Priloga 1.C).

```
SensorInstallation ::= SEQUENCE {
   sensorPairingDateFirst               SensorPairingDate,
   firstVuApprovalNumber                VuApprovalNumber,
   firstVuSerialNumber                  VuSerialNumber,
   sensorPairingDateCurrent             SensorPairingDate,
   currentVuApprovalNumber              VuApprovalNumber,
   currentVUSerialNumber                VuSerialNumber
}
```

ssensorPairingDateFirst je datum prvog uparivanja senzora kretanja s jedinicom u vozilu.

firstVuApprovalNumber je homologacijski broj prve jedinice u vozilu uparene sa senzorom kretanja.
firstVuSerialNumber je serijski broj prve jedinice u vozilu uparene sa senzorom kretanja.
sensorPairingDateCurrent je datum trenutnog uparivanja senzora kretanja s jedinicom u vozilu.
currentVuApprovalNumber je homologacijski broj jedinice u vozilu trenutno uparene sa senzorom kretanja.
currentVuSerialNumber je serijski broj jedinice u vozilu trenutno uparene sa senzorom kretanja.

2.142. SensorInstallationSecData

Informacije sačuvane na kartici radionice koje se odnose na sigurnosne podatke potrebne za uparivanje senzora kretanja s jedinicama u vozilu (zahtjevi 308 i 331 iz Priloga 1.C).
Prva generacija:

```
SensorInstallationSecData ::= TdesSessionKey
```

Dodjela vrijednosti: u skladu s normom ISO 16844-3.
Druga generacija:
Kako je opisano u Dodatku 11., na kartici radionice arhiviraju se najviše tri ključa za uparivanje jedinice u vozilu i senzora kretanja. Ti ključevi imaju različite verzije ključa.

```
SensorInstallationSecData ::= SEQUENCE {
   kMWCKey1                    KMWCKey,
   kMWCKey2                    KMWCKey OPTIONAL,
   kMWCKey3                    KMWCKey OPTIONAL
}
```

2.143. SensorOSIdentifier

Identifikator operativnog sistema senzora kretanja.

```
SensorOSIdentifier ::= IA5String(SIZE(2))
```

Dodjela vrijednosti: specifična za proizvođača.

2.144. SensorPaired

Prva generacija:
Informacije sačuvane u jedinici u vozilu koje se odnose na identifikaciju senzora kretanja uparenog s jedinicom u vozilu (zahtjev 079 iz Priloga 1.B).

```
SensorPaired ::= SEQUENCE {
   sensorSerialNumber          SensorSerialNumber,
   sensorApprovalNumber        SensorApprovalNumber,
   sensorPairingDateFirst      SensorPairingDate
}
```

sensorSerialNumber jeserijski broj senzora kretanja trenutno uparenog s jedinicom u vozilu.
sensorApprovalNumber je homologacijski broj senzora kretanja trenutno uparenog s jedinicom u vozilu.
sensorPairingDateFirst je datum prvog uparivanja jedinice u vozilu i senzora kretanja koji je trenutno uparen s jedinicom u vozilu.

2.145. SensorPairedRecord

Druga generacija:
Informacije sačuvane u jedinici u vozilu koje se odnose na identifikaciju senzora kretanja uparenog s jedinicom u vozilu (zahtjev 97 iz Priloga 1.C).

```
SensorPairedRecord ::= SEQUENCE {
   sensorSerialNumber          SensorSerialNumber,
   sensorApprovalNumber        SensorApprovalNumber,
   sensorPairingDate           SensorPairingDate
}
```

sensorSerialNumber je serijski broj senzora kretanja uparenog s jedinicom u vozilu.
sensorApprovalNumber je homologacijski broj tog senzora kretanja.
sensorPairingDate je datum uparivanja tog senzora kretanja s jedinicom u vozilu.

2.146. SensorPairingDate

Datum uparivanja senzora kretanja s jedinicom u vozilu.

```
SensorPairingDate ::= TimeReal
```

Dodjela vrijednosti: Neodređeno.

2.147. SensorSCIdentifier

Identifikator sigurnosne komponente senzora kretanja.

```
SensorSCIdentifier ::= IA5String(SIZE(8))
```

Dodjela vrijednosti: specifična za proizvođača komponente.

2.148. SensorSerialNumber

Serijski broj senzora kretanja.

```
SensorSerialNumber ::= ExtendedSerialNumber
```

2.149. Signature

Digitalni potpis.
Prva generacija:

```
Signature ::= OCTET STRING (SIZE(128))
```

Dodjela vrijednosti: u skladu s Dodatkom 11., „Zajednički sigurnosni mehanizmi”.
Druga generacija:

```
Signature ::= OCTET STRING (SIZE(64..132))
```

Dodjela vrijednosti: u skladu s Dodatkom 11., „Zajednički sigurnosni mehanizmi”.

2.150. SignatureRecordArray

Druga generacija:
Niz potpisa i meta podaci koji se upotrebljavaju u postupku preuzimanja.

```
SignatureRecordArray ::= SEQUENCE {
   recordType                    RecordType,
   recordSize                    INTEGER(1..65535),
   noOfRecords                   INTEGER(0..65535),
   records                       SET SIZE(noOfRecords) OF Signature
}
```

recordType označava vrstu zapisa (Signature). **Dodjela vrijednosti**: Vidjeti RecordType
recordSize je veličina podatka Signature u bajtovima.
noOfRecords je broj zapisâ u nizu zapisa. Vrijednost se postavlja na 1 jer potpisi mogu biti različitih dužina.
records je niz potpisa.

2.151. SimilarEventsNumber

Broj sličnih događaja u određenom danu (zahtjev 094 iz Priloga 1.B i zahtjev 117 iz Priloga 1.C).

```
SimilarEventsNumber ::= INTEGER(0..255)
```

Dodjela vrijednosti: Vrijednost 0 se ne upotrebljava, vrijednost 1 znači da je tog dana zabilježen i pohranjen samo jedan događaj te vrste, vrijednost 2 znači da su tog dana zabilježena dva takva događaja (samo je jedan pohranjen), …, 255 znači da je toga dana zabilježeno 255 ili više takvih događaja.

2.152. SpecificConditionRecord

Informacije sačuvane na kartici vozača ili radionice ili u jedinici u vozilu koje se odnose na posebne uslove (zahtjevi 130, 276, 301, 328 i 355 iz Priloga 1.C).

```
SpecificConditionRecord ::= SEQUENCE {
   entryTime                     TimeReal,
   specificConditionType         SpecificConditionType
}
```

entryTime je datum i vrijeme unosa.
specificConditionType je kod koji označava poseban uvjet.

2.153. SpecificConditions

Informacije sačuvane na kartici vozača ili radionice ili u jedinici u vozilu koje se odnose na poseban uvjet (zahtjevi 131, 277, 302, 329 i 356 iz Priloga 1.C).
Druga generacija:

```
SpecificConditions ::= SEQUENCE {
   conditionPointerNewestRecord     INTEGER(0..NoOfSpecificConditionRecords-1),
   specificConditionRecords         SET SIZE(NoOfSpecificConditionRecords) OF
                                    SpecificConditionRecord
}
```

controlPointerNewestRecord je indeks posljednjeg ažuriranog zapisa o posebnim uslovima.
Dodjela vrijednosti: Broj koji odgovara brojniku zapisa o posebnim uslovima, a započinje s „0" za prvu pojavu zapisâ o posebnim uslovima u strukturi.
specificConditionRecords je niz zapisa koji sadržiju informacije o zabilježenim posebnim uslovima.

2.154. SpecificConditionType

Kod koji označava posebne uslove (zahtjevi 050b, 105a, 212a i 230a iz Priloga 1.B te zahtjev 62 iz Priloga 1.C).

```
SpecificConditionType ::= INTEGER(0..255)
```

Prva generacija:
Dodjela vrijednosti:
'00'H RFU
'01'H izvan područja primjene – početak
'02'H izvan područja primjene – kraj
'03'H vožnja trajektom/vozom
'04'H .. 'FF'H RFU
Druga generacija:
Dodjela vrijednosti:
'00'H RFU
'01'H izvan područja primjene – početak
'02'H izvan područja primjene – kraj
'03'H vožnja trajektom/vozom – početak
'04'H vožnja trajektom/vozom – kraj
'05'H .. 'FF'H RFU

2.155. Speed

Brzina vozila (km/h),

```
Speed ::= INTEGER(0..255)
```

Dodjela vrijednosti: Vrijednost u kilometrima po satu u radnom rasponu od 0 do 220 km/h.

2.156. SpeedAuthorised

Najviša dopuštena brzina vozila (definicija (hh)).

```
SpeedAuthorised ::= Speed
```

2.157. SpeedAverage

Prosječna brzina u prethodno određenom trajanju (km/h).

```
SpeedAverage ::= Speed
```

2.158. SpeedMax

Najviša brzina izmjerena u prethodno određenom trajanju.

```
SpeedMax ::= Speed
```

2.159. TachographPayload

Druga generacija:
Za definiciju ove vrste podataka vidjeti Dodatak 14.

2.160. Rezervisano za buduću upotrebu

Druga generacija:
Podaci iz tahografa šifrirani DER-TLV-om, odnosno podaci koji se šalju šifrirani u RTM poruci. Šifriranje je opisano u Dodatku 11. dijelu B. poglavlju 13.

```
TachographPayloadEncrypted ::= SEQUENCE {
   tag                                OCTET STRING(SIZE(1)),
   length                             OCTET STRING(SIZE(1..2)),
   paddingContentIndicatorByte        OCTET STRING(SIZE(1)),
   encryptedData                      OCTET STRING(SIZE(16..192))
}
```

tag je dio koda DER-TLV i postavlja se na „87” (vidjeti Dodatak 11. dio B poglavlje 13.).
length je dio koda DER-TLV i kodira dužinu vrijednosti paddingContentIndicatorByte i encryptedData navedenih u nastavu.
paddingContentIndicatorByte postavlja se na „00”.
encryptedData je šifrirani tachographPayload kako je utvrđeno u Dodatku 11. dijelu B poglavlju 13. Dužina tih podataka u oktetima uvijek je višestruke broja 16.

2.161. TDesSessionKey

Prva generacija:
Ključ trostrukog DES postupka.

```
TDesSessionKey ::= SEQUENCE {
   tDesKeyA                           OCTET STRING (SIZE(8)),
   tDesKeyB                           OCTET STRING (SIZE(8))
}
```

Dodjela vrijednosti: nije dodatno utvrđena.

2.162. TimeReal

Kod za polje s datumom i vremenom, pri čemu su datum i vrijeme izraženi kao sekunde prošle od 00h.00m.00s. na dan 1. siječnja 1970. UTC.

```
TimeReal (INTEGER:TimeRealRange) ::= INTEGER (0..TimeRealRange)
```

Dodjela vrijednosti – **oktetno poravnavanje**: broj sekundi prošlih od ponoći 1. januara 1970. UTC.
Datum i vrijeme ne mogu biti dalji od 2106. godine.

2.163. TyreSize

Oznaka dimenzija guma.

```
TyreSize ::= IA5String(SIZE(15))
```

Dodjela vrijednosti: u skladu s Direktivom 92/23 (EEZ) od 31.3.1992., SL L 129, str. 95.

2.164. VehicleIdentificationNumber

Identifikacijska oznaka vozila (VIN) koja se odnosi na cijelo vozilo, a uobičajeno se radi o serijskom broju šasije ili broju okvira.

```
VehicleIdentificationNumber ::= IA5String(SIZE(17))
```

Dodjela vrijednosti: Kako je definisana u normi ISO 3779.

2.165. VehicleIdentificationNumberRecordArray

Druga generacija:
Identifikacijska oznaka vozila i meta podaci kako se upotrebljavaju u postupku preuzimanja.

```
VehicleIdentificationNumberRecordArray ::= SEQUENCE {
   recordType                         RecordType,
   recordSize                         INTEGER(1..65535),
   noOfRecords                        INTEGER(0..65535),
   records                            SET SIZE(noOfRecords) OF
                                      VehicleIdentificationNumber
}
```

recordType označava vrstu zapisa (VehicleIdentificationNumber). **Dodjela vrijednosti**: Vidjeti RecordType
recordSize je veličina podatka VehicleIdentificationNumber u bajtovima.
noOfRecords je broj zapisâ u nizu zapisa.
records je niz zapisa o identifikacijskim brojevima vozila.

2.166. VehicleRegistrationIdentification

Identifikacija vozila, jedinstvena za Evropu (VRN i država članica).

```
VehicleRegistrationIdentification ::= SEQUENCE {
   vehicleRegistrationNation          NationNumeric,
   vehicleRegistrationNumber          VehicleRegistrationNumber
}
```

vehicleRegistrationNation je država u kojoj je vozilo registrirano.
vehicleRegistrationNumber je registracijski broj vozila (VRN).

2.167. VehicleRegistrationNumber

Registracijski broj vozila (VRN). Registracijski broj dodjeljuje tijelo nadležno za registraciju.

```
VehicleRegistrationNumber ::= SEQUENCE {
   codePage                           INTEGER (0..255),
   vehicleRegNumber                   OCTET STRING (SIZE(13))
}
```

codePage označava skup znakova definisan u poglavlju 4.,
vehicleRegNumber je VRN kodiran s pomoću posebnog skupa znakova.

Dodjela vrijednosti: Specifično za državu.

2.168. VehicleRegistrationNumberRecordArray

Druga generacija:

Registracijski broj vozila i meta podaci kako se upotrebljavaju u postupku preuzimanja.

```
VehicleRegistrationNumberRecordArray ::= SEQUENCE {
   recordType                    RecordType,
   recordSize                    INTEGER(1..65535),
   noOfRecords                   INTEGER(0..65535),
   records                       SET SIZE(noOfRecords) OF
                                 VehicleRegistrationNumber
}
```

recordType označava vrstu zapisa (VehicleRegistrationNumber). **Dodjela vrijednosti**: Vidjeti RecordType

recordSize je veličina podatka VehicleRegistrationNumber u bajtovima.

noOfRecords je broj zapisâ u nizu zapisa.

records je niz zapisa o registracijskim brojevima vozila.

2.169. VuAbility

Druga generacija:

Informacije sačuvane u jedinici u vozilu koje označuju mogu li se u jedinici u vozilu upotrebljavati tahografske kartice prve generacije (zahtjev 121 iz Priloga 1.C).

Dodjela vrijednosti – oktetno poravnavanje: 'xxxxxxxa' B (8 bitova)

Za sposobnost podržavanja kartica prve generacije:

'a'B sposobnost podržavanja tahografskih kartica prve generacije:
'0' B prva generacija je podržana,
'1' B prva generacija nije podržana,

'xxxxxxx'B RFU

2.170. VuActivityDailyData

Prva generacija:

Informacije sačuvane u jedinici u vozilu koje se odnose na izmjene aktivnosti i/ili izmjene stanja vožnje i/ili izmjene statusa kartice na određeni kalendarski dan (zahtjev 084 iz Priloga 1.B i zahtjevi 105, 106 i 107 iz Priloga 1.C) i na statuse otvora u 00:00 h tog dana.

```
VuActivityDailyData ::= SEQUENCE {
   noOfActivityChanges           INTEGER SIZE(0..1440),
   activityChangeInfos           SET SIZE(noOfActivityChanges) OF
                                 ActivityChangeInfo
}
```

noOfActivityChanges je broj riječi ActivityChangeInfo u nizu activityChangeInfos.

activityChangeInfos je niz riječi ActivityChangeInfo sačuvanih u jedinici u vozilu za određeni dan. Uvijek uključuje dvije riječi ActivityChangeInfo koje označuju status dvaju otvora u 00:00 h tog dana.

2.171. VuActivityDailyRecordArray

Druga generacija:

Informacije sačuvane u jedinici u vozilu koje se odnose na izmjene aktivnosti i/ili izmjene stanja vožnje i/ili izmjene statusa kartice na određeni kalendarski dan (zahtjevi 105, 106 i 107 iz Priloga 1.C) i na statuse otvora u 00:00 h tog dana.

```
VuActivityDailyRecordArray ::= SEQUENCE {
   recordType                    RecordType,
   recordSize                    INTEGER(1..65535),
   noOfRecords                   INTEGER(0..65535),
   records                       SET SIZE(noOfRecords) OF ActivityChangeInfo
}
```

recordType označava vrstu zapisa (ActivityChangeInfo). **Dodjela vrijednosti**: Vidjeti RecordType

recordSize je veličina podatka ActivityChangeInfo u bajtovima.

noOfRecords je broj zapisâ u nizu zapisa.

records je niz riječi ActivityChangeInfo sačuvanih u jedinici u vozilu za određeni dan. Uvijek uključuje dvije riječi ActivityChangeInfo koje označuju status dvaju otvora u 00:00 h tog dana.

2.172. VuApprovalNumber

Homologacijski broj jedinice u vozilu.

Prva generacija:

```
VuApprovalNumber ::= IA5String(SIZE(8))
```

Dodjela vrijednosti: Neodređeno.

Druga generacija:

```
VuApproValNumber ::= IA5String(SIZE(16))
```

Dodjela vrijednosti:

Homologacijski broj daje se u skladu s onime objavljenim na odgovarajućoj internetskoj stranici Evropske komisije, odnosno, na primjer, uključujući spojnice ako postoje. Homologacijski broj mora biti lijevo poravnat.

2.173. VuCalibrationData

Prva generacija:

Informacije sačuvane u jedinici u vozilu koje se odnose na kalibriranje uređaja za evidentiranje podataka (zahtjev 098 iz Priloga 1.B).

```
VuCalibrationData ::= SEQUENCE {
   noOfVuCalibrationRecords                INTEGER(0..255),
   vuCalibrationRecords                    SET SIZE(noOfVuCalibrationRecords) OF
                                           VuCalibrationRecord
}
```

noOfVuCalibrationRecords je broj zapisa koje sadrži niz vuCalibrationRecords.
vuCalibrationRecords je niz zapisa o kalibriranju.

2.174. VuCalibrationRecord

Informacije sačuvane u jedinici u vozilu koje se odnose na kalibriranje uređaja za evidentiranje podataka (zahtjev 098 iz Priloga 1.B i zahtjevi 119 i 120 iz Priloga 1.C).
Prva generacija:

```
VuCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                      CalibrationPurpose,
   workshopName                            Name,
   workshopAddress                         Address,
   workshopCardNumber                      FullCardNumber,
   workshopCardExpiryDate                  TimeReal,
   vehicleIdentificationNumber             VehicleIdentificationNumber,
   vehicleRegistrationIdentification       VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant          W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment           K-ConstantOfRecordingEquipment,
   lTyreCircumference                      L-TyreCircumference,
   tyreSize                                TyreSize,
   authorisedSpeed                         SpeedAuthorised,
   oldOdometerValue                        OdometerShort,
   newOdometerValue                        OdometerShort,
   oldTimeValue                            TimeReal,
   newTimeValue                            TimeReal,
   nextCalibrationDate                     TimeReal
}
```

calibrationPurpose je svrha kalibriranja.
workshopName, workshopAddress su naziv i adresa radionice.
workshopCardNumber označava karticu radionice upotrijebljenu tokom kalibriranja.
workshopCardExpiryDate je datum isteka važenja kartice.
vehicleIdentificationNumber je VIN.
vehicleRegistrationIdentification sadrži VRN i državu članicu registracije.
wVehicleCharacteristicConstant je karakteristični koeficijent vozila.
kConstantOfRecordingEquipment je konstanta uređaja za evidentiranje podataka.
lTyreCircumference je djelatni opseg guma tačka.
tyreSize je oznaka za dimenzije guma postavljenih na vozilo.
authorisedSpeed je odobrena brzina vozila.
oldOdometerValue, newOdometerValue su stare i nove vrijednosti na brojaču kilometara.
oldTimeValue, newTimeValue su stari i novi datum i vrijeme.
nextCalibrationDate je datum sljedećeg kalibriranja vrste utvrđene u podatku CalibrationPurpose koje sprovodi tijelo ovlašteno za pregled.
Druga generacija:

```
VuCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                      CalibrationPurpose,
   workshopName                            Name,
   workshopAddress                         Address,
   workshopCardNumber                      FullCardNumber,
   workshopCardExpiryDate                  TimeReal,
   vehicleIdentificationNumber             VehicleIdentificationNumber,
   vehicleRegistrationIdentification       VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant          W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment           K-ConstantOfRecordingEquipment,
   lTyreCircumference                      L-TyreCircumference,
   tyreSize                                TyreSize,
   authorisedSpeed                         SpeedAuthorised,
   oldOdometerValue                        OdometerShort,
   newOdometerValue                        OdometerShort,
   oldTimeValue                            TimeReal,
   newTimeValue                            TimeReal,
   nextCalibrationDate                     TimeReal,
   sealDataVu                              SealDataVu
}
```

Uz podatkovne elemente navedene za prvu generaciju upotrebljava se i sljedeći:
sealDataVu pruža informacije o plombama stavljenima na različite sastavne dijelove vozila.

2.175. VuCalibrationRecordArray

Druga generacija:
Informacije sačuvane u jedinici u vozilu koje se odnose na kalibriranje uređaja za evidentiranje podataka (zahtjevi 119 i 120 iz Priloga 1.C).

```
VuCalibrationRecordArray ::= SEQUENCE {
   recordType                              RecordType,
   recordSize                              INTEGER(1..65535),
   noOfRecords                             INTEGER(0..65535),
   records                                 SET SIZE(noOfRecords) OF
                                           VuCalibrationRecord
}
```

recordType označava vrstu zapisa (VuCalibrationRecord). **Dodjela vrijednosti**: Vidjeti RecordType
recordSize je veličina podatka VuCalibrationRecord u bajtovima.

noOfRecords je broj zapisâ u nizu zapisa.
records je niz zapisa o kalibriranju.

2.176. VuCardIWData

Prva generacija:
Informacije sačuvane u jedinici u vozilu koje se odnose na cikluse umetanja kartica vozača ili radionice u jedinicu u vozilu i cikluse uklanjanja tih kartica iz jedinice u vozilu (zahtjev 081 iz Priloga 1.B i zahtjev 103 iz Priloga 1.C).

```
VuCardIWData ::= SEQUENCE {
   noOfIWRecords                    INTEGER(0..2^8-1),
   vuCardIWRecords                  SET SIZE(noOfIWRecords) OF VuCardIWRecord
}
```

nnoOfIWRecords je broj zapisâ u nizu uCardIWRecords.
vuCardIWRecords je niz zapisa koji se odnose na cikluse umetanja kartice ili cikluse njezina uklanjanja.

2.177. VuCardIWRecord

Informacije sačuvane u jedinici u vozilu koje se odnose na ciklus umetanja kartice vozača ili radionice u jedinicu u vozilu i ciklus uklanjanja te kartice iz jedinice u vozilu (zahtjev 081 iz Priloga 1.B i zahtjev 102 iz Priloga 1.C).
Prva generacija:

```
VuCardIWRecord ::= SEQUENCE {
   cardHolderName                   HolderName,
   fullCardNumber                   FullCardNumber,
   cardExpiryDate                   TimeReal,
   cardInsertionTime                TimeReal,
   vehicleOdometerValueAtInsertion  OdometerShort,
   cardSlotNumber                   CardSlotNumber,
   cardWithdrawalTime               TimeReal,
   vehicleOdometerValueAtWithdrawal OdometerShort,
   previousVehicleInfo              PreviousVehicleInfo,
   manualInputFlag                  ManualInputFlag
}
```

cardHolderName su prezime i imena vlasnika kartice vozača ili radionice sačuvani na kartici.
fullCardNumber je vrsta kartice, država članica koja ju je izdala i broj kartice kako su sačuvani na kartici.
cardExpiryDate je datum isteka važenja kartice pohranjen na kartici.
cardInsertionTime je datum i vrijeme umetanja.
vehicleOdometerValueAtInsertion je stanje brojača kilometara vozila pri umetanju kartice.
cardSlotNumber je otvor u koji je kartica umetnuta.
cardWithdrawalTime je datum i vrijeme uklanjanja.
vehicleOdometerValueAtWithdrawal je stanje brojača kilometara vozila pri uklanjanju kartice.
previousVehicleInfo sadrži informacije o prethodnom vozilu koje je vozač koristio, kako su sačuvane na kartici.
manualInputFlag je znak kojim se označava je li vlasnik kartice ručno unio aktivnosti vozača pri umetanju kartice.
Druga generacija:

```
VuCardIWRecord ::= SEQUENCE {
   cardHolderName                   HolderName,
   fullCardNumberAndGeneration      FullCardNumberAndGeneration,
   cardExpiryDate                   TimeReal,
   cardInsertionTime                TimeReal,
   vehicleOdometerValueAtInsertion  OdometerShort,
   cardSlotNumber                   CardSlotNumber,
   cardWithdrawalTime               TimeReal,
   vehicleOdometerValueAtWithdrawal OdometerShort,
   previousVehicleInfo              PreviousVehicleInfo,
   manualInputFlag                  ManualInputFlag
}
```

Umjesto fullCardNumber, u podatkovnoj strukturi za drugu generaciju upotrebljava se sljedeći podatkovni element.
fullCardNumberAndGeneration je vrsta kartice, država članica koja ju je izdala te broj kartice i njezina generacija, kako su sačuvani na kartici.

2.178. VuCardIWRecordArray

Druga generacija:
Informacije sačuvane u jedinici u vozilu koje se odnose na cikluse umetanja kartica vozača ili radionice u jedinicu u vozilu i cikluse uklanjanja tih kartica iz jedinice u vozilu (zahtjev 103 iz Priloga 1.C).

```
VuCardIWRecordArray ::= SEQUENCE {
   recordType                       RecordType,
   recordSize                       INTEGER(1..65535),
   noOfRecords                      INTEGER(0..65535),
   records                          SET SIZE(noOfRecords) OF VuCardIWRecord
}
```

recordType označava vrstu zapisa (VuCardIWRecord). **Dodjela vrijednosti**: Vidjeti RecordType
recordSize je veličina podatka VuCardIWRecord u bajtovima.
noOfRecords je broj zapisâ u nizu zapisa.
records je niz zapisa koji se odnose na cikluse umetanja kartice ili cikluse njezina uklanjanja.

2.179. VuCardRecord

Druga generacija:
informacije arhivirane u jedinici u vozilu koje se odnose na korištenu karticu tahografa (zahtjev 132) iz Priloga I.C).

```
VuCardRecord ::= SEQUENCE {
cardNumberAndGenerationInformation      FullCardNumberAndGeneration,
cardExtendedSerialNumber                ExtendedSerialNumber,
cardStructureVersion                    CardStructureVersion,
cardNumber                              CardNumber
}
```

cardNumberAndGenerationInformation je potpuni broj kartice i generacija korištene kartice (vrsta podataka 2.74.).
cardExtendedSerialNumber očitan iz datoteke EF_ICC u MF-u kartice.
cardStructureVersion očitan iz datoteke EF_Application_Identification u DF_Tachograph_G2.
cardNumber očitan iz datoteke EF_Identification u DF_Tachograph_G2.

2.180. VuCardRecordArray

Druga generacija:
Informacije sačuvane u jedinici u vozilu koje se odnose na kartice tahografa korištene s tom jedinicom u vozilu. Te su informacije namijenjene analizi jedinice u vozilu - problemi s karticom (zahtjev 132 iz Priloga 1.C).

```
VuCardRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF VuCardRecord
}
```

recordType označava vrstu zapisa (VuCardRecord). **Dodjela vrijednosti**: Vidjeti RecordType
recordSize je veličina podatka VuCardRecord u bajtovima.
noOfRecords je broj zapisâ u nizu zapisa.
records je niz zapisa koji se odnose na tahografske kartice korištene s tom jedinicom u vozilu.

2.181. VuCertificate

Certifikat javnog ključa jedinice u vozilu.

```
VuCertificate ::= Certificate
```

2.182. VuCertificateRecordArray

Druga generacija:
Certifikat jedinice u vozilu i meta podaci kako se upotrebljavaju u postupku preuzimanja.

```
VuCertificateRecordArray ::= SEQUENCE {
   recordType                       RecordType,
   recordSize                       INTEGER(1..65535),
   noOfRecords                      INTEGER(0..65535),
   records                          SET SIZE(noOfRecords) OF VuCertificate
}
```

recordType označava vrstu zapisa (VuCertificate). **Dodjela vrijednosti**: Vidjeti RecordType
recordSize je veličina podatka VuCertificate u bajtovima.
noOfRecords je broj zapisâ u nizu zapisa. Vrijednost se postavlja na 1 jer certifikati mogu biti različitih dužina.
records je niz zapisa o certifikatima jedinice u vozilu.

2.183. VuCompanyLocksData

Prva generacija:
Informacije sačuvane u jedinici u vozilu koje se odnose na blokade od strane preduzeća (zahtjev 104 iz Priloga 1.B).

```
VuCompanyLocksData ::= SEQUENCE {
   noOfLocks                        INTEGER(0..255),
   vuCompanyLocksRecords            SET SIZE(noOfLocks) OF VuCompanyLocksRecord
}
```

noOfLocks jebroj blokada navedenih u podatku vuCompanyLocksRecords.
vuCompanyLocksRecords je niz zapisa o blokadama od strane preduzeća.

2.184. VuCompanyLocksRecord

Informacije sačuvane u jedinici u vozilu koje se odnose na jednu blokadu od strane preduzeća (zahtjev 104 iz Priloga 1.B i zahtjev 128 iz Priloga 1.C).
Prva generacija:

```
VuCompanyLocksRecord ::= SEQUENCE {
   lockInTime                       TimeReal,
   lockOutTime                      TimeReal,
   companyName                      Name,
   companyAddress                   Address,
   companyCardNumber                FullCardNumber
}
```

lockInTime, lockOutTime su datum i vrijeme postavljanja i uklanjanja blokade.
companyName, companyAddress su naziv i adresa preduzeća povezanog s postavljanjem blokade.
companyCardNumber označava karticu korištenu pri postavljanju blokade.
Druga generacija:

```
VuCompanyLocksRecord ::= SEQUENCE {
   lockInTime                          TimeReal,
   lockOutTime                         TimeReal,
   companyName                         Name,
   companyAddress                      Address,
   companyCardNumberAndGeneration      FullCardNumberAndGeneration
}
```

Umjesto companyCardNumber, u podatkovnoj strukturi za drugu generaciju upotrebljava se sljedeći podatkovni element.

companyCardNumberAndGeneration označava karticu, uključujući njezinu generaciju, korištenu pri postavljanju blokade.

2.185. VuCompanyLocksRecordArray

Druga generacija:

Informacije sačuvane u jedinici u vozilu koje se odnose na blokade od strane preduzeća (zahtjev 128 iz Priloga 1.C).

```
VuCompanyLocksRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuCompanyLocksRecord
}
```

recordType označava vrstu zapisa (VuCompanyLocksRecord). **Dodjela vrijednosti**: Vidjeti RecordType

recordSize je veličina podatka VuCompanyLocksRecord u bajtovima.

noOfRecords je broj zapisâ u nizu zapisa. Vrijednost 0..255.

records je niz zapisa o blokadama od strane preduzeća.

2.186. VuControlActivityData

Prva generacija:

Informacije sačuvane u jedinici u vozilu koje se odnose na kontrole sprovedene s pomoću te jedinice u vozilu (zahtjev 102 iz Priloga 1.B).

```
VuControlActivityData ::= SEQUENCE {
   noOfControls                        INTEGER(0..20),
   vuControlActivityRecords            SET SIZE(noOfControls) OF
                                       VuControlActivityRecord
}
```

noOfLocks je broj kontrola naveden u podatku vuControlActivityRecords.

vuControlActivityRecords je niz zapisa o nadzornim aktivnostima.

2.187. VuControlActivityRecord

Informacije sačuvane u jedinici u vozilu koje se odnose na kontrolu provedenu s pomoću te jedinice u vozilu (zahtjev 102 iz Priloga 1.B i zahtjev 126 iz Priloga 1.C).

Prva generacija:

```
VuControlActivityRecord ::= SEQUENCE {
   controlType                         ControlType,
   controlTime                         TimeReal,
   controlCardNumber                   FullCardNumber,
   downloadPeriodBeginTime             TimeReal,
   downloadPeriodEndTime               TimeReal
}
```

controlType je vrsta kontrole.

controlTime je datum i vrijeme kontrole.

controlCardNumber označava kontrolnu karticu korištenu pri kontroli.

downloadPeriodBeginTime je vrijeme koje označava početak perioda za koje se preuzimaju podaci, u slučaju preuzimanja.

downloadPeriodEndTime je vrijeme koje označava kraj perioda za koje se preuzimaju podaci, u slučaju preuzimanja.

Druga generacija:

```
VuControlActivityRecord ::= SEQUENCE {
   controlType                         ControlType,
   controlTime                         TimeReal,
   controlCardNumberAndGeneration      FullCardNumberAndGeneration,
   downloadPeriodBeginTime             TimeReal,
   downloadPeriodEndTime               TimeReal
}
```

Umjesto controlCardNumber, u podatkovnoj strukturi za drugu generaciju upotrebljava se sljedeći podatkovni element.

controlCardNumberAndGeneration označava kontrolnu karticu korištenu pri kontroli, uključujući njezinu generaciju.

2.188. VuControlActivityRecordArray

Druga generacija:

Informacije sačuvane u jedinici u vozilu koje se odnose na kontrole sprovedene s pomoću te jedinice u vozilu (zahtjev 126 iz Priloga 1.C).

```
VuControlActivityRecordArray ::= SEQUENCE {
   recordType                    RecordType,
   recordSize                    INTEGER(1..65535),
   noOfRecords                   INTEGER(0..65535),
   records                       SET SIZE(noOfRecords) OF
                                 VuControlActivityRecord
}
```

recordType označava vrstu zapisa (VuControlActivityRecord). **Dodjela vrijednosti**: Vidjeti RecordType
recordSize je veličina podatka VuControlActivityRecord u bajtovima.
noOfRecords je broj zapisâ u nizu zapisa.
records je niz zapisa o nadzornim aktivnostima jedinice u vozilu.

2.189. VuDataBlockCounter

Brojač pohranjen na kartici koji uzastopno označava cikluse umetanja kartice u jedinice u vozilu i njihovo uklanjanje iz jedinica u vozilu.

```
VuDataBlockCounter ::= BCDString(SIZE(2))
```

Dodjela vrijednosti: Redni brojevi s najvećom vrijednošću od 9 999, zatim ponovno od 0.

2.190. VuDetailedSpeedBlock

Informacije sačuvane u jedinici u vozilu koje se odnose na detaljnu brzinu vozila u minuti tokom koje se vozilo kretalo (zahtjev 093 iz Priloga 1.B i zahtjev 116 iz Priloga 1.C).

```
VuDetailedSpeedBlock ::= SEQUENCE {
   speedBlockBeginDate    TimeReal,
   speedsPerSecond        SEQUENCE SIZE(60) OF Speed
}
```

speedBlockBeginDate je datum i vrijeme prve vrijednosti brzine unutar bloka.
speedsPerSecond je kronološki niz izmjerenih brzina svake sekunde u minuti, počevši od speedBlockBeginDate (uključno).

2.191. VuDetailedSpeedBlockRecordArray

Druga generacija:
Informacije sačuvane u jedinici u vozilu koje se odnose na detaljnu brzinu vozila.

```
VuDetailedSpeedBlockRecordArray ::= SEQUENCE {
   recordType                    RecordType,
   recordSize                    INTEGER(1..65535),
   noOfRecords                   INTEGER(0..65535),
   records                       SET SIZE(noOfRecords) OF
                                 VuDetailedSpeedBlock
}
```

recordType označava vrstu zapisa (VVuDetailedSpeedBlock). **Dodjela vrijednosti**: Vidjeti RecordType
recordSize je veličina podatka VuDetailedSpeedBlock u bajtovima.
noOfRecords je broj zapisâ u nizu zapisa.
records je niz zapisa o detaljnim blokovima brzina.

2.192. VuDetailedSpeedData

Prva generacija:
Informacije sačuvane u jedinici u vozilu koje se odnose na detaljnu brzinu vozila.

```
VuDetailedSpeedData ::= SEQUENCE {
   noOfSpeedBlocks                  INTEGER(0..2^16-1),
   vuDetailedSpeedBlocks            SET SIZE(noOfSpeedBlocks) OF
                                    VuDetailedSpeedBlock
}
```

noOfSpeedBlocks je broj blokova brzina u nizu vuDetailedSpeedBlocks.
vuDetailedSpeedBlocks je niz zapisa o detaljnim blokovima brzina.

2.193. VuDownloadablePeriod

Najstariji i najnoviji datumi za koje su sačuvani podaci u jedinici u vozilu koji se odnose na aktivnosti vozača (zahtjevi 081, 084 ili 087 iz Priloga 1.B i zahtjevi 102, 105, 108 iz Priloga 1.C).

```
VuDownloadablePeriod ::= SEQUENCE {
   minDownloadableTime                 TimeReal
   maxDownloadableTime                 TimeReal
}
```

minDownloadableTime je datum i vrijeme najstarijeg podatka o umetanju kartice ili promjeni aktivnosti ili unosu mjesta pohranjenog u jedinici u vozilu.
maxDownloadableTime je najstariji podatak o uklanjanju kartice ili promjeni aktivnosti ili unos mjesta i vremena pohranjen u jedinici u vozilu.

2.194. VuDownloadablePeriodRecordArray

Druga generacija:
VUDownloadablePeriod i meta podaci koji se upotrebljavaju u postupku preuzimanja.

```
VuDownloadablePeriodRecordArray ::= SEQUENCE {
   recordType                    RecordType,
   recordSize                    INTEGER(1..65535),
   noOfRecords                   INTEGER(0..65535),
   records                       SET SIZE(noOfRecords) OF
                                 VuDownloadablePeriod
}
```

recordType označava vrstu zapisa (VuDownloadablePeriod). **Dodjela vrijednosti**: Vidjeti RecordType
recordSize je veličina podatka VuDownloadablePeriod u bajtovima.
noOfRecords je broj zapisâ u nizu zapisa.
records je niz zapisa o VuDownloadablePeriod.

2.195. VuDownloadActivityData

Informacije sačuvane u jedinici u vozilu koje se odnose na posljednje preuzimanje podataka s nje (zahtjev 105 iz Priloga 1.B i zahtjev 129 iz Priloga 1.C).
Prva generacija:

```
VuDownloadActivityData ::= SEQUENCE {
   downloadingTime                  TimeReal,
   fullCardNumber                   FullCardNumber,
   companyOrWorkshopName            Name
}
```

downloadingTime je datum i vrijeme preuzimanja.
fullCardNumber označava karticu upotrijebljenu za odobrenje preuzimanja podataka.
companyOrWorkshopName je naziv preduzeća ili radionice.
Druga generacija:

```
VuDownloadActivityData ::= SEQUENCE {
   downloadingTime                  TimeReal,
   fullCardNumberAndGeneration      FullCardNumberAndGeneration,
   companyOrWorkshopName            Name
}
```

Umjesto fullCardNumber, u podatkovnoj strukturi za drugu generaciju upotrebljava se sljedeći podatkovni element.
fullCardNumberAndGeneration označava karticu upotrijebljenu za odobrenje preuzimanja podataka i njezinu generaciju.

2.196. VuDownloadActivityDataRecordArray

Druga generacija:
Informacije koje se odnose na posljednje preuzimanje podataka s jedinice u vozilu (zahtjev 129 iz Priloga 1.C).

```
VuDownloadActivityDataRecordArray ::= SEQUENCE {
   recordType                       RecordType,
   recordSize                       INTEGER(1..65535),
   noOfRecords                      INTEGER(0..65535),
   records                          SET SIZE(noOfRecords) OF VuDownloadActivityData
}
```

recordType označava vrstu zapisa (VuDownloadActivityData). **Dodjela vrijednosti**: Vidjeti RecordType
recordSize je veličina podatka VuDownloadActivityData u bajtovima.
noOfRecords je broj zapisâ u nizu zapisa.
records je niz zapisa o aktivnostima preuzimanja podataka.

2.197. VuEventData

Prva generacija:
Informacije sačuvane u jedinici u vozilu koje se odnose na događaje (zahtjev 094 iz Priloga 1.B, osim dijela u pogledu događaja prekoračenja brzine).

```
VuEventData ::= SEQUENCE {
   noOfVuEvents                     INTEGER(0..255),
   vuEventRecords                   SET SIZE(noOfVuEvents) OF VuEventRecord
}
```

noOfVuEvents je broj događaja navedenih u nizu vuEventRecords.
vuEventRecords je niz zapisa o događajima.

2.198. VuEventRecord

Informacije sačuvane u jedinici u vozilu koje se odnose na određeni događaj (zahtjev 094 iz Priloga 1.B i zahtjev 117 iz Priloga 1.C, osim dijela u pogledu događaja prekoračenja brzine).
Prva generacija:

```
VuEventRecord ::= SEQUENCE {
   eventType                        EventFaultType,
   eventRecordPurpose               EventFaultRecordPurpose,
   eventBeginTime                   TimeReal,
   eventEndTime                     TimeReal,
   cardNumberDriverSlotBegin        FullCardNumber,
   cardNumberCodriverSlotBegin      FullCardNumber,
   cardNumberDriverSlotEnd          FullCardNumber,
   cardNumberCodriverSlotEnd        FullCardNumber,
   similarEventsNumber              SimilarEventsNumber
}
```

eventType je vrsta događaja.
eventRecordPurpose je svrha za koju je zabilježen taj događaj.
eventBeginTime je datum i vrijeme početka događaja.
eventEndTime je datum i vrijeme završetka događaja.
cardNumberDriverSlotBegin označava karticu umetnutu u otvor vozača na početku događaja.
cardNumberCodriverSlotBegin označava karticu umetnutu u otvor suvozača na početku događaja.
cardNumberDriverSlotEnd označava karticu umetnutu u otvor vozača na završetku događaja.
cardNumberCodriverSlotEnd označava karticu umetnutu u otvor suvozača na završetku događaja.

similarEventsNumber je broj sličnih događaja tog dana.
Taj se niz može upotrebljavati za sve događaje osim događaje prekoračenja brzine.
Druga generacija:

```
VuEventRecord ::= SEQUENCE {
   eventType                          EventFaultType,
   eventRecordPurpose                 EventFaultRecordPurpose,
   eventBeginTime                     TimeReal,
   eventEndTime                       TimeReal,
   cardNumberAndGenDriverSlotBegin    FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin  FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd      FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd    FullCardNumberAndGeneration,
   similarEventsNumber                SimilarEventsNumber,
   manufacturerSpecificEventFaultData ManufacturerSpecificEventFaultData
}
```

Uz podatkovne elemente navedene za prvu generaciju upotrebljavaju se i sljedeći:
manufacturerSpecificEventFaultData sadrži dodatne informacije o događaju, specifične za proizvođača.
Umjesto cardNumberDriverSlotBegin, cardNumberCodriverSlotBegin, cardNumberDriverSlotEnd, i cardNumberCodriverSlotEnd, u podatkovnoj strukturi za drugu generaciju upotrebljavaju se sljedeći podatkovni elementi.
cardNumberAndGenDriverSlotBegin označava karticu umetnutu u otvor vozača na početku događaja i njezinu generaciju.
cardNumberAndGenCodriverSlotBegin označava karticu umetnutu u otvor suvozača na početku događaja i njezinu generaciju.
cardNumberAndGenDriverSlotEnd označava karticu umetnutu u otvor vozača na završetku događaja i njezinu generaciju.
cardNumberAndGenCodriverSlotEnd označava karticu umetnutu u otvor suvozača na završetku događaja i njezinu generaciju.
Ako događaj predstavlja proturječnost u vremenu, podatke eventBeginTime i eventEndTime tumači se kako slijedi:
eventBeginTime je datum i vrijeme na uređaju za evidentiranje podataka.
eventEndTime je datum i vrijeme na uređaju GNSS-a.

2.199. VuEventRecordArray

Druga generacija:
Informacije sačuvane u jedinici u vozilu koje se odnose na događaje (zahtjev 117 iz Priloga 1.C, osim dijela u pogledu događaja prekoračenja brzine).

```
VuEventRecordArray ::= SEQUENCE {
   recordType                         RecordType,
   recordSize                         INTEGER(1..65535),
   noOfRecords                        INTEGER(0..65535),
   records                            SET SIZE(noOfRecords) OF VuEventRecord
}
```

recordType označava vrstu zapisa (VuEventRecord). **Dodjela vrijednosti**: Vidjeti RecordType
recordSize je veličina podatka VuEventRecord u bajtovima.
noOfRecords je broj zapisâ u nizu zapisa.
records je niz zapisa o događajima.

2.200. VuFaultData

Prva generacija:
Informacije sačuvane u jedinici u vozilu koje se odnose na kvarove (zahtjev 096 iz Priloga 1.B).

```
VuFaultData ::= SEQUENCE {
   noOfVuFaults                       INTEGER(0..255),
   vuFaultRecords                     SET SIZE(noOfVuFaults) OF VuFaultRecord
}
```

noOfVuFaults je broj kvarova koje sadrži niz vuFaultRecords.
vuFaultRecords je niz zapisa o kvarovima.

2.201. VuFaultRecord

Informacije sačuvane u jedinici u vozilu koje se odnose na kvar (zahtjev 096 iz Priloga 1.B i zahtjev 118 iz Priloga 1.C).
Prva generacija:

```
VuFaultRecord ::= SEQUENCE {
   faultType                          EventFaultType,
   faultRecordPurpose                 EventFaultRecordPurpose,
   faultBeginTime                     TimeReal,
   faultEndTime                       TimeReal,
   cardNumberDriverSlotBegin          FullCardNumber,
   cardNumberCodriverSlotBegin        FullCardNumber,
   cardNumberDriverSlotEnd            FullCardNumber,
   cardNumberCodriverSlotEnd          FullCardNumber
}
```

faultType je vrsta kvara uređaja za evidentiranje podataka.
faultRecordPurpose je svrha za koju je zabilježen taj kvar.
faultBeginTime je datum i vrijeme početka kvara.
faultEndTime je datum i vrijeme završetka kvara.
cardNumberDriverSlotBegin označava karticu umetnutu u otvor vozača na početku kvara.

cardNumberCodriverSlotBegin označava karticu umetnutu u otvor suvozača na početku kvara.
cardNumberDriverSlotEnd označava karticu umetnutu u otvor vozača na završetku kvara.
cardNumberCodriverSlotEnd označava karticu umetnutu u otvor suvozača na završetku kvara.
Druga generacija:

```
VuFaultRecord ::= SEQUENCE {
   faultType                        EventFaultType,
   faultRecordPurpose               EventFaultRecordPurpose,
   faultBeginTime                   TimeReal,
   faultEndTime                     TimeReal,
   cardNumberAndGenDriverSlotBegin  FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd    FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd  FullCardNumberAndGeneration,
   manufacturerSpecificEventFaultData ManufacturerSpecificEventFaultData
}
```

Uz podatkovne elemente navedene za prvu generaciju upotrebljava se i sljedeći:
manufacturerSpecificEventFaultData sadrži dodatne informacije o kvaru, specifične za proizvođača.
Umjesto cardNumberDriverSlotBegin, cardNumberCodriverSlotBegin, cardNumberDriverSlotEnd, i cardNumberCodriverSlotEnd, u podatkovnoj strukturi za drugu generaciju upotrebljavaju se sljedeći podatkovni elementi:
cardNumberAndGenDriverSlotBegin označava karticu umetnutu u otvor vozača na početku kvara i njezinu generaciju.
cardNumberAndGenCodriverSlotBegin označava karticu umetnutu u otvor suvozača na početku kvara i njezinu generaciju.
cardNumberAndGenDriverSlotEnd označava karticu umetnutu u otvor vozača na završetku kvara i njezinu generaciju.
cardNumberAndGenCodriverSlotEnd označava karticu umetnutu u otvor suvozača na završetku kvara i njezinu generaciju.

2.202. VuFaultRecordArray

Druga generacija:
Informacije sačuvane u jedinici u vozilu koje se odnose na kvarove (zahtjev 118 iz Priloga 1.C).

```
VuFaultRecordArray ::= SEQUENCE {
   recordType                       RecordType,
   recordSize                       INTEGER(1..65535),
   noOfRecords                      INTEGER(0..65535),
   records                          SET SIZE(noOfRecords) OF VuFaultRecord
}
```

recordType označava vrstu zapisa (VuFaultRecord). **Dodjela vrijednosti**: Vidjeti RecordType
recordSize je veličina podatka VuFaultRecord u bajtovima.
noOfRecords je broj zapisâ u nizu zapisa.
records je niz zapisa o kvarovima.

2.203. VuGNSSADRecord

Druga generacija:
informacije arhivirane u jedinici u vozilu koje se odnose na položaj vozila prema GNSS-u ako akumulisano vrijeme vožnje dostigne višekratnih tri sata (zahtjevi 108) i 110) iz Priloga I.C).

```
VuGNSSADRecord ::= SEQUENCE {
   timeStamp                        TimeReal,
   cardNumberAndGenDriverSlot       FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlot     FullCardNumberAndGeneration,
   gnssPlaceRecord                  GNSSPlaceRecord,
   vehicleOdometerValue             OdometerShort
}
```

timeStamp je datum i vrijeme kad akumulisano vrijeme vožnje dostiže višekratnik tri sata.
cardNumberAndGenDriverSlot označava karticu umetnutu u otvor vozača i njezinu generaciju.
cardNumberAndGenCodriverSlot označava karticu umetnutu u otvor suvozača i njezinu generaciju.
gnssPlaceRecord sadrži informacije o položaju vozila.
vehicleOdometerValue je stanje brojača kilometara kad akumulisano vrijeme vožnje dostiže višekratnik tri sata.

2.204. VuGNSSADRecordArray

Druga generacija:
informacije arhivirane u jedinici u vozilu koje se odnose na položaj vozila prema GNSS-u ako akumulisano vrijeme vožnje dostigne višekratnik tri sata (zahtjevi 108) i 110) iz Priloga I.C).

```
VuGNSSADRecordArray ::= SEQUENCE {
   recordType                       RecordType,
   recordSize                       INTEGER(1..65535),
   noOfRecords                      INTEGER(0..65535),
   records                          SET SIZE(noOfRecords) OF VuGNSSADRecord
}
```

recordType označava vrstu zapisa (VuGNSSADRecord).
Dodjela vrijednosti: Vidjeti RecordType.
recordSize je veličina podatka VuGNSSADRecord u bajtovima.
noOfRecords je broj zapisâ u nizu zapisa.
records je niz zapisa GNSS-a o akumulisanom razdoblju vožnje.

2.205. VuIdentification

Informacije sačuvane u jedinici u vozilu koje se odnose na identifikaciju jedinice u vozilu (zahtjev 075 iz Priloga 1.B i zahtjevi 93 i 121 iz Priloga 1.C).

Prva generacija:

```
VuIdentification ::= SEQUENCE {
   vuManufacturerName                VuManufacturerName,
   vuManufacturerAddress             VuManufacturerAddress,
   vuPartNumber                      VuPartNumber,
   vuSerialNumber                    VuSerialNumber,
   vuSoftwareIdentification          VuSoftwareIdentification,
   vuManufacturingDate               VuManufacturingDate,
   vuApprovalNumber                  VuApprovalNumber
}
```

vuManufacturerName je naziv proizvođača jedinice u vozilu.
vuManufacturerAddress je adresa proizvođača jedinice u vozilu.
vuPartNumber je kataloški broj jedinice u vozilu.
vuSerialNumber je serijski broj jedinice u vozilu.
vuSoftwareIdentification označava softver ugrađen u jedinicu u vozilu.
vuManufacturingDate je datum proizvodnje jedinice u vozilu.
cardApprovalNumber je homologacijski broj jedinice u vozilu.

Druga generacija:

```
VuIdentification ::= SEQUENCE {
   vuManufacturerName                VuManufacturerName,
   vuManufacturerAddress             VuManufacturerAddress,
   vuPartNumber                      VuPartNumber,
   vuSerialNumber                    VuSerialNumber,
   vuSoftwareIdentification          VuSoftwareIdentification,
   vuManufacturingDate               VuManufacturingDate,
   vuApprovalNumber                  VuApprovalNumber,
   vuGeneration                      Generation,
   vuAbility                         VuAbility
}
```

Uz podatkovne elemente navedene za prvu generaciju upotrebljavaju se i sljedeći:
vuGeneration označava generaciju jedinice u vozilu.
vuAbility pruža informacije o tome podržava li jedinica u vozilu tahografske kartice prve generacije ili ne.

2.206. VuIdentificationRecordArray

Druga generacija:

VuIdentification i meta podaci koji se upotrebljavaju u postupku preuzimanja.

```
VuIdentificationRecordArray ::= SEQUENCE {
   recordType                        RecordType,
   recordSize                        INTEGER(1..65535),
   noOfRecords                       INTEGER(0..65535),
   records                           SET SIZE(noOfRecords) OF VuIdentification
}
```

recordType označava vrstu zapisa (VuIdentification). **Dodjela vrijednosti**: Vidjeti RecordType
recordSize je veličina podatka VuIdentification u bajtovima.
noOfRecords je broj zapisâ u nizu zapisa.
records je niz zapisa VuIdentification.

2.207. VuITSConsentRecord

Druga generacija:

Informacije sačuvane u jedinici u vozilu koje se odnose na pristanak vozača u pogledu upotrebe inteligentnih prijevoznih sistema.

```
VuITSConsentRecord ::= SEQUENCE {
   cardNumberAndGen                  FullCardNumberAndGeneration,
   consent                           BOOLEAN
}
```

cardNumberAndGen označava karticu i njezinu generaciju. To mora biti kartica vozača ili kartica radionice.
consent je znak koji označava je li vozač pristao na upotrebu inteligentnih prijevoznih sistema u dotičnom vozilu / jedinici u vozilu.
Dodjela vrijednosti:
TRUE označava pristanak vozača na upotrebu inteligentnih prijevoznih sistema.
FALSE označava da je vozač odbio upotrebu inteligentnih prijevoznih sistema.

2.208. VuITSConsentRecordArray

Druga generacija:

Informacije sačuvane u jedinici u vozilu koje se odnose na pristanak vozača u pogledu upotrebe inteligentnih prijevoznih sistema (zahtjev 200 iz Priloga 1.C).

```
VuITSConsentRecordArray ::= SEQUENCE {
   recordType                        RecordType,
   recordSize                        INTEGER(1..65535),
   noOfRecords                       INTEGER(0..65535),
   records                           SET SIZE(noOfRecords) OF VuITSConsentRecord
}
```

recordType označava vrstu zapisa (VuITSConsentRecord). **Dodjela vrijednosti**: Vidjeti RecordType
recordSize je veličina podatka VuITSConsentRecord u bajtovima.

noOfRecords je broj zapisâ u nizu zapisa.
records je niz zapisa o pristanku na upotrebu ITS-a.

2.209. VuManufacturerAddress

Adresa proizvođača jedinice u vozilu.

```
VuManufacturerAddress ::= Address
```

Dodjela vrijednosti: Neodređeno.

2.210. VuManufacturerName

Naziv proizvođača jedinice u vozilu.

```
VuManufacturerName ::= Name
```

Dodjela vrijednosti: Neodređeno.

2.211. VuManufacturingDate

Datum proizvodnje jedinice u vozilu.

```
VuManufacturingDate ::= TimeReal
```

Dodjela vrijednosti: Neodređeno.

2.212. VuOverSpeedingControlData

Informacije sačuvane u jedinici u vozilu koje se odnose na događaje prekoračenja brzine od posljednjee kontrole u pogledu prekoračenja brzine (zahtjev 095 iz Priloga 1.B i zahtjev 117 iz Priloga 1.C).

```
VuOverSpeedingControlData ::= SEQUENCE {
   lastOverspeedControlTime            TimeReal,
   firstOverspeedSince                 TimeReal,
   numberOfOverspeedSince              OverspeedNumber
}
```

lastOverspeedControlTime je datum i vrijeme posljednje kontrole u pogledu prekoračenja brzine.
firstOverspeedSince je datum i vrijeme prvog prekoračenja brzine nakon provedbe te kontrole u pogledu prekoračenja brzine.
numberOfOverspeedSince je broj događaja prekoračenja brzine od posljednje kontrole u pogledu prekoračenja brzine.

2.213. VuOverSpeedingControlDataRecordArray

Druga generacija:
VuOverSpeedingControlData i meta podaci koji se upotrebljavaju u postupku preuzimanja.

```
VuOverSpeedingControlDataRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuOverSpeedingControlData
}
```

recordType označava vrstu zapisa (VuOverSpeedingControlData). **Dodjela vrijednosti**: Vidjeti RecordType
recordSize je veličina podatka VuOverSpeedingControlData u bajtovima.
noOfRecords je broj zapisâ u nizu zapisa.
records je niz zapisa o podacima o kontroli u pogledu prekoračenja brzine.

2.214. VuOverSpeedingEventData

Prva generacija:
Informacije sačuvane u jedinici u vozilu koje se odnose na događaje prekoračenja brzine (zahtjev 094 iz Priloga 1.B).

```
VuOverSpeedingEventData ::= SEQUENCE {
   noOfVuOverSpeedingEvents            INTEGER(0..255),
   vuOverSpeedingEventRecords          SET SIZE(noOfVuOverSpeedingEvents) OF
                                       VuOverSpeedingEventRecord
}
```

noOfVuOverSpeedingEvents je broj zapisa koje sadrži niz vuOverSpeedingEventRecords.
vuOverSpeedingEventRecords je niz zapisa o događajima prekoračenja brzine.

2.215. VuOverSpeedingEventRecord

Prva generacija:
Informacije sačuvane u jedinici u vozilu koje se odnose na događaje prekoračenja brzine (zahtjev 094 iz Priloga 1.B i zahtjev 117 iz Priloga 1.C).

```
VuOverSpeedingEventRecord ::= SEQUENCE {
   eventType                           EventFaultType,
   eventRecordPurpose                  EventFaultRecordPurpose,
   eventBeginTime                      TimeReal,
   eventEndTime                        TimeReal,
   maxSpeedValue                       SpeedMax,
   averageSpeedValue                   SpeedAverage,
   cardNumberDriverSlotBegin           FullCardNumber,
   similarEventsNumber                 SimilarEventsNumber
}
```

eventType je vrsta događaja.
eventRecordPurpose je svrha za koju je zabilježen taj događaj.
eventBeginTime je datum i vrijeme početka događaja.
eventEndTime je datum i vrijeme završetka događaja.
maxSpeedValue je najviša brzina izmjerena tokom događaja.

averageSpeedValue je aritmetički prosjek brzine izmjerene tokom događaja..
cardNumberDriverSlotBegin označava karticu umetnutu u otvor vozača na početku događaja.
similarEventsNumber je broj sličnih događaja tog dana.
Druga generacija:
Informacije sačuvane u jedinici u vozilu koje se odnose na događaje prekoračenja brzine (zahtjev 094 iz Priloga 1.B i zahtjev 117 iz Priloga 1.C).

```
VuOverSpeedingEventRecord ::= SEQUENCE {
   eventType                        EventFaultType,
   eventRecordPurpose               EventFaultRecordPurpose,
   eventBeginTime                   TimeReal,
   eventEndTime                     TimeReal,
   maxSpeedValue                    SpeedMax,
   averageSpeedValue                SpeedAverage,
   cardNumberAndGenDriverSlotBegin  FullCardNumberAndGeneration,
   similarEventsNumber              SimilarEventsNumber
}
```

Umjesto cardNumberDriverSlotBegin, u podatkovnoj strukturi za drugu generaciju upotrebljava se sljedeći podatkovni element:
cardNumberAndGenDriverSlotBegin označava karticu umetnutu u otvor vozača na početku događaja i njezinu generaciju.

2.216. VuOverSpeedingEventRecordArray

Druga generacija:
Informacije sačuvane u jedinici u vozilu koje se odnose na događaje prekoračenja brzine (zahtjev 117 iz Priloga 1.C).

```
VuOverSpeedingEventRecordArray ::= SEQUENCE {
   recordType                       RecordType,
   recordSize                       INTEGER(1..65535),
   noOfRecords                      INTEGER(0..65535),
   records                          SET SIZE(noOfRecords) OF
                                    VuOverSpeedingEventRecord
}
```

recordType označava vrstu zapisa (VuOverSpeedingEventRecord). **Dodjela vrijednosti**: Vidjeti RecordType
recordSize je veličina podatka VuOverSpeedingEventRecord u bajtovima.
noOfRecords je broj zapisâ u nizu zapisa.
records je niz zapisa o događajima prekoračenja brzine.

2.217. VuPartNumber

Kataloški broj jedinice u vozilu.

```
VuPartNumber ::= IA5String(SIZE(16))
```

Dodjela vrijednosti: Specifična za proizvođača jedinice u vozilu.

2.218. VuPlaceDailyWorkPeriodData

Prva generacija:
Informacije sačuvane u jedinici u vozilu koje se odnose na mjesta na kojima vozači započinju ili završavaju period dnevnog rada (zahtjev 087 iz Priloga 1.B i zahtjevi 108 i 110 iz Priloga 1.C).

```
VuPlaceDailyWorkPeriodData ::= SEQUENCE {
   noOfPlaceRecords                 INTEGER(0..255),
   vuPlaceDailyWorkPeriodRecords    SET SIZE(noOfPlaceRecords) OF
                                    VuPlaceDailyWorkPeriodRecord
}
```

noOfPlaceRecords je broj zapisâ koje sadrži niz vuPlaceDailyWorkPeriodRecords.
vuPlaceDailyWorkPeriodRecords je niz zapisa o mjestu.

2.219. VuPlaceDailyWorkPeriodRecord

Prva generacija:
Informacije sačuvane u jedinici u vozilu koje se odnose na mjesto na kojem vozač započinje ili završava period dnevnog rada (zahtjev 087 iz Priloga 1.B i zahtjevi 108 i 110 iz Priloga 1.C).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {
   fullCardNumber                   FullCardNumber,
   placeRecord                      PlaceRecord
}
```

fullCardNumber je vrsta kartice vozača, država članica koja je izdala karticu i broj kartice.
placeRecord sadrži informacije povezane s unesenim mjestom.
Druga generacija:
Informacije sačuvane u jedinici u vozilu koje se odnose na mjesto na kojem vozač započinje ili završava period dnevnog rada (zahtjev 087 iz Priloga 1.B i zahtjevi 108 i 110 iz Priloga 1.C).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {
   fullCardNumberAndGeneration      FullCardNumberAndGeneration,
   placeRecord                      PlaceRecord
}
```

Umjesto fullCardNumber, u podatkovnoj strukturi za drugu generaciju upotrebljava se sljedeći podatkovni element:
fullCardNumberAndGeneration je vrsta kartice, država članica koja ju je izdala te broj kartice i njezina generacija, kako su sačuvani na kartici.

2.220. VuPlaceDailyWorkPeriodRecordArray

Druga generacija:

Informacije sačuvane u jedinici u vozilu koje se odnose na mjesta na kojima vozači započinju ili završavaju period dnevnog rada (zahtjevi 108 i 110 iz Priloga 1.C).

```
VuPlaceDailyWorkPeriodRecordArray ::= SEQUENCE {
   recordType                       RecordType,
   recordSize                       INTEGER(1..65535),
   noOfRecords                      INTEGER(0..65535),
   records                          SET SIZE(noOfRecords) OF
                                    VuPlaceDailyWorkPeriodRecord
}
```

recordType označava vrstu zapisa (VuPlaceDailyWorkPeriodRecord). **Dodjela vrijednosti**: Vidjeti RecordType
recordSize je veličina podatka VuPlaceDailyWorkPeriodRecord u bajtovima.
noOfRecords je broj zapisâ u nizu zapisa.
records je niz zapisa povezanih s mjestom.

2.221. VuPrivateKey

Prva generacija:
Privatni ključ jedinice u vozilu.

```
VuPrivateKey ::= RSAKeyPrivateExponent
```

2.222. VuPublicKey

Prva generacija:
Javni ključ jedinice u vozilu.

```
VuPublicKey ::= PublicKey
```

2.223. VuSerialNumber

Serijski broj jedinice u vozilu (zahtjev 075 iz Priloga 1.B i zahtjev 93 iz Priloga 1.C).

```
VuSerialNumber ::= ExtendedSerialNumber
```

2.224. VuSoftInstallationDate

Datum ugradnje verzije softvera u jedinicu u vozilu.

```
VuSoftInstallationDate ::= TimeReal
```

Dodjela vrijednosti: Neodređeno.

2.225. VuSoftwareIdentification

Informacije sačuvane u jedinici u vozilu koje se odnose na ugrađeni softver.

```
VuSoftwareIdentification ::= SEQUENCE {
   vuSoftwareVersion                VuSoftwareVersion,
   vuSoftInstallationDate           VuSoftInstallationDate
}
```

vuSoftwareVersion je broj verzije softvera u jedinici u vozilu.
vuSoftInstallationDate je datum ugradnje verzije softvera.

2.226. VuSoftwareVersion

Broj verzije softvera u jedinici u vozilu.

```
VuSoftwareVersion ::= IA5String(SIZE(4))
```

Dodjela vrijednosti: Neodređeno.

2.227. VuSpecificConditionData

Prva generacija:
Informacije sačuvane u jedinici u vozilu koje se odnose na posebne uslove.

```
VuSpecificConditionData ::= SEQUENCE {
   noOfSpecificConditionRecords     INTEGER(0..2^16-1)
   specificConditionRecords         SET SIZE (noOfSpecificConditionRecords) OF
                                    SpecificConditionRecord
}
```

noOfSpecificConditionRecords je broj zapisâ koje sadrži niz specificConditionRecords.
specificConditionRecords je niz zapisa povezanih s posebnim uslovima.

2.228. VuSpecificConditionRecordArray

Druga generacija:
Informacije sačuvane u jedinici u vozilu koje se odnose na posebne uslove (zahtjev 130 iz Priloga 1.C).

```
VuSpecificConditionRecordArray ::= SEQUENCE {
   recordType                       RecordType,
   recordSize                       INTEGER(1..65535),
   noOfRecords                      INTEGER(0..65535),
   records                          SET SIZE(noOfRecords) OF
                                    SpecificConditionRecord
}
```

recordType označava vrstu zapisa (SpecificConditionRecord). **Dodjela vrijednosti**: Vidjeti RecordType
recordSize je veličina podatka SpecificConditionRecord u bajtovima.
noOfRecords je broj zapisâ u nizu zapisa.
records je niz zapisa povezanih s posebnim uslovima.

2.229. VuTimeAdjustmentData

Prva generacija:
Informacije sačuvane u jedinici u vozilu koje se odnose na podešavanje vremena koje se izvršava izvan okvira redovnog kalibriranja (zahtjev 101 iz Priloga 1.B).

```
VuTimeAdjustmentData ::= SEQUENCE {
   noOfVuTimeAdjRecords             INTEGER(0..6),
   vuTimeAdjustmentRecords          SET SIZE(noOfVuTimeAdjRecords) OF
                                    VuTimeAdjustmentRecord
}
```

noOfVuTimeAdjRecords je broj zapisâ u vuTimeAdjustmentRecords**.**

sealRecords je niz zapisa o podešavanju vremena.

2.230. Rezervisano za buduću upotrebu

Druga generacija:

Informacije sačuvane u jedinici u vozilu koje se odnose na podešavanje vremena na temelju podataka o vremenu iz GNSS-a (zahtjevi 124 i 125 iz Priloga 1.C).

```
VuTimeAdjustmentGNSSRecord ::= SEQUENCE {
   oldTimeValue                    TimeReal,
   newTimeValue                    TimeReal
}
```

oldTimeValue, newTimeValue su stari i novi datum i vrijeme.

2.231. Rezervisano za buduću upotrebu

Druga generacija:

Informacije sačuvane u jedinici u vozilu koje se odnose na podešavanje vremena izvršeno na temelju podataka o vremenu iz GNSS-a (zahtjevi 124 i 125 iz Priloga 1.C).

```
VuTimeAdjustmentGNSSRecordArray ::= SEQUENCE {
   recordType                      RecordType,
   recordSize                      INTEGER(1..65535),
   noOfRecords                     INTEGER(0..65535),
   records                         SET SIZE(noOfRecords) OF
                                   VuTimeAdjustmentGNSSRecord
}
```

recordType označava vrstu zapisa (VuTimeAdjustmentGNSSRecord). **Dodjela vrijednosti**: Vidjeti RecordType

recordSize je veličina podatka VuTimeAdjustmentGNSSRecord u bajtovima.

noOfRecords je broj zapisâ u nizu zapisa.

records je niz zapisa o podešavanju vremena na temelju GNSS-a.

2.232. VuTimeAdjustmentRecord

Informacije sačuvane u jedinici u vozilu koje se odnose na podešavanje vremena koje se izvršava izvan okvira redovnog kalibriranja (zahtjev 101 iz Priloga 1.B i zahtjevi 124 i 125 iz Priloga 1.C).

Prva generacija:

```
VuTimeAdjustmentRecord ::= SEQUENCE {
   oldTimeValue                    TimeReal,
   newTimeValue                    TimeReal,
   workshopName                    Name,
   workshopAddress                 Address,
   workshopCardNumber              FullCardNumber
}
```

oldTimeValue, newTimeValue su stari i novi datum i vrijeme.

workshopName, workshopAddress su naziv i adresa radionice.

workshopCardNumber označava karticu radionice upotrijebljenu radi podešavanja vremena.

Druga generacija:

```
VuTimeAdjustmentRecord ::= SEQUENCE {
   oldTimeValue                    TimeReal,
   newTimeValue                    TimeReal,
   workshopName                    Name,
   workshopAddress                 Address,
   workshopCardNumberAndGeneration FullCardNumberAndGeneration
}
```

Umjesto workshopCardNumber, u podatkovnoj strukturi za drugu generaciju upotrebljava se sljedeći podatkovni element.

workshopCardNumberAndGeneration označava karticu radionice upotrijebljenu radi podešavanja vremena i njezinu generaciju.

2.233. VuTimeAdjustmentRecordArray

Druga generacija:

Informacije sačuvane u jedinici u vozilu koje se odnose na podešavanje vremena koje se izvršava izvan okvira redovnog kalibriranja (zahtjevi 124 i 125 iz Priloga 1.C).

```
VuTimeAdjustmentRecordArray ::= SEQUENCE {
   recordType                      RecordType,
   recordSize                      INTEGER(1..65535),
   noOfRecords                     INTEGER(0..65535),
   records                         SET SIZE(noOfRecords) OF
                                   VuTimeAdjustmentRecord
}
```

recordType označava vrstu zapisa (VuTimeAdjustmentRecord). **Dodjela vrijednosti**: Vidjeti RecordType

recordSize je veličina podatka VuTimeAdjustmentRecord u bajtovima.

noOfRecords je broj zapisâ u nizu zapisa.

records je niz zapisa o podešavanju vremena.

2.234. WorkshopCardApplicationIdentification

Informacije sačuvane na kartici radionice koje se odnose na identifikaciju primjene kartice (zahtjevi 307 i 330 iz Priloga 1.C).

Prva generacija:

```
WorkshopCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfEventsPerType                   NoOfEventsPerType,
   noOfFaultsPerType                   NoOfFaultsPerType,
   activityStructureLength             CardActivityLengthRange,
   noOfCardVehicleRecords              NoOfCardVehicleRecords,
   noOfCardPlaceRecords                NoOfCardPlaceRecords,
   noOfCalibrationRecords              NoOfCalibrationRecords
}
```

typeOfTachographCardId označava vrstu upotrijebljene kartice.
cardStructureVersion utvrđuje verziju strukture koja je primijenjena na kartici.
noOfEventsPerType je broj događaja po vrsti događaja koji se najviše može sačuvati na kartici.
noOfFaultsPerType je broj kvarova po vrsti kvara koji se najviše može sačuvati na kartici.
activityStructureLength označava broj bajtova dostupnih za arhiviranje zapisa o aktivnostima.
noOfCardVehicleRecords je broj zapisa o vozilu koji se najviše može sačuvati na kartici.
noOfCardPlaceRecords je broj zapisa o mjestima koji se najviše može sačuvati na kartici.
noOfCalibrationRecords je broj zapisa o aktivnostima kalibriranja koji se najviše može sačuvati na kartici.
Druga generacija:

```
WorkshopCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfEventsPerType                   NoOfEventsPerType,
   noOfFaultsPerType                   NoOfFaultsPerType,
   activityStructureLength             CardActivityLengthRange,
   noOfCardVehicleRecords              NoOfCardVehicleRecords,
   noOfCardPlaceRecords                NoOfCardPlaceRecords,
   noOfCalibrationRecords              NoOfCalibrationRecords,
   noOfGNSSADRecords                   NoOfGNSSADRecords,
   noOfSpecificConditionRecords        NoOfSpecificConditionRecords,
   noOfCardVehicleUnitRecords          NoOfCardVehicleUnitRecords
}
```

Uz podatkovne elemente navedene za prvu generaciju upotrebljavaju se i sljedeći:
noOfGNSSADRecords je broj zapisa GNSS-a o akumulisanom razdoblju vožnje koji se najviše može arhivirati na kartici.
noOfSpecificConditionRecords je broj zapisa o posebnim uslovima koji se najviše može arhivirati na kartici.
noOfCardVehicleUnitRecords je broj zapisa o korištenim jedinicama u vozilu koji se najviše može arhivirati na kartici.

2.235. WorkshopCardCalibrationData

Informacije sačuvane na kartici radionice koje se odnose na aktivnosti radionice izvršene s karticom (zahtjevi 314, 316, 337 i 339 iz Priloga 1.C).

```
WorkshopCardCalibrationData ::= SEQUENCE {
   calibrationTotalNumber              INTEGER(0 .. 2^16-1),
   calibrationPointerNewestRecord      INTEGER(0 .. NoOfCalibrationRecords-1),
   calibrationRecords                  SET SIZE(NoOfCalibrationRecords) OF
                                       WorkshopCardCalibrationRecord
}
```

calibrationTotalNumber je ukupan broj kalibriranja izvršenih s karticom.
calibrationPointerNewestRecord je indeks posljednjeg ažuriranog zapisa o kalibriranju.
Dodjela vrijednosti: Broj koji odgovara brojniku zapisa o kalibriranju, a započinje s „0” za prvu pojavu zapisâ o kalibriranju u strukturi.
calibrationRecords je niz zapisa koji sadržiju informacije o kalibriranju i/ili podešavanju vremena.

2.236. WorkshopCardCalibrationRecord

Informacije sačuvane na kartici radionice koje se odnose na kalibriranje izvršeno s karticom (zahtjevi 314 i 337 iz Priloga 1.C).
Prva generacija:

```
WorkshopCardCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                  CalibrationPurpose,
   vehicleIdentificationNumber         VehicleIdentificationNumber,
   vehicleRegistration                 VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant      W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment       K-ConstantOfRecordingEquipment,
   lTyreCircumference                  L-TyreCircumference,
   tyreSize                            TyreSize,
   authorisedSpeed                     SpeedAuthorised,
   oldOdometerValue                    OdometerShort,
   newOdometerValue                    OdometerShort,
   oldTimeValue                        TimeReal,
   newTimeValue                        TimeReal,
   nextCalibrationDate                 TimeReal,
   vuPartNumber                        VuPartNumber,
   vuSerialNumber                      VuSerialNumber,
   sensorSerialNumber                  SensorSerialNumber
}
```

calibrationPurpose je svrha kalibriranja.
vehicleIdentificationNumber je VIN.
vehicleRegistration sadrži VRN i državu članicu registracije.

wVehicleCharacteristicConstant je karakteristični koeficijent vozila.
kConstantOfRecordingEquipment je konstanta uređaja za evidentiranje podataka.
lTyreCircumference je djelatni opseg guma tačka.
tyreSize je oznaka za dimenzije guma postavljenih na vozilo.
authorisedSpeed je najveća odobrena brzina vozila.
oldOdometerValue, newOdometerValue su stare i nove vrijednosti na brojaču kilometara.
oldTimeValue, newTimeValue su stari i novi datum i vrijeme.
nextCalibrationDate je datum sljedećeg kalibriranja vrste utvrđene u podatku CalibrationPurpose koje sprovodi tijelo ovlašteno za pregled.
vuPartNumber, **vuSerialNumber** i **sensorSerialNumber** su podatkovni elementi za identifikaciju uređaja za evidentiranje podataka.
Druga generacija:

```
WorkshopCardCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                  CalibrationPurpose,
   vehicleIdentificationNumber         VehicleIdentificationNumber,
   vehicleRegistration                 VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant      W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment       K-ConstantOfRecordingEquipment,
   lTyreCircumference                  L-TyreCircumference,
   tyreSize                            TyreSize,
   authorisedSpeed                     SpeedAuthorised,
   oldOdometerValue                    OdometerShort,
   newOdometerValue                    OdometerShort,
   oldTimeValue                        TimeReal,
   newTimeValue                        TimeReal,
   nextCalibrationDate                 TimeReal,
   vuPartNumber                        VuPartNumber,
   vuSerialNumber                      VuSerialNumber,
   sensorSerialNumber                  SensorSerialNumber,
   sensorGNSSSerialNumber              SensorGNSSSerialNumber,
   rcmSerialNumber                     RemoteCommunicationModuleSerialNumber,
   sealDataCard                        SealDataCard
}
```

Uz podatkovne elemente navedene za prvu generaciju upotrebljavaju se i sljedeći:
sensorGNSSSerialNumber identifikuje spoljni uređaj GNSS-a.
rcmSerialNumber identifikuje modul za komunikaciju na daljinu.
sealDataCard pruža informacije o plombama stavljenima na različite sastavne dijelove vozila.

2.237. WorkshopCardHolderIdentification

Informacije sačuvane na kartici radionice koje se odnose na identifikaciju vlasnika kartice (zahtjevi 311 i 334 iz Priloga 1.C).

```
WorkshopCardHolderIdentification ::= SEQUENCE {
   workshopName                        Name,
   workshopAddress                     Address,
   cardHolderName                      HolderName,
   cardHolderPreferredLanguage         Language
}
```

workshopName je naziv radionice vlasnika kartice.
workshopAddress je adresa radionice vlasnika kartice.
cardHolderName je prezime i ime (imena) vlasnika kartice (na primjer, ime mehaničara).
cardHolderPreferredLanguage je odabrani jezik vlasnika kartice.

2.238. WorkshopCardPIN

Lični identifikacijski broj kartice radionice (zahtjevi 309 i 332 iz Priloga 1.C).

```
WorkshopCardPIN ::= IA5String(SIZE(8))
```

Dodjela vrijednosti: PIN poznat vlasniku kartice, desno popunjen s bajtima 'FF' do 8 bajtova.

2.239. W-VehicleCharacteristicConstant

Karakteristični koeficijent vozila (definicija (k)).

```
W-VehicleCharacteristicConstant ::= INTEGER(0..2^16-1))
```

Dodjela vrijednosti: Broj impulsa po kilometru u radnom rasponu od 0 do 64 255 impulsa/km.

2.240. VuPowerSupplyInterruptionRecord

Druga generacija:
Informacije sačuvane u jedinici u vozilu koje se odnose na događaje prekida napajanja (zahtjev 117 iz Priloga 1.C).

```
VuPowerSupplyInterruptionRecord ::= SEQUENCE {
   eventType                           EventFaultType,
   eventRecordPurpose                  EventFaultRecordPurpose,
   eventBeginTime                      TimeReal,
   eventEndTime                        TimeReal,
   cardNumberAndGenDriverSlotBegin     FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd       FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin   FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd     FullCardNumberAndGeneration,
   similarEventsNumber                 SimilarEventsNumber
}
```

eventType je vrsta događaja.

eventRecordPurpose je svrha za koju je zabilježen taj događaj..
eventBeginTime je datum i vrijeme početka događaja.
eventEndTime je datum i vrijeme završetka događaja.
cardNumberAndGenDriverSlotBegin označava karticu umetnutu u otvor vozača na početku događaja i njezinu generaciju.
cardNumberAndGenDriverSlotEnd označava karticu umetnutu u otvor vozača na kraju događaja i njezinu generaciju.
cardNumberAndGenCodriverSlotBegin označava karticu umetnutu u otvor suvozača na početku događaja i njezinu generaciju.
cardNumberAndGenCodriverSlotEnd označava karticu umetnutu u otvor suvozača na kraju događaja i njezinu generaciju.
similarEventsNumber je broj sličnih događaja tog dana.

2.241. VuPowerSupplyInterruptionRecordArray

Druga generacija:
Informacije sačuvane u jedinici u vozilu koje se odnose na događaje prekida napajanja (zahtjev 117 iz Priloga 1.C).

```
VuPowerSupplyInterruptionRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuPowerSupplyInterruptionRecord
}
```

recordType označava vrstu zapisa (VuPowerSupplyInterruptionRecord). **Dodjela vrijednosti**: Vidjeti RecordType
recordSize je veličina podatka VuPowerSupplyInterruptionRecord u bajtovima.
noOfRecords je broj zapisâ u nizu zapisa.
records je niz zapisa o događajima prekida napajanja.

2.242. VuSensorExternalGNSSCoupledRecordArray

Druga generacija:
Niz zapisa SensorExternalGNSSCoupledRecord i meta podaci koji se upotrebljavaju u postupku preuzimanja.

```
VuSensorExternalGNSSCoupledRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       SensorExternalGNSSCoupledRecord
}
```

recordType označava vrstu zapisa (SensorExternalGNSSCoupledRecord). **Dodjela vrijednosti**: Vidjeti RecordType
recordSize je veličina podatka SensorExternalGNSSCoupledRecord u bajtovima.
noOfRecords je broj zapisâ u nizu zapisa.
records je niz zapisa o uparivanju senzora s spoljnim uređajem GNSS-a.

2.243. VuSensorPairedRecordArray

Druga generacija:
Niz zapisa SensorPairedRecord i meta podaci koji se upotrebljavaju u postupku preuzimanja.

```
VuSensorPairedRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF SensorPairedRecord
}
```

recordType označava vrstu zapisa (SensorPairedRecord). **Dodjela vrijednosti**: Vidjeti RecordType
recordSize je veličina podatka SensorPairedRecord u bajtovima.
noOfRecords je broj zapisâ u nizu zapisa.
records je niz zapisa o uparivanju senzora.

3. DEFINICIJE VRIJEDNOSTI I RASPONA VELIČINE

Definicija promjenljivih vrijednosti koje se upotrebljavaju u definicijama u stavu 2.

```
TimeRealRange ::= 2^31-1
```

4. SKUPINE ZNAKOVA (CHARACTER SETS)

Za IA5Strings upotrebljavaju se ASCII znakovi definisani u normi ISO/IEC 8824-1. Radi čitljivosti i lakšeg upućivanja, u nastavu je navedena dodjela vrijednosti. U slučaju nepodudarnosti, norma ISO/IEC 8824-1 ima prednost nad ovom informativnom bilješkom.

```
  ! " # $ % & ' ( ) * + , - . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ?
@ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [ \ ] ^ _
` a b c d e f g h i j k l m n o p q r s t u v w x y z { | } ~
```

U drugim se nizovima znakova (adresa, naziv, VehicleRegistrationNumber) upotrebljavaju i znakovi iz raspona decimalnih kodova od 161 do 255 od sljedećih 8-bitnih standardnih skupina znakova, koje utvrđuje broj kodne stranice: Standardni skup znakova	Kodna stranica (Decimalno)
ISO/IEC 8859-1 Latinica-1 Zapadnoevropski	1

ISO/IEC 8859-2 Latinica-2 Srednjeevropski	2
ISO/IEC 8859-3 Latinica-3 Južnoevropski	3
ISO/IEC 8859-5 Latinica/Ćirilica	5
ISO/IEC 8859-7 Latinica/Grčki	7
ISO/IEC 8859-9 Latinica-5 Turski	9
ISO/IEC 8859-13 Latinica-7 Baltički krug	13
ISO/IEC 8859-15 Latinica-9	15
ISO/IEC 8859-16 Latinica-10 Jugoistačnoevropski	16
KOI8-R Latinica/Ćirilica	80
KOI8-U Latinica/Ćirilica	85

5. KODIRANJE

Pri kodiranju u skladu s pravilima o kodiranju ASN.1, sve definisane vrste podataka kodiraju se u skladu s normom ISO/IEC 8825-2, usklađena inačica.

6. IDENTIFIKATORI OBJEKTA I IDENTIFIKATORI APLIKACIJE

6.1. Identifikatori objekta

Identifikatori objekta (OID-ovi) navedeni u ovome poglavlju odnose se isključivo na drugu generaciju. Ti su OID-ovi utvrđeni u TR-03110-3, a ovdje ih se ponavlja u svrhu cjelovitosti. Ti su OID-ovi sadržani u podstablu bsi-de:

```
bsi-de OBJECT IDENTIFIER ::= {
   itu-t(0) identified-organization(4) etsi(0)
   reserved(127) etsi-identified-organization(0) 7
}
```

Identifikatori postupka autentifikacije jedinice u vozilu

```
id-TA          OBJECT IDENTIFIER ::= {bsi-de protocols(2) smartcard(2) 2}

id-TA-ECDSA                OBJECT IDENTIFIER ::= {id-TA 2}

id-TA-ECDSA-SHA-256 OBJECT IDENTIFIER ::= {id-TA-ECDSA 3}

id-TA-ECDSA-SHA-384 OBJECT IDENTIFIER ::= {id-TA-ECDSA 4}

id-TA-ECDSA-SHA-512 OBJECT IDENTIFIER ::= {id-TA-ECDSA 5}
```

Primjer: Ako se autentifikaciju jedinice u vozilu planira izvršiti s pomoću SHA-384, potrebno je upotrijebiti identifikator objekta (u ASN.1 zapisu) `bsi-de protocols(2) smartcard(2) 2 2 4`. Vrijednost je ovog identifikatora objekta u zapisu s tačkama (*dot notation*) `0.4.0.127.0.7.2.2.2.2.4`.

	Zapis s tačkama (*Dot notation*)	**Zapis u bajtovima (*Byte notation*)**
id-TA-ECDSA-SHA-256	0.4.0.127.0.7.2.2.2.2.3	'04 00 7F 00 07 02 02 02 02 03'
id-TA-ECDSA-SHA-384	0.4.0.127.0.7.2.2.2.2.4	'04 00 7F 00 07 02 02 02 02 04'
id-TA-ECDSA-SHA-512	0.4.0.127.0.7.2.2.2.2.5	'04 00 7F 00 07 02 02 02 02 05'

Identifikatori postupka autentifikacije čipa

```
id-CA          OBJECT IDENTIFIER ::= {bsi-de protocols(2) smartcard(2) 3}

id-CA-ECDH                      OBJECT IDENTIFIER ::= {id-CA 2}

id-CA-ECDH-AES-CBC-CMAC-128     OBJECT IDENTIFIER ::= {id-CA-ECDH 2}

id-CA-ECDH-AES-CBC-CMAC-192     OBJECT IDENTIFIER ::= {id-CA-ECDH 3}

id-CA-ECDH-AES-CBC-CMAC-256     OBJECT IDENTIFIER ::= {id-CA-ECDH 4}
```

Primjer: Autentifikacija čipa izvršena je s pomoću ECDH algoritma i stvoren je AES ključ razmjene podataka dug 128 bitova. Taj će se ključ razmjene podataka zatim upotrijebiti u CBC načinu rada radi osiguranja tajnosti podataka i s CMAC algoritmom radi osiguranja vjerodostojnosti podataka. Stoga je potrebno upotrijebiti identifikator objekta (u ASN.1 zapisu) `bsi-de protocols(2) smartcard(2) 3 2 2`. Vrijednost je ovog identifikatora objekta u zapisu s tačkama (*dot notation*) `0.4.0.127.0.7.2.2.3.2.2`.

	Zapis s tačkama (*Dot notation*)	**Zapis u bajtovima (*Byte notation*)**
id-CA-ECDH-AES-CBC-CMAC-128	0.4.0.127.0.7.2.2.3.2.2	'04 00 7F 00 07 02 02 03 02 02'
id-CA-ECDH-AES-CBC-CMAC-192	0.4.0.127.0.7.2.2.3.2.3	'04 00 7F 00 07 02 02 03 02 03'
id-CA-ECDH-AES-CBC-CMAC-256	0.4.0.127.0.7.2.2.3.2.4	'04 00 7F 00 07 02 02 03 02 04'

6.2. Identifikatori aplikacije

Druga generacija:

Identifikator aplikacije (AID) za spoljni uređaj GNSS-a (druge generacije) određen je s 'FF 44 54 45 47 4D'. To je vlasnički AID u skladu s normom ISO/IEC 7816-4.

Napomena: Zadnjih 5 bajtova kodira DTEGM za spoljni uređaj GNSS-a pametnog tahografa.

Identifikator aplikacije za aplikaciju tahografske kartice druge generacije određen je s 'FF 53 4D 52 44 54'. To je vlasnički AID u skladu s normom ISO/IEC 7816-4.

SPECIFIKACIJE TAHOGRAFSKE KARTICE
SADRŽAJ

1. UVOD

1.1. Kratice

Za potrebe ovog dodatka primjenjuju se sljedeće kratice:

AC	Uslovi pristupa (engl. Access conditions)
AES	Standard naprednog šifriranja (engl. Advanced Encryption Standard)
AID	Identifikator aplikacije (engl. Application Identifier)
ALW	Uvijek (engl. Always)
APDU	Podatkovna jedinica protokola aplikacije (struktura naredbe) (engl. Application Protocol Data Unit)
ATR	Odziv na povraćaj u početno stanje (engl. Answer to Reset)
AUT	Autentificiran.
C6, C7	Kontakti br. 6 i 7 kartice kako su opisani u normi ISO/IEC 7816-2
cc	Satni ciklusi (engl. clock cycles)
CHV	Informacije za provjeru vlasnika kartice (engl. Card holder Verification Information)
CLA	Bajt razreda određene APDU naredbe (engl. Class byte of an APDU command)
DSRC	Namjenski komunikacijski sistem kratkog dometa (engl. Dedicated Short Range Communication)
DF	Namjenska datoteka (engl. Dedicated File) DF može sadržiti druge datoteke (EF ili DF)
ECC	Kriptografija na temelju eliptičke krivulje (engl. Elliptic Curve Cryptography)

EF Elementarna datoteka (engl. Elementary File)
etu Elementarna jedinica vremena (engl. elementary time unit)
G1 Prva generacija
G2 Druga generacija
IC Integrirani krug (engl. Integrated Circuit)
ICC Kartica s integrisanim krugovima (engl. Integrated Circuit Card)
ID Identifikator (engl. Identifier)
IFD Naprava sučelja (engl. Interface Device)
IFS Veličina informacijskog polja (engl. Information Field Size)
IFSC Veličina informacijskog polja na kartici (engl. Information Field Size for the card)
IFSD Veličina informacijskog polja naprave (za terminal) (engl. Information Field Size Device (for the Terminal))
INS Bajt instrukcije određene APDU naredbe (engl. Instruction byte of an APDU command)
Lc Dužina ulaznih podataka za naredbu APDU (engl. Length of the input data for a APDU command)
Le Dužina očekivanih podataka (izlazni podaci za naredbu) (engl. Length of the expected data (output data for a command))
MF Glavna datoteka (temeljni DF) (engl. Master File (root DF))
NAD Adresa čvora upotrijebljena u protokolu T = 1 (engl. Node Address used in T=1 protocol)
NEV Nikad (engl. Never)
P1-P2 Parametarski bajtovi (engl. Parameter bytes)
PIN Lični identifikacijski broj (engl. Personal Identification Number)
PRO SM Zaštićeno sigurnim prenosom poruka (engl. Protected with secure messaging)
PTS Odabir prenosa protokola (engl. Protocol Transmission Selection)
RFU Rezervisano za buduću upotrebu (engl. Reserved for Future Use)
RST Povraćajak u početno stanje (kartice) (engl. Reset (of the card))
SFID Kratki EF identifikator (engl. Short EF Identifier)
SM Sigurne poruke (engl. Secure Messaging)
SW1-SW2 Statusni bajtovi (engl. Status bytes)
TS Početni ATR znak (engl. Initial ATR character)
VPP Napon programiranja (engl. Programming Voltage)
VU Jedinica u vozilu (engl. Vehicle Unit)
XXh Vrijednost XX u heksadecimalnom zapisu
'XXh' Vrijednost XX u heksadecimalnom zapisu
|| Simbol ulančavanja 03||04 = 0304
CHA ovlaštenje nosioca certifikata (eng. Certificate Holder Authorisation)
DO podatkovni objekt (eng. Data Object)";

1.2. Literatura

U ovome su Dodatku upotrijebljeni sljedeći izvori:

ISO/IEC 7816-2 Identification cards – Integrated circuit cards – Part 2: Dimensions and location of the contacts. ISO/IEC 7816-2:2007.
ISO/IEC 7816-3 Identification cards – Integrated circuit cards – Part 3: Electrical interface and transmission protocols. ISO/IEC 7816-3:2006.
ISO/IEC 7816-4 Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange. ISO/IEC 7816-4:2013 + Cor 1: 2014.
ISO/IEC 7816-6 Identification cards – Integrated circuit cards – Part 6: Interindustry data elements for interchange. ISO/IEC 7816-6:2004 + Cor 1: 2006.
ISO/IEC 7816-8 Identification cards – Integrated circuit cards – Part 8: Commands for security operations. ISO/IEC 7816-8:2004.
ISO/IEC 9797-2 Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function. ISO/IEC 9797-2:2011

2. ELEKTRIČNA I FIZIČKA OBILJEŽJA

TCS_01 Ako nije drukčije propisano, svi elektronički signali moraju biti u skladu s normom ISO/IEC 7816-3.
TCS_02 Položaj i dimenzije kontakata kartice moraju biti u skladu s ISO/IEC 7816-2.

2.1. Napon napajanja i potrošnja struje

TCS_03 Kartica radi u skladu sa specifikacijama u granicama potrošnje naznačenima u normi ISO/IEC 7816-3.
TCS_04 Kartica radi s Vcc = 3V (±0,3 V) ili s Vcc = 5V (±0,5 V).
Napon se odabire prema ISO/IEC 7816-3.

2.2. Napon programiranja V_{pp}

TCS_05 Kartica ne zahtijeva napon programiranja na pinu C6. Očekuje se da pin C6 nije priključen na IFD. Kontakt C6 može se priključiti na V_{cc} u kartici, ali ne smije ga se uzemljiti. Ovaj se napon ni u kojem slučaju ne bi trebao interpretirati.

2.3. Generisanje i frekvencija sata

TCS_06 Kartica radi u frekvencijskom rasponu od 1 do 5 MHz, a može podržavati i više frekvencije. Unutar jedne sesije rada s karticom, frekvencija sata može odstupati za ±2 %. Frekvenciju sata generiše jedinica u vozilu, a ne sama kartica. Radni ciklus se može izmjenjivati između 40 i 60 %.
TCS_07 Spoljni sat može se zaustaviti u uslovima sadržanima u datoteci kartice EF ICC. Prvi bajt sadržaja datoteke EF ICC kodira uslove režima Clockstop:

Niska	Visoka		
Bit 3	Bit 2	Bit 1	
0	0	1	Clockstop dopušten, nema povlaštene nivoe
0	1	1	Clockstop dopušten, povlaštena je visoka nivo
1	0	1	Clockstop dopušten, povlaštena je niska nivo
0	0	0	Clockstop nije dopušten
0	1	0	Clockstop je dopušten isključivo na visokoj nivou
1	0	0	Clockstop je dopušten isključivo na niskoj nivou

Bitovi od 4 do 8 se ne koriste.

2.4. Kontakt I/O

TCS_08 Kontakt I/O C7 upotrebljava se za prijam podataka iz IFD-a i odašiljanje podataka u IFD. Tokom rada, u režimu odašiljanja treba bitiili kartica ili IFD. Ako su obje jedinice u režimu odašiljanja, to ne uzrokuje oštećenje kartice. Kad ne odašilje, kartica ulazi u režim prijama.

2.5. Stanja kartice

TCS_09 Dok je priključeno napajanje, kartica radi u dva stanja:
radno stanje tokom izvršavanja naredbe ili spajanja s digitalnom jedinicom,
stanje mirovanja u svako drugo vrijeme; u tom stanju kartica zadržava sve podatke.

3. HARDVER I KOMUNIKACIJA

3.1. Uvod

Ovaj stavak opisuje minimalnu funkcionalnost koju moraju imati tahografske kartice i jedinice u vozilu kako bi se osigurali ispravan rad i interoperabilnost.
Tahografske kartice su što je više moguće sukladne raspoloživim primjenjivim ISO/IEC normama (posebno ISO/IEC 7816). No ipak, naredbe i protokoli su u cijelosti opisani kako bi se odredila neka ograničena uporaba ili neke razlike ako ih ima. Ako nije drukčije naznačeno, navedene naredbe u cijelosti su u skladu sa spomenutim normama.

3.2. Protokol prenosa

TCS_10 Protokol prenosa u skladu je s normom ISO/IEC 7816-3 za T = 0 i T = 1. Konkretno, jedinica vozila mora raspoznati produženja vremena čekanja koje odašilje kartica.

3.2.1 *Protokoli*

TCS_11 Kartica mora podržavati protokol **T = 0** i protokol **T = 1**. Kartice mogu podržavati i druge protokole koji se odnose na kontakte.
TCS_12 **T = 0** zadani je protokol te je stoga potrebna naredba **PTS** za prelaz na protokol **T = 1**.
TCS_13 Naprave podržavaju **neposrednu konvenciju** u oba protokola te je stoga za karticu obavezna neposredna konvencija.
TCS_14 Bajt **Veličina informacijskog polja na kartici** prisutan je pri ATR-u u znaku TA3. Ta vrijednost iznosi najmanje 'F0h' (= 240 bajta).
Na protokole se primjenjuju sljedeća ograničenja:
TCS_15 **T = 0**
— Naprava sučelja podržava odgovor na I/O nakon vršnog signala na RST od 400 cc.
— Naprava sučelja mora moći iščitati znakove s razmakom od 12 etu.
— Naprava sučelja mora moći iščitati pogrešan znak i njegovo ponavljanje ako su razmaknuti za 13 etu. Ako je otkriven pogrešan znak, može se pojaviti signal pogreške na I/O između 1 etu i 2 etu. Naprava podržava kašnjenje od 1 etu.
— Naprava sučelja prihvaća 33-bajtni ATR (TS + 32).
— Ako je u ATR prisutan TC1, za znakove koje šalje naprava sučelja prisutno je dodatno zaštitno vrijeme, iako znakovi koje šalje kartica i dalje mogu biti razmaknuti za 12 etu. Ovo vrijedi i za znak ACK, koji kartica šalje nakon znaka P3 koji je odaslala naprava sučelja.
— Naprava sučelja uzima u obzir znak NUL koji odašilje kartica.
— Naprava sučelja prihvaća komplementarne režime za ACK.
— Naredba kojom se potražuje odgovor (get-response) ne može se koristiti u režimu ulančavanja za dobivanje podataka čija bi dužina mogla prelaziti 255 bajtova.
TCS_16 **T = 1**
— Bajt NAD: ne upotrebljava se (NAD se postavlja na '00').
— S-block ABORT: ne upotrebljava se.
— Pogreška stanja S-block VPP: ne upotrebljava se.
— Ukupna dužina ulančavanja podatkovnog polja ne prelazi 255 bajta (što osigurava IFD).
— Veličina informacijskog polja naprave (IFSD) naznačena je s pomoću IFD-a neposredno nakon ATR-a: IFD odašilje S-Block IFS zahtjev nakon ATR-a, a kartica šalje nazad S-Block IFS. Preporučena vrijednost za IFSD je 254 bajta.
— Kartica ne traži ponovno podešavanje IFS-a.

3.2.2 *ATR*

TCS_17 Naprava provjerava bajtove ATR u skladu s normom ISO/IEC 7816-3. Ne vrši se provjera na istorijskim znakovima ATR.
Primjer osnovnog bi-protokola ATR u skladu s normom ISO/IEC 7816-3.

Znak	Vrijednost	Napomene
TS	'3Bh'.	Označava neposrednu konvenciju.
T0	'85h'.	TD1 prisutan; prisutno je pet istorijskih bajtova.
TD1	'80h'	TD2 prisutan; upotrebljava se T = 0

TD2	'11h'.	TA3 prisutan; upotrebljava se T = 1
TA3	'XXh' (najmanje 'F0h')	Veličina informacijskog polja na kartici (IFSC)
TH1 do TH5	'XXh'	Istorijski znakovi
TCK	'XXh'	Znak za arhiviranje (isključivi OR, tj. XOR)

TCS_18 Nakon ATR-a (odziv na povraćaj u početno stanje) implicitno se odabire glavna datoteka (MF) i ona postaje trenutni direktorij.

3.2.3 *PTS*

TCS_19 T = 0 je zadani protokol. Za postavljanje protokola T = 1 uređaj šalje kartici PTS (poznat i kao PPS).

TCS_20 Kako su protokoli T = 0 i T = 1 obvezni, osnovni PTS za izmjenu protokola obvezan je za karticu.

Kako je naznačeno u normi ISO/IEC 7816-3, PTS se može upotrebljavati za prelaz na brzine prenosa podataka više od zadane brzine prenosa podataka koju predlaže kartica u ATR (bajt TA(1)), ako postoji.

Za karticu su više brzine prenosa podataka neobvezne.

TCS_21 Ako nije podržana niti jedna brzina prenosa podataka osim zadane (ili ako odabrana brzina prenosa podataka nije podržana), kartica ispravno odgovara na PTS u skladu s normom ISO/IEC 7816-3 ispuštanjem bajta PPS1.

Primjeri osnovnih PTS za odabir protokola su sljedeći:

Znak	**Vrijednost**	**Napomene**
PPSS	'FFh'	Početni znak.
PPS0	'00h' ili '01h'	Nema PPS1 do PPS3; '00h' za odabir T0, '01h' za odabir T1.
PK	'XXh'	Znak za arhiviranje: 'XXh' = 'FFh' ako je PPS0 = '00h', 'XXh' = 'FEh' ako je PPS0 = '01h'.

3.3. Uslovi pristupa

TCS_22 Pravilom za pristup utvrđuju se odgovarajući sigurnosni uslovi za način pristupa, odnosno naredbu. Ako su ti sigurnosni zahtjevi ispunjeni, obrađuje se odgovarajuća naredba.

TCS_23 Sljedeći se sigurnosni uslovi upotrebljavaju u tahografskim karticama:

Kratica	**Značenje**
ALW	Radnja je uvijek moguća i može se izvesti bez ograničenja. APDU naredbe i odgovori šalju se u običnom tekstu, odnosno bez sigurnog prenosa poruka.
NEV	Radnja nikad nije moguća.
PLAIN-C	APDU naredbe šalju se u običnom tekstu, odnosno bez sigurnog prenosa poruka.
PWD	Radnju je moguće provesti samo ako je PIN kartice radionice uspješno provjeren, odnosno ako je postavljen status „PIN_Verified" unutarnje sigurnosti kartice. Naredbu se mora slati bez sigurnog prenosa poruka.
EXT-AUT-G1	Radnju je moguće provesti samo ako je naredba EXTERNAL AUTHENTICATE za autentifikaciju prve generacije (vidjeti Dodatak 11. dio A) uspješno provedena.
SM-MAC-G1	APDU (naredba i odgovor) mora se primjenjivati u sigurnom prenosu poruka u prvoj generaciji u načinu rada namijenjenom isključivo autentifikaciji (vidjeti Dodatak 11. dio A).
SM-C-MAC-G1	Naredba APDU mora se primjenjivati u sigurnom prenosu poruka u prvoj generaciji u načinu rada namijenjenom isključivo autentifikaciji (vidjeti Dodatak 11. dio A).
SM-R-ENC-G1	Odgovor APDU mora se primjenjivati u sigurnom prenosu poruka u prvoj generaciji u načinu rada namijenjenom šifriranju (vidjeti Dodatak 11. dio A), odnosno ne vraća se kod za autentifikaciju poruke.
SM-R-ENC-MAC-G1	Odgovor APDU mora se primjenjivati u sigurnom prenosu poruka u prvoj generaciji u načinu rada namijenjenom šifriranju i zatim autentifikaciji (*encrypt-then-authenticate mode*) (vidjeti Dodatak 11. dio A).
SM-MAC-G2	APDU (naredba i odgovor) mora se primjenjivati u sigurnom prenosu poruka u drugoj generaciji u načinu rada namijenjenom isključivo autentifikaciji (vidjeti Dodatak 11. dio B).
SM-C-MAC-G2	Naredba APDU mora se primjenjivati u sigurnom prenosu poruka u drugoj generaciji u načinu rada namijenjenom isključivo autentifikaciji (vidjeti Dodatak 11. dio B).
SM-R-ENC-MAC-G2	Odgovor APDU mora se primjenjivati u sigurnom prenosu poruka u drugoj generaciji u načinu rada namijenjenom šifriranju i zatim autentifikaciji (*encrypt-then-authenticate mode*) (vidjeti Dodatak 11. dio B).

TCS_24 Ti sigurnosni uslovi mogu biti povezani na sljedeće načine:

AND (‚i'): svi sigurnosni uslovi moraju biti ispunjeni

OR (‚ili'): barem jedan sigurnosni uvjet mora biti ispunjen

Uslovi pristupa datotečnom sistemu, odnosno naredbe SELECT, READ BINARY i UPDATE BINARY, utvrđeni su u poglavlju 4. Uslovi pristupa za preostale naredbe utvrđeni su u tablicama u nastavu. Termin ‚nije primjenjivo' koristi se ako nema zahtjeva koji bi podržao naredbu. U tom slučaju naredba može ili ne mora biti podržana, ali uvjet pristupa je izvan područja primjene.

TCS_25 U aplikaciji DF tahografa prve generacije upotrebljavaju se sljedeći uslovi pristupa:

„Naredba	**Kartica vozača**	**Kartica radionice**	**Kontrolna kartica**	**Kartica preduzeće**
External Authenticate				
— Za autentifikaciju prve generacije	ALW	ALW	ALW	ALW
— Za autentifikaciju druge generacije	ALW	PWD	ALW	ALW
Internal Authenticate	ALW	PWD	ALW	ALW
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	Nije primjenljivo	Nije primjenljivo	Nije primjenljivo	Nije primjenljivo

PSO: Compute Digital Signature	ALW ILI SM-MAC-G2	ALW ILI SM-MAC-G2	Nije primjenljivo	Nije primjenljivo
PSO: Hash	Nije primjenljivo	Nije primjenljivo	ALW	Nije primjenljivo
PERFORM HASH of FILE	ALW ILI SM-MAC-G2	ALW ILI SM-MAC-G2	Nije primjenljivo	Nije primjenljivo
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Nije primjenljivo	Nije primjenljivo	ALW	Nije primjenljivo
Verify	Nije primjenljivo	ALW	Nije primjenljivo	Nije primjenljivo";

TCS_26 U aplikaciji DF tahografa druge generacije upotrebljavaju se sljedeći uslovi pristupa:

„Naredba	**Kartica vozača**	**Kartica radionice**	**Kontrolna kartica**	**Kartica preduzeće**
External Authenticate				
— Za autentifikaciju prve generacije	Nije primjenljivo	Nije primjenljivo	Nije primjenljivo	Nije primjenljivo
— Za autentifikaciju druge generacije	ALW	PWD	ALW	ALW
Internal Authenticate	Nije primjenljivo	Nije primjenljivo	Nije primjenljivo	Nije primjenljivo
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	Nije primjenljivo	ALW	ALW	Nije primjenljivo
PSO: Compute Digital Signature	ALW ILI SM-MAC-G2	ALW ILI SM-MAC-G2	Nije primjenljivo	Nije primjenljivo
PSO: Hash	Nije primjenljivo	Nije primjenljivo	ALW	Nije primjenljivo
PERFORM HASH of FILE	ALW ILI SM-MAC-G2	ALW ILI SM-MAC-G2	Nije primjenljivo	Nije primjenljivo
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Nije primjenljivo	Nije primjenljivo	ALW	Nije primjenljivo
Verify	Nije primjenljivo	ALW	Nije primjenljivo	Nije primjenljivo

TCS_27 U glavnoj datoteci upotrebljavaju se sljedeći uslovi pristupa:

„Naredba	**Kartica vozača**	**Kartica radionice**	**Kontrolna kartica**	**Kartica preduzeće**
External Authenticate				
— za autentifikaciju prve generacije	Nije primjenljivo	Nije primjenljivo	Nije primjenljivo	Nije primjenljivo
— za autentifikaciju prve generacije	ALW	PWD	ALW	ALW
Internal Authenticate	Nije primjenljivo	Nije primjenljivo	Nije primjenljivo	Nije primjenljivo
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	Nije primjenljivo	Nije primjenljivo	Nije primjenljivo	Nije primjenljivo
PSO: Compute Digital Signature	Nije primjenljivo	Nije primjenljivo	Nije primjenljivo	Nije primjenljivo
PSO: Hash	Nije primjenljivo	Nije primjenljivo	Nije primjenljivo	Nije primjenljivo
PERFORM HASH of FILE	Nije primjenljivo	Nije primjenljivo	Nije primjenljivo	Nije primjenljivo
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Nije primjenljivo	Nije primjenljivo	Nije primjenljivo	Nije primjenljivo
Verify	Nije primjenljivo	ALW	Nije primjenljivo	Nije primjenljivo"

TCS_28 Tahografska kartica može, ali ne mora, prihvatiti naredbu više nivoe sigurnosti od one navedene u sigurnosnim uslovima. Odnosno, ako je sigurnosni uvjet ALW (ili PLAIN-C), kartica može prihvatiti naredbu sa sigurnim prenosom poruka (način rada sa šifriranjem i/ili autentifikacijom). Ako se sigurnosnim uslovom zahtijeva siguran prenos poruka u načinu rada s autentifikacijom, tahografska kartica može prihvatiti naredbu sa sigurnim prenosom poruka iste generacije u načinu rada s autentifikacijom i šifriranjem.

Napomena: U opisima naredbi navedeno je više informacija o podržavanju naredbi za različite vrste tahografskih kartica i različite namjenske datoteke (DF-ove).

3.4. Pregled kodova naredbi i pogrešaka

Naredbe i ustroj datoteka izvedeni su i usklađeni s normom ISO/IEC 7816-4.

Ovaj odjeljak opisuje sljedeće parove naredbi i odgovora APDU: Varijante naredbi koje podržavaju aplikacije prve i druge generacije navedene su u odgovarajućim opisima naredbi.

Naredba	**INS**
SELECT	'A4h'
READ BINARY	'B0h', 'B1h'
UPDATE BINARY	'D6h', 'D7h'
GET CHALLENGE	'84h'
VERIFY	'20h'
GET RESPONSE	'C0h'
PERFORM SECURITY OPERATION	'2Ah'
— VERIFY CERTIFICATE	
— COMPUTE DIGITAL SIGNATURE	
— VERIFY DIGITAL SIGNATURE	
— HASH	

— PERFORM HASH OF FILE	
— PROCESS DSRC MESSAGE	
INTERNAL AUTHENTICATE	‘88h’
EXTERNAL AUTHENTICATE	‘82h’
MANAGE SECURITY ENVIRONMENT	‘22h’
— SET DIGITAL SIGNATURE TEMPLATE	
— SET AUTHENTICATION TEMPLATE	
GENERAL AUTHENTICATE	‘86h’

TCS_29 Statusne riječi SW1 SW2 uključene su u svaki odgovor i označuju stanje obrade naredbe.

SW1	SW2	Značenje
90	00	Normalna obrada.
61	XX	Normalna obrada. XX = broj raspoloživih bajtova odgovora.
62	81	Obrada uz upozorenje. Dio vraćenih podataka može biti neispravan
63	00	Neuspjela autentifikacija (upozorenje)
63	CX	Pogrešan CHV (PIN). ‚X' je brojač preostalih pokušaja.
64	00	Pogreška u izvršenju – stanje postojane memorije nepromijenjeno. Pogreška u integritetu.
65	00	Pogreška u izvršenju – stanje postojane memorije promijenjeno
65	81	Pogreška u izvršenju – stanje postojane memorije promijenjeno – pogreška memorije
66	88	fSigurnosna pogreška: pogrešan kriptografski kontrolni zbir (tokom sigurnog prenosa poruka) ili pogrešan certifikat (tokom provjere certifikata) ili pogrešan kriptogram (tokom vanjske autentifikacije) ili pogrešan potpis (tokom provjere potpisa)
67	00	Pogrešna dužina (pogrešan Lc ili Le)
68	83	Zadnja očekivana naredba u lancu
69	00	Zabranjena naredba (nema odgovora u T = 0)
69	82	Sigurnosni status nije zadovoljen.
69	83	Blokiran način autentifikacije.
69	85	Uslovi uporabe nisu zadovoljeni.
69	86	Naredba nije dopuštena (nema trenutačnog EF-a).
69	87	Nedostaju očekivani podatkovni objekti sigurnog prenosa poruka
69	88	Neispravni podatkovni objekti sigurnog prenosa poruka
6A	80	Pogrešni parametri u podatkovnom polju
6A	82	Datoteka nije pronađena.
6A	86	Pogrešni parametri P1-P2.
6A	88	Podaci na koje upućuje naredba nisu pronađeni.
6B	00	Pogrešni parametri (protuvrijednost izvan EF-a).
6C	XX	Pogrešna dužina, SW2 označava tačnu dužinu. Nikakvo podatkovno polje nije uzvraćeno.
6D	00	Naredbeni kôd nije podržan ili nije važeći.
6E	00	Razred nije podržan.
6F	00	- Ostale pogreške provjere

Dodatne statusne riječi definisane normom ISO/IEC 7816-4 mogu se uzvratiti ako njihovo ponašanje nije izričito spomenuto u ovom dodatku.

Na primjer, sljedeće statusne riječi mogu se uzvratiti:

6881: logički kanal nije podržan

6882: siguran prenos poruke nije podržan

TCS_30 Ako je ispunjen više od jednog uslova za greške u jednoj APDU naredbi, kartica može uzvratiti bilo koju od odgovarajućih statusnih riječi.

3.5. Opis naredbi

U ovom su poglavlju opisane obvezne naredbe za tahografske kartice.

Daljnje predmetne pojedinosti, povezane s obuhvaćenim kriptografskim radnjama navedene su u Dodatku 11. „Zajednički sigurnosni mehanizmi" za tahografe prve i druge generacije.

Sve naredbe opisane su nezavisno o korištenom protokolu (T = 0 ili T = 1). Uvijek su naznačeni APDU bajtovi CLA, INS, PI, P2, Lc i Le. Ako Lc ili Le nisu potrebni za opisanu naredbu, pridružena dužina, vrijednost i opis su prazni.

TCS_31 Ako se zahtijevaju oba bajta dužine (Lc i Le), opisanu naredbu potrebno je podijeliti u dva dijela ako IFD upotrebljava protokol T = 0: IFD šalje naredbu kako je opisana s P3 = Lc + podaci te zatim šalje naredbu GET RESPONSE (vidjeti tačku 3.5.6) s P3 = Le.

TCS_32 Ako se zahtijevaju oba bajta dužine, a Le = 0 (sigurni prenos poruka):

— prilikom korištenja protokola T = 1, kartica odgovara na Le = 0 slanjem svih raspoloživih izlaznih podataka

— prilikom korištenja protokola T = 0, IFD šalje prvu naredbu s P3 = Lc + podaci, kartica (na taj implicitni Le = 0) odgovara statusnim bajtovima ‘**61La**’, pri čemu je La broj raspoloživih bajtova odgovora. IFD potom generiše naredbu GET RESPONSE s P3 = La za čitanje podataka.

TCS_33 Tahografska kartica može podržavati produžena polja dužine u skladu s normom ISO/IEC 7816-4. Tahografska kartica koja podržava produžena polja dužine:

— pokazuje podržavanje produženog polja dužine u ATR

— dostavlja podržane veličine međuspremnika s pomoću informacija o produženju u EF ATR/INFO, vidjeti TCS_146.
— naznačuje podržava li produžena polja dužine za T = 1 i/ili T = 0 u EF Extended Length, vidjeti TCS_147.
— podržava produžena polja dužina za aplikacije tahografa prve i druge generacije.

Napomene:

Sve su naredbe namijenjene kratkim poljima dužine. Način upotrebe produženih APDU-ova jasan je iz norme ISO/IEC 7816-4.

Naredbe su uopšteno navedene za nešifrirani način, odnosno bez sigurnog prenosa poruka jer je nivo sigurnog prenosa poruka utvrđena u Dodatku 11. Iz uslova pristupa za naredbu jasno je podržavaju li se njome siguran prenos poruka i siguran prenos poruka za prvu generaciju i/ili drugu generaciju. Neke su varijante naredbi opisane sa sigurnim prenosom poruka kako bi se prikazala upotreba sigurnog prenosa poruka.

TCS_34 Jedinica u vozilu sprovodi cjelokupan protokol uzajamne autentifikacije jedinice u vozilu druge generacije i kartice unutar jedne sesije, uključujući provjeru certifikata (prema potrebi) u DF tahografu, DF tahografu druge generacije ili u MF-u.

3.5.1 *SELECT*

Ova naredba u skladu je s normom ISO/IEC 7816-4, ali ima ograničenu primjenu u poređenju s naredbom utvrđenom u normi.

Naredba SELECT upotrebljava se za sljedeće:
— odabir DF-a aplikacije (obvezan odabir po imenu),
— odabir elementarne datoteke koja odgovara ID-u predane datoteke.

3.5.1.1 Odabir po nazivu (AID)

Ova naredba omogućava odabir DF-a aplikacije na kartici.

TCS_35 Ova naredba može se izvoditi sa svakog mjesta u strukturi datoteke (poslije ATR ili u bilo kojem trenutku).

TCS_36 Odabir aplikacije vraća trenutno sigurnosno okruženje u početno stanje. Nakon odabira aplikacije, više se ne odabire trenutni javni ključ. Gubi se i uvjet pristupa EXT-AUT-G1. Ako je naredba izvršena bez sigurnog prenosa poruka, ključevi prethodnog sigurnog prenosa poruka više nisu dostupni.

TCS_37 **Poruka naredbe**

Bajt	Dužina	Vrijednost	Opis
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'04h'.	Odabir po nazivu (AID)
P2	1	'0Ch'	Ne očekuje se odgovor.
Lc	1	'NNh'	Broj bajtova poslanih na karticu (dužina AID-a): '06h' za tahografsku aplikaciju
#6-#(5+NN)	NN	'XX..XXh'	AID: 'FF 54 41 43 48 4F' za aplikaciju prve generacije tahografa AID: 'FF 53 4D 52 44 54' za aplikaciju druge generacije tahografa

Za naredbu SELECT nije potreban nikakav odgovor (ako u T = 1 nema Le, ili se ne traži odgovor kod T = 0).

TCS_38 **Odgovor na poruku (ne traži se odgovor)**

Bajt	Dužina	Vrijednost	Opis
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna, kartica uzvraća '**9000**'.
— Ako nije pronađena aplikacija koja odgovara AID, uzvraćeno stanje obrade je '**6A82**',
— U T = 1, ako je prisutan bajt Le, uzvraćeno stanje je '**6700**',
— U T = 0, ako se traži odgovor poslije naredbe SELECT, uzvraćeno stanje je '**6900**'
— Ako se odabrana aplikacija smatra neispravnom (u atributima datoteke otkrivena je pogreška u integritetu), uzvraćeno stanje obrade je ,**6400' ili ,6500'.**

3.5.1.2 Odabir elementarne datoteke upotrebom njezina identifikatora datoteke

TCS_39 **Poruka naredbe**

TCS_40 Tahografska kartica mora podržavati siguran prenos poruka u drugoj generaciji kako je utvrđeno u Dodatku 11. dijelu B. za ovu varijantu naredbe.

Bajt	Dužina	Vrijednost	Opis
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'02h'	Odabir EF-a u okviru trenutnog DF-a
P2	1	'0Ch'	Ne očekuje se odgovor.
Lc	1	'02h'	Broj bajtova poslanih na karticu
#6-#7	2	'XXXXh'	Identifikator datoteke

Za naredbu SELECT nije potreban nikakav odgovor (ako u T = 1 nema Le, ili se ne traži odgovor kod T = 0).

TCS_41 **Odgovor na poruku (ne traži se odgovor)**

Bajt	Dužina	Vrijednost	Opis
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna, kartica uzvraća '**9000**'.
— Ako nije nađena datoteka koja odgovara identifikatoru datoteke, uzvraćeno stanje obrade je '**6A82**'.
— U T = 1, ako je prisutan bajt Le, uzvraćeno stanje je '**6700**',
— U T = 0, ako se traži odgovor poslije naredbe SELECT, uzvraćeno stanje je '**6900**'
— Ako se odabrana datoteka smatra neispravnom (u atributima datoteke otkrivena je pogreška u integritetu), uzvraćeno stanje obrade je **,6400' ili ,6500'.**

3.5.2 *READ BINARY*

Ova naredba u skladu je s normom ISO/IEC 7816-4, ali ima ograničenu primjenu u poređenju s naredbom utvrđenom u normi.

Naredba READ BINARY upotrebljava se za čitanje podataka iz transparentne datoteke.

Odgovor kartice se sastoji od uzvraćanja pročitanih podataka koji se mogu neobvezno zatvoriti u strukturu sigurnog čitanja poruke.

3.5.2.1 Naredba s pomakom u P1-P2

Ova naredba omogućava IFD-u čitanje podataka iz trenutno odabranog EF-a bez sigurnog prenosa poruka.

Napomena: Ova naredba se bez sigurnog prenosa poruka može upotrebljavati samo za potrebe očitavanja datoteke koja podržava ALW sigurnosni uvjet pri načinu pristupa za očitavanje.

TCS_42 **Poruka naredbe**

Bajt	Dužina	Vrijednost	Opis
CLA	1	'00h'	
INS	1	'B0h'	Binarno čitanje
P1	1	'XXh'	Pomak u bajtovima od početka datoteke: najvažniji bajt
P2	1	'XXh'	Pomak u bajtovima od početka datoteke: najmanje važan bajt
Le	1	'XXh'	Očekivana dužina podatka. Broj bajtova koje se očitava.

Napomena: bit 8 u P1 mora biti postavljen na 0.

TCS_43 **Odgovor na poruku**

Bajt	Dužina	Vrijednost	Opis
#1-#X	X	'XX..XXh'	Očitani podaci
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna, kartica uzvraća '**9000**'.

— Ako nije odabran EF, uzvraćeno stanje obrade je '**6986**'.

— Ako za odabranu datoteku nisu ispunjeni sigurnosni uslovi, naredba se prekida s '**6982**'.

— Ako pomak ne odgovara veličini EF-a (pomak > veličine EF-a), uzvraćeno stanje obrade je '**6B00**'.

— Ako veličina podataka koje treba pročitati ne odgovara veličini EF-a (pomak + Le > veličine EF-a), uzvraćeno stanje obrade je '**6700**' ili '**6Cxx**', pri čemu je 'xx' tačna dužina.

— ako je otkrivena pogreška u integritetu unutar atributa datoteke, kartica će datoteku smatrati neispravnom i nepopravljivom, te je uzvraćeno stanje obrade ‚**6400' ili ‚6500'.**

— Ako je otkrivena pogreška u integritetu u sačuvanim podacima, kartica uzvraća tražene podatke, a uzvraćeno stanje obrade je '**6281**'.

3.5.2.1.1 Naredba sa sigurnim prenosom poruke (primjeri)

Ova naredba omogućava IFD-u čitanje podataka iz trenutno odabranog EF-a uz siguran prenos poruka radi povjere integriteta primljenih podataka i zaštite povjerljivosti podataka ako se primjenjuje sigurnosni uvjet SM-R-ENC-MAC-G1 (prva generacija) ili SM-R-ENC-MAC-G2 (druga generacija).

TCS_44 **Poruka naredbe**

Bajt	Dužina	Vrijednost	Opis
CLA	1	'0Ch'	Traži se siguran prenos poruka
INS	1	'B0h'	Binarno čitanje
P1	1	'XXh'	P1 (pomak u bajtovima od početka datoteke): najvažniji bajt
P2	1	'XXh'	P2 (pomak u bajtovima od početka datoteke): najmanje važan bajt
Lc	1	'XXh'	Dužina ulaznih podataka za siguran prenos poruka
#6	1	'97h'	T_{LE}: Oznaka za očekivanu specifikaciju dužine.
#7	1	'01h'	L_{LE}: Dužina očekivane dužine
#8	1	'NNh'	Specifikacija očekivane dužine (izvorni Le): broj bajtova koje se očitava
#9	1	'8Eh'	T_{CC}: oznaka za kriptografski kontrolni zbir
#10	1	'XXh'	L_{CC}: dužina sljedećeg kriptografskog kontrolnog zbira '04h' za siguran prenos poruka u prvoj generaciji (vidjeti Dodatak 11. dio A) '08h', '0Ch' ili '10h' zavisno o dužini AES ključa za siguran prenos poruka u drugoj generaciji (vidjeti Dodatak 11. dio B)
#11-#(10+L)	L	'XX..XXh'	Kriptografski kontrolni zbir
Le	1	'00h'	Kako je utvrđeno u normi ISO/IEC 7816-4.

TCS_45 **Odgovor na poruku ako se ne zahtijeva SM-R-ENC-MAC-G1 (prva generacija) / SM-R-ENC-MAC-G2 (druga generacija) i ako je ulazni format za siguran prenos poruka tačan:**

„Bajt	Dužina	Vrijednost	Opis
#1	1	'81h'	T_{PV}: oznaka za vrijednost nešifriranih podataka
#2	L	'NNh' ili '81 NNh'	L_{PV}: dužina uzvraćenih podataka (= izvorni Le). L iznosi 2 bajta ako je L_{PV} > 127 bajtova.
#(2+L) - #(1+L+NN)	NN	'XX..XXh'	Vrijednost nešifriranih podataka
#(2+L+NN)	1	'99h'	Oznaka za status obrade (SW1-SW2) – neobavezna za siguran prenos poruka u prvoj generaciji
#(3+L+NN)	1	'02h'	Dužina statusa obrade – neobavezna za siguran prenos poruka u prvoj generaciji

#(4+L+NN) - #(5+L+NN)	2	'XX XXh'	Status obrade nezaštićenog odgovora APDU – neobvezan za siguran prenos poruka u prvoj generaciji
#(6+L+NN)	1	'8Eh'	TCC: oznaka za kriptografski kontrolni zbir
#(7+L+NN)	1	'XXh'	LCC: dužina sljedećeg kriptografskog kontrolnog zbira '04h' za siguran prenos poruka u prvoj generaciji (vidjeti Dodatak 11. dio A) '08h', '0Ch' ili '10h' zavisno o dužini AES ključa za siguran prenos poruka u drugoj generaciji (vidjeti Dodatak 11. dio B)
#(8+L+NN)- #(7+M+L+NN)	M	'XX..XXh'	Kriptografski kontrolni zbir
SW	2	'XXXXh'	Statusne riječi (SW1,SW2)";

TCS_46 **Odgovor na poruku ako se zahtijeva SM-R-ENC-MAC-G1 (prva generacija) / SM-R-ENC-MAC-G2 (druga generacija) i ako je ulazni format za siguran prenos poruka tačan:**

„Bajt	Dužina	Vrijednost	Opis
#1	1	'87h'	$T_{PI\ CG}$: oznaka za šifrirane podatke (kriptogram)
#2	L	'MMh' ili '81 MMh'	$L_{PI\ CG}$: dužina uzvraćenih šifriranih podataka (razlikuje se od izvornog Le naredbe zbog popunjenja). L iznosi 2 bajta ako je LPI CG > 127 bajtova
#(2+L)- #(1+L+MM)	MM	'01XX..XXh'	Šifrirani podaci: indikator popunjenja i kriptogram
#(2+L+MM)	1	'99h'	Oznaka za status obrade (SW1-SW2) – neobavezna za siguran prenos poruka u prvoj generaciji
#(3+L+MM)	1	'02h'	Dužina statusa obrade – neobavezna za siguran prenos poruka u prvoj generaciji
#(4+L+MM) - #(5+L+MM)	2	'XX XXh'	Status obrade nezaštićenog odgovora APDU – neobvezan za siguran prenos poruka u prvoj generaciji
#(6+L+MM)	1	'8Eh'	TCC: oznaka za kriptografski kontrolni zbir
#(7+L+MM)	1	'XXh'	LCC: dužina sljedećeg kriptografskog kontrolnog zbira '04h' za siguran prenos poruka u prvoj generaciji (vidjeti Dodatak 11. dio A) '08h', '0Ch' ili '10h' zavisno o dužini AES ključa za siguran prenos poruka u drugoj generaciji (vidjeti Dodatak 11. dio B)
#(8+L+MM)- #(7+N+L+MM)	N	'XX..XXh'	Kriptografski kontrolni zbir
SW	2	'XXXXh'	Statusne riječi (SW1,SW2)";

Naredba READ BINARY može uzvratiti stanja normalne obrade navedena u TCS_43 pod oznakom '99h' kako je opisano u TCS_59 upotrebom strukture sigurne razmjene poruka odgovora.
Osim toga, mogu se dogoditi i neke pogreške karakteristične za siguran prenos poruka. U tom se slučaju stanje obrade jednostavno vraća bez uključivanja strukture sigurnog prenosa poruka.

TCS_47 **Poruka odgovora kod netačnog ulaznog formata za siguran prenos poruka**

Bajt	Dužina	Vrijednost	Opis
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

— Ako ne postoji ključ trenutne sesije, uzvraća se stanje obrade '**6A88**'. To se može dogoditi ako još nije napravljen ključ sesije ili ako je važnost ključa sesije istekla (u tom slučaju IFD mora ponovo pokrenuti postupak međusobne autentifikacije za postavljanje novog ključa sesije).
— Ako neki očekivani podatkovni objekti (kako su prethodno navedeni) nedostaju u formatu sigurnog prenosa poruka, uzvraća se stanje obrade '**6987**': do ove pogreške dolazi ako nema očekivane oznake ili ako naredbodavni sadržaj nije pravilno izrađen.
— Ako neki podatkovni objekti nisu točni, uzvraćeno stanje obrade je '**6988**': ova pogreška se događa ako su prisutne sve tražene oznake, ali su neke dužine različite od očekivanih.
— Ako provjera kriptografskog kontrolnog zbira ne uspije, uzvraćeno stanje obrade je '**6688**'.

3.5.2.2 Naredba s kratkim EF identifikatorom (identifikator elementarne datoteke)

Ovom se varijantom naredbe omogućava IFD-u da odabere EF putem kratkog EF identifikatora i da očita podatke s tog EF-a.
TCS_48 Tahografska kartica mora podržavati tu varijantu naredbe za sve elementarne datoteke s utvrđenim kratkim EF identifikatorom. Ti su kratki EF identifikatori opisani u poglavlju 4.

TCS_49 **Poruka naredbe**

Bajt	Dužina	Vrijednost	Opis
CLA	1	'00h'	
INS	1	'B0h'	Binarno čitanje
P1	1	'XXh'	Bit 8 postavlja se na 1 Bitovi 7 i 6 postavljaju se na 00 Bit 5 – 1 kodira kratki EF identifikator odgovarajućeg EF-a
P2	1	'XXh'	Kodira pomak s 0 do 255 bajtova u EF-u na koji upućuje P1
Le	1	'XXh'	Očekivana dužina podatka. Broj bajtova koje se očitava.

Napomena: Kratki EF identifikatori koji se upotrebljavaju u aplikaciji tahografa druge generacije utvrđeni su u poglavlju 4.
Ako P1 kodira kratki EF identifikator, a naredba je uspješna, utvrđeni EF postaje trenutno odabrani EF (trenutni EF).
TCS_50 **Odgovor na poruku**

Bajt	Dužina	Vrijednost	Opis
#1-#L	L	'XX..XXh'	Očitani podaci
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna, kartica uzvraća '**9000**'.
— Ako nije nađena datoteka koja odgovara kratkom EF identifikatoru, uzvraćeno stanje obrade je '**6A82**'.
— Ako za odabranu datoteku nisu ispunjeni sigurnosni uslovi, naredba se prekida s '**6982**'.
— Ako pomak ne odgovara veličini EF-a (pomak > veličine EF-a), uzvraćeno stanje obrade je '**6B00**'.
— Ako veličina podataka koje treba pročitati ne odgovara veličini EF-a (pomak + Le > veličine EF-a), uzvraćeno stanje obrade je '**6700**' ili '**6Cxx**', pri čemu je 'xx' tačna dužina.
— ako je otkrivena pogreška u integritetu unutar atributa datoteke, kartica će datoteku smatrati neispravnom i nepopravljivom, te je uzvraćeno stanje obrade **‚6400' ili ‚6500'.**
— Ako je otkrivena pogreška u integritetu u sačuvanim podacima, kartica uzvraća tražene podatke, a uzvraćeno stanje obrade je '**6281**'.

3.5.2.3 Naredba s neparnim bajtom instrukcije

Ovom se varijantom naredbe omogućava IFD-u da očita podatke iz EF-a koji sadržiju 32 768 ili više bajtova.
TCS_51 Tahografska kartica koja podržava EF-ove s 32 768 ili više bajtova mora podržavati tu varijantu naredbe za te EF-ove. Tahografska kartica može, ali ne mora podržavati tu varijantu naredbe za druge EF-ove, osim za EF Sensor_Installation_Data, vidjeti TCS_156 i TCS_160.
TCS_52 **Poruka naredbe**

Bajt	Dužina	Vrijednost	Opis
CLA	1	'00h'	
INS	1	'B1h'	Binarno čitanje
P1	1	'00h'	Trenutni EF
P2	1	'00h'	
Lc	1	'NNh'	Lc Dužina pomaka podatkovnog objekta.
#6-#(5+NN)	NN	'XX..XXh'	Pomak podatkovnog objekta: Oznaka '54h' Dužina '01h' ili '02h' Vrijednost pomak
Le	1	'XXh'	Kako je utvrđeno u normi ISO/IEC 7816-4"

U slučaju protokola T = 1 uzvraćeno stanje obrade je '6700' u slučaju da je Le = '01h'.";
IFD kodira dužinu pomaka podatkovnog objekta s najmanjim mogućim brojem okteta, odnosno upotrebom bajta dužine '01h' IFD kodira pomak od 0 do 255, a upotrebom bajta dužine '02h' pomak od '256' do '65 535' bajtova.
U slučaju protokola T = 0 kartica pretpostavlja da je vrijednost Le = '00h' ako nije primijenjen siguran prenos poruka.
TCS_53 **Odgovor na poruku**

Bajt	Dužina	Vrijednost	Opis
#1-#L	L	'XX..XXh'	Očitani podaci sažeti su u diskrecijskom podatkovnom objektu s oznakom '53h'.
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna, kartica uzvraća '**9000**'.
— Ako nije odabran EF, uzvraćeno stanje obrade je '**6986**'.
— Ako za odabranu datoteku nisu ispunjeni sigurnosni uslovi, naredba se prekida s '**6982**'.
— Ako pomak ne odgovara veličini EF-a (pomak > veličine EF-a), uzvraćeno stanje obrade je '**6B00**'.
— Ako veličina podataka koje treba pročitati ne odgovara veličini EF-a (pomak + Le > veličine EF-a), uzvraćeno stanje obrade je '**6700**' ili '**6Cxx**', pri čemu je 'xx' tačna dužina.
— Ako je otkrivena pogreška u integritetu unutar atributa datoteke, kartica će datoteku smatrati neispravnom i nepopravljivom, te je uzvraćeno stanje obrade **‚6400' ili ‚6500'.**
— Ako je otkrivena pogreška u integritetu u sačuvanim podacima, kartica uzvraća tražene podatke, a uzvraćeno stanje obrade je '**6281**'.

3.5.2.3.1 Naredba sa sigurnim prenosom poruke (primjer)

U sljedećem je primjeru prikazana upotreba sigurnog prenosa poruka ako se primjenjuje sigurnosni uvjet SM-MAC-G2.
TCS_54 Poruka naredbe

Bajt	Dužina	Vrijednost	Opis
CLA	1	'0Ch'	Traži se siguran prenos poruka
INS	1	'B1h'	Binarno čitanje
P1	1	'00h'	Trenutni EF
P2	1	'00h'	
Lc	1	'XXh'	Dužina polja zaštićenih podataka
#6	1	'B3h'	Oznaka za vrijednost nešifriranih podataka u BER-TLV
#7	1	'NNh'	L_{PV}: dužina poslanih podataka
#(8)-	NN	'XX..XXh'	Nešifrirani podaci kodirani u BER-TLV, odnosno pomak podatkovnog objekta s

#(7+NN)			oznakom ‘54’
#(8+NN)	1	‘97h’	T_{LE}: Oznaka za očekivanu specifikaciju dužine.
#(9+NN)	1	‘01h’	L_{LE}: Dužina očekivane dužine
#(10+NN)	1	‘XXh’	Specifikacija očekivane dužine (izvorni Le): broj bajtova koje se očitava
#(11+NN)	1	‘8Eh’	T_{CC}: oznaka za kriptografski kontrolni zbir
#(12+NN)	1	‘XXh’	L_{CC}: dužina sljedećeg kriptografskog kontrolnog zbira ‘08h’, ‘0Ch’ ili ‘10h’ zavisno o dužini AES ključa za siguran prenos poruka u drugoj generaciji (vidjeti Dodatak 11. dio B)
#(13+NN)-#(12+M+NN)	M	‘XX..XXh’	Kriptografski kontrolni zbir
Le	1	‘00h’	Kako je utvrđeno u normi ISO/IEC 7816-4.

TCS_55 Poruka odgovora ako je naredba bila uspješna

Bajt	Dužina	Vrijednost	Opis
#1	1	‘B3h’	Nešifrirani podaci kodirani u BER-TLV
#2	L	‘NNh’ ili ‘81 NNh’	L_{PV}: dužina uzvraćenih podataka (= izvorni Le). L iznosi 2 bajta ako je L_{PV} > 127 bajtova.
#(2+L)-#(1+L+NN)	NN	‘XX..XXh’	Vrijednost nešifriranih podataka kodiranih u BER-TLV, odnosno očitani podaci sažeti u diskrecijskom podatkovnom objektu s oznakom ‘53h’.
#(2+L+NN)	1	‘99h’	Status obrade nezaštićenog odgovora APDU
#(3+L+NN)	1	‘02h’	Dužina statusa obrade
#(4+L+NN) – #(5+L+NN)	2	‘XX XXh’	Status obrade nezaštićenog odgovora APDU
#(6+L+NN)	1	‘8Eh’	T_{CC}: oznaka za kriptografski kontrolni zbir
#(7+L+NN)	1	‘XXh’	L_{CC}: dužina sljedećeg kriptografskog kontrolnog zbira ‘08h’, ‘0Ch’ ili ‘10h’ zavisno o dužini AES ključa za siguran prenos poruka u drugoj generaciji (vidjeti Dodatak 11. dio B)
#(8+L+NN)-#(7+M+L+NN)	M	‘XX..XXh’	Kriptografski kontrolni zbir
SW	2	‘XXXXh’	Statusne riječi (SW1, SW2)

3.5.3 *UPDATE BINARY*

Ova naredba u skladu je s normom ISO/IEC 7816-4, ali ima ograničenu primjenu u poređenju s naredbom utvrđenom u normi.

Poruka naredbe UPDATE BINARY započinje ažuriranjem (brisanje + pisanje) bitova koji su već sadržani u binarnom EF-u, s bitovima danim u naredbi APDU.

3.5.3.1 Naredba s pomakom u P1-P2

Ova naredba omogućava IFD-u upisivanje podataka u trenutno odabran EF bez da kartica provjerava integritet primljenih podataka.

Napomena: Ova se naredba bez sigurnog prenosa poruka može upotrebljavati samo za potrebe ažuriranja datoteke koja podržava ALW sigurnosni uvjet za način pristupa za ažuriranje.

TCS_56 **Poruka naredbe**

Bajt	Dužina	Vrijednost	Opis
CLA	1	‘00h’	
INS	1	‘D6h’	Binarno ažuriranje
P1	1	‘XXh’	Pomak u bajtovima od početka datoteke: najvažniji bajt
P2	1	‘XXh’	Pomak u bajtovima od početka datoteke: najmanje važan bajt
Lc	1	‘NNh’	Lc Dužina podataka koje se ažurira. broj bajtova koje se upisuje.
#6-#(5+NN)	NN	‘XX..XXh’	Podaci koji se zapisuju

Napomena: bit 8 u P1 mora biti postavljen na 0.

TCS_57 **Odgovor na poruku**

Bajt	Dužina	Vrijednost	Opis
SW	2	‘XXXXh’	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna, kartica uzvraća ‘**9000**’.

— Ako nije odabran EF, uzvraćeno stanje obrade je ‘**6986**’.

— Ako za odabranu datoteku nisu ispunjeni sigurnosni uslovi, naredba se prekida s ‘**6982**’.

— Ako pomak ne odgovara veličini EF-a (pomak > veličine EF-a), uzvraćeno stanje obrade je ‘**6B00**’.

— Ako veličina podataka koje treba upisati nije u skladu s veličinom EF-a (pomak + Lc > veličine EF-a), uzvraćeni status obrade je ‘**6700**’.

— Ako je otkrivena pogreška u integritetu unutar atributa datoteke, kartica će datoteku smatrati neispravnom i nepopravljivom, te je uzvraćeno stanje obrade ‘**6400**’ ili ‘**6500**’.

— Ako zapisivanje nije uspješno, uzvraćeno stanje obrade je ‘**6581**’.

3.5.3.1.1 Naredba sa sigurnim prenosom poruke (primjeri)

Ova naredba omogućava IFD-u upisivanje podataka u trenutno odabran EF, a kartica provjerava integritet primljenih podataka. Budući da nije tražena povjerljivost podataka, podaci nisu šifrirani.

TCS_58 **Poruka naredbe**

Bajt	Dužina	Vrijednost	Opis
CLA	1	‘0Ch’	Traži se siguran prenos poruka
INS	1	‘D6h’	Binarno ažuriranje
P1	1	‘XXh’	Pomak u bajtovima od početka datoteke: najvažniji bajt
P2	1	‘XXh’	Pomak u bajtovima od početka datoteke:

			najmanje važan bajt
Lc	1	'XXh'	Dužina polja zaštićenih podataka
#6	1	'81h'	T_{PV}: Oznaka za vrijednost nešifriranih podataka
#7	L	'NNh' ili '81 NNh'	L_{PV}: dužina poslanih podataka. L iznosi 2 bajta ako je L_{PV} > 127 bajtova.
#(7+L)- #(6+L+NN)	NN	'XX..XXh'	Vrijednost nešifriranih podataka (podaci koje se upisuje)
#(7+L+NN)	1	'8Eh'	T_{CC}: oznaka za kriptografski kontrolni zbir
#(8+L+NN)	1	'XXh'	L_{CC}: Dužina sljedećeg kriptografskog kontrolnog zbira '04h' za siguran prenos poruka u prvoj generaciji (vidjeti Dodatak 11. dio A) '08h', '0Ch' ili '10h' zavisno o dužini AES ključa za siguran prenos poruka u drugoj generaciji (vidjeti Dodatak 11. dio B)
#(9+L+NN)- #(8+M+L+NN)	M	'XX..XXh'	Kriptografski kontrolni zbir
Le	1	'00h'	Kako je utvrđeno u normi ISO/IEC 7816-4.

TCS_59 **Poruka odgovora kod tačnog ulaznog formata za siguran prenos poruka**

Bajt	Dužina	Vrijednost	Opis
#1	1	'99h'	T_{SW}: oznaka za statusne riječi (koje treba zaštititi sa CC)
#2	1	'02h'	L_{SV}: dužina uzvraćenih statusnih riječi
#3-#4	2	'XXXXh'	Status obrade nezaštićenog odgovora APDU
#5	1	'8Eh'	T_{CC}: oznaka za kriptografski kontrolni zbir
#6	1	'XXh'	L_{CC}: dužina sljedećeg kriptografskog kontrolnog zbira '04h' za siguran prenos poruka u prvoj generaciji (vidjeti Dodatak 11. dio A) '08h', '0Ch' ili '10h' zavisno o dužini AES ključa za siguran prenos poruka u drugoj generaciji (vidjeti Dodatak 11. dio B)
#7-#(6+L)	L	'XX..XXh'	Kriptografski kontrolni zbir
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

„Redovna" stanja obrade opisana za naredbu UPDATE BINARY bez sigurnog prenosa poruka (vidjeti tačku 3.5.3.1) mogu se uzvratiti tako da se koristi prethodno opisana struktura poruka odgovora.

Osim toga, mogu se dogoditi i neke pogreške karakteristične za siguran prenos poruka. U tom se slučaju stanje obrade jednostavno vraća bez uključivanja strukture sigurnog prenosa poruka:

TCS_60 **Poruka odgovora ako je u sigurnom prenosu poruka došlo do pogreške**

Bajt	Dužina	Vrijednost	Opis
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

— Ako ne postoji ključ trenutne sesije, uzvraća se stanje obrade '**6A88**'.

— Ako neki očekivani podatkovni objekti (kako su prethodno navedeni) nedostaju u formatu sigurnog prenosa poruka, uzvraća se stanje obrade '**6987**': do ove pogreške dolazi ako nema očekivane oznake ili ako naredbodavni sadržaj nije pravilno izrađen.

— Ako neki podatkovni objekti nisu točni, uzvraćeno stanje obrade je '**6988**': ova pogreška se događa ako su prisutne sve tražene oznake, ali su neke dužine različite od očekivanih.

— Ako provjera kriptografskog kontrolnog zbira ne uspije, uzvraćeno stanje obrade je '**6688**'.

3.5.3.2 Naredba s kratkim EF identifikatorom

Ovom se varijantom naredbe omogućava IFD-u da odabere EF putem kratkog EF identifikatora i da upiše podatke s tog EF-a.

TCS_61 Tahografska kartica mora podržavati tu varijantu naredbe za sve elementarne datoteke s utvrđenim kratkim EF identifikatorom. Ti su kratki EF identifikatori opisani u poglavlju 4.

TCS_62 **Poruka naredbe**

Bajt	Dužina	Vrijednost	Opis
CLA	1	'00h'	
INS	1	'D6h'	Binarno ažuriranje
P1	1	'XXh'	Bit 8 postavlja se na 1 Bitovi 7 i 6 postavljaju se na 00 Bit 5 – 1 kodira kratki EF identifikator odgovarajućeg EF-a
P2	1	'XXh'	Kodira pomak s 0 do 255 bajtova u EF-u na koji upućuje P1
Lc	1	'NNh'	Lc Dužina podataka koje se ažurira. broj bajtova koje se upisuje.
#6-#(5+NN)	NN	'XX..XXh'	Podaci koji se zapisuju

TCS_63 **Odgovor na poruku**

Bajt	Dužina	Vrijednost	Opis
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

Napomena: Kratki EF identifikatori koji se upotrebljavaju u aplikaciji tahografa druge generacije utvrđeni su u poglavlju 4.

Ako P1 kodira kratki EF identifikator, a naredba je uspješna, utvrđeni EF postaje trenutno odabrani EF (trenutni EF).

— Ako je naredba uspješna, kartica uzvraća '**9000**'.

— Ako nije nađena datoteka koja odgovara kratkom EF identifikatoru, uzvraćeno stanje obrade je '**6A82**'.

— Ako za odabranu datoteku nisu ispunjeni sigurnosni uslovi, naredba se prekida s '**6982**'.

— Ako pomak ne odgovara veličini EF-a (pomak > veličine EF-a), uzvraćeno stanje obrade je '**6B00**'.

— Ako veličina podataka koje treba upisati nije u skladu s veličinom EF-a (pomak + Lc > veličine EF-a), uzvraćeni status obrade je '**6700**'.

— ako je otkrivena pogreška u integritetu unutar atributa datoteke, kartica će datoteku smatrati neispravnom i nepopravljivom, te je uzvraćeno stanje obrade ,**6400' ili ,6500'.**
— Ako zapisivanje nije uspješno, uzvraćeno stanje obrade je '**6581**'.

3.5.3.3 Naredba s neparnim bajtom instrukcije

Ovom se varijantom naredbe omogućava IFD-u da upiše podatke u EF koji sadržiju 32 768 ili više bajtova.
TCS_64 Tahografska kartica koja podržava EF-ove s 32 768 ili više bajtova mora podržavati tu varijantu naredbe za te EF-ove. Tahografska kartica može, ali ne mora podržavati tu varijantu naredbe za druge EF-ove.
TCS_65 **Poruka naredbe**

Bajt	Dužina	Vrijednost	Opis
CLA	1	'00h'	
INS	1	'D7h'	Binarno ažuriranje
P1	1	'00h'	Trenutni EF
P2	1	'00h'	
Lc	1	'NNh'	Lc Dužina podataka u polju s podacima naredbe
#6-#(5+NN)	NN	'XX..XXh'	Pomak podatkovnog objekta s oznakom '54h' || Diskrecijski podatkovni objekt s oznakom '53h' koji sažima podatke koje se upisuje

IFD kodira dužinu pomaka podatkovnog objekta i diskrecijskog podatkovnog objekta s najmanjim mogućim brojem okteta, odnosno upotrebom bajta dužine '01h' IFD kodira pomak/dužinu od 0 do 255, a upotrebom bajta dužine '02h' pomak/dužinu od '256' do '65 535 ' bajtova
TCS_66 **Odgovor na poruku**

Bajt	Dužina	Vrijednost	Opis
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna, kartica uzvraća '**9000**'.
— Ako nije odabran EF, uzvraćeno stanje obrade je '**6986**'.
— Ako za odabranu datoteku nisu ispunjeni sigurnosni uslovi, naredba se prekida s '**6982**'.
— Ako pomak ne odgovara veličini EF-a (pomak > veličine EF-a), uzvraćeno stanje obrade je '**6B00**'.
— Ako veličina podataka koje treba upisati nije u skladu s veličinom EF-a (pomak + Lc > veličine EF-a), uzvraćeni status obrade je '**6700**'.
— Ako je otkrivena pogreška u integritetu unutar atributa datoteke, kartica će datoteku smatrati neispravnom i nepopravljivom, te je uzvraćeno stanje obrade '**6400**' ili '**6500**'.
— Ako zapisivanje nije uspješno, uzvraćeno stanje obrade je '**6581**'.

3.5.3.3.1 Naredba sa sigurnim prenosom poruke (primjer)

U sljedećem je primjeru prikazana upotreba sigurnog prenosa poruka ako se primjenjuje sigurnosni uvjet SM-MAC-G2.
TCS_67 Poruka naredbe

Bajt	Dužina	Vrijednost	Opis
CLA	1	'0Ch'	Traži se siguran prenos poruka
INS	1	'D7h'	Binarno ažuriranje
P1	1	'00h'	Trenutni EF
P2	1	'00h'	
Lc	1	'XXh'	Dužina polja zaštićenih podataka
#6	1	'B3h'	Oznaka za vrijednost nešifriranih podataka u BER-TLV
#7	L	'NNh' ili '81 NNh'	L_{PV}: dužina poslanih podataka. L iznosi 2 bajta ako je L_{PV} > 127 bajtova.
#(7+L)-#(6+L+NN)	NN	'XX..XXh'	Nešifrirani podaci kodirani u BER-TLV, odnosno pomak podatkovnog objekta s oznakom '54h' || Diskrecijski podatkovni objekt s oznakom '53h' koji sažima podatke koje se upisuje
#(7+L+NN)	1	'8Eh'	T_{CC}: oznaka za kriptografski kontrolni zbir
#(8+L+NN)	1	'XXh'	L_{CC}: dužina sljedećeg kriptografskog kontrolnog zbira '08h', '0Ch' ili '10h' zavisno o dužini AES ključa za siguran prenos poruka u drugoj generaciji (vidjeti Dodatak 11. dio B)
#(9+L+NN)-#(8+M+L+NN)	M	'XX..XXh'	Kriptografski kontrolni zbir
Le	1	'00h'	Kako je utvrđeno u normi ISO/IEC 7816-4.

TCS_68 Poruka odgovora ako je naredba bila uspješna

Bajt	Dužina	Vrijednost	Opis
#1	1	'99h'	T_{SW}: oznaka za statusne riječi (koje treba zaštititi sa CC)
#2	1	'02h'	L_{SV}: dužina uzvraćenih statusnih riječi
#3-#4	2	'XXXXh'	Status obrade nezaštićenog odgovora APDU
#5	1	'8Eh'	T_{CC}: oznaka za kriptografski kontrolni zbir
#6	1	'XXh'	L_{CC}: dužina sljedećeg kriptografskog kontrolnog zbira '08h', '0Ch' ili '10h' zavisno o dužini AES ključa za siguran prenos poruka u drugoj generaciji (vidjeti Dodatak 11. dio B)
#7-#(6+L)	L	'XX..XXh'	Kriptografski kontrolni zbir
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

3.5.4 *GET CHALLENGE*

Ova naredba u skladu je s normom ISO/IEC 7816-4, ali ima ograničenu primjenu u poređenju s naredbom utvrđenom u normi.
Naredbom GET CHALLENGE se od kartice traži izdavanje zahtjeva za ključnu riječ (tj. *challenge*) radi korištenja u sigurnosnom postupku u kojem se kartici šalju kriptogram ili šifrirani podaci.

TCS_69 Zahtjev za ključnu riječ koji izdaje kartica vrijedi samo za sljedeću naredbu koja upotrebljava zahtjev za lozinku poslan kartici.

TCS_70 **Poruka naredbe**

Bajt	Dužina	Vrijednost	Opis
CLA	1	'00h'	
INS	1	'84h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Le	1	'08h'	Le (dužina očekivanog zahtjeva za ključnu riječ).

TCS_71 **Odgovor na poruku**

Bajt	Dužina	Vrijednost	Opis
#1-#8	8	'XX..XXh'	Zahtjev za ključnu riječ
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna, kartica uzvraća '**9000**'.
— Ako se Le razlikuje od '08h', stanje obrade je '**6700**'.
— Ako parametri P1-P2 nisu točni, stanje obrade je '**6A86**'.

3.5.5 *VERIFY*

Ova naredba u skladu je s normom ISO/IEC 7816-4, ali ima ograničenu primjenu u poređenju s naredbom utvrđenom u normi.
Kako bi se podržala ta naredba, potrebna je samo kartica radionice.
Druge vrste tahografskih kartica mogu, ali ne moraju izvršavati tu naredbu, ali za njih nije personaliziran referentni CHV. Stoga te kartice ne mogu uspješno izvršiti tu naredbu. Ponašanje drugih vrsta tahografskih kartica koje nisu kartice radionice, odnosno kad se uzvrati kod pogreške, nije u području primjene ove specifikacije ako se šalje ta naredba.
Naredba VERIFY na kartici započinje usporedbu između CHV (PIN) podataka koji su poslani iz naredbe s referentnim CHV-om sačuvanim na kartici.
TCS_72 PIN koji unosi korisnik mora biti kodiran u ASCII i desno popunjen bajtima 'FFh' do dužine od 8 bajtova IFD-a, vidjeti i vrstu podataka WorkshopCardPIN u Dodatku 1.
TCS_73 Aplikacije tahografa prve i druge generacije upotrebljavaju isti referentni CHV.
TCS_74 Tahografskom karticom provjerava se je li naredba ispravno kodirana. Ako naredba nije ispravno kodirana, kartica ne uspoređuje CHV vrijednosti, ne umanjuje stanje brojača preostalih pokušaja CHV-a i ne vraća sigurnosni status „PIN_Verified" u početno stanje, nego prekida naredbu. Naredba je kodirana ispravno ako bajtovi CLA, INS, P1, P2, Lc imaju određene vrijednosti, Le nije prisutan, a polje s podacima naredbe ispravne je dužine.
TCS_75 Ako je naredba uspješna, brojač preostalih pokušaja CHV-a pokreće se iznova. Početna je vrijednost brojača preostalih pokušaja CHV-a 5. Ako je naredba uspješna, karticom se postavlja status unutarnje sigurnosti „PIN_Verified". Kartica vraća taj sigurnosni status u početno stanje ako je kartica vraćena u početno stanje ili ako CHV kod poslan u naredbi ne odgovara pohranjenom referentnom CHV-u.
Napomena: Upotrebom istog referentnog CHV-a i globalnog sigurnosnog statusa zaposlenik radionice ne mora ponovno unositi PIN nakon što odabere drugi DF aplikacije tahografa.
TCS_76 Neuspješna usporedba bilježi se na kartici, odnosno brojač preostalih pokušaja CHV-a umanjuje se za jedan, kako bi se ograničio broj naknadnih pokušaja upotrebe referentnog CHV-a.

TCS_77 **Poruka naredbe**

Bajt	Dužina	Vrijednost	Opis
CLA	1	'00h'	
INS	1	'20h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2 (provjereni CHV implicitno je poznat)
Lc	1	'08h'	Dužina poslanog koda CHV
#6-#13	8	'XX..XXh'	CHV

TCS_78 **Odgovor na poruku**

Bajt	Dužina	Vrijednost	Opis
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna, kartica uzvraća '**9000**'.
— Ako nije pronađen referentni CHV, uzvraćeno stanje obrade je '**6A88**'.
— Ako je CHV blokiran (brojač preostalih pokušaja za CHV je nula), uzvraćeno stanje obrade je '**6983**'. Kada se jednom nađe u tom stanju, CHV se više nikada ne može uspješno predočiti.
— Ako je usporedba neuspješna, brojač preostalih pokušaja umanjuje se te se uzvraća status '**63CX**' (X > 0 pri čemu je X brojač preostalih pokušaja CHV-a).
— Ako se referentni CHV smatra neispravnim, uzvraćeno stanje obrade je '**6400**' ili '**6581**'.
— Ako se Lc razlikuje od '08h', stanje obrade je '**6700**'.

3.5.6 *GET RESPONSE*

Ova je naredba u skladu s normom ISO/IEC 7816-4.
Ova naredba (potrebna i dostupna samo za protokol T = 0) se koristi za prenos pripremljenih podataka s kartice na sučelje tahografa (primjer gdje naredba uključuje i Lc i Le).

Naredba GET RESPONSE mora biti izdata neposredno nakon naredbe za pripremu podataka, inače se podaci gube. Nakon izvršenja naredbe GET RESPONSE (osim ako nastupi pogreška '61xx' ili '6Cxx', vidjeti u nastavu), ranije pripremljeni podaci više nisu dostupni.

TCS_79 **Poruka naredbe**

Bajt	Dužina	Vrijednost	Opis
CLA	1	'00h'	
INS	1	'C0h'	
P1	1	'00h'	
P2	1	'00h'	
Le	1	'XXh'	Broj bajtova koji se očekuje

TCS_80 **Odgovor na poruku**

Bajt	Dužina	Vrijednost	Opis
#1-#X	X	'XX..XXh'	Podaci
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna, kartica uzvraća '**9000**'.
— Ako kartica nije pripremila nikakve podatke, uzvraćeno stanje obrade je '**6900**' ili '**6F00**'.
— Ako Le prelazi broj raspoloživih bajtova ili ako je Le nula, uzvraćeno stanje obrade je '**6Cxx**', pri čemu 'xx' označava tačan broj raspoloživih bajtova. U tom su slučaju pripremljeni podaci još uvijek dostupni za iduću naredbu GET RESPONSE.
— Ako Le nije nula, a manji je od broja raspoloživih bajtova, kartica normalno šalje tražene podatke, a uzvraćeno stanje obrade je '**61xx**', pri čemu 'xx' označava broj dodatnih bajtova koji su još uvijek raspoloživi za iduću naredbu GET RESPONSE.
— Ako naredba nije podržana (protokol T = 1), kartica uzvraća '**6D00**'.

3.5.7 *PSO: VERIFY CERTIFICATE*

Ova naredba u skladu je s normom ISO/IEC 7816-8, ali ima ograničenu primjenu u poređenju s naredbom utvrđenom u normi.
Naredbu VERIFY CERTIFICATE kartica koristi za dobivanje izspoljnog javnog ključa i provjeru njegove važenja.

3.5.7.1 Naredba za prvu generaciju – par odgovora

TCS_81 Ovu varijantu naredbe podržavaju samo aplikacije tahografa prve generacije.
TCS_82 Ako je naredba VERIFY CERTIFICATE uspješna, javni ključ se arhivira za buduću upotrebu u sigurno okruženje. Ovaj se ključ izričito postavlja za primjenu u sigurnosnim naredbama (INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE ili VERIFY CERTIFICATE) upotrebom MSE naredbe (vidjeti tačku 3.5.11) s pomoću identifikatora ključa.
TCS_83 U svakom slučaju, naredba VERIFY CERTIFICATE upotrebljava javni ključ koji je ranije odabran u sklopu MSE naredbe za otvaranje certifikata. Ovaj javni ključ mora biti onaj države članice ili evropski.
TCS_84 **Poruka naredbe**

Bajt	Dužina	Vrijednost	Opis
CLA	1	'00h'	
INS	1	'2Ah'	Izrada sigurnosne operacije
P1	1	'00h'	P1
P2	1	'AEh'	P2: podaci koji nisu kodirani po BER-TLV (ulančavanje podatkovnih elemenata)
Lc	1	'C2h'	Lc Dužina certifikata, 194 bajta
#6-#199	194	'XX..XXh'	Certifikat: ulančavanje podatkovnih elemenata (opisano u Dodatku 11.)

TCS_85 **Odgovor na poruku**

Bajt	Dužina	Vrijednost	Opis
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna, kartica uzvraća '**9000**'.
— Ako provjera certifikata ne uspije, uzvraćeno stanje obrade je '**6688**'. Postupak provjere i otvaranja certifikata opisan je u Dodatku 11. za prvu i drugu generaciju.
— Ako u sigurnosnom okruženju nije prisutan javni ključ, uzvraća se stanje obrade '**6A88**'.
— Ako se odabrani javni ključ (upotrijebljen za otvaranje certifikata) smatra oštećenim, uzvraćeno stanje obrade je '**6400**' ili '**6581**'.
— Samo za prvu generaciju: Ako je CHA.LSB (CertificateHolderAuthorisation.equipmentType) odabranog javnog ključa (upotrijebljen za otvaranje certifikata) različit od '00' (odnosno ne pripada državi članici niti je evropski), uzvraćeno je stanje obrade '**6985**'.

3.5.7.2 Naredba za drugu generaciju – par odgovora

Zavisno o veličini krivulje, ECC certifikati mogu biti toliko dugački da ih je nemoguće prenijeti u jednom APDU-u. U tom se slučaju mora upotrijebiti ulančavanje naredbi u skladu s normom ISO/IEC 7816-4 te prenijeti certifikat u dvama uzastopnim PSO-ima: Provjera certifikata APDU-ova.
Struktura certifikata i parametri domene definisani su u Dodatku 11.
TCS_86 Naredbu je moguće izvršiti u MF-u, DF-u tahografa i DF-u tahografa druge generacije, vidjeti i TCS_33.
TCS_87 **Poruka naredbe**

Bajt	Dužina	Vrijednost	Opis
CLA	1	'X0h'	CLA bajt označava ulančavanje naredbi: '00h' jedina ili zadnja naredba u lancu '10h' nije zadnja naredba u lancu
INS	1	'2Ah'	Izrada sigurnosne operacije

P1	1	'00h'	
P2	1	'BEh'	Provjera samoopisnog certifikata
Lc	1	'XXh'	Dužina podatkovnog polja naredbe, vidjeti TCS_88 i TCS_89.
#6-#5+L	L	'XX..XXh'	DER-TLV kodirani podaci: Podatkovni objekt tijela ECC certifikata kao prvi podatkovni objekt ulančan s podatkovnim objektom potpisa ECC certifikata kao drugim podatkovnim objektom ili dijelom tog lanca. Oznaka '7F21' i odgovarajuća dužina ne šalju se. Redoslijed je tih objekata utvrđen.

TCS_88 Za kratke APDU-ove primjenjuju se sljedeće odredbe: IFD upotrebljava najmanji broj APDU-ova potreban za slanje naredbe i šalje najveći mogući broj bajtova u prvoj naredbi APDU-a u skladu s vrijednošću bajta veličine informacijskog polja na kartici, vidjeti TCS_14. Ako se IFD drukčije ponaša, ponašanje kartice nalazi se izvan područja primjene.

TCS_89 Za produžene APDU-ove primjenjuju se sljedeće odredbe: Ako certifikat ne stane u jedan APDU, kartica mora podržavati ulančavanje naredbi. IFD upotrebljava najmanji broj APDU-ova potreban za slanje naredbe i šalje najveći mogući broj bajtova u prvoj naredbi APDU-a. Ako se IFD drukčije ponaša, ponašanje kartice nalazi se izvan područja primjene.

Napomena: U skladu s Dodatkom 11., kartica arhivira certifikat ili relevantan sadržaj certifikata te ažurira currentAuthenicatedTime.

Struktura poruka odgovora i statusnih riječi odgovara definiciji iz TCS_85.

TCS_90 Uz kodove pogrešaka navedene u TCS_85, kartica može uzvratiti sljedeće kodove pogrešaka:

— Ako CHA.LSB (CertificateHolderAuthorisation.equipmentType) odabranog javnog ključa (upotrijebljenog za otvaranje certifikata) nije prikladan za provjeru certifikata u skladu s Dodatkom 11., uzvraćeno je stanje obrade '**6985**'.

— Ako je currentAuthenticatedTime kasniji od datuma isteka certifikata, uzvraćeno je stanje obrade '**6985**'.

— Ako je zadnja naredba u lancu očekivana, kartica uzvraća '**6883**'.

— Ako se u polju s podacima naredbe šalju neispravni parametri, kartica uzvraća '**6A80**' (isto vrijedi i u slučaju da podatkovni objekti nisu poslani utvrđenim redoslijedom).

3.5.8 *INTERNAL AUTHENTICATE*

Ova je naredba u skladu s normom ISO/IEC 7816-4.

TCS_91 Sve tahografske kartice moraju podržavati tu naredbu u DF-u tahografa prve generacije. Naredba može, ali ne mora biti dostupna u MF-u i/ili DF-u tahografa druge generacije. Ako je tako, izvršavanje naredbe završava odgovarajućim kodom pogreške jer je privatni ključ kartice (Card.SK) za protokol autentifikacije za prvu generaciju dostupan samo u DF-u tahografa prve generacije.

Primjenom INTERNAL AUTHENTICATE naredbe, IFD može autentificirati karticu. Postupak autentifikacije je opisan je u Dodatku 11. Sadrži sljedeća očitovanja:

TCS_92 Naredba INTERNAL AUTHENTICATE upotrebljava privatni ključ kartice (odabran implicitno) za potpisivanje autentifikacijskih podataka, uključujući K1 (prvi element za dogovor o ključu sesije) i RND1 te upotrebljava trenutno (putem posljednje naredbe MSE) odabrani javni ključ za šifriranje potpisa i oblikovanje autentifikacijskog tokena (podrobnije u Dodatku 11.).

TCS_93 **Poruka naredbe**

Bajt	Dužina	Vrijednost	Opis
CLA	1	'00h'	CLA
INS	1	'88h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Lc	1	'10h'	Dužina podataka poslanih na karticu
#6 – #13	8	'XX..XXh'	Zahtjev za ključnu riječ upotrijebljen za autentifikaciju kartice
#14 -#21	8	'XX..XXh'	VU.CHR (vidjeti Dodatak 11.)
Le	1	'80h'	Dužina podataka koji se očekuju od kartice

TCS_94 **Odgovor na poruku**

Bajt	Dužina	Vrijednost	Opis
#1-#128	128	'XX..XXh'	Token autentifikacije kartice (vidjeti Dodatak 11.)
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna, kartica uzvraća '**9000**'.

— Ako u sigurnosnom okruženju nije prisutan javni ključ, uzvraćeno je stanje obrade '**6A88**'.

— Ako u sigurnosnom okruženju nije prisutan privatan ključ, uzvraćeno je stanje obrade '**6A88**'.

— Ako VU.CHR ne odgovara identifikatoru trenutnog javnog ključa, uzvraćeno je stanje obrade '**6A88**'.

— Ako se odabrani privatni ključ smatra neispravnim, uzvraćeno je stanje obrade '**6400**' ili '**6581**'.

TCS_95 Ako je naredba INTERNAL AUTHENTICATE uspješna, trenutni ključ sesije, ako postoji, briše se i više nije dostupan. Da bi se dobio novi ključ sesije, naredba EXTERNAL AUTHENTICATE za autentifikaciju mehanizma prve generacije treba biti uspješno izvršena.

3.5.9 *EXTERNAL AUTHENTICATE*

Ova je naredba u skladu s normom ISO/IEC 7816-4.

Kartica naredbom EXTERNAL AUTHENTICATE može autentificirati IFD. Postupak autentifikacije opisan je u Dodatku 11. za tahografe prve i druge generacije (autentifikacija jedinice u vozilu).

TCS_96 Varijantu naredbe za mehanizam uzajamne autentifikacije prve generacije podržavaju samo aplikacije tahografa prve generacije.

TCS_97 Varijantu naredbe za uzajamnu autentifikaciju kartice i jedinice u vozilu moguće je izvesti samo u MF-u, DF-u tahografa i DF-u tahografa druge generacije, vidjeti i TCS_34. Ako je naredba EXTERNAL AUTHENTICATE druge generacije uspješna, trenutni ključ sesije prve generacije, ako postoji, briše se i više nije dostupan.
Napomena: Za ključ sesije druge generacije vidjeti Dodatak 11., stavke CSM_193 i CSM_195. Ako su ključevi sesije druge generacije uspostavljeni i tahografska kartica dobiva nešifriranu naredbu EXTERNAL AUTHENTICATE APDU, ona prekida sesiju sigurnog prenosa poruka druge generacije i uništava ključeve sesije druge generacije.

TCS_98 **Poruka naredbe**

Bajt	Dužina	Vrijednost	Opis
CLA	1	'00h'	CLA
INS	1	'82h'	INS
P1	1	'00h'	Implicitno poznati ključevi i algoritmi
P2	1	'00h'	
Lc	1	'XXh'	Lc (dužina podataka poslanih na karticu)
#6-#(5+L)	L	'XX..XXh'	Autentifikacija prve generacije: Kriptogram (vidjeti Dodatak 11. dio A) Autentifikacija druge generacije: Potpis koji je generisao IFD (vidjeti Dodatak 11. dio B)

TCS_99 **Odgovor na poruku**

Bajt	Dužina	Vrijednost	Opis
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna, kartica uzvraća '**9000**'.
— Ako CHA trenutno postavljenog javnog ključa nije lanac AID-a aplikacije tahografa i vrste jedinice u vozilu, uzvraćeno je stanje obrade '**6F00**'.
— Ako neposredno prije naredbe nema naredbe GET CHALLENGE, uzvraćeno je stanje obrade '**6985**'.
Aplikacija tahografa prve generacije može uzvratiti sljedeće dodatne kodove pogrešaka:
— Ako u sigurnosnom okruženju nije prisutan javni ključ, uzvraća se stanje obrade '**6A88**'.
— Ako u sigurnosnom okruženju nije prisutan privatan ključ, uzvraćeno je stanje obrade '**6A88**'.
— Ako je provjera kriptograma pogrešna, uzvraćeno stanje obrade je '**6688**'.
— Ako se odabrani privatni ključ smatra neispravnim, uzvraćeno je stanje obrade '**6400**' ili '**6581**'.
Varijanta naredbe za autentifikaciju druge generacije može uzvratiti sljedeći dodatni kod pogreške:
— Ako je provjera potpisa neuspjela, kartica uzvraća '**6300**'.

3.5.10 *GENERAL AUTHENTICATE*

Ova se naredba upotrebljava za protokol autentifikacije čipa druge generacije utvrđen u Dodatku 11. dijelu B te je u skladu s normom ISO/IEC 7816-4.
TCS_100 Naredbu je moguće izvršiti u MF-u, DF-u tahografa i DF-u tahografa druge generacije, vidjeti i TCS_34.

TCS_101 **Poruka naredbe**

Bajt	Dužina	Vrijednost	Opis
CLA	1	'00h'	
INS	1	'86h'	
P1	1	'00h'	Implicitno poznati ključevi i protokol
P2	1	'00h'	
Lc	1	'NNh'	Lc: dužina sljedećeg podatkovnog polja
#6-#(5+L)	L	'7Ch' + L_{7C} + '80h' + L_{80} + 'XX..XXh'	DER-TLV kodirana vrijednost kratkotrajnog (ephemeral) javnog ključa (vidjeti Dodatak 11.) Jedinica u vozilu šalje podatkovne objekte tim redoslijedom.
5 + L + 1	1	'00h'	Kako je utvrđeno u normi ISO/IEC 7816-4";

TCS_102 **Odgovor na poruku**

Bajt	Dužina	Vrijednost	Opis
#1-#L	L	'7Ch' + L_{7C} + '81h' + '08h' + 'XX..XXh' + '82h' + L_{82} + 'XX..XXh'	DER-TLV kodirani podaci dinamičke autentifikacije: *nonce* (broj koji se koristi jednom) i token autentifikacije (vidjeti Dodatak 11.)
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna, kartica uzvraća '**9000**'.
— Kartica uzvraća '**6A80**' kako bi se ukazalo na neispravne parametre u podatkovnom polju.
— Kartica uzvraća '**6982**' ako naredba External Authenticate nije uspješno provedena
Objekt odgovora dinamičke autentifikacije podataka '7Ch'
— mora biti prisutan ako je operacija uspješna, odnosno ako su statusne riječi '**9000**',
— ne smije biti prisutan u slučaju pogreške u izvršavanju ili pogreške provjere, odnosno ako su statusne riječi u rasponu od '**6400**' do '**6FFF**' te
— ne mora biti prisutan u slučaju upozorenja, odnosno ako su statusne riječi u rasponu od '**6200**' do '**63FF**'.

3.5.11 *MANAGE SECURITY ENVIRONMENT*

Ova se naredba koristi za postavljanje javnoga ključa za potrebe autentifikacije.

3.5.11.1 Naredba za prvu generaciju – par odgovora

Ova je naredba u skladu s normom ISO/IEC 7816-4. Primjena ove naredbe ograničena je u poređenju s odgovarajućom normom.
TCS_103 Ovu naredbu podržavaju samo aplikacije tahografa prve generacije.
TCS_104 Ključ naveden u podatkovnom polju MSE ostaje trenutni javni ključ do sljedeće ispravne naredbe MSE, odabire se DF ili se kartica vraća u početno stanje.
TCS_105 Ako navedeni ključ (već) nije na kartici, sigurno okruženje ostaje nepromijenjeno.

TCS_106 **Poruka naredbe**

Bajt	Dužina	Vrijednost	Opis
CLA	1	'00h'	CLA
INS	1	'22h'	INS
P1	1	'C1h'	P1: navedeni ključ vrijedi za sve kriptografske radnje
P2	1	'B6h'	P2 (navedeni podaci o digitalnom potpisu)
Lc	1	'0Ah'	Lc: dužina sljedećeg podatkovnog polja
#6	1	'83h'	Oznaka za navođenje javnog ključa u asimetričnim slučajevima
#7	1	'08h'	Dužina reference ključa (identifikatora ključa)
#8-#15	8	'XX..XXh'	Identifikator ključa kako je utvrđen u Dodatku 11.

TCS_107 **Odgovor na poruku**

Bajt	Dužina	Vrijednost	Opis
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna, kartica uzvraća '**9000**'.
— Ako u kartici nema navedenog ključa, uzvraćeno je stanje obrade '**6A88**'.
— Ako u formatu sigurnog prenosa poruka nedostaju neki očekivani podatkovni objekti, uzvraćeno je stanje obrade '**6987**'. To se može dogoditi ako nema oznake '83h',
— Ako su određeni podatkovni objekti neispravni, uzvraćeno je stanje obrade '**6988**'. To se može dogoditi ako dužina identifikatora ključa nije '08h'.
— Ako se odabrani ključ smatra neispravnim, uzvraćeno je stanje obrade '**6400**' ili '**6581**'.

3.5.11.2 Naredba za drugu generaciju – parovi odgovora

Za autentifikaciju druge generacije tahografska kartica podržava sljedeći MSE: Utvrđene verzije naredbe koje su u skladu s normom ISO/IEC 7816-4. Te verzije naredbe nisu podržane u autentifikaciji prve generacije.

3.5.11.2.1 MSE:SET AT za autentifikaciju čipa

Sljedeća se MSE:SET AT naredba upotrebljava za odabir parametara za autentifikaciju čipa koja se sprovodi naknadnom naredbom GENERAL AUTHENTICATE (opšta autentifikacija).
TCS_108 Naredbu je moguće izvršiti u MF-u, DF-u tahografa i DF-u tahografa druge generacije, vidjeti i TCS_34.
TCS_109 **MSE:SET AT Poruka naredbe za autentifikaciju čipa**

Bajt	Dužina	Vrijednost	Opis
CLA	1	'00h'	
INS	1	'22h'	
P1	1	'41h'	Utvrđeno za unutarnju autentifikaciju
P2	1	'A4h'	Autentifikacija
Lc	1	'NNh'	Lc: dužina sljedećeg podatkovnog polja
#6-#(5+L)	L	'80h' + '0Ah' + 'XX..XXh'	DER-TLV kodirano upućivanje na kriptografski mehanizam: Identifikator objekta ili autentifikacija čipa (samo vrijednost, izostavlja se oznaka '06h'). Vidjeti Dodatak 1. za vrijednosti identifikatora objekta; upotrebljava se zapis u bajtovima (*byte notation*). Vidjeti Dodatak 11. za smjernice u pogledu odabira jednog od tih identifikatora objekta.

3.5.11.2.2 MSE:SET AT za autentifikaciju jedinice u vozilu

Sljedeća se MSE:SET AT naredba upotrebljava za odabir parametara i ključeva za autentifikaciju jedinice u vozilu koja se sprovodi naknadnom naredbom EXTERNAL AUTHENTICATE (vanjska autentifikacija).
TCS_110 Naredbu je moguće izvršiti u MF-u, DF-u tahografa i DF-u tahografa druge generacije, vidjeti i TCS_34.
TCS_111 **Poruka naredbe MSE:SET AT za autentifikaciju jedinice u vozilu**

Bajt	Dužina	Vrijednost	Opis
CLA	1	'00h'	
INS	1	'22h'	
P1	1	'81h'	Utvrđeno za vanjsku autentifikaciju
P2	1	'A4h'	Autentifikacija
Lc	1	'NNh'	Lc: dužina sljedećeg podatkovnog polja
#6-#(5+L)	L	'80h' + '0Ah' + 'XX..XXh'	DER-TLV kodirano upućivanje na kriptografski mehanizam: Identifikator objekta ili autentifikacija jedinice u vozilu (samo vrijednost, izostavlja se oznaka '06h'). Vidjeti Dodatak 1. za vrijednosti identifikatora objekta; upotrebljava se zapis u bajtovima (*byte notation*). Vidjeti Dodatak 11. za smjernice u pogledu odabira jednog od tih identifikatora objekta.
		'83h' + '08h' + 'XX..XXh'	DER-TLV kodirano upućivanje javnog ključa jedinice u vozilu upućivanjem na vlasnika certifikata koje je spomenuto u njegovu certifikatu.
		'91h' + L_{91} + 'XX..XXh'	DER-TLV kodiran komprimirani prikaz kratkotrajnog javnog ključa jedinice u vozilu koji će se upotrebljavati tokom autentifikacije čipa (vidjeti Dodatak 11.)

3.5.11.2.3 MSE:SET DST

Sljedeća se MSE:SET DST naredba upotrebljava za postavljanje javnog ključa bilo
— za provjeru potpisa koji je dobiven u naknadnoj naredbi PSO: Verify Digital Signature ili
— za provjeru potpisa certifikata koji je dobiven u naknadnoj naredbi PSO: Verify Certificate.
TCS_112 Naredbu je moguće izvršiti u MF-u, DF-u tahografa i DF-u tahografa druge generacije, vidjeti i TCS_33.
TCS_113 **Poruka naredbe MSE:SET:DST**

Bajt	Dužina	Vrijednost	Opis
CLA	1	'00h'	
INS	1	'22h'	
P1	1	'81h'	Utvrđeno za provjeru
P2	1	'B6h'	Digitalni potpis

Lc	1	'NNh'	Lc: dužina sljedećeg podatkovnog polja
#6-#(5+L)	L	'83h' + '08h' + 'XX…XXh'	DER-TLV kodirano upućivanje javnog ključa, odnosno upućivanje na vlasnika certifikata u certifikatu javnog ključa (vidjeti Dodatak 11.)

Za sve verzije naredbi struktura odgovora na poruku i statusne riječi navedene su sljedećim:

TCS_114 **Odgovor na poruku**

Bajt	Dužina	Vrijednost	Opis
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna, kartica uzvraća '**9000**'. Protokol je odabran i pokrenut.

— '**6A80**' označava neispravne parametre u podatkovnom polju naredbe.

— '**6A88**' označava da navedeni podaci (odnosno navedeni ključ) nisu dostupni.

— Ako je currentAuthenticatedTime kartice kasniji od datuma isteka odabranog javnog ključa, uzvraćeno stanje obrade je **‚6A88'.**

Napomena: u slučaju naredbe MSE: SET AT za naredbu autentifikacije jedinice u vozilu, navedeni ključ je javni ključ VU_MA. Kartica će postaviti javni ključ VU_MA za upotrebu, ako je on dostupan u njezinoj memoriji, koji je jednak upućivanju na nosioca certifikata (CHR) dostupnom u podatkovnom polju naredbe (kartica može identifikovati javne ključeve VU_MA s pomoću polja CHA certifikata). Kartica će uzvratiti '6A 88' na ovu naredbu u slučaju da je dostupan samo javni ključ VU_Sign ili da nije dostupan javni ključ jedinice u vozilu. Vidjeti definiciju polja CHA u Dodatku 11. i definiciju vrste podataka equipmentType u Dodatku 1.

Slično, u slučaju da je naredba MSE: SET DST koja upućuje na EQT (tj. na jedinicu u vozilu ili karticu) poslana kontrolnoj kartici, u skladu s CSM_234 navedeni ključ uvijek je ključ EQT_Sign koji se treba koristiti za provjeru digitalnog potpisa. U skladu sa slikom 13. u Dodatku 11., kontrolna kartica će uvijek arhivirati relevantan javni ključ EQT_Sign. U nekim slučajevima kontrolna kartica možda je pohranila povezani javni ključ EQT_MA. Kontrolna kartica uvijek postavlja javni ključ EQT_Sign za korištenje kad primi naredbu MSE: SET DST.

3.5.12 *PSO: HASH*

Ova naredba služi za prenos rezultata izračuna raspršivanja izvršenim na nekim podacima na karticu. Ova se naredba upotrebljava za provjeru digitalnog potpisa. Vrijednost raspršivanja privremeno se arhivira za sljedeću naredbu PSO: Verify Digital Signature

Ova je naredba u skladu s normom ISO/IEC 7816-8. Primjena ove naredbe ograničena je u poređenju s odgovarajućom normom.

Da bi DF-ovi tahografa i DF-ovi tahografa druge generacije mogli podržati tu naredbu potrebna je samo kontrolna kartica.

Druge vrste tahografskih kartica mogu, ali ne moraju sprovoditi tu naredbu. Naredba može, ali ne mora biti dostupna u MF-u.

Aplikacija kontrolne kartice prve generacije podržava samo SHA-1.

TCS_115 Privremeno arhivirana vrijednost raspršivanja briše se ako je nova vrijednost raspršivanja izračunana naredbom PSO: HASH, ako je odabran DF i ako je tahografska kartica vraćena u početno stanje.

TCS_116 **Poruka naredbe**

Bajt	Dužina	Vrijednost	Opis
CLA	1	'00h'	CLA
INS	1	'2Ah'	Izrada sigurnosne operacije
P1	1	'90h'	Vraćanje koda raspršivanja (*hash code*)
P2	1	'A0h'	Oznaka; podatkovno polje sadrži DO-ove potrebne za raspršivanje
Lc	1	'XXh'	Dužina Lc sljedećeg podatkovnog polja
#6	1	'90h'	Oznaka za kod raspršivanja
#7	1	'XXh'	Dužina L koda raspršivanja: '14h' u aplikaciji prve generacije (vidjeti Dodatak 11. dio A) '20h', '30h' ili '40h' u aplikaciji druge generacije (vidjeti Dodatak 11. dio B)
#8-#(7+L)	L	'XX..XXh'	Kod raspršivanja (*hash code*)

TCS_117 **Odgovor na poruku**

Bajt	Dužina	Vrijednost	Opis
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna, kartica uzvraća '**9000**'.

— Ako nedostaju neki očekivani podatkovni objekti (kako su prethodno navedeni), uzvraćeno je stanje obrade '**6987**'. To se može dogoditi ako nema jedne od oznaka '90h',

— Ako su određeni podatkovni objekti neispravni, uzvraćeno je stanje obrade '**6988**'. Do te pogreške dolazi ako je potrebna oznaka prisutna, ali joj se dužina razlikuje od '14h' za SHA-1, '20h' za SHA-256, '30h' za SHA-384, '40h' za SHA-512 (aplikacije druge generacije).

3.5.13 *PERFORM HASH of FILE*

Ova naredba nije u skladu s ISO/IEC 7816-8. Stoga bajt CLA ove naredbe ukazuje na to da slijedi vlasnička uporaba funkcije PERFORM SECURITY OPERATION / HASH.

Da bi DF-ovi tahografa i DF-ovi tahografa druge generacije mogli podržati tu naredbu potrebne su samo kartica vozača i kartica radionice.

Druge vrste tahografskih kartica mogu, ali ne moraju sprovoditi tu naredbu. Ako ovu naredbu sprovodi kartica preduzeća ili kontrolna kartica, naredbu se sprovodi kako je navedeno u ovome poglavlju.

Naredba može, ali ne mora biti dostupna u MF-u. Ako je tako, naredba se izvršava kako je navedeno u ovome poglavlju, odnosno ne dopušta se izračun vrijednosti raspršivanja, nego se izvršavanje naredbe završava odgovarajućim kodom pogreške.

TCS_118 Naredba PERFORM HASH OF FILE upotrebljava se za raspršivanje podatkovnog područja trenutno odabranog transparentnog EF-a.
TCS_119 Tahografska kartica mora podržavati ovu naredbu samo za EF-ove navedene u poglavlju 4. pod DF_Tachograph i DF_Tachograph_G2, uz sljedeću iznimku. Tahografska kartica ne podržava naredbu za EF Sensor_Installation_Data u DF-u tahografa druge generacije.
TCS_120 Rezultat operacije raspršivanja privremeno se arhivira na kartici. Zatim ga se može upotrijebiti za dobivanje digitalnog potpisa datoteke upotrebom naredbe PSO: COMPUTE DIGITAL SIGNATURE.
TCS_121 Privremeno arhivirana vrijednost raspršivanja datoteke briše se ako je nova vrijednost raspršivanja datoteke izračunana naredbom PERFORM HASH of FILE, ako je odabran DF i ako je tahografska kartica vraćena u početno stanje.
TCS_122 Aplikacija tahografa prve generacije mora podržavati SHA-1.
TCS_123 Tahografska aplikacija druge generacije podržava algoritam SHA-2 (SHA-256, SHA-384 ili SHA-512), određen s pomoću slijeda šifri u Dodatku 11., dijelu B za ključ potpisa kartice Card_Sign.";
TCS_124 **Poruka naredbe**

„Bajt	Dužina	Vrijednost	Opis
CLA	1	'80h'	CLA
INS	1	'2Ah'	Izrada sigurnosne operacije
P1	1	'90h'	Oznaka: Hash
P2	1	'00h'	Algoritam implicitno poznat Za tahografsku aplikaciju prve generacije: SHA-1 Za tahografsku aplikaciju druge generacije: algoritam SHA-2 (SHA-256, SHA-384 ili SHA-512) određen s pomoću slijeda šifri u Dodatku 11., dijelu B za ključ potpisa kartice Card_Sign";

TCS_125 **Odgovor na poruku**

Bajt	Dužina	Vrijednost	Opis
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna, kartica uzvraća '**9000**'.
— Ako trenutni EF ne dopušta tu naredbu (EF Sensor_Installation_Data u DF-u tahografa druge generacije), uzvraćeno je stanje obrade '**6985**'.
— Ako se odabrani EF smatra neispravnim (u atributima datoteke ili sačuvanim podacima otkrivena je pogreška u integritetu), uzvraćeno je stanje obrade '**6400**' ili '**6581**'.
— Ako odabrana datoteka nije transparentna datoteka ili ako nema trenutnog EF, uzvraćeno je stanje obrade '**6986**'.

3.5.14 *PSO: COMPUTE DIGITAL SIGNATURE*

Ova se naredba upotrebljava za izračun digitalnog potpisa prethodno izračunanog koda raspršivanja (vidjeti PERFORM HASH OF FILE, tačka 3.5.13.).
Da bi DF-ovi tahografa i DF-ovi tahografa druge generacije mogli podržati tu naredbu potrebne su samo kartica vozača i kartica radionice.
Druge vrste tahografskih kartica mogu, ali ne moraju izvršavati tu naredbu, ali ne smiju imati ključ potpisa. Stoga te kartice ne mogu tu naredbu provesti uspješno, nego izbacuju odgovarajući kod pogreške.
Naredba može, ali ne mora biti dostupna u MF-u. Ako je tako, izvršavanje naredbe završava odgovarajućim kodom pogreške.
Ova je naredba u skladu s normom ISO/IEC 7816-8. Primjena ove naredbe ograničena je u poređenju s odgovarajućom normom.
TCS_126 Ova se naredba upotrebljava za izračun digitalnog potpisa prethodno izračunanog koda raspršivanja (vidjeti PERFORM HASH OF FILE, tačka 3.5.13.).
Da bi DF-ovi tahografa i DF-ovi tahografa druge generacije mogli podržati tu naredbu, potrebne su samo kartica vozača i kartica radionice.
Druge vrste tahografskih kartica mogu, ali ne moraju sprovoditi tu naredbu. U slučaju tahografskih aplikacija druge generacije, samo kartica vozača i kartica radionice imaju ključ potpisa druge generacije, druge kartice ne mogu uspješno izvršiti naredbu i završiti izvršavanje naredbe odgovarajućim kodom pogreške.
Naredba može, ali ne mora biti dostupna u MF-u. Ako naredba nije dostupna u MF-u, izvršavanje naredbe završava odgovarajućim kodom pogreške.
Ova naredba je u skladu s normom ISO/IEC 7816-8. Primjena ove naredbe ograničena je u poređenju s odgovarajućom normom.
TCS_127 Za izračun digitalnog potpisa upotrebljava se privatni ključ kartice koji je kartici implicitno poznat.
TCS_128 Aplikacije tahografa prve generacije izvršavaju digitalni potpis upotrebom metode popunjavanja koja je u skladu s PKCS1 (za više pojedinosti vidjeti Dodatak 11.).
TCS_129 Aplikacije tahografa druge generacije izračunavaju digitalni potpis na temelju eliptičke krivulje (za više pojedinosti vidjeti Dodatak 11.).
TCS_130 **Poruka naredbe**

Bajt	Dužina	Vrijednost	Opis
CLA	1	'00h'	CLA
INS	1	'2Ah'	Izrada sigurnosne operacije
P1	1	'9Eh'	Digitalni potpis koji treba uzvratiti
P2	1	'9Ah'	Oznaka: podatkovno polje sadrži podatke koje treba potpisati. Ako nije obuhvaćeno podatkovno polje, pretpostavlja se da su podaci već na kartici (raspršivanje datoteke).
Le	1	'NNh'	Dužina očekivanog potpisa

TCS_131 **Odgovor na poruku**

Bajt	Dužina	Vrijednost	Opis
#1-#L	L	'XX..XXh'	Potpis prethodno izračunanog raspršivanja
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna, kartica uzvraća '**9000**'.
— Ako se implicitno odabrani privatni ključ smatra neispravnim, uzvraćeno je stanje obrade '**6400**' ili '**6581**'.
— Ako raspršivanje izračunano prethodnom naredbom PERFORM HASH of File nije dostupno, uzvraćeno je stanje obrade '**6985**'.

3.5.15 *PSO: VERIFY DIGITAL SIGNATURE*

Ova se naredba upotrebljava za provjeru digitalnog potpisa koji se pruža kao ulazni podatak čije je raspršivanje poznato kartici. Kartica implicitno poznaje algoritam potpisa.
Ova je naredba u skladu s normom ISO/IEC 7816-8. Primjena ove naredbe ograničena je u poređenju s odgovarajućom normom.
Da bi DF-ovi tahografa i DF-ovi tahografa druge generacije mogli podržati tu naredbu potrebna je samo kontrolna kartica.
Druge vrste tahografskih kartica mogu, ali ne moraju sprovoditi tu naredbu. Naredba može, ali ne mora biti dostupna u MF-u.
TCS_132 Naredba VERIFY DIGITAL SIGNATURE uvijek upotrebljava javni ključ odabran prethodnom naredbom Manage Security Environment, MSE: SET DST i prethodnim kodom raspršivanja unesenim s pomoću naredbe PSO: HASH.
TCS_133 **Poruka naredbe**

„Bajt	Dužina	Vrijednost	Opis
CLA	1	'00h'	CLA
INS	1	'2Ah'	Izrada sigurnosne operacije
P1	1	'00h'	
P2	1	'A8h'	Oznaka: podatkovno polje sadrži DO-ove potrebne za provjeru
Lc	1	'XXh'	Dužina Lc sljedećeg podatkovnog polja
#6	1	'9Eh'	Oznaka za digitalni potpis
#7 ili #7-#8	L	'NNh' ili '81 NNh'	Dužina digitalnog potpisa (L je 2 bajta ako je digitalni potpis dulji od 127 bajtova): 128 bajtova kodiranih u skladu s Dodatkom 11. dijelom A u pogledu aplikacije tahografa prve generacije. Za aplikacije tahografa druge generacije dužina ovisi o odabranoj krivulji (vidjeti Dodatak 11. dio B).
#(7+L)-#(6+L+NN)	NN	'XX..XXh'	Sadržaj digitalnog potpisa";

TCS_134 **Odgovor na poruku**

Bajt	Dužina	Vrijednost	Opis
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna, kartica uzvraća '**9000**'.
— Ako provjera potpisa ne uspije, uzvraćeno je stanje obrade '**6688**'. Postupak provjeravanja opisan je u Dodatku 11.
— Ako nije odabran javni ključ, uzvraćeno je stanje obrade '**6A88**'.
— Ako nedostaju neki očekivani podatkovni objekti (kako su prethodno navedeni), uzvraćeno je stanje obrade '**6987**'. To se može dogoditi ako nema jedne od traženih oznaka.
— Ako kod raspršivanja nije dostupan za obradu naredbe (zbog prethodne naredbe PSO: Hash), uzvraćeno je stanje obrade '**6985**'.
— Ako su određeni podatkovni objekti neispravni, uzvraćeno je stanje obrade '**6988**'. To se može dogoditi ako je dužina traženih podatkovnih objekata neispravna.
— Ako se odabrani javni ključ smatra neispravnim, uzvraćeno je stanje obrade '**6400**' ili '**6581**'.
— Ako CHA.LSB (CertificateHolderAuthorisation.equipmentType) odabranog javnog ključa (upotrijebljenog za provjeru digitalnog potpisa) nije prikladan za provjeru digitalnog potpisa u skladu s Dodatkom 11., uzvraćeno je stanje obrade **'6985'**.

3.5.16 *PROCESS DSRC MESSAGE*

Ova se naredba upotrebljava za provjeru integriteta i autentičnosti DSRC poruke i dešifriranje podataka poslanih s jedinice u vozilu nadzornom tijelu ili radionici putem DSRC poveznice. Kartica proizvodi ključ za šifriranje i MAC ključ koji se upotrebljavaju za zaštitu DSRC poruke kako je opisano u poglavlju 13. Dodatka 11. dijela B.
Da bi DF-ovi tahografa druge generacije mogli podržati tu naredbu potrebne su samo kontrolna kartica i kartica radionice.
Druge vrste tahografskih kartica mogu, ali ne moraju izvršavati tu naredbu, ali te kartice ne smiju imati DSRC glavni ključ. Stoga te kartice ne mogu tu naredbu provesti uspješno, nego izbacuju odgovarajući kod pogreške.
Naredba može, ali ne mora biti dostupna u MF-u i/ili DF-u tahografa. Ako je tako, izvršavanje naredbe završava odgovarajućim kodom pogreške.
TCS_135 DSRC glavni ključ dostupan je samo u DF-u tahografa druge generacije, tj. kontrolna kartica i kartica radionice podržavaju uspješnu ssprovođenje naredbe samo u DF-u tahografa druge generacije.
TCS_136 Naredbom se samo dešifriraju DSRC podaci i provjerava kriptografski kontrolni zbir, ali se ne tumače ulazni podaci.
TCS_137 Redoslijed podatkovnih objekata u podatkovnom polju naredbe utvrđen je u ovoj specifikaciji.

TCS_138 **Poruka naredbe**

Bajt	Dužina	Vrijednost	Opis
CLA	1	'80h'	Vlasnički CLA
INS	1	'2Ah'	Izrada sigurnosne operacije
P1	1	'80h'	Podaci odziva: nešifrirana vrijednost
P2	1	'B0h'	Podaci naredbe: nešifrirana vrijednost kodirana u BER-TLV i uključujući DO-ove sigurnog prenosa poruka
Lc	1	'NNh'	Dužina Lc sljedećeg podatkovnog polja
#6-#(5+L)	L	'87h' + L_{87}+ 'XX..XXh'	DER-TLV kodirani bajt indikatora popunjenja-sadržaja nakon kojeg slijedi kodirani prenos podataka tahografa. Za bajt indikatora popunjenja-sadržaja upotrebljava se vrijednost '00h' ('bez dodatnih indikatora' u skladu s normom ISO/IEC 7816-4:2013, tablica 52.). Mehanizam šifriranja opisan je u Dodatku 11. dijelu B. poglavlju 13. Dopuštene su vrijednosti za dužinu L_{87} višekratnici dužine AES bloka uvećano za 1 za bajt indikatora popunjenja-sadržaja, odnosno od 17 bajtova do 193 bajta, uključivo. *Napomena:* Za SM podatkovni objekt s oznakom '87h' vidjeti normu ISO/IEC 7816-4:2013, tablicu 49.
		'81h' + '10h'	DER-TLV kodirani kontrolni referentni predložak za povjerljivost koji ugniježđuje ulančavanje sljedećih podatkovnih elemenata (vidjeti Dodatak 1. DSRCSecurityData i poglavlje 13. Dodatka 11. dijela B): — vremenski žig od 4 bajta — brojač od 3 bajta — serijski broj jedinice u vozilu od 8 bajtova — verzija DSRC glavnog ključa od 1 bajta *Napomena:* Za SM podatkovni objekt s oznakom '81h' vidjeti normu ISO/IEC 7816-4:2013, tablicu 49.
		'8Eh' + L_{8E} + 'XX..XXh'	DER-TLV kodiran MAC putem DSRC poruke. Za MAC algoritam i izračun vidjeti poglavlje 13. Dodatka 11. dijela B. *Napomena:* Za SM podatkovni objekt s oznakom '8Eh' vidjeti normu ISO/IEC 7816-4:2013, tablicu 49.
5 + L + 1	1	'00h'	Kako je utvrđeno u normi ISO/IEC 7816-4

TCS_139 **Odgovor na poruku**

Bajt	Dužina	Vrijednost	Opis
#1-#L	L	'XX..XXh'	Podaci kojih nema (u slučaju pogreške) ili dešifrirani podaci (uklonjeno popunjavanje)
SW	2	'XXXXh'	Statusne riječi (SW1, SW2)

— Ako je naredba uspješna, kartica uzvraća '**9000**'.
— '**6A80**' označava neispravne parametre u podatkovnom polju naredbe (isto vrijedi i u slučaju da podatkovni objekti nisu poslani utvrđenim redoslijedom).
— '**6A88**' označava da navedeni podaci nisu dostupni, odnosno da navedeni DSRC glavni ključ nije dostupan.
— '**6900**' označava da je provjera kriptografskog kontrolnog zbira ili dešifriranje podataka bilo neuspješno.
— '6985' označava da je oznaka vremena od 4 bajta u podatkovnom polju naredbe ranija od cardValidityBegin ili kasnija od cardExpiryDate.

4. STRUKTURA KARTICA TAHOGRAFA

Ovaj stavak propisuje strukture datoteka tahografskih kartica za arhiviranje dostupnih podataka.
Ne propisuje unutarnje strukture koje zavise o proizvođaču kartice, npr. zaglavlja datoteke, ni arhiviranje podatkovnih elemenata potrebnih samo za internu upotrebu, primjerice EuropeanPublicKey, [illegible] ili WorkshopCardPin. kao ni postepene s tim elementima.
TCS_140 Na tahografskoj kartici druge generacije nalazi se glavna datoteka MF te aplikacija tahografa prve i druge generacije iste vrste (npr. aplikacije za kartice vozača).
TCS_141 Tahografska kartica mora podržavati barem najmanji broj zapisa utvrđen za odgovarajuće aplikacije, a ne podržava više zapisa od najvećeg broja zapisa utvrđenog za odgovarajuće aplikacije.
U ovome poglavlju utvrđeni su najveći i najmanji brojevi zapisa za različite aplikacije.
Sigurnosni uslovi koji se upotrebljavaju u uslovima pristupa u cijelom ovom poglavlju navedeni su u poglavlju 3.3.
Uopšteno, način pristupa „read" (očitavanje) označava naredbu READ BINARY s parnim i, ako je podržan, neparnim INS bajtom, uz iznimku EF-a Sensor_Installation_Data na kartici radionice, vidjeti TCS_156 i TCS_160.
Način pristupa „update" (ažuriranje) označava naredbu UPDATE BINARY s parnim i, ako je podržan, neparnim INS bajtom, a način pristupa „select" (odabir) naredbu SELECT.

4.1. Glavna datoteka MF

TCS_142 Glavna datoteka MF nakon personalizacije ima sljedeću trajnu strukturu datoteka i sljedeće trajne uslove za pristup datotekama:
Napomena: SFID kratkog EF indikatora navodi se kao decimalni broj, na primjer vrijednost 30 odgovara vrijednosti 11110 u binarnom zapisu.

Datoteka	ID datoteke	SFID	Uvjeti pristupa: Čitanje / Odabir	Uvjeti pristupa: Ažuriranje
MF	3F00h			
EF ICC	0002h		ALW	NEV
EF IC	0005h		ALW	NEV
EF DIR	2F00h	30	ALW	NEV
EF ATR/INFO (conditional)	2F01h	29	ALW	NEV
EF Extended_Length (conditional)	0003h	28	ALW	NEV
DF Tachograph	0500h		SC1	
DF Tachograph_G2			SC1	

U ovoj se tablici upotrebljava sljedeća kratica za sigurnosni uvjet:
SC1 ALW ILI SM-MAC-G2
TCS_143 Strukture svih EF-ova moraju biti transparentne.
TCS_144 Glavna datoteka MF ima sljedeću strukturu podataka:

Datoteka / podatkovni element	Broj zapisa	Veličina (u bajtovima): Min	Veličina (u bajtovima): Maks	Zadane vrijednosti
MF		43	104	
EF ICC		25	25	
CardIccIdentification		25	25	
clockStop		1	1	[00]
cardExtendedSerialNumber		8	8	[00..00]
cardApprovalNumber		8	8	[20..20]
cardPersonaliserID		1	1	[00]
embedderIcAssemblerId		5	5	[00..00]
icIdentifier		2	2	[00 00]
EF IC		8	8	
CardChipIdentification		8	8	
icSerialNumber		4	4	[00..00]
icManufacturingReferences		4	4	[00..00]
EF DIR		20	20	
See TCS_145		20	20	[00..00]
EF ATR/INFO		7	228	
See TCS_146		7	228	[00..00]
EF EXTENDED_LENGTH		3	3	
See TCS_147		3	3	[00..00]
DF Tachograph				
DF Tachograph_G2				

TCS_145 Osnovna datoteka EF DIR sadrži sljedeće podatkovne objekte vezane uz aplikaciju. '61 08 4F 06 FF 54 41 43 48 4F 61 08 4F 06 FF 53 4D 52 44 54'
TCS_146 Osnovna datoteka EF ATR/INFO prisutna je ako tahografska kartica u svojem ATR-u naznači da podržava produžena polja. U tom slučaju EF ATR/INFO sadrži podatkovni objekt s informacijama o produženju (DO '7F66') kako je utvrđeno u tački 12.7.1. norme ISO/IEC 7816-4:2013.
TCS_147 Osnovna datoteka EF Extended_Length prisutna je ako tahografska kartica u svojem ATR-u naznači da podržava produžena polja. U tom slučaju EF sadrži sljedeći podatkovni objekt: '02 01 xx' ako vrijednost 'xx' označava jesu li produžena polja podržana za protokole T = 1 i/ili T = 0.
Vrijednost '01' označava da su produžena polja podržana za protokol T = 1.
Vrijednost '10' označava da su produžena polja podržana za protokol T = 0.
Vrijednost '11' označava da su produžena polja podržana za protokole T = 1 i T = 0.

4.2. Aplikacija kartice vozača

4.2.1 *Aplikacija kartice vozača prve generacije*

TCS_148 Aplikacija kartice vozača prve generacije nakon personalizacije ima sljedeću trajnu strukturu datoteka i sljedeće trajne uslove za pristup datotekama:

Datoteka	ID datoteke	Uvjeti prisnupa: Čitanje	Uvjeti prisnupa: Odabir	Uvjeti prisnupa: Ažuriranje
DF Tachograph	'0500h'		SC1	
EF Application_Identification	'0501h'	SC2	SC1	NEV
EF Card_Certificate	'C100h'	SC2	SC1	NEV
EF CA_Certificate	'C108h'	SC2	SC1	NEV
EF Identification	'0520h'	SC2	SC1	NEV
EF Card_Download	'050Eh'	SC2	SC1	SC1
EF Driving_Licence_Info	'0521h'	SC2	SC1	NEV
EF Events_Data	'0502h'	SC2	SC1	SC1
EF Faults_Data	'0503h'	SC2	SC1	SC1
EF Driver_Activity_Data	'0504h'	SC2	SC1	SC1
EF Vehicles_Used	'0505h'	SC2	SC1	SC1
EF Places	'0506h'	SC2	SC1	SC1
EF Current_Usage	'0507h'	SC2	SC1	SC1
EF Control_Activity_Data	'0508h'	SC2	SC1	SC1
EF Specific_Conditions	'0522h'	SC2	SC1	SC1

U ovoj se tablici upotrebljavaju sljedeće kratice za sigurnosne uslove:
SC1 ALW ILI SM-MAC-G2
SC2 ALW ILI SM-MAC-G1 ILI SM-MAC-G2
SC3 SM-MAC-G1 ILI SM-MAC-G2

TCS_149 Strukture svih EF-ova moraju biti transparentne.
TCS_150 Aplikacija kartice vozača prve generacije ima sljedeću strukturu podataka:

Datoteka / podatkovni element	Broj zapisa	Veličina (u bajtovima) Min	Maks	Zadane vrijednosti
DF Tachograph		11378	24826	
EF Application_Identification		10	10	
DriverCardApplicationIdentification		10	10	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		1	1	{00}
EF Card_Certificate		194	194	
CardCertificate		194	194	{00..00}
EF CA_Certificate		194	194	
MemberStateCertificate		194	194	{00..00}
EF Identification		143	143	
CardIdentification		65	65	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
DriverCardHolderIdentification		78	78	
cardHolderName		72	72	
holderSurname		36	36	{00..20..20}
holderFirstNames		36	36	{00..20..20}
cardHolderBirthDate		4	4	{00..00}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		4	4	
LastCardDownload		4	4	
EF Driving_Licence_Info		53	53	
CardDrivingLicenceInformation		53	53	
drivingLicenceIssuingAuthority		36	36	{00..20..20}
drivingLicenceIssuingNation		1	1	{00}
drivingLicenceNumber		16	16	{20..20}
EF Events_Data		864	1728	
CardEventData		864	1728	
cardEventRecords	6	144	288	
CardEventRecord	n	24	24	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00..20..20}
EF Faults_Data		576	1152	
CardFaultData		576	1152	
cardFaultRecords	2	288	576	
CardFaultRecord	n	24	24	
faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				

vehicleRegistrationNation		1	1	[00]
vehicleRegistrationNumber		14	14	[00, 20..20]
EF Driver_Activity_Data		5548	13780	
CardDriverActivity		5548	13780	
activityPointerOldestDayRecord		2	2	[00 00]
activityPointerNewestRecord		2	2	[00 00]
activityDailyRecords	n.	5544	13776	[00..00]
EF Vehicles_Used		2606	6202	
CardVehiclesUsed		2606	6202	
vehiclePointerNewestRecord		2	2	[00 00]
cardVehicleRecords		2604	6200	
CardVehicleRecord	n.	31	31	
vehicleOdometerBegin		3	3	[00..00]
vehicleOdometerEnd		3	3	[00..00]
vehicleFirstUse		4	4	[00..00]
vehicleLastUse		4	4	[00..00]
vehicleRegistration				
vehicleRegistrationNation		1	1	[00]
vehicleRegistrationNumber		14	14	[00, 20..20]
vuDataBlockCounter		2	2	[00 00]
EF Places		841	1121	
CardPlaceDailyWorkPeriod		841	1121	
placePointerNewestRecord		1	1	[00]
placeRecords		840	1120	
PlaceRecord	n.	10	10	
entryTime		4	4	[00..00]
entryTypeDailyWorkPeriod		1	1	[00]
dailyWorkPeriodCountry		1	1	[00]
dailyWorkPeriodRegion		1	1	[00]
vehicleOdometerValue		3	3	[00..00]
EF Current_Usage		19	19	
CardCurrentUse		19	19	
sessionOpenTime		4	4	[00..00]
sessionOpenVehicle				
vehicleRegistrationNation		1	1	[00]
vehicleRegistrationNumber		14	14	[00, 20..20]
EF Control_Activity_Data		46	46	
CardControlActivityDataRecord		46	46	
controlType		1	1	[00]
controlTime		4	4	[00..00]
controlCardNumber				
cardType		1	1	[00]
cardIssuingMemberState		1	1	[00]
cardNumber		16	16	[20..20]
controlVehicleRegistration				
vehicleRegistrationNation		1	1	[00]
vehicleRegistrationNumber		14	14	[00, 20..20]
controlDownloadPeriodBegin		4	4	[00..00]
controlDownloadPeriodEnd		4	4	[00..00]
EF Specific_Conditions		280	280	
SpecificConditionRecord	56	5	5	
entryTime		4	4	[00..00]
SpecificConditionType		1	1	[00]

TCS_151 Sljedeće vrijednosti, koje se upotrebljavaju za navođenje veličina u prethodnoj tablici, predstavljaju najniži i najviši broj zapisa koji struktura podataka kartice vozača mora upotrebljavati za aplikaciju prve generacije:

		Minimalno	Maksimalno
n.	NbOfEventsPerType	6	12
n.	NbOfFaultsPerType	12	24
n.	NbOfCardVehicleRecords	84	200
n.	NbOfCardPlaceRecords	84	112
n.	CardActivityLengthRange	5 544 bajta (28 dana * 0/1 promjena aktivnosti)	13 776 bajtova (28 dana * 240 promjena aktivnosti)

4.2.2 *Aplikacija kartice vozača druge generacije*

TCS_152 Aplikacija kartice vozača druge generacije nakon personalizacije ima sljedeću trajnu strukturu datoteka i sljedeće trajne uslove za pristup datotekama:

Napomena: SFID kratkog EF indikatora navodi se kao decimalni broj, na primjer vrijednost 30 odgovara vrijednosti 11110 u binarnom zapisu.

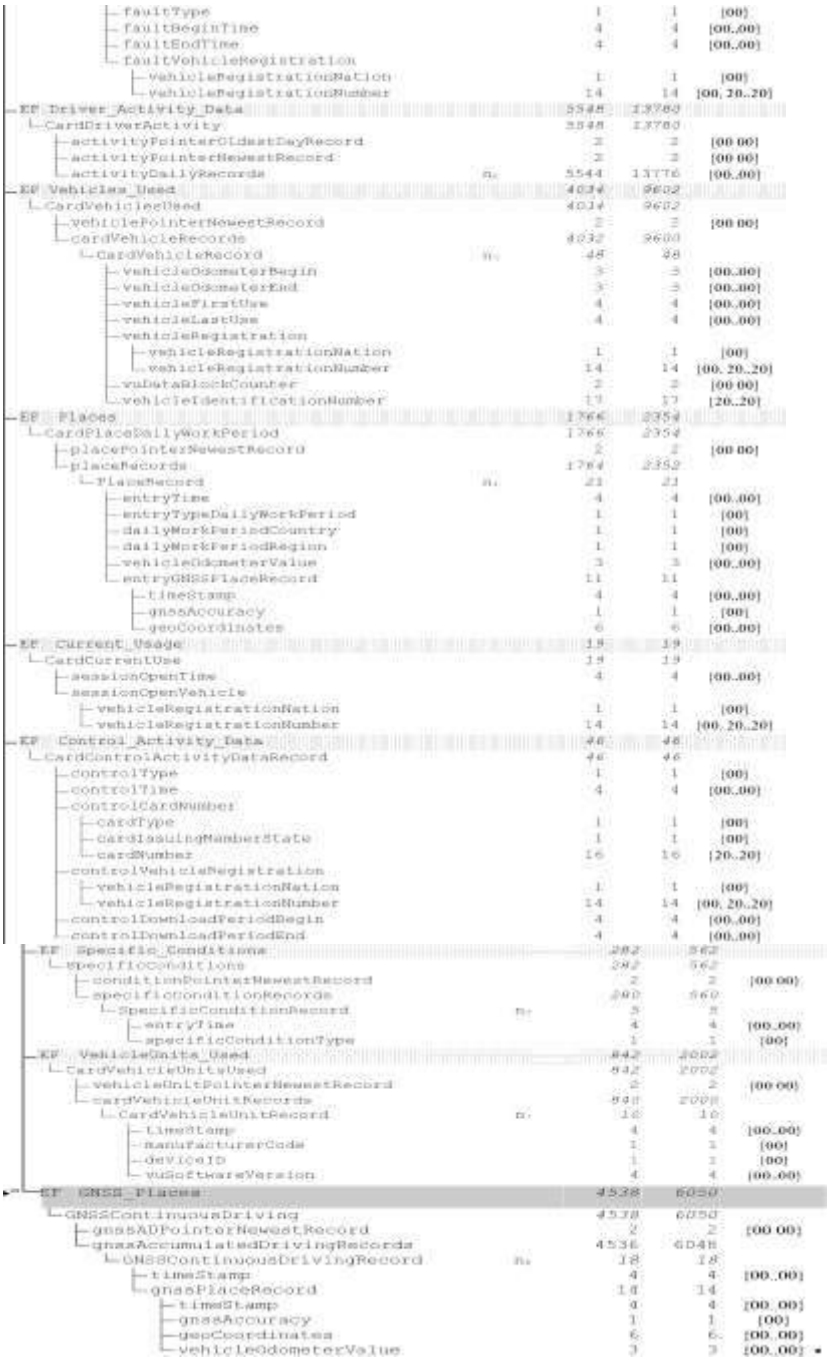
Datoteka	ID datoteke	SFID	Uvjeti pristupa	
			Čitanje / Oklabir	Ažuriranje
DF Tachograph_G2			SC1	
EF Application_Identification	'0501h'	1	SC1	NEV
EF CardMA_Certificate	'C100h'	2	SC1	NEV
EF CardSignCertificate	'C101h'	3	SC1	NEV
EF CA_Certificate	'C108h'	4	SC1	NEV
EF Link_Certificate	'C109h'	5	SC1	NEV
EF Identification	'0520h'	6	SC1	NEV
EF Card_Download	'050Eh'	7	SC1	SC1
EF Driving_Licence_Info	'0521h'	10	SC1	NEV
EF Events_Data	'0502h'	12	SC1	SM-MAC-G2
EF Faults_Data	'0503h'	13	SC1	SM-MAC-G2
EF Driver_Activity_Data	'0504h'	14	SC1	SM-MAC-G2
EF Vehicles_Used	'0505h'	15	SC1	SM-MAC-G2
EF Places	'0506h'	16	SC1	SM-MAC-G2
EF Current_Usage	'0507h'	17	SC1	SM-MAC-G2
EF Control_Activity_Data	'0508h'	18	SC1	SM-MAC-G2
EF Specific_Conditions	'0522h'	19	SC1	SM-MAC-G2
EF VehicleUnits_Used	'0523h'	20	SC1	SM-MAC-G2
EF GNSS_Places	'0524h'	21	SC1	SM-MAC-G2

U ovoj se tablici upotrebljava sljedeća kratica za sigurnosni uvjet:
SC1 ALW ILI SM-MAC-G2

TCS_153 Strukture svih EF-ova moraju biti transparentne.

TCS_154 Aplikacija kartice vozača druge generacije ima sljedeću strukturu podataka:

Datoteka / podatkovni element	Broj zapisa	Veličina (u bajtovima) Min.	Maks.	Zadane vrijednosti
EF Tachograph_G2		20268	40316	
EF Application_Identification		17	17	
DriverCardApplicationIdentification		17	17	
typeOfTachographCardId		1	1	[00]
cardStructureVersion		2	2	[00 00]
noOfEventsPerType		1	1	[00]
noOfFaultsPerType		1	1	[00]
activityStructureLength		2	2	[00 00]
noOfCardVehicleRecords		2	2	[00 00]
noOfCardPlaceRecords		2	2	[00 00]
noOfGNSSADRecords		2	2	[00 00]
noOfSpecificConditionRecords		2	2	[00 00]
noOfCardVehicleUnitRecords		2	2	[00 00]
EF CardMA_Certificate		204	341	
CardMACertificate		204	341	[00..00]
EF CardSignCertificate		204	341	
CardSignCertificate		204	341	[00..00]
EF CA_Certificate		204	341	
MemberStateCertificate		204	341	[00..00]
EF Link_Certificate		204	341	
LinkCertificate		204	341	[00..00]
EF Identification		143	143	
CardIdentification		65	65	
cardIssuingMemberState		1	1	[00]
cardNumber		16	16	[20..20]
cardIssuingAuthorityName		36	36	[20..20]
cardIssueDate		4	4	[00..00]
cardValidityBegin		4	4	[00..00]
cardExpiryDate		4	4	[00..00]
DriverCardHolderIdentification		78	78	
cardHolderName		72	72	
holderSurname		36	36	[00..20..20]
holderFirstNames		36	36	[00..20..20]
cardHolderBirthDate		4	4	[00..00]
cardHolderPreferredLanguage		2	2	[20 20]
EF Card_Download		4	4	
LastCardDownload		4	4	
EF Driving_Licence_Info		53	53	
CardDrivingLicenceInformation		53	53	
drivingLicenceIssuingAuthority		36	36	[00..20..20]
drivingLicenceIssuingNation		1	1	[00]
drivingLicenceNumber		16	16	[20..20]
EF Events_Data		1584	3168	
CardEventData		1584	3168	
cardEventRecords	11	144	288	
CardEventRecord	n	24	24	
eventType		1	1	[00]
eventBeginTime		4	4	[00..00]
eventEndTime		4	4	[00..00]
eventVehicleRegistration				
vehicleRegistrationNation		1	1	[00]
vehicleRegistrationNumber		14	14	[00..20..20]
EF Faults_Data		576	1152	
CardFaultData		576	1152	
cardFaultRecords	2	288	576	
CardFaultRecord	n	24	24	


faultType 1 1 [00]
faultBeginTime 4 4 [00..00]
faultEndTime 4 4 [00..00]
faultVehicleRegistration
vehicleRegistrationNation 1 1 [00]
vehicleRegistrationNumber 14 14 [00..20..20]
EF Driver_Activity_Data 5548 13780
CardDriverActivity 5548 13780
activityPointerOldestDayRecord 2 2 [00 00]
activityPointerNewestRecord 2 2 [00 00]
activityDailyRecords n. 5544 13776 [00..00]
EF Vehicles_Used 4034 9602
CardVehiclesUsed 4034 9602
vehiclePointerNewestRecord 2 2 [00 00]
cardVehicleRecords 4032 9600
CardVehicleRecord n. 48 48
vehicleOdometerBegin 3 3 [00..00]
vehicleOdometerEnd 3 3 [00..00]
vehicleFirstUse 4 4 [00..00]
vehicleLastUse 4 4 [00..00]
vehicleRegistration
vehicleRegistrationNation 1 1 [00]
vehicleRegistrationNumber 14 14 [00..20..20]
vuDataBlockCounter 2 2 [00 00]
vehicleIdentificationNumber 17 17 [20..20]
EF Places 1766 2354
CardPlaceDailyWorkPeriod 1766 2354
placePointerNewestRecord 2 2 [00 00]
placeRecords 1764 2352
PlaceRecord n. 21 21
entryTime 4 4 [00..00]
entryTypeDailyWorkPeriod 1 1 [00]
dailyWorkPeriodCountry 1 1 [00]
dailyWorkPeriodRegion 1 1 [00]
vehicleOdometerValue 3 3 [00..00]
entryGNSSPlaceRecord 11 11
timeStamp 4 4 [00..00]
gnssAccuracy 1 1 [00]
geoCoordinates 6 6 [00..00]
EF Current_Usage 19 19
CardCurrentUse 19 19
sessionOpenTime 4 4 [00..00]
sessionOpenVehicle
vehicleRegistrationNation 1 1 [00]
vehicleRegistrationNumber 14 14 [00..20..20]
EF Control_Activity_Data 46 46
CardControlActivityDataRecord 46 46
controlType 1 1 [00]
controlTime 4 4 [00..00]
controlCardNumber
cardType 1 1 [00]
cardIssuingMemberState 1 1 [00]
cardNumber 16 16 [20..20]
controlVehicleRegistration
vehicleRegistrationNation 1 1 [00]
vehicleRegistrationNumber 14 14 [00..20..20]
controlDownloadPeriodBegin 4 4 [00..00]
controlDownloadPeriodEnd 4 4 [00..00]
EF Specific_Conditions 282 562
SpecificConditions 282 562
conditionPointerNewestRecord 2 2 [00 00]
specificConditionRecords 280 560
SpecificConditionRecord n. 5 5
entryTime 4 4 [00..00]
specificConditionType 1 1 [00]
EF Vehicle_Units_Used 842 2002
CardVehicleUnitsUsed 842 2002
vehicleUnitPointerNewestRecord 2 2 [00 00]
cardVehicleUnitRecords 840 2000
CardVehicleUnitRecord n. 10 10
TimeStamp 4 4 [00..00]
manufacturerCode 1 1 [00]
deviceID 1 1 [00]
vuSoftwareVersion 4 4 [00..00]
EF GNSS_Places 4538 6050
GNSSContinuousDriving 4538 6050
gnssADPointerNewestRecord 2 2 [00 00]
gnssAccumulatedDrivingRecords 4536 6048
GNSSContinuousDrivingRecord n. 18 18
timeStamp 4 4 [00..00]
gnssPlaceRecord 14 14
timeStamp 4 4 [00..00]
gnssAccuracy 1 1 [00]
geoCoordinates 6 6 [00..00]
vehicleOdometerValue 3 3 [00..00]

TCS_155 Sljedeće vrijednosti, koje se upotrebljavaju za navođenje veličina u prethodnoj tablici, predstavljaju najniži i najviši broj zapisa koji struktura podataka kartice vozača mora upotrebljavati za aplikaciju druge generacije:

		Minimalno	Maksimalno
n_1	NoOfEventsPerType	6	12
n_2	NoOfFaultsPerType	12	24
n_3	NoOfCardVehicleRecords	84	200
n_4	NoOfCardPlaceRecords	84	112
n_5	CardActivityLengthRange	5 544 bajta (28 dana * 93 promjene aktivnosti)	13 776 bajtova (28 dana * 240 promjena aktivnosti)
n_6	NoOfCardVehicleUnitRecords	84	200
n_7	NoOfGNSSADRecords	252	336 *
n_8	NoOfSpecificConditionRecords	56	112

4.3. Aplikacije kartice radionice

4.3.1 *Aplikacija kartice radionice prve generacije*

TCS_156 Aplikacija kartice radionice prve generacije nakon personalizacije ima sljedeću trajnu strukturu datoteka i sljedeće trajne uslove za pristup datotekama:

Datoteka	ID datoteke	Uvjeti pristupa: Čitanje	Odabir	Ažuriranje
└─DF Tachograph	0500h		SC1	
├─EF Application_Identification	0501h	SC2	SC1	NEV
├─EF Card_Certificate	C100h	SC2	SC1	NEV
├─EF CA_Certificate	C108h	SC2	SC1	NEV
├─EF Identification	0520h	SC2	SC1	NEV
├─EF Card_Download	050Eh	SC2	SC1	SC1
├─EF Calibration	050Ah	SC2	SC1	SC3
├─EF Vendor_Installation_Data	0508h	SC4	SC1	NEV
├─EF Events_Data	0502h	SC2	SC1	SC3
├─EF Faults_Data	0503h	SC2	SC1	SC3
├─EF Driver_Activity_Data	0504h	SC2	SC1	SC3
├─EF Vehicles_Used	0505h	SC2	SC1	SC3
├─EF Places	0506h	SC2	SC1	SC3
├─EF Current_Usage	0507h	SC2	SC1	SC3
├─EF Control_Activity_Data	0508h	SC2	SC1	SC3
└─EF Specific_Conditions	0522h	SC2	SC1	SC3

U ovoj se tablici upotrebljavaju sljedeće kratice za sigurnosne uslove:

SC1 ALW ILI SM-MAC-G2
SC2 ALW ILI SM-MAC-G1 ILI SM-MAC-G2
SC3 SM-MAC-G1 ILI SM-MAC-G2
SC4 Za naredbu READ BINARY s parnim INS bajtom:
(SM-C-MAC-G1 I SM-R-ENC-MAC-G1) ILI
(SM-C-MAC-G2 I SM-R-ENC-MAC-G2)
Za naredbu READ BINARY s neparnim INS bajtom (ako je podržan): NEV";

TCS_157 Strukture svih EF-ova moraju biti transparentne.

TCS_158 Aplikacija kartice radionice prve generacije ima sljedeću strukturu podataka:


Datoteka / podatkovni element
Broj zapisa
Veličina (u bajtovima)
Min
Maks
Zadane vrijednosti

TCS_159 Sljedeće vrijednosti, koje se upotrebljavaju za navođenje veličina u prethodnoj tablici, predstavljaju najniži i najviši broj zapisa koji struktura podataka kartice radionice mora upotrebljavati za aplikaciju prve generacije:

		Minimalno	Maksimalno
n_1	NoOfEventsPerType	3	3
n_2	NoOfFaultsPerType	6	6
n_3	NoOfCardVehicleRecords	4	8
n_4	NoOfCardPlaceRecords	6	8
n_5	NoOfCalibrationRecords	88	255
n_6	CardActivityLengthRange	198 bajtova (1 dan * 93 promjene aktivnosti)	492 bajta (1 dan * 240 promjena aktivnosti)

4.3.2 *Aplikacija kartice radionice druge generacije*

TCS_160 Aplikacija kartice radionice druge generacije nakon personalizacije ima sljedeću trajnu strukturu datoteka i sljedeće trajne uslove za pristup datotekama:

Napomena: SFID kratkog EF indikatora navodi se kao decimalni broj, na primjer vrijednost 30 odgovara vrijednosti 11110 u binarnom zapisu.

Datoteka	ID datoteke	SFID	Uvjeti pristupa		
			Čitanje	Odabir	Ažuriranje
DF Tachograph_G2			SC1	SC1	
EF Application_Identification	'0501h'	1	SC1	SC1	NEV
EF CardMA_Certificate	'C100h'	2	SC1	SC1	NEV
EF CardSign_Certificate	'C101h'	3	SC1	SC1	NEV
EF CA_Certificate	'C108h'	4	SC1	SC1	NEV
EF Link_Certificate	'C109h'	5	SC1	SC1	NEV
EF Identification	'0520h'	6	SC1	SC1	NEV
EF Card_Download	'0509h'	7	SC1	SC1	SC1
EF Calibration	'050Ah'	10	SC1	SC1	SM-MAC-G2
EF Sensor_Installation_Data	'0508h'	11	SC5	SM-MAC-G2	NEV
EF Events_Data	'0502h'	12	SC1	SC1	SM-MAC-G2
EF Faults_Data	'0503h'	13	SC1	SC1	SM-MAC-G2
EF Driver_Activity_Data	'0504h'	14	SC1	SC1	SM-MAC-G2
EF Vehicles_Used	'0505h'	15	SC1	SC1	SM-MAC-G2
EF Places	'0506h'	16	SC1	SC1	SM-MAC-G2
EF Current_Usage	'0507h'	17	SC1	SC1	SM-MAC-G2
EF Control_Activity_Data	'0508h'	18	SC1	SC1	SM-MAC-G2
EF Specific_Conditions	'0522h'	19	SC1	SC1	SM-MAC-G2
EF VehicleUnits_Used	'0523h'	20	SC1	SC1	SM-MAC-G2
EF GNSS_Places	'0524h'	21	SC1	SC1	SM-MAC-G2

U ovoj se tablici upotrebljavaju sljedeće kratice za sigurnosne uslove:

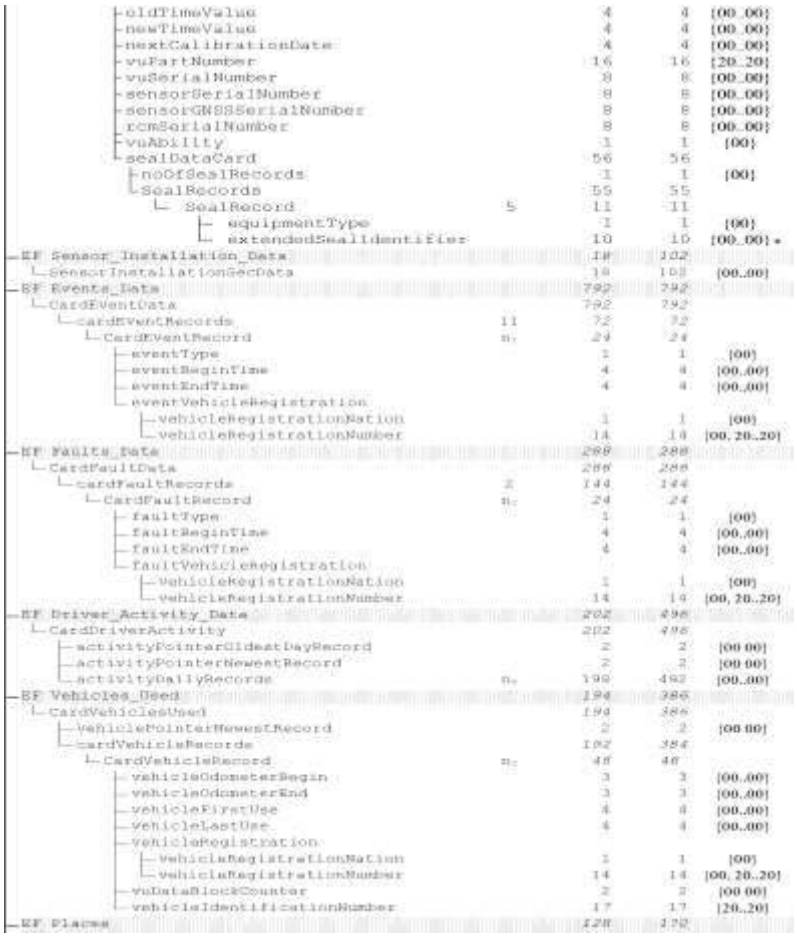
SC1 ALW ILI SM-MAC-G2

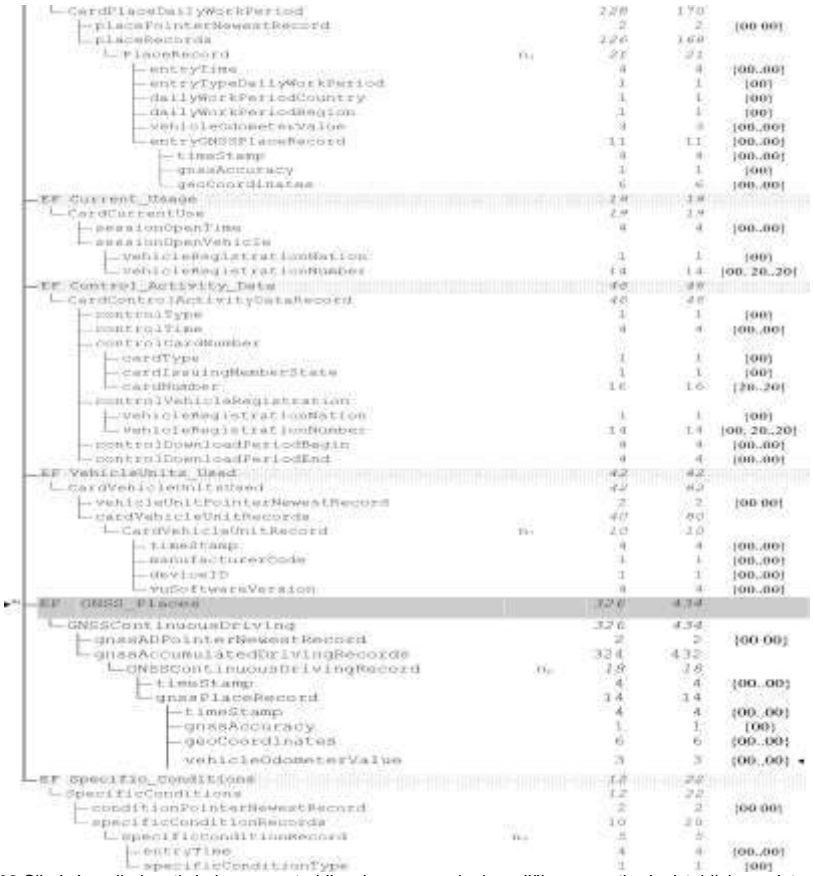
SC5 Za naredbu READ BINARY s parnim INS bajtom: SM-C-MAC-G2 I SM-R-ENC-MAC-G2
Za naredbu READ BINARY s neparnim INS bajtom (ako je podržan): NEV

TCS_161 Strukture svih EF-ova moraju biti transparentne.

TCS_162 Aplikacija kartice radionice druge generacije ima sljedeću strukturu podataka:

Datoteka / podatkovni element	Broj zapisa	Veličina (u bajtovima) Min.	Maks.	Zadane vrijednosti
DF Tachograph_G2	1878		49787	
EF Application_Identification	19		19	
WorkshopCardApplicationIdentificatio	19		19	
typeOfTachographCardId	1		1	{00}
cardStructureVersion	2		2	{00 00}
noOfEventsPerType	1		1	{00}
noOfFaultsPerType	1		1	{00}
activityStructureLength	2		2	{00 00}
noOfCardVehicleRecords	2		2	{00 00}
noOfCardPlaceRecords	2		2	{00 00}
noOfCalibrationRecords	2		2	{00 00}
noOfGNSSADRecords	2		2	{00 00}
noOfSpecificConditionRecords	2		2	{00 00}
noOfCardVehicleUnitRecords	2		2	{00 00}
EF CardMA_Certificate	204		341	
CardMACertificate		204	341	{00..00}
EF CardSignCertificate		204	341	
CardSignCertificate		204	341	{00..00}
EF CA_Certificate		204	341	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		204	341	
LinkCertificate		204	341	{00..00}
EF Identification		211	211	
CardIdentification		65	65	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00..20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
WorkshopCardHolderIdentification		146	146	
workshopName		36	36	{00..20..20}
workshopAddress		36	36	{00..20..20}
cardHolderName				
holderSurname		36	36	{00..20..20}
holderFirstNames		36	36	{00..20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		2	2	
NoOfCalibrationsSinceDownload		2	2	{00 00}
EF Calibration		15668	45394	
WorkshopCardCalibrationData		15668	45394	
calibrationTotalNumber		2	2	{00 00}
calibrationPointerNewestRecord		2	2	{00}
calibrationRecords		15664	45390	
WorkshopCardCalibrationRecord	n_1	178	178	
calibrationPurpose		1	1	{00}
vehicleIdentificationNumber		17	17	{20..20}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00..20..20}
wVehicleCharacteristicConstant		2	2	{00 00}
kConstantOfRecordingEquipment		2	2	{00 00}
lTyreCircumference		2	2	{00 00}
tyreSize		15	15	{20..20}
authorisedSpeed		1	1	{00}
oldOdometerValue		3	3	{00..00}
newOdometerValue		3	3	{00..00}


oldTimeValue 4 4 [00..00]
newTimeValue 4 4 [00..00]
nextCalibrationDate 4 4 [00..00]
vuPartNumber 16 16 [20..20]
vuSerialNumber 8 8 [00..00]
sensorSerialNumber 8 8 [00..00]
sensorGNSSSerialNumber 8 8 [00..00]
rcmSerialNumber 8 8 [00..00]
vuAbility 1 1 [00]
sealDataCard 56 56
noOfSealRecords 1 1 [00]
SealRecords 55 55
SealRecord 5 11 11
equipmentType 1 1 [00]
extendedSealIdentifier 10 10 [00..00] •
EF Sensor_Installation_Data 18 102
SensorInstallationSecData 18 102 [00..00]
EF Events_Data 792 792
CardEventData 792 792
cardEventRecords 11 72 72
CardEventRecord n. 24 24
eventType 1 1 [00]
eventBeginTime 4 4 [00..00]
eventEndTime 4 4 [00..00]
eventVehicleRegistration
vehicleRegistrationNation 1 1 [00]
vehicleRegistrationNumber 14 14 [00, 20..20]
EF Faults_Data 288 288
CardFaultData 288 288
cardFaultRecords 2 144 144
CardFaultRecord n. 24 24
faultType 1 1 [00]
faultBeginTime 4 4 [00..00]
faultEndTime 4 4 [00..00]
faultVehicleRegistration
vehicleRegistrationNation 1 1 [00]
vehicleRegistrationNumber 14 14 [00, 20..20]
EF Driver_Activity_Data 202 498
CardDriverActivity 202 498
activityPointerOldestDayRecord 2 2 [00 00]
activityPointerNewestRecord 2 2 [00 00]
activityDailyRecords n. 198 492 [00..00]
EF Vehicles_Used 194 386
CardVehiclesUsed 194 386
vehiclePointerNewestRecord 2 2 [00 00]
cardVehicleRecords 192 384
CardVehicleRecord n. 48 48
vehicleOdometerBegin 3 3 [00..00]
vehicleOdometerEnd 3 3 [00..00]
vehicleFirstUse 4 4 [00..00]
vehicleLastUse 4 4 [00..00]
vehicleRegistration
vehicleRegistrationNation 1 1 [00]
vehicleRegistrationNumber 14 14 [00, 20..20]
vuDataBlockCounter 2 2 [00 00]
vehicleIdentificationNumber 17 17 [20..20]
EF Places 128 170



TCS_163 Sljedeće vrijednosti, koje se upotrebljavaju za navođenje veličina u prethodnoj tablici, predstavljaju najniži i najviši broj zapisa koji struktura podataka kartice radionice mora upotrebljavati za aplikaciju druge generacije:

		Minimalno	Maksimalno
n_1	NoOfEventsPerType	3	3
n_2	NoOfFaultsPerType	6	6
n_3	NoOfCardVehicleRecords	4	8
n_4	NoOfCardPlaceRecords	6	8
n_5	NoOfCalibrationRecords	88	255
n_6	CardActivityLengthRange	198 bajtova (1 dan * 93 promjena aktivnosti)	492 bajta (1 dan * 240 promjena aktivnosti)
n_7	NoOfCardVehicleUnitRecords	4	8
n_8	NoOfGNSSADRecords	18	24
n_9	NoOfSpecificConditionRecords	2	4

4.4. Aplikacije kontrolne kartice

4.4.1 *Aplikacija kontrolne kartice prve generacije*

TCS_164 Aplikacija kontrolne kartice prve generacije nakon personalizacije ima sljedeću trajnu strukturu datoteka i sljedeće trajne uslove za pristup datotekama:

Datoteka	ID datoteke	Uvjeti pristupa: Čitanje	Uvjeti pristupa: Ažuriranje	Uvjeti pristupa: Ažuriranje
EF Tachograph	'0500'			
EF Application_Identification	'0501'	SC2	SC1	NEV
EF Card_Certificate	'C100'	SC2	SC1	NEV
EF CA_Certificate	'C108'	SC2	SC1	NEV
EF Identification	'0520'	SC6	SC1	NEV
EF Controller_Activity_Data	'050C'	SC2	SC1	SC5

U ovoj se tablici upotrebljavaju sljedeće kratice za sigurnosne uslove:

SC1 ALW ILI SM-MAC-G2
SC2 ALW ILI SM-MAC-G1 ILI SM-MAC-G2
SC3 SM-MAC-G1 ILI SM-MAC-G2
SC6 EXT-AUT-G1 ILI SM-MAC-G1 ILI SM-MAC-G2

TCS_165 Strukture svih EF-ova moraju biti transparentne.

TCS_166 Aplikacija kontrolne kartice prve generacije ima sljedeću strukturu podataka:

Datoteka / podatkovni element	Broj zapisa	Veličina (u bajtovima) Min	Maks	
DF Tachograph		11104	24526	
EF Application_Identification		5	5	
ControlCardApplicationIdentification		5	5	
typeOfTachographCardId		1	1	[00]
cardStructureVersion		2	2	[00 00]
noOfControlActivityRecords		2	2	[00 00]
EF Card_Certificate		194	194	
CardCertificate		194	194	[00..00]
EF CA_Certificate		194	194	
MemberStateCertificate		194	194	[00..00]
EF Identification		211	211	
CardIdentification		65	65	
cardIssuingMemberState		1	1	[00]
cardNumber		16	16	[20..20]
cardIssuingAuthorityName		36	36	[00..20..20]
cardIssueDate		4	4	[00..00]
cardValidityBegin		4	4	[00..00]
cardExpiryDate		4	4	[00..00]
ControlCardHolderIdentification		146	146	
controlBodyName		36	36	[00..20..20]
controlBodyAddress		36	36	[00..20..20]
cardHolderName				
holderSurname		36	36	[00..20..20]
holderFirstNames		36	36	[00..20..20]
cardHolderPreferredLanguage		2	2	[20 20]
EF Controller_Activity_Data		10582	23922	
ControlCardControlActivityData		10582	23922	
controlPointerNewestRecord		2	2	[00 00]
controlActivityRecords		10580	23920	
controlActivityRecord	n	46	46	
controlType		1	1	[00]
controlTime		4	4	[00..00]
controlledCardNumber				
cardType		1	1	[00]
cardIssuingMemberState		1	1	[00]
cardNumber		16	16	[20..20]
controlledVehicleRegistration				
vehicleRegistrationNation		1	1	[00]
vehicleRegistrationNumber		14	14	[00..20..20]
controlDownloadPeriodBegin		4	4	[00..00]
controlDownloadPeriodEnd		4	4	[00..00]

TCS_167 Sljedeće vrijednosti, koje se upotrebljavaju za navođenje veličina u prethodnoj tablici, predstavljaju najniži i najviši broj zapisa koji struktura podataka kontrolne kartice mora upotrebljavati za aplikaciju prve generacije:

		Minimalno	Maksimalno
n	NoOfControlActivityRecords	230	520

4.4.2 *Aplikacija kontrolne kartice druge generacije*

TCS_168 Aplikacija kontrolne kartice druge generacije nakon personalizacije ima sljedeću trajnu strukturu datoteka i sljedeće trajne uslove za pristup datotekama:

Napomena: SFID kratkog EF indikatora navodi se kao decimalni broj, na primjer vrijednost 30 odgovara vrijednosti 11110 u binarnom zapisu.

Datoteka	ID datoteke	SFID	Uvjeti pristupa: Čitanje / Ažuriranje	Ažuriranje
DF Tachograph_G2			SC1	
EF Application_Identification	'0501'	1	SC1	NEV
EF CardMA_Certificate	'C100'	2	SC1	NEV
EF CA_Certificate	'C108'	4	SC1	NEV
EF Link_Certificate	'C109'	5	SC1	NEV
EF Identification	'0520'	6	SC1	NEV
EF Controller_Activity_Data	'050C'	14	SC1	SM-MAC-G2

U ovoj se tablici upotrebljava sljedeća kratica za sigurnosni uvjet:

SC1 ALW ILI SM-MAC-G2

TCS_169 Strukture svih EF-ova moraju biti transparentne.

TCS_170 Aplikacija kontrolne kartice druge generacije ima sljedeću strukturu podataka:

Datoteka / podatkovni element	Broj zapisa	Veličina (u bajtovima) Min	Maks	
DF Tachograph_G2		11410	25161	
EF Application_Identification		5	5	
ControlCardApplicationIdentification		5	5	
typeOfTachographCardId		1	1	[00]
cardStructureVersion		2	2	[00 00]
noOfControlActivityRecords		2	2	[00 00]
EF CardMA_Certificate		204	341	
CardMACertificate		204	341	[00..00]
EF CA_Certificate		204	341	
MemberStateCertificate		204	341	[00..00]
EF Link_Certificate		204	341	
LinkCertificate		204	341	[00..00]
EF Identification		211	211	
CardIdentification		65	65	
cardIssuingMemberState		1	1	[00]
cardNumber		16	16	[20..20]
cardIssuingAuthorityName		36	36	[00..20..20]
cardIssueDate		4	4	[00..00]
cardValidityBegin		4	4	[00..00]
cardExpiryDate		4	4	[00..00]
ControlCardHolderIdentification		146	146	
controlBodyName		36	36	[00..20..20]
controlBodyAddress		36	36	[00..20..20]
cardHolderName				
holderSurname		36	36	[00..20..20]
holderFirstNames		36	36	[00..20..20]
cardHolderPreferredLanguage		2	2	[20 20]
EF Controller_Activity_Data		10582	23922	
ControlCardControlActivityData		10582	23922	
controlPointerNewestRecord		2	2	[00 00]
controlActivityRecords		10580	23920	
controlActivityRecord	n	46	46	
controlType		1	1	[00]
controlTime		4	4	[00..00]
controlledCardNumber				
cardType		1	1	[00]
cardIssuingMemberState		1	1	[00]
cardNumber		16	16	[20..20]
controlledVehicleRegistration				
vehicleRegistrationNation		1	1	[00]
vehicleRegistrationNumber		14	14	[00..20..20]
controlDownloadPeriodBegin		4	4	[00..00]
controlDownloadPeriodEnd		4	4	[00..00]

TCS_171 Sljedeće vrijednosti, koje se upotrebljavaju za navođenje veličina u prethodnoj tablici, predstavljaju najniži i najviši broj zapisa koji struktura podataka kontrolne kartice mora upotrebljavati za aplikaciju druge generacije:

		Minimalno	Maksimalno
n	NoOfControlActivityRecords	230	520

4.5. Aplikacije kartice preduzeća

4.5.1 *Aplikacija kartice preduzeća prve generacije*

TCS_172 Aplikacija kartice preduzeća prve generacije nakon personalizacije ima sljedeću trajnu strukturu datoteka i sljedeće trajne uslove za pristup datotekama:

Datoteka	ID datoteke	Uvjeti pristupa: Čitanje	Odabir	Ažuriranje
DF Tachograph	'0500h'		SC1	
EF Application_Identification	'0501h'	SC2	SC1	NEV
EF Card_Certificate	'C100h'	SC2	SC1	NEV
EF CA_Certificate	'C108h'	SC2	SC1	NEV
EF Identification	'0520h'	SC6	SC1	NEV
EF Company_Activity_Data	'050Dh'	SC2	SC1	SC3

U ovoj se tablici upotrebljavaju sljedeće kratice za sigurnosne uslove:

SC1 ALW ILI SM-MAC-G2
SC2 ALW ILI SM-MAC-G1 ILI SM-MAC-G2
SC3 SM-MAC-G1 ILI SM-MAC-G2
SC6 EXT-AUT-G1 ILI SM-MAC-G1 ILI SM-MAC-G2

TCS_173 Strukture svih EF-ova moraju biti transparentne.

TCS_174 Aplikacija kartice preduzeća prve generacije ima sljedeću strukturu podataka:

Datoteka / podatkovni element	Broj zapisa	Veličina (u bajtovima) Min	Maks	Zadane vrijednosti
DF Tachograph		23214	24498	
EF Application_Identification		5	5	
CompanyCardApplicationIdentification		5	5	
typeOfTachographCardId		1	1	[00]
cardStructureVersion		2	2	[00 00]
noOfCompanyActivityRecords		2	2	[00 00]
EF Card_Certificate		194	194	
CardCertificate		194	194	[00..00]
EF CA_Certificate		194	194	
MemberStateCertificate		194	194	[00..00]
EF Identification		139	139	
CardIdentification		65	65	
cardIssuingMemberState		1	1	[00]
cardNumber		16	16	[20..20]
cardIssuingAuthorityName		36	36	[00, 20..20]
cardIssueDate		4	4	[00..00]
cardValidityBegin		4	4	[00..00]
cardExpiryDate		4	4	[00..00]
CompanyCardHolderIdentification		74	74	
companyName		36	36	[00, 20..20]
companyAddress		36	36	[00, 20..20]
cardHolderPreferredLanguage		2	2	[20 20]
EF Company_Activity_Data		10582	23922	
CompanyActivityData		10582	23922	
companyPointerNewestRecord		2	2	[00 00]
companyActivityRecords		10580	23920	
companyActivityRecord	n_c	46	46	
companyActivityType		1	1	[00]
companyActivityTime		4	4	[00..00]
cardNumberInformation				
cardType		1	1	[00]
cardIssuingMemberState		1	1	[00]
cardNumber		16	16	[20..20]
vehicleRegistrationInformation				
vehicleRegistrationNation		1	1	[00]
vehicleRegistrationNumber		14	14	[00, 20..20]
downloadPeriodBegin		4	4	[00..00]
downloadPeriodEnd		4	4	[00..00]

TCS_175 Sljedeće vrijednosti, koje se upotrebljavaju za navođenje veličina u prethodnoj tablici, predstavljaju najniži i najviši broj zapisa koji struktura podataka kartice preduzeća mora upotrebljavati za aplikaciju prve generacije:

		Minimalno	Maksimalno
n_c	NrOfCompanyActivityRecords	230	520

4.5.2 *Aplikacija kartice preduzeća druge generacije*

TCS_176 Aplikacija kartice preduzeća druge generacije nakon personalizacije ima sljedeću trajnu strukturu datoteka i sljedeće trajne uslove za pristup datotekama:

Napomena: SFID kratkog EF indikatora navodi se kao decimalni broj, na primjer vrijednost 30 odgovara vrijednosti 11110 u binarnom zapisu.

Datoteka	ID datoteke	SFID	Uvjeti pristupa: Čitanje / Odabir	Uvjeti pristupa: Ažuriranje
DF Tachograph_G2			SC1	
EF Application_Identification	'0501h'	1	SC1	NEV
EF CardMA_Certificate	'C100h'	2	SC1	NEV
EF CA_Certificate	'C108h'	4	SC1	NEV
EF Link_Certificate	'C109h'	5	SC1	NEV
EF Identification	'0520h'	6	SC1	NEV
EF Company_Activity_Data	'0500h'	14	SC1	SM-MAC-G2

U ovoj se tablici upotrebljava sljedeća kratica za sigurnosni uvjet:

SC1 ALW ILI SM-MAC-G2

TCS_177 Strukture svih EF-ova moraju biti transparentne.

TCS_178 Aplikacija kartice preduzeća druge generacije ima sljedeću strukturu podataka:

Datoteka / podatkovni element	Broj zapisa	Veličina (u bajtovima) Min	Maks	Zadane vrijednosti
DF Tachograph_G2		11350	25003	
EF Application_Identification		5	5	
CompanyCardApplicationIdentification		5	5	
typeOfTachographCardId		1	1	[00]
cardStructureVersion		2	2	[00 00]
noOfCompanyActivityRecords		2	2	[00 00]
EF CardMA_Certificate		204	341	
CardMACertificate		204	341	[00..00]
EF CA_Certificate		204	341	
MemberStateCertificate		204	341	[00..00]
EF Link_Certificate		204	341	
LinkCertificate		204	341	[00..00]
EF Identification		139	139	
CardIdentification		65	65	
cardIssuingMemberState		1	1	[00]
cardNumber		16	16	[20..20]
cardIssuingAuthorityName		36	36	[00..20..20]
cardIssueDate		4	4	[00..00]
cardValidityBegin		4	4	[00..00]
cardExpiryDate		4	4	[00..00]
CompanyCardHolderIdentification		74	74	
companyName		36	36	[00..20..20]
companyAddress		36	36	[00..20..20]
cardHolderPreferredLanguage		2	2	[20 20]
EF Company_Activity_Data		10582	23932	
CompanyActivityData		10582	23932	
companyPointerNewestRecord		2	2	[00 00]
companyActivityRecords		10580	23930	
companyActivityRecord	n_c	46	46	
companyActivityType		1	1	[00]
companyActivityTime		4	4	[00..00]
cardNumberInformation				
cardType		1	1	[00]
cardIssuingMemberState		1	1	[00]
cardNumber		16	16	[20..20]
vehicleRegistrationInformation				
vehicleRegistrationNation		1	1	[00]
vehicleRegistrationNumber		14	14	[00..20..20]
downloadPeriodBegin		4	4	[00..00]
downloadPeriodEnd		4	4	[00..00]

TCS_179 Sljedeće vrijednosti, koje se upotrebljavaju za navođenje veličina u prethodnoj tablici, predstavljaju najniži i najviši broj zapisa koji struktura podataka kartice preduzeća mora upotrebljavati za aplikaciju druge generacije:

		Minimalno	Maksimalno
n_c	NoOfCompanyActivityRecords	230	520

Dodatak 3.

PIKTOGRAMI

PIC_001 Tahograf može neobavezno upotrebljavati sljedeće piktograme i kombinacije piktograma (ili piktograme i kombinacije piktograma koji su dovoljno slični da ih je nedvosmisleno moguće povezati s ovima):

1. OSNOVNI PIKTOGRAMI

	Osobe	Radnje	Načini rada
	Preduzeće		Način rada preduzeće
	Nadzornik	Kontrola	Kontrolni način
	Vozač	Vožnja	Operativni način
	Radionica / ispitno mjesto	Pregled/kalibracija	Kalibracijski način
	Proizvođač		

	Aktivnosti	Trajanje
	Pripravnost	Period tekuće pripravnosti
	Vožnja	Neprekidno vrijeme vožnje
	Odmor	Period tekućeg odmora
	Ostali rad	Period tekućeg rada
	Pauza	Kumulativno vrijeme pauze
	Nepoznato	

	Oprema	Funkcije
	Otvor vozača	
	Otvor suvozača	
	Kartica	
	Sat	
	Prikaz	Prikazivanje
	Vanjska arhiviranje podataka	Preuzimanje podataka
	Napajanje	
	Pisač/ispis	Ispisivanje
	Senzor	
	Veličina guma	
	Vozilo / jedinica u vozilu	
	GNSS uređaj	
	Uređaj za otkrivanje na daljinu	
	ITS sučelje	

	Posebna stanja
	Izvan područja primjene
	Vožnja trajektom/vozom

	Razno		
	Događaji		Pogreške
	Početak dnevnog radnog vremena		Kraj dnevnog radnog vremena
	Mjesto		
	Ručni unos aktivnosti vozača		
	Sigurnost		
	Brzina		
	Vrijeme		
	Ukupno/sažetak		

	Oznake
24h	Dnevno
	Nedeljno
	Dva nedelje
	Od ili do

2. KOMBINACIJE PIKTOGRAMA

	Razno		
	Mjesto kontrole		
	Mjesto početka dnevnog radnog vremena		Mjesto kraja dnevnog radnog vremena
▼M1			
	Položaj nakon 3 sata akumulisanog vremena vožnje		
▼B			
	Od (vrijeme)		Do (vrijeme)
	Iz vozila		
OUT	Početak aktivnosti izvan područja primjene	OUT	Završetak aktivnosti izvan područja primjene

	Kartice
	Kartica vozača
	Kartica preduzeće
	Kontrolna kartica
	Kartica radionice
	Bez kartice

	Vožnja
	Vožnja u posadi
	Vrijeme vožnje u tjedan dana
	Vrijeme vožnje u dva nedelje

	Ispisi
24h	Dnevni ispis aktivnosti vozača s kartice
24h	Dnevni ispis aktivnosti vozača iz jedinice u vozilu
	Ispis događaja i kvarova s kartice
	Ispis događaja i kvarova iz jedinice u vozilu
	Ispis tehničkih podataka
	Ispis prekoračenja brzine

	Događaji
	Umetanje nevažeće kartice
	Konflikt kartica
	Vremensko preklapanje
	Vožnja bez odgovarajuće kartice
	Umetanje kartice tokom vožnje
	Posljednja razmjena podataka s karticom nije ispravno zatvorena
	Prekoračenje brzine
	Prekid napajanja
	Pogreška u podacima o kretanju
	Konflikt u kretanju vozila
	Povreda sigurnosti
	Vremenski konflikt ili prilagodba vremena (od strane radionice)
	Kontrola prekoračenja brzine
	Izostanak podataka o položaju iz prijamnika GNSS-a ili greška u komunikaciji s vanjskim uređajem GNSS-a
	Greška u komunikaciji s uređajem za komunikaciju na daljinu

	Kvarovi
	Kvar kartice (otvor vozača)
	Kvar kartice (otvor suvozača)
	Kvar zaslona
	Pogreška pri preuzimanju podataka
	Kvar pisača
	Kvar senzora
	Interni kvar jedinice u vozilu (VU)
	Kvar GNSS uređaja
	Kvar uređaja za otkrivanje na daljinu

	Postupak ručnog unosa
	I dalje isto dnevno radno vrijeme?
	Kraj prethodnog radnog vremena?
	Potvrdite ili unesite mjesto kraja radnog vremena
	Unesite vrijeme početka
	Potvrdite ili unesite mjesto početka radnog vremena

Napomena: dodatne kombinacije piktograma za formiranje bloka ispisa ili identifikatora zapisa utvrđene su u Dodatku 4.

Dodatak 4

ISPISI

SADRŽAJ

1. UOPŠTENO

Svaki ispis nastaje ulančavanjem raznih podatkovnih blokova, koji se mogu identifikovati s pomoću identifikatora bloka.

Jedan podatkovni blok sadrži jedan ili više zapisa, koji se mogu identifikovati s pomoću identifikatora zapisa.

PRT_001 Kad identifikator bloka neposredno prethodi identifikatoru zapisa, identifikator zapisa se ne ispisuje.

PRT_002 Ako je neka podatkovna stavka nepoznata ili se ne smije ispisati zbog prava na pristup podacima, umjesto nje ispisuju se praznine.

PRT_003 Ako je sadržaj cijelog retka nepoznat ili ga ne treba ispisivati, izostavlja se cijeli redak.

PRT_004 Numerička podatkovna polja ispisuju se u desnom poravnanju, s razmakom za tisuće i milijune i bez vodećih nula.

PRT_005 Polja s podatkovnim nizovima ispisuju se u lijevom poravnanju i popunjavaju prazninama do dužine podatkovne stavke ili se prema potrebi skraćuju na dužinu podatkovne stavke (imena i adrese).

PRT_006 U slučaju kraja retka zbog dugog teksta, kao prvi znak novog retka ispisuje se poseban znak (tačka na sredini visine retka, „•").

2. SPECIFIKACIJA PODATKOVNOG BLOKA

U ovom se poglavlju upotrebljavaju sljedeći dogovoreni formati bilježenja:

— **masno** otisnutim slovima označava se običan tekst koji treba ispisati (pri čemu se tekst ispisuje normalnim slovima),

— normalnim znakovima označavaju se varijable (piktogrami ili podaci) koje se prilikom ispisa zamjenjuju svojim vrijednostima,

— nazivi varijabli nadopunjeni su podcrtavanjem za prikaz dužine podatkovne stavke raspoložive za varijablu,

— datumi se navode u formatu „dd/mm/gggg" (dan, mjesec, godina). Može se upotrebljavati i oblik „dd.mm.gggg",

— izraz „identifikacija kartice" je oznaka koja se sastoji od vrste kartice prikazane kombinacijom piktograma kartice, šifre države članice koja ju je izdala, kose crte te broja kartice s indeksom zamjene i indeksom obnavljanja odvojenima razmakom:

P		x	x	x	/	x	x	x	x	x	x	x	x	x	x	x	x	x	x		x		x
kombinacija piktograma kartice		šifra države članice koja je izdala karticu				prvih 14 znamenaka broja kartice (po mogućnosti s indeksom rednog broja kartice)															indeks zamjene		indeks obnavljanja

PRT_007 Za ispise se upotrebljavaju sljedeći podatkovni blokovi i/ili zapisi, u skladu sa sljedećim značenjima i formatima:

Broj bloka ili zapisa Značenje	Data Format
1. ***Datum i vrijeme ispisa dokumenta***	▼ dd/mm/yyyy hh:mm **(UTC)**
2. ***Vrsta ispisa*** Identifikator bloka Ispis kombinacije piktograma (vidjeti Dodatak 3.), postavka uređaja za ograničavanje brzine (samo za ispis prekoračenja brzine)	----------▼---------- Picto xxx **km/h**
3. ***Identifikacija nositelja kartice*** Identifikator bloka P = piktogram „osoba" Prezime nositelja kartice Ime(na) nositelja kartice (ako postoji) Identifikacija kartice Datum isteka valjanosti kartice (ako postoji) i broj generacije kartice (GEN 1 ili GEN 2) (*)	----------P---------- P Last_Name_____ First_Name_____ Card_Identification_____ dd/mm/yyyy - GEN 2

U slučaju neosobne kartice koja ne sadržava prezime nositelja kartice, umjesto toga se tiska naziv poduzeća, radionice ili nadzornog tijela.

(*) Broj generacije kartice može ispisati samo pametni tahograf.

4. ***Identifikacija vozila*** Identifikator bloka VIN Država članica registracije i registracijski broj vozila (VRN)	----------A---------- A VIN_____ Nat/VRN_____
5. ***Identifikacija jedinice u vozilu (VU)*** Identifikator bloka Naziv proizvođača jedinice u vozilu Kataloški broj jedinice u vozilu Broj generacije jedinice u vozilu (*)	----------B---------- B VU_Manufacturer_____ VU_Part_Number__ GEN 2

(*) Broj generacije kartice može ispisati samo pametni tahograf.

6. ***Zadnja kalibracija tahografa*** Identifikator bloka Naziv radionice Identifikacija kartice radionice Datum kalibracije	----------T---------- T Last_Name_____ Card_Identification_____ T dd/mm/yyyy

7. ***Zadnja kontrola (od strane službenika za kontrolu)***

Identifikator bloka
Identifikacija kartice nadzornika
Datum, vrijeme i vrsta kontrole

```
----------▣----------
Card Identification_____
▣ dd/mm/yyyy hh:mm ppppp
```

Vrsta kontrole: do pet piktograma. Vrsta kontrole može biti (kombinacija) sljedećeg:
▣: preuzimanje podataka s kartice, ▼: preuzimanje podataka s VU-a, ▼: ispis, □: prikaz, ⚲:provjera kalibracije na cesti

8. ***Aktivnosti vozača pohranjene na kartici prema redoslijedu nastanka***

Identifikator bloka
Datum upita (kalendarski dan ispisa) + brojač dnevne nazočnosti kartice

```
----------▣----------
    dd/mm/yyyy  xxx
```

8.a *Stanje izvan područja primjene na početku ovog dana* (ostaviti prazno ako nije otvoreno stanje izvan područja primjene)

```
----------OUT----------
```

8.1. *Razdoblje u kojem kartica nije bila umetnuta*
8.1.a Identifikator zapisa (početak razdoblja)
8.1.b *Nepoznato razdoblje* Vrijeme početka, trajanje
8.1.c *Ručno unesena aktivnost*
Piktogram aktivnosti, vrijeme početka, trajanje

```
  --------------------
?       hh:mm hhhmm
A       hh:mm hhhmm
```

8.2. *Umetanje kartice u utor S*
Identifikator zapisa; S = piktogram utora
Država članica registracije vozila i registracijski broj vozila (VRN)
Stanje brojača kilometara vozila pri umetanju kartice

```
  ---------S---------
A Nat/VRN__________
  x xxx xxx km
```

8.3. *Aktivnost (dok je kartica bila umetnuta)*
Piktogram aktivnosti, vrijeme početka, trajanje, status posade (piktogram posade za status POSADA, prazno ako je JEDAN VOZAČ)

```
A       hh:mm hhhmm ⚉⚉
```

8.3.a *Posebno stanje* Vrijeme unosa, piktogram posebnog stanja (ili kombinacija piktograma)

```
        hh:mm ---pppp---
```

8.4. *Vađenje kartice*
Brojač kilometara vozila i prijeđena udaljenost od zadnjeg umetanja za koje je poznat brojač kilometara

```
  x xxx xxx km; x xxx km
```

9. ***Aktivnosti vozača pohranjene u jedinici u vozilu, po utoru, kronološkim redom***

Identifikator bloka
Datum upita (kalendarski dan ispisa)
Brojač kilometara vozila u 00:00 i 24:00

```
----------▣----------
      dd/mm/yyyy
x xxx xxx - x xxx xxx km
```

10. ***Aktivnosti koje se obavljaju u utoru S***

Identifikator bloka

```
----------S----------
```

10.a *Stanje izvan područja primjene na početku ovog dana* (ostaviti prazno ako nije otvoreno stanje izvan područja primjene)

```
----------OUT----------
```

10.1. *Razdoblje kada u utoru S nema kartice*
Identifikator zapisa
Nije umetnuta kartica
Brojač kilometara vozila na početku razdoblja

```
  --------------------
⚉▣---
  x xxx xxx km
```

10.2. *Umetanje kartice*
Identifikator zapisa o umetanju kartice
Prezime vozača

```
  --------------------
▣ Last Name_____________
```

	Ime vozača	First_Name_____
	Identifikacija kartice vozača	Card_Identification____
	Datum isteka valjanosti kartice (ako postoji) i broj generacije kartice (GEN 1 ili GEN 2) (*)	dd/mm/yyyy - GEN 2
	Država članica registracije i registracijski broj (VRN) prethodno korištenog vozila	A+Nat/VRN_____
	Datum i vrijeme vađenja kartice iz prethodnog vozila	dd/mm/yyyy hh:mm
	Prazni redak	
	Brojač kilometara vozila pri umetanju kartice. Znak ručnog unosa aktivnosti vozača (M: da, prazno: ne).	x xxx xxx km M
	Ako nije bilo umetanja kartice vozača na dan kad se vrši ispis, tada se za blok 10.2. upotrebljava očitanje podataka brojača kilometara od zadnjeg dostupnog umetanja kartice prije tog dana.	
10.3.	*Aktivnost*	
	Piktogram aktivnosti, vrijeme početka, trajanje, status posade (piktogram posade za status POSADA, prazno ako je JEDAN VOZAČ)	A hh:mm hhhmm ⊕⊕
10.3.a	*Posebno stanje* Vrijeme unosa, piktogram posebnog stanja (ili kombinacija piktograma)	hh:mm ---pppp---
10.4.	*Vađenje kartice ili kraj razdoblja „bez kartice"*	
	Brojač kilometara vozila pri vađenju kartice ili na kraju razdoblja „bez kartice" i prijeđena udaljenost od umetanja kartice ili od početka razdoblja „bez kartice".	x xxx xxx km; x xxx km

(*) Broj generacije kartice može ispisati samo pametni tahograf.

11.	***Dnevni sažetak***	
	Identifikator bloka	----------Σ----------
11.1.	***Dnevni sažetak jedinice u vozilu za razdoblja bez kartice u utoru vozača***	
	Identifikator bloka	1⊕⊡---
11.2.	***Dnevni sažetak jedinice u vozilu za razdoblja bez kartice u utoru suvozača***	
	Identifikator bloka	2⊕⊡---
11.3.	***Dnevni sažetak jedinice u vozilu po vozaču***	
	Identifikator zapisa	----------
	Prezime vozača	⊕ Last_Name_____
	Ime(na) vozača	First_Name_____
	Identifikacija kartice vozača	Card_Identification____
▸[m] 11.4.	*Ulaz mjesta početka ili kraja dnevnog radnog vremena*	
	pi = piktogram početka / kraja, vrijeme, država, regija	pihh:mm Cou Reg
	zemljopisna dužina zabilježenog položaja	lon ±DDD°MM.M'
	zemljopisna širina zabilježenog položaja	lat ± DD°MM.M
	oznaka vremena kada je položaj utvrđen	hh:mm
	Brojač kilometara	x xxx xxx km ◂
▸[m] 11.5.	*Položaj nakon 3 sata akumuliranog vremena vožnje*	
	pi = položaj nakon 3 sata akumuliranog vremena vožnje	
	vrijeme	pihh:mm
	zemljopisna dužina zabilježenog položaja	lon ± DDD°MM.M
	zemljopisna širina zabilježenog položaja	lat ± DD°MM.M '
	oznaka vremena kada je položaj utvrđen	hh:mm
	Brojač kilometara	x xxx xxx km ◂
11.6.	*Aktivnosti ukupno (s kartice)*	
	Ukupno trajanje vožnje, prijeđena udaljenost	⊕ hhhmm x xxx km
	Ukupno trajanje rada i pripravnosti	✕ hhhmm ⊡ hhhmm
	Ukupno trajanje odmora i nepoznatih aktivnosti	⊢ hhhmm ? hhhmm
	Ukupno trajanje aktivnosti posade	⊕⊕ hhhmm
11.7.	*Aktivnosti ukupno (razdoblja bez kartice u utoru vozača)*	
	Ukupno trajanje vožnje, prijeđena udaljenost	⊕ hhhmm x xxx km
	Ukupno trajanje rada i pripravnosti	✕ hhhmm ⊡ hhhmm
	Ukupno trajanje odmora	⊢ hhhmm

11.8.	*Aktivnosti ukupno (razdoblja bez kartice u utoru suvozača)*	
	Ukupno trajanje rada i pripravnosti	⚒ hh:mm ⧈ hh:mm
	Ukupno trajanje odmora	⊢ hh:mm
11.9.	*Aktivnosti ukupno (po vozaču, uključuje oba utora)*	
	Ukupno trajanje vožnje, prijeđena udaljenost	⊕ hh:mm x xxx km
	Ukupno trajanje rada i pripravnosti	⚒ hh:mm ⧈ hh:mm
	Ukupno trajanje odmora	⊢ hh:mm
	Ukupno trajanje aktivnosti posade	⊕⊕ hh:mm

Ako se traži dnevni ispis za tekući dan, informacije o dnevnom sažetku računaju se iz podataka dostupnih u vrijeme ispisa.

12.	***Događaji i/ili kvarovi pohranjeni na kartici***	
12.1.	Identifikator bloka zadnjih pet „događaja i kvarova" s kartice	----------!×▣----------
12.2.	Identifikator bloka svih zabilježenih „događaja" na kartici	----------!▣----------
12.3.	Identifikator bloka svih zabilježenih „kvarova" na kartici	----------×▣----------
12.4.	*Zapis događaja i/ili kvara*	
	Identifikator zapisa	----------
	Piktogram događaja/kvara, svrha zapisa, datum i vrijeme početka	Pic (p) dd/mm/yyyy hh:mm
	Dodatna šifra događaja/kvara (ako postoji), trajanje	!xx hh:mm
	Država članica registracije i registracijski broj vozila (VRN) u kojem se dogodio događaj ili kvar	⍋ Nat/VRN_____

13.	***Događaji i/ili kvarovi koji su pohranjeni ili u tijeku u jedinici u vozilu (VU)***	
13.1.	Identifikator bloka zadnjih pet „događaja i kvarova" iz VU-a	----------!×⍋----------
13.2.	Identifikator bloka svih zabilježenih „događaja" ili „događaja" u tijeku u VU-u	----------!⍋----------
13.3.	Identifikator bloka svih zabilježenih „kvarova" ili „kvarova" u tijeku u VU-u	----------×⍋----------
13.4.	*Zapis događaja i/ili kvara*	
	Identifikator zapisa	----------
	Piktogram događaja/kvara, svrha zapisa, datum i vrijeme početka	Pic (p) dd/mm/yyyy hh:mm
	Dodatna šifra događaja/kvara (ako postoji), broj sličnih događaja tog dana, trajanje	!xx (xxx) hh:mm
	Identifikacija kartica umetnutih na početku ili na kraju događaja ili kvara (do četiri retka bez ponavljanja istih brojeva kartica dva puta)	Card_Identification_____ Card_Identification_____ Card_Identification_____ Card_Identification_____
	Slučaj kad nije bila umetnuta nijedna kartica	▣---
	Podatci specifični za proizvođača	< Literal><ErrorCode>

Svrha zapisa (p) je numerička šifra koja objašnjava zašto je događaj ili kvar zabilježen, a šifrirana je u skladu s podatkovnim elementom `EventFaultRecordPurpose`.

`Literal` je literal specifičan za proizvođača tahografa s najviše 12 znakova.

`ErrorCode` je šifra pogreške specifična za proizvođača tahografa s najviše 12 znakova.

14. ***Identifikacija jedinice u vozilu (VU)***

Identifikator bloka	----------B----------
Naziv proizvođača VU-a	B Name_____
Adresa proizvođača VU-a	Address_____
Kataloški broj VU-a	PartNumber_____
Homologacijski broj VU-a	Apprv_____
Serijski broj VU-a	S/N_____
Godina proizvodnje VU-a	yyyy
Verzija programa u VU-u i datum instalacije	V xxxx dd/mm/yyyy

15. ***Identifikacija senzora***

Identifikator bloka	----------A----------
15.1. *Zapis o uparivanju*	
Serijski broj senzora	A S/N_____
Homologacijski broj senzora	Apprv_____
Datum uparivanja senzora	dd/mm/yyyy hh:mm

16. *Identifikacija uređaja GNSS-a*

Identifikator bloka	----------▚----------
16.1. *Zapis o spajanju*	
Serijski broj vanjskog uređaja GNSS-a	▚ S/N_____
Homologacijski broj vanjskog uređaja GNSS-a	Apprv_____
Datum spajanja vanjskog uređaja GNSS-a	dd/mm/yyyy hh:mm

17. ***Podatci o kalibraciji***

Identifikator bloka	----------T----------
17.1. *Zapis o kalibraciji*	
Identifikator zapisa	----------
Radionica koja je izvršila kalibraciju	T Workshop_name_____
Adresa radionice	Workshop_address_____
Identifikacija kartice radionice	Card_Identification_____
Datum isteka valjanosti kartice radionice	dd/mm/yyyy
Prazni redak	
Datum kalibracije + svrha kalibracije	T dd/mm/yyyy (p)
VIN	A VIN_____
Država članica registracije i registracijski broj vozila (VRN)	Nat/VRN_____
Karakteristični koeficijent vozila	w xx xxx Imp/km
Konstanta uređaja za bilježenje podataka	k xx xxx Imp/km
Effective circumference of wheel tyres	l xx xxx mm
Veličina montiranih guma	• TyreSize_____
Postavka uređaja za ograničavanje brzine	> xxx km/h
Stare i nove vrijednosti na brojaču kilometara	x xxx xxx - x xxx xxx km

Svrha kalibracije (p) je numerička šifra koja objašnjava zašto su zabilježeni ti kalibracijski parametri, a šifrirana je u skladu s podatkovnim elementom `CalibrationPurpose`.

18.	***Prilagodba vremena***	
	Identifikator bloka	----------⚙----------
18.1.	*Zapis o prilagodbi vremena*	
	Identifikator zapisa	-------------------
	Stari datum i vrijeme	!● dd/mm/yyyy hh:mm
	Novi datum i vrijeme	● dd/mm/yyyy hh:mm
	Radionica koja je izvršila prilagodbu vremena	T Workshop_name_____
	Adresa radionice	Workshop_address____
	Identifikacija kartice radionice	Card_Identification_____
	Datum isteka valjanosti kartice radionice	dd/mm/yyyy

19.	***Posljednji događaj i kvar zabilježeni u jedinici u vozilu***	
	Identifikator bloka	----------!×▲----------
	Datum i vrijeme posljednjeg događaja	! dd/mm/yyyy hh:mm
	Datum i vrijeme posljednjega kvara	× dd/mm/yyyy hh:mm

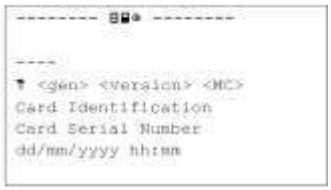
20.	***Informacije o kontroli prekoračenja brzine***	
	Identifikator bloka	----------»»----------
	Datum i vrijeme posljednje KONTROLE PREKORAČENJA BRZINE	»▯dd/mm/yyyy hh:mm
	Datum/vrijeme prvog prekoračenja brzine i broj događaja prekoračenja brzine od tada	»»dd/mm/yyyy hh:mm (nnn)

21.	***Zapis o prekoračenju brzine***	
21.1.	Identifikator bloka „Prvo prekoračenje brzine nakon zadnje kalibracije"	--------»»T---------
21.2.	Identifikator bloka „Pet najozbiljnijih prekoračenja u zadnjih 365 dana"	-------»»(365)------
21.3.	Identifikator bloka „Najozbiljnije prekoračenje za svaki od deset zadnjih dana pojave"	-------»»(10)-------
21.4.	Identifikator zapisa	-------------------
	Datum, vrijeme i trajanje	»»dd/mm/yyyy hh:mm hhhmm
	Najveća i prosječna brzina, broj sličnih događaja tog dana	xxx **km/h** xxx **km/h**(xxx)
	Prezime vozača	● Last_Name_____
	Ime(na) vozača	First_Name_____
	Identifikacija kartice vozača	Card_Identification_____
21.5.	Ako u bloku nema zapisa o prekoračenju brzine	»»---

22.	***Ručno unesene informacije***	
	Identifikator bloka	----------
22.1.	Mjesto kontrole	▯● .....
22.2.	Potpis nadzornika	▯ .....
22.3.	Od (vrijeme)	●● .....
22.4.	Do (vrijeme)	+● .....
22.5.	Potpis vozača	● .....

„Ručno unesene informacije": umetnuti dovoljno praznih redaka iznad prostora za ručni upis tako da se stvarno mogu upisati traženi podatci ili staviti potpis.

23. ***Posljednje kartice umetnute u jedinicu u vozilu***
Identifikator bloka
23.1. Umetnuta kartica
Identifikator zapisa
Vrsta kartice, generacija, verzija, proizvođač (*)
Identifikacija kartice
Serijski broj kartice
Datum i vrijeme posljednjeg umetanja kartice



(*) (sve u jednom retku)
pri čemu je
type of card (vrsta kartice): piktogram, jedan znak + razmak,
gen (generacija): GEN1 ili GEN2, 4 znaka + razmak,
version (verzija): do 10 znakova,
MC: šifra proizvođača, 3 znaka.

3. SPECIFIKACIJE ISPISA

U ovom se poglavlju upotrebljavaju sljedeći dogovoreni zapisi:

N	Ispis broja bloka ili zapisa N
N	Ispis broja bloka ili zapisa N ponovljen onoliko puta koliko je potrebno
X/Y	Ispis bloka ili zapisa X i/ili Y prema potrebi, ponavljajući onoliko puta koliko je potrebno

3.1. Dnevni ispis aktivnosti vozača s kartice

PRT_008 Dnevni ispis aktivnosti vozača s kartice u skladu je sa sljedećim formatom:

1.	Datum i vrijeme ispisa dokumenta
2.	Vrsta ispisa
3.	Identifikacija nadzornika (ako je kontrolna kartica umetnuta u VU)
3.	Identifikacija vozača (iz kartice koja je predmet ispisa + GEN)
4.	Identifikacija vozila (vozilo iz kojeg se uzima ispis)
5.	Identifikacija VU-a (VU iz kojeg se uzima ispis + GEN)
6.	Zadnja kalibracija VU-a
7.	Zadnja kontrola kojoj je bio podvrgnut vozač
8.	Razdjelnik aktivnosti vozača
8.a	Stanje izvan područja primjene na početku ovog dana
8.1.a / 8.1.b / 8.1.c / 8.2. / 8.3. / 8.3.a / 8.4.	Aktivnosti vozača po redoslijedu napauza
11.	Razdjelnik dnevnog sažetka
11.4.	Mjesta unijeta hronološkim redom
11.5.	Položaj nakon 3 sata akumulisanog vremena vožnje hronološkim
11.6.	Aktivnosti ukupno
12.1.	Događaji ili kvarovi s razdjelnika kartice
12.4.	Zapisi događaja/kvarova (zadnjih pet događaja ili kvarova arhivirani na kartici)
13.1.	Događaji ili kvarovi s razdjelnika VU-a
13.4.	Zapisi događaja/kvarova (zadnjih pet događaja ili kvarova arhivirani ili u toku u VU-u)
22.1.	Mjesto kontrole
22.2.	Potpis nadzornika
22.5.	Potpis vozača

3.2. Dnevni ispis aktivnosti vozača iz jedinice u vozilu (VU)

PRT_009 Dnevni ispis aktivnosti vozača iz VU-a u skladu je sa sljedećim formatom:

1.	Datum i vrijeme ispisa dokumenta
2.	Vrsta ispisa
3.	Identifikacija nosioca kartice (za sve kartice umetnute u VU + GEN)
4.	Identifikacija vozila (vozilo iz kojeg se uzima ispis)
5.	Identifikacija VU-a (VU iz kojeg se uzima ispis + GEN)
6.	Zadnja kalibracija ovog VU-a
7.	Zadnja kontrola ovog tahografa
9.	Razdjelnik aktivnosti vozača
10.	Razdjelnik otvora vozača (otvor 1)
10.a	Stanje izvan područja primjene na početku ovog dana
10.1. / 10.2. / 10.3. / 10.3.a / 10.4.	Aktivnosti hronološkim redom (otvor vozača)
10.	Razdjelnik otvora suvozača (otvor 2)
10.a	Stanje izvan područja primjene na početku ovog dana
10.1. / 10.2. / 10.3. / 10.3.a / 10.4.	Aktivnosti hronološkim redom (otvor suvozača)
11.	Razdjelnik dnevnog sažetka
11.1.	Sažetak perioda bez kartice u otvoru vozača
11.4.	Mjesta unijeta hronološkim redom
11.5.	Položaj nakon 3 sata akumulisanog vremena vožnje hronološkim redoslijedom
11.7.	Aktivnosti ukupno

11.2.	Sažetak perioda bez kartice u otvoru suvozača
11.4.	Mjesta unijeta hronološkim redom
11.5.	Položaj nakon 3 sata akumulisanog vremena vožnje hronološkim redoslijedom
11.8.	Aktivnosti ukupno
11.3.	Sažetak aktivnosti za vozača, uključena oba otvora
11.4.	Mjesta koja je taj vozač unio hronološkim redoslijedom
11.5.	Položaj nakon 3 sata akumulisanog vremena vožnje hronološkim redoslijedom
11.9.	Aktivnosti ukupno za tog vozača
13.1.	Razdjelnik događaja i kvarova
13.4.	Zapisi događaja/kvarova (zadnjih pet događaja ili kvarova arhivirani ili u toku u VU-u)
22.1.	Mjesto kontrole
22.2.	Potpis nadzornika
22.3.	Od (vrijeme) (prostor za vozača bez kartice da navede
22.4.	Do (vrijeme) perioda koja se odnose na njega)
22.5.	Potpis vozača

3.3. Ispis događaja i kvarova s kartice

PRT_010 Ispis događaja i kvarova s kartice u skladu je sa sljedećim formatom:

1.	Datum i vrijeme ispisa dokumenta
2.	Vrsta ispisa
3.	Identifikacija nadzornika (ako je kontrolna kartica umetnuta u VU + GEN)
3.	Identifikacija vozača (iz kartice koja je predmet ispisa)
4.	Identifikacija vozila (vozilo iz kojeg se uzima ispis)
12.2.	Razdjelnik događaja
12.4.	Zapisi događaja (svi događaji arhivirani na kartici)
12.3.	Razdjelnik kvarova
12.4.	Zapisi o kvarovima (svi kvarovi arhivirani na kartici)
22.1.	Mjesto kontrole
22.2.	Potpis nadzornika
22.5.	Potpis vozača

3.4. Ispis događaja i kvarova iz VU-a

PRT_011 Ispis događaja i kvarova iz VU-a u skladu je sa sljedećim formatom:

1.	Datum i vrijeme ispisa dokumenta
2.	Vrsta ispisa
3.	Identifikacija nosioca kartice (za sve kartice umetnute u VU + GEN)
4.	Identifikacija vozila (vozilo iz kojeg se uzima ispis)
13.2.	Razdjelnik događaja
13.4.	Zapisi događaja (svi događaji arhivirani ili u toku u VU-u)
13.3.	Razdjelnik kvarova
13.4.	Zapisi o kvarovima (sve pogreške arhivirane ili u toku u VU-u)
22.1.	Mjesto kontrole
22.2.	Potpis nadzornika
22.5.	Potpis vozača

3.5. Ispis tehničkih podataka

PRT_012 Ispis tehničkih podataka u skladu je sa sljedećim formatom:

1.	Datum i vrijeme ispisa dokumenta
2.	Vrsta ispisa
3.	Identifikacija nosioca kartice (za sve kartice umetnute u VU + GEN)
4.	Identifikacija vozila (vozilo iz kojeg se uzima ispis)
14.	Identifikacija jedinice u vozilu (VU)
15.	Identifikacija senzora
15.1.	Podaci o uparivanju senzora (svi raspoloživi podaci hronološkim redom)
16.	Identifikacija uređaja GNSS-a
16.1.	Podaci o spajanju vanjskog uređaja GNSS-a (svi raspoloživi podaci hronološkim redom)
17.	Razdjelnik podataka o kalibraciji
17.1.	Zapisi o kalibraciji (svi raspoloživi zapisi hronološkim redom)
18.	Razdjelnik prilagodbe vremena
18.1.	Zapisi o prilagodbi vremena (svi raspoloživi zapisi od zapisa o prilagodbi vremena i od zapisa o kalibraciji)
19.	Posljednji događaj i kvar zabilježeni u VU-u

3.6. Ispis prekoračenja brzine

PRT_013 Ispis prekoračenja brzine u skladu je sa sljedećim formatom:

1.	Datum i vrijeme ispisa dokumenta
2.	Vrsta ispisa
3.	Identifikacija nosioca kartice (za sve kartice umetnute u VU + GEN)
4.	Identifikacija vozila (vozilo iz kojeg se uzima ispis)
20.	Informacije o kontroli prekoračenja brzine
21.1.	Identifikator podataka o prekoračenju brzine
21.4. / 21.5.	Prvo prekoračenje brzine nakon zadnje kalibracije
21.2.	Identifikator podataka o prekoračenju brzine
21.4. / 21.5.	Pet najozbiljnijih prekoračenja brzine u zadnjih 365 dana
21.3.	Identifikator podataka o prekoračenju brzine
21.4. / 21.5.	Najozbiljnije prekoračenje brzine za svaki od deset zadnjih dana pojave

22.1.	Mjesto kontrole
22.2.	Potpis nadzornika
22.5.	Potpis vozača

3.7. Istorijski podaci o umetnutim karticama

PRT_014 Ispis istorijskih podataka o umetnutim karticama u skladu je sa sljedećim formatom:

1.	Datum i vrijeme ispisa dokumenta
2.	Vrsta ispisa
3.	Identifikacije nosioca kartice (za sve kartice umetnute u VU)
23.	Posljednja kartica umetnuta u VU
23.1.	Umetnute kartice (do 88 zapisa)
12.3.	Razdjelnik kvarova

Dodatak 5

PRIKAZ

U ovom se Dodatku upotrebljavaju sljedeći dogovoreni formati bilježenja:

— **masno** otisnuti znakovi označuju običan tekst koji se prikazuje (pri čemu se tekst prikazuje normalnim znakovima),

— normalni znakovi označuju varijable (piktograme ili podatke) koje se prilikom prikaza zamjenjuju svojim vrijednostima:

dd mm yyyy : dan, mjesec, godina,
hh : sati,
mm : minute,
D : piktogram trajanja,
EF : kombinacija piktograma događaja ili kvarova,
O : piktogram načina rada.

DIS_001 Tahograf prikazuje podatke primjenom sljedećeg formata:

Podaci	**Format**
Standardni prikaz	
Lokalno vrijeme	
Način rada	
Informacije koje se odnose na vozača	
Informacije koje se odnose na suvozača	
Otvoreno stanje izvan područja primjene	
Prikaz upozorenja	
Prekoračenje neprekidnog vremena vožnje	
Događaj ili kvar	
Ostali prikazi	
datum po UTC-u	
vrijeme	
Neprekidno vrijeme vožnje i kumulativno vrijeme pauze vozača	
Neprekidno vrijeme vožnje i kumulativno vrijeme pauze suvozača	
Ukupno vrijeme vožnje vozača u prethodnom i tekućem tjednu	
Ukupno vrijeme vožnje suvozača u prethodnom i tekućem tjednu	

Dodatak 6

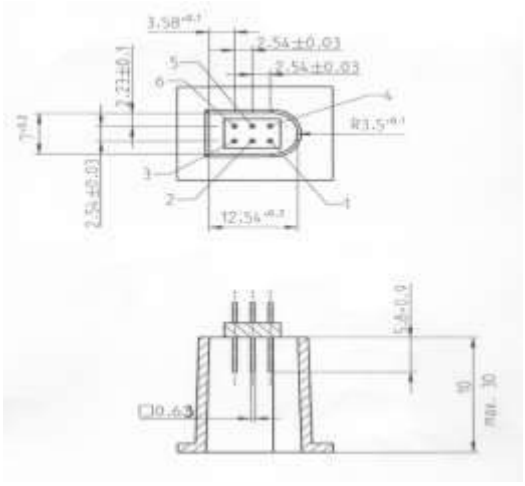
PREDNJI PRIKLJUČAK ZA KALIBRACIJU I PREUZIMANJE PODATAKA

SADRŽAJ

1. HARDVER

1.1. Priključak

INT_001 Priključak za preuzimanje podataka / kalibraciju je 6-pinski priključak, dostupan s prednje strane bez potrebe isključivanja bilo kojeg dijela tahografa, i koji udovoljava sljedećem nacrtu (sve dimenzije izražene su u milimetrima):



Sljedeći dijagram prikazuje tipični priključak za 6-pinsko uparivanje:

1.2. Raspored kontakata

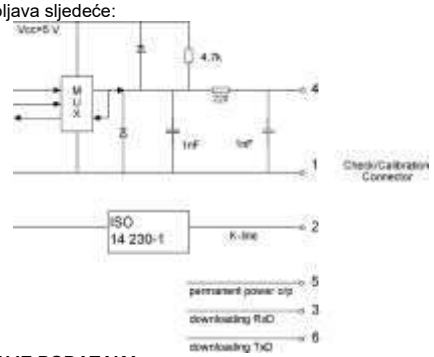
INT_002 Kontakti se raspoređuju prema sljedećoj tablici:

Pin	Opis	Napomena
1	Akumulator – minus	Priključen na negativni pol akumulatora vozila
2	Podatkovna komunikacija	K-linija (ISO 14230-1)

3	RxD – preuzimanje podataka	Unos podataka u tahograf
4	Ulazni/izlazni signal	Kalibracija
5	Stalna izlazna snaga	Raspon napona je onaj koji je na vozilu, umanjen za 3 V kako bi se omogućio pad napona na zaštitnim strujnim krugovima. Snaga 40 mA
6	TxD – preuzimanje podataka	Izlaz podataka iz tahografa

1.3. Blok dijagram

INT_003 Blok dijagram zadovoljava sljedeće:



2. SUČELJE ZA PREUZIMANJE PODATAKA

INT_004 Sučelje za preuzimanje podataka zadovoljava specifikacije RS232.

INT_005 Sučelje za preuzimanje podataka upotrebljava jedan početni bit, osam podatkovnih bitova, s LSB-om (najmanje značajnim bitom) na početku, jedan parni paritetni bit i jedan zaustavni bit.

Organizacija podatkovnog bajta

Početni bit : jedan bit na logičkoj nivou 0;
Podatkovni bitovi : prenose se s LSB-om (najmanje značajnim bitom) na početku;
Paritetni bit : parni paritet
Zaustavni bit : jedan bit na logičkoj nivou 1.

Kod prenosa numeričkih podataka sastavljenih od više bajtova, najznačajniji bajt prenosi se prvi, a najmanje značajan bajt posljednji.

INT_006 Brzine prenosa podataka moraju biti prilagodljive u rasponu od 9 600 bps do 115 200 bps. Prenos se postiže pri najvišoj mogućoj brzini prenosa, pri čemu je početna brzina prenosa podataka nakon početka komunikacije postavljena na 9 600 bps.

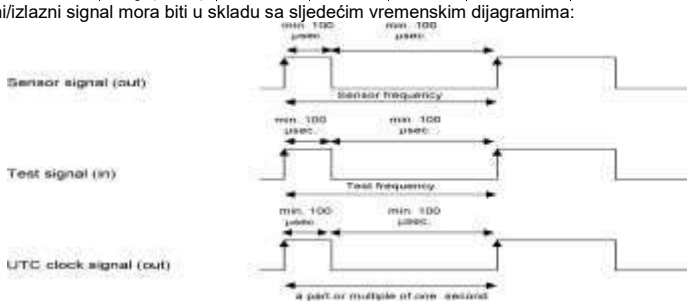
3. Sučelje za kalibraciju

INT_007 Podatkovna komunikacija mora ispunjavati zahtjeve norme ISO 14230-1 *Road vehicles – Diagnostic systems – Keyword protocol 2000 – Part 1: Physical layer*, prvo izdatje: 1999.

INT_008 Ulazni/izlazni signal mora zadovoljavati sljedeće električne specifikacije:

Parametar	Najmanje	Tipično	Najviše	Napomena
U_{low} (ulazni)			1,0 V	I = 750 µA
U_{high} (ulazni)	4 V			I = 200 µA
Frekvencija			4 kHz	
U_{low} (izlazni)			1,0 V	I = 1 mA
U_{high} (izlazni)	4 V			I = 1 mA

INT_009 Ulazni/izlazni signal mora biti u skladu sa sljedećim vremenskim dijagramima:



Dodatak 7.

PROTOKOLI PREUZIMANJA PODATAKA

SADRŽAJ

1. UVOD

U ovom se Dodatku navode postupci za obavljanje različitih vrsta preuzimanja podataka na vanjski medij za arhiviranje podataka (ESM) zajedno s protokolima koje treba provesti kako bi se osigurao ispravan prenos podataka i potpuna shodnost formata preuzetih podataka, čime se svakom nadzorniku omogućava da pregleda te podatke te da može kontrolirati njihovu autentičnost i cjelovitost prije analize.

1.1. Područje primjene

Podaci se mogu preuzeti na ESM:

— iz jedinice u vozilu posebnom namjenskom opremom (IDE) priključenom na jedinicu u vozilu (VU),

— s tahografske kartice putem IDE-a opremljenog napravom kartičnog sučelja (IFD),

— s tahografske kartice preko jedinice u vozilu putem IDE-a priključenog na VU.

Da bi se omogućila provjera autentičnosti i integriteta preuzetih podataka arhivirani na ESM, podaci se preuzimaju potpisom stavljenim shodno Dodatku 11. „Zajednički sigurnosni mehanizmi”. Identifikacija uređaja izvora (jedinica u vozilu ili kartica) i njegovi sigurnosni certifikati (države članice i opreme) također se preuzimaju. Onaj tko provjerava podatke mora posjedovati vlastiti pouzdan evropski javni ključ.

Podaci preuzeti s jedinice u vozilu potpisuju se u skladu s Dodatkom 11. „Zajednički sigurnosni mehanizmi”, dijelom B (sistem tahografa druge generacije), osim kad nadzor vozača obavlja nadležno tijelo za kontrolu izvan

EU-a, koristeći kontrolnu karticu prve generacije, u slučaju čega se podaci potpisuju u skladu s Dodatkom 11. „Zajednički sigurnosnih mehanizmi”, dijelom A (sistem tahografa prve generacije), u skladu s Dodatkom 15. „Migracija”, zahtjevom MIG_015.
U ovom se Dodatku, dakle, utvrđuju dvije vrste preuzimanja podataka iz VU-u:
— vrsta preuzimanja podataka s jedinice u vozilu druge generacije, koja osigurava strukturu podataka druge generacije, potpisana u skladu s Dodatkom 11. „Zajednički sigurnosni mehanizmi”, dijelom B,
— vrsta preuzimanja podataka s jedinice u vozilu prve generacije, koja osigurava strukturu podataka prve generacije, potpisana u skladu s Dodatkom 11. „Zajednički sigurnosni mehanizmi”, dijelom A.
Slično tomu, postoje dvije vrste preuzimanja podataka s kartice vozača druge generacije umetnute u VU, kako je utvrđeno u stavcima 3. i 4. ovog Dodatka.

1.2. Skraćenice i zabilješke

U ovom se Dodatku upotrebljavaju sljedeće skraćenice:

AID identifikator aplikacije (eng. Application Identifier)
ATR odziv na povraćaj u početno stanje (eng. Answer To Reset)
CS bajt kontrolnog zbira (eng. Checksum Byte)
DF namjenska datoteka (eng. Dedicated File)
DS_ dijagnostički proces (eng. Diagnostic Session)
EF elementarna datoteka (eng. Elementary File)
ESM vanjski medij za arhiviranje podataka (eng. External Storage Medium)
FID identifikator datoteke (eng. File Identifier) (ID datoteke (File ID))
FMT formatni bajt (eng. Format Byte) (prvi bajt zaglavlja poruke)
ICC kartica s integriranim krugovima (eng. Integrated Circuit Card)
IDE posebna namjenska oprema (eng. Intelligent Dedicated Equipment): oprema koja se upotrebljava za preuzimanje podataka na ESM (npr. osobno računalo)
IFD naprava sučelja (eng. Interface Device)
KWP protokol Keyword 2000 (eng. Keyword Protocol 2000)
LEN bajt dužine (eng. Length Byte) (posljednji bajt zaglavlja poruke)
PPS protokol odabira parametra (eng. Protocol Parameter Selection)
PSO izvođenje sigurnosne radnje (eng. Perform Security Operation)
SID identifikator usluge (eng. Service Identifier)
SRC izvorni bajt (eng. Source Byte)
TGT ciljni bajt (eng. Target Byte)
TLV vrijednost dužine oznake (eng. Tag Length Value)
TREP parametar odgovora za prenos (eng. Transfer Response Parameter)
TRTP parametar zahtjeva za prenos (eng. Transfer Request Parameter)
VU jedinica u vozilu (eng. Vehicle Unit)

2. PREUZIMANJE PODATAKA S JEDINICE U VOZILU (VU)

2.1. Postupak preuzimanja podataka

Za preuzimanje podataka s jedinice u vozilu korisnik mora obaviti sljedeće radnje:
— umetnuti svoju tahografsku karticu u otvor jedinice u vozilu (*1),
— priključiti IDE na priključak za preuzimanje podataka iz jedinice u vozilu,
— uspostaviti vezu između IDE-a i jedinice u vozilu,
— odabrati na IDE-u podatke za preuzimanje i poslati zahtjev jedinici u vozilu,
— zaključiti proces preuzimanja podataka.

2.2. Protokol preuzimanja podataka

Protokol je strukturiran na načelu nadređen-podređen, pri čemu IDE ima nadređenu, a jedinica u vozilu podređenu ulogu.
Struktura, vrste i tok poruka načelno su utemeljeni na protokolu Keyword 2000 (KWP) (ISO 14230-2 *Road vehicles – Diagnostic systems – Keyword protocol 2000 – Part 2*: *Data link layer*).
Aplikacijska nivo u načelu se temelji na sadašnjem nacrtu ISO 14229-1 (*Road vehicles – Diagnostic systems – Part 1*: *Diagnostic services*, verzija 6. od 22. februar 2001.).

2.2.1 *Struktura poruke*

DDP_002 Sve poruke koje se razmjenjuju između IDE-a i jedinice u vozilu formatirane su u strukturi koja se sastoji od tri dijela:
— zaglavlja koje čine formatni bajt (FMT), ciljni bajt (TGT), izvorni bajt (SRC) i eventualno bajt za dužinu (LEN),
— podatkovnog polja koje čine bajt identifikatora usluge (SID) i promjenjivi broj podatkovnih bajtova koji može obuhvaćati neobavezni bajt dijagnostičke razmjene podataka (DS_) ili neobavezni bajt parametara prenosa (TRTP ili TREP),
— kontrolnog zbira koji čini bajt kontrolnog zbira (CS).

Zaglavlje				**Podatkovno polje**					**Kontrolni zbir**
FMT	**TGT**	**SRC**	**LEN**	**SID**	**PODACI**	**…**	**…**	**…**	**CS**
4 bajta				najviše 255 bajtova					1 bajt

Bajtovi TGT i SRC predstavljaju fizičku adresu primatelja i tvorca poruke. Vrijednosti su F0 Hex za IDE i EE Hex za jedinicu u vozilu.
Bajt LEN je dužina dijela podatkovnog polja.
Bajt kontrolnog zbira je 8-bitni zbir serije modula 256 svih bajtova poruke s izuzetkom samog kontrolnog zbira.
Bajtovi FMT, SID, DS_, TRTP i TREP definisani su u nastavu ovog dokumenta.

DDP_003 Kada su podaci koje prenosi poruka dulji od raspoloživog prostora u dijelu podatkovnog polja, poruka se u stvarnosti šalje u nekoliko dijelova poruke. Svaki dio poruke nosi zaglavlje, isti SID, TREP i 2-bajtni brojač dijelova poruke koji označava broj dijelova poruke u cjelokupnoj poruci. Kako bi se omogućilo provjeravanje pogrešaka i prekid, IDE potvrđuje svaki dio poruke. IDE može primiti dio poruke, tražiti da se ona ponovo prenese, zahtijevati od jedinice u vozilu da ponovo počne ili prekine prenos.
DDP_004 Ako posljednji dio poruke sadrži tačno 255 bajtova u podatkovnom polju, mora se staviti zadnji dio poruke s praznim podatkovnim poljem (osim SID TREP i brojača dijelova poruke) kako bi se označio kraj poruke.
Primjer:

Zaglavlje	**SID**	**TREP**	**Poruka**	**CS**
4 bajta	dulja od 255 bajtova			

Prenosi se kao:

Zaglavlje	**SID**	**TREP**	**00**	**01**	**Dio poruke 1**	**CS**
4 bajta	255 bajtova					

Zaglavlje	**SID**	**TREP**	**00**	**02**	**Dio poruke 2**	**CS**
4 bajta	255 bajtova					

…

Zaglavlje	**SID**	**TREP**	**xx**	**yy**	**Dio poruke n**	**CS**
4 bajta	kraća od 255 bajtova					

ili kao:

Zaglavlje	**SID**	**TREP**	**00**	**01**	**Dio poruke 1**	**CS**
4 bajta	255 bajtova					

Zaglavlje	**SID**	**TREP**	**00**	**02**	**Dio poruke 2**	**CS**
4 bajta	255 bajtova					

…

Zaglavlje	**SID**	**TREP**	**xx**	**yy**	**Dio poruke n**	**CS**
4 bajta	255 bajtova					

Zaglavlje	**SID**	**TREP**	**xx**	**yy + 1**	**CS**
4 bajta	4 bajta				

2.2.2 *Vrste poruka*

Komunikacijski protokol za preuzimanje podataka između jedinice u vozilu i IDE-a zahtijeva razmjenu osam različitih vrsta poruka.
U sljedećoj se tablici nalazi sažeti prikaz tih poruka.

Struktura poruke	**Najviše 4 bajta Zaglavlje**				**Najviše 255 bajta Podaci**			**1 bajt Kontrolni zbir**
IDE -> **<- VU**	**FMT**	**TGT**	**SRC**	**LEN**	**SID**	**DS_ / TRTP**	**DATA**	**CS**
Zahtjev za početak komunikacije	81	EE	F0		81			E0
Pozitivan odgovor za početak komunikacije	80	F0	EE	03	C1		EA, 8F	9 B
Zahtjev za početak dijagnostičke razmjene podataka	80	EE	F0	02	10	81		F1
Pozitivan odgovor za početak dijagnostičke razmjene podataka	80	F0	EE	02	50	81		31
Usluga upravljanja vezom								
Provjera brzine prenosa podataka (stadij 1)								
9 600 Bd	80	EE	F0	04	87		01,01,01	EC
19 200 Bd	80	EE	F0	04	87		01,01,02	ED
38 400 Bd	80	EE	F0	04	87		01,01,03	EE
57 600 Bd	80	EE	F0	04	87		01,01,04	EF
115 200 Bd	80	EE	F0	04	87		01,01,05	F0
Pozitivan odgovor na provjeru brzine prenosa podataka	80	F0	EE	02	C7		01	28
Prelazna brzina prenosa podataka (stadij 2)	80	EE	F0	03	87		02,03	ED
Zahtjev za prihvat podataka	80	EE	F0	0A	35		00,00,00,00,00,FF,FF, FF,FF	99
Pozitivan odgovor na zahtjev za prihvat podataka	80	F0	EE	03	75		00,FF	D5
Zahtjev za prenos podataka								
Nadzor	80	EE	F0	02	36	01 ili 21		97
Aktivnosti	80	EE	F0	06	36	02 ili 22	Datum	CS

Događaji i kvarovi	80	EE	F0	02	36	03 ili 23	Datum	99
Detaljna brzina	80	EE	F0	02	36	04 ili 24	Datum	9A
Tehnički podaci	80	EE	F0	02	36	05 ili 25	Datum	9B
Preuzimanje podataka s kartice	80	EE	F0	02	36	06	Otvor	CS
Pozitivan odgovor na zahtjev za prenos podataka	80	F0	EE	Len	76	TREP	Podaci	CS
Zahtjev za prekid prenosa podataka	80	EE	F0	01	37			96
Pozitivan odgovor na zahtjev za prekid prenosa	80	F0	EE	01	77			D6
Zahtjev za prekid komunikacije	80	EE	F0	01	82			E1
Pozitivan odgovor na zahtjev za prekid komunikacije	80	F0	EE	01	C2			21
Potvrda dijela poruke	80	EE	F0	Len	83		Podaci	CS
Negativni odgovori								
Opšte odbijanje	80	F0	EE	03	7F	Sid Req	10	CS
Usluga nije podržana	80	F0	EE	03	7F	Sid Req	11	CS
Podfunkcija nije podržana	80	F0	EE	03	7F	Sid Req	12	CS
Neispravna dužina poruke	80	F0	EE	03	7F	Sid Req	13	CS
Neispravni uslovi ili pogreška u slijedu zahtjeva	80	F0	EE	03	7F	Sid Req	22	CS
Zahtjev izvan dometa	80	F0	EE	03	7F	Sid Req	31	CS
Prihvat podataka nije prihvaćen	80	F0	EE	03	7F	Sid Req	50	CS
Čekanje na odgovor	80	F0	EE	03	7F	Sid Req	78	CS
Podaci nisu dostupni	80	F0	EE	03	7F	Sid Req	FA	CS

Napomene:

— TRTP od 21 do 25 koriste se za zahtjeve za preuzimanje podataka s jedinice u vozilu druge generacije, TRTP od 01 do 05 koriste se za zahtjeve za preuzimanje podataka s jedinice u vozilu prve generacije, koje može prihvatiti samo jedinica u vozilu u okviru nadzora vozača koji obavlja nadležno tijelo za kontrolu izvan EU-a, koristeći kontrolnu karticu prve generacije.

— TRTP od 11 do 19 te od 31 do 39 rezervisani su za zahtjeve za preuzimanjem specifične za proizvođača.

— Sid Req = Sid odgovarajućeg zahtjeva.

— TREP = TRTP odgovarajućeg zahtjeva.

— Osjenčana polja označuju da se ne prenosi ništa.

— Izraz prihvat (s gledišta IDE-a) upotrebljava se zbog usklađenosti s normom ISO 14229. Znači isto što i preuzimanje podataka (s gledišta jedinice u vozilu).

— Potencijalni 2-bajtni brojači dijelova poruke nisu prikazani u ovoj tablici.

— Otvor je broj otvora, ili „1” (kartica u otvoru vozača) ili „2” (kartica u otvoru suvozača).

— U slučaju da otvor nije naveden, jedinica u vozilu (VU) odabire otvor 1 ako je kartica umetnuta u taj otvor, dok otvor 2 odabire samo kada je to izričito odabrao korisnik.

2.2.2.1 Zahtjev za početak komunikacije (SID 81)

DDP_005 Ovu poruku šalje IDE za uspostavljanje komunikacijske veze s jedinicom u vozilu. Početne komunikacije uvijek se obavljaju pri brzini od 9 600 bauda (dok se brzina prenosa podataka eventualno ne promijeni upotrebom odgovarajućih usluga upravljanja vezom).

2.2.2.2 Pozitivan odgovor za početak komunikacije (SID C1)

DDP_006 Ovu poruku šalje jedinica u vozilu (VU) kao pozitivan odgovor na zahtjev za početak komunikacije. Ona sadrži 2 bajta ključa ‘EA’‘8F’, koji označuju da jedinica podržava protokol sa zaglavljem koje sadrži podatke o ciljanom izvoru i dužini.

2.2.2.3 Zahtjev za početak dijagnostičke razmjene podataka (SID 10)

DDP_007 Poruku sa zahtjevom za početak dijagnostičke razmjene podataka šalje IDE radi davanja zahtjeva za novu dijagnostičku razmjenu podataka s jedinicom u vozilu. Podfunkcija „standardni proces” (81 Hex) označava da je potrebno otvoriti standardnu dijagnostičku razmjenu podataka.

2.2.2.4 Pozitivan odgovor za početak dijagnostike (SID 50)

DDP_008 Poruku s pozitivnim odgovorom za početak dijagnostičke razmjene podataka šalje jedinica u vozilu (VU) kao pozitivan odgovor na zahtjev za početak dijagnostičke razmjene podataka.

2.2.2.5 Usluga upravljanja vezom (SID 87)

DDP_052 IDE upotrebljava uslugu upravljanja vezom za pokretanje postupka promjene brzine prenosa podataka. Taj se postupak odvija u dva koraka. U prvom koraku IDE predlaže promjenu brzine prenosa podataka navodeći novu brzinu. Po primitku pozitivne poruke iz jedinice u vozilu, IDE odašilje potvrdu promjene brzine prenosa podataka u jedinicu u vozilu (drugi korak). IDE potom prelazi na novu brzinu prenosa podataka. Po primitku potvrde jedinica u vozilu prelazi na novu brzinu prenosa podataka.

2.2.2.6 Pozitivan odgovor na zahtjev za upravljanje vezom (SID C7)

DDP_053 Pozitivan odgovor na zahtjev za upravljanje vezom šalje jedinica u vozilu kao pozitivan odgovor na zahtjev za uslugu upravljanja vezom (prvi korak). Napominje se da nema odgovora na zahtjev za potvrdom (drugi korak).

2.2.2.7 Zahtjev za prihvat podataka (SID 35)

DDP_009 Poruku sa zahtjevom za prihvat podataka IDE šalje jedinici u vozilu kao obavještenje da je zatražena radnja prihvata podataka. Za ispunjavanje zahtjeva norme ISO 14229 obuhvaćeni su podaci koji sadržiju pojedinosti o adresi, veličini i formatu zatraženih podataka. S obzirom na to da su oni za IDE nepoznati prije preuzimanja podataka, adresa memorije postavlja se na 0, format je nešifriran i nekomprimiran i veličina memorije je postavljena na maksimum.

2.2.2.8 Pozitivan odgovor na zahtjev za prihvat podataka (SID 75)

DDP_010 Poruku s pozitivnim odgovorom na zahtjev za prihvat podataka jedinica u vozilu šalje IDE-u kao obavještenje da je jedinica u vozilu spremna za preuzimanje podataka. Za ispunjenje zahtjeva norme ISO 14229, u toj se poruci s pozitivnim odgovorom navode podaci koji obavještavaju IDE da će daljnje poruke s pozitivnim odgovorom na zahtjev za prenos podataka sadržiti najviše 00FFh bajtova.

2.2.2.9 Zahtjev za prenos podataka (SID 36)

DDP_011 Zahtjev za prenos podataka šalje IDE da bi jedinici u vozilu naznačio koju vrstu podataka treba preuzeti. Jednobajtni parametar zahtjeva za prenos podataka (TRTP) označava vrstu prenosa.

Postoji šest vrsta prenosa podataka. Za preuzimanje podataka s jedinice u vozilu, dvije različite vrijednosti TRTP-a mogu se koristiti za svaku vrstu prenosa:

Vrsta prenosa podatka	**Vrijednost TRTP-a za preuzimanje podataka prve generacije**	**Vrijednost TRTP-a za preuzimanje podataka druge generacije**
Pregled	01	21
Aktivnosti navedenog dana	02	22
Događaji ili kvarovi	03	23
Detaljna brzina	04	24
Tehnički podaci	05	25

Vrsta prenosa podatka	Vrijednost TRTP-a
Preuzimanje podataka s kartice	06

DDP_054 IDE mora obavezno zahtijevati prenos pregleda podataka (TRTP 01 ili 21) tokom procesa preuzimanja podataka s obzirom na to da se samo time osigurava da se certifikati jedinice u vozilu zabilježe unutar preuzete datoteke (i omogućava provjera digitalnog potpisa).

U drugom slučaju (TRTP 02 ili 22) poruka sa zahtjevom za prenos podataka obuhvaća oznaku kalendarskog dana (u formatu [illegible]) za koji treba preuzeti podatke.

2.2.2.10 Pozitivan odgovor za prenos podataka (SID 76)

DDP_012 Pozitivan odgovor za prenos podataka šalje jedinica u vozilu kao odgovor na zahtjev za prenos podataka. Poruka sadrži zahtijevane podatke s parametrom odgovora za prenos (TREP) koji odgovara TRTP-u zahtjeva.

DDP_055 U prvom slučaju (TREP 01 ili 21) jedinica u vozilu poslat će podatke koji pomažu operatoru IDE-a da izabere podatke koje želi dalje preuzeti. Ta poruka sadrži sljedeće informacije:

— sigurnosni certifikati,
— identifikacija vozila,
— trenutni datum i vrijeme jedinice u vozilu,
— najraniji i najkasniji datum na koji je moguće preuzeti podatke (podaci iz jedinice u vozilu),
— oznaka prisustva kartice u jedinici u vozilu,
— prethodno preuzimanje podataka od strane preduzeće,
— blokade preduzeće,
— prethodne kontrole.

2.2.2.11 Zahtjev za prekid prenosa (SID 37)

DDP_013 Zahtjev za prekid prenosa IDE šalje jedinici u vozilu kao obavještenje da je proces preuzimanja podataka završen.

2.2.2.12 Pozitivan odgovor na zahtjev za prekid prenosa (SID 77)

DDP_014 Poruku s pozitivnim odgovorom na zahtjev za prekid prenosa jedinica u vozilu šalje kao potvrdu zahtjeva za prekid prenosa.

2.2.2.13 Zahtjev za prekid komunikacije (SID 82)

DDP_015 Poruku sa zahtjevom za prekid komunikacije IDE šalje za prekid komunikacijske veze s jedinicom u vozilu.

2.2.2.14 Pozitivan odgovor na zahtjev za prekid komunikacije (SID C2)

DDP_016 Poruku s pozitivnim odgovorom za prekid komunikacije jedinica u vozilu šalje kao potvrdu zahtjeva za prekid komunikacije.

2.2.2.15 Potvrda dijela poruke (SID 83)

DDP_017 Potvrdu dijela poruke IDE šalje za potvrdu primitka svakog dijela poruke koja se prenosi u više dijelova. Podatkovno polje sadrži SID koji se prima od jedinice u vozilu i 2-bajtni kod kako slijedi:
— MsgC + 1 potvrđuje ispravan primitak broja dijela poruke MsgC.
— IDE šalje zahtjev jedinici u vozilu da pošalje sljedeći dio poruke.
— MsgC ukazuje na problem s primitkom broja dijela poruke MsgC.
— IDE ponovno šalje zahtjev jedinici u vozilu da pošalje taj dio poruke.
— FFFF zahtijeva kraj poruke.
— Tim se postupkom IDE može služiti za okončanje prenosa poruke iz jedinice u vozilu iz bilo kojeg razloga.
Posljednji dio neke poruke (bajt LEN < 255) može se potvrditi bilo kojim od navedenih kodova ili se ne mora potvrditi.
Odgovori jedinice u vozilu koji se sastoje od više dijelova poruke sljedeći su:
— Pozitivan odgovor za prenos podataka (SID 76).

2.2.2.16 Negativan odgovor (SID 7F)

DDP_018 Poruku s negativnim odgovorom jedinica u vozilu šalje kao odgovor na prethodno navedene poruke zahtjeva ako jedinica u vozilu ne može udovoljiti zahtjevu. Podatkovna polja poruke sadržiju SID odgovora (7F), SID zahtjeva i kod koji označava razlog za negativan odgovor. Na raspolaganju su sljedeći kodovi:
— 10 opšte odbacivanje
— Radnja se ne može obaviti zbog razloga koji nije naveden u nastavu.
— 11 usluga nije podržana
— SID zahtjeva nije razumljiv.
— 12 podfunkcija nije podržana
— DS_ ili TRTP zahtjeva nije razumljiv ili nema daljnjih dijelova poruke koje treba prenijeti.
— 13 neispravna dužina poruke
— Dužina primljene poruke pogrešna je.
— 22 uslovi nisu ispravni ili pogreška u slijedu zahtjeva
— Zahtijevana usluga nije aktivna ili slijed poruka zahtjeva nije ispravan.
— 31 zahtjev izvan raspona
— Zapis parametra zahtjeva (podatkovno polje) nije važeći.
— 50 prihvat podataka nije prihvaćen
— Zahtjev se ne može izvršiti (jedinica u vozilu u neprimjerenom načinu rada ili unutarnja pogreška jedinice u vozilu).
— 78 čekanje na odgovor
— Zahtijevana radnja ne može se pravovremeno dovršiti i jedinica u vozilu nije spremna za prihvaćanje drugog zahtjeva.
— FA podaci nisu dostupni
— Podatkovni objekt zahtjeva za prenos podataka nije dostupan u jedinici u vozilu (na primjer, nije umetnuta kartica, vrsta preuzimanja podataka iz jedinice u vozilu zatražena od strane nadležnog tijela za kontrolu izvan EU-a).

2.2.3 *Tok poruke*

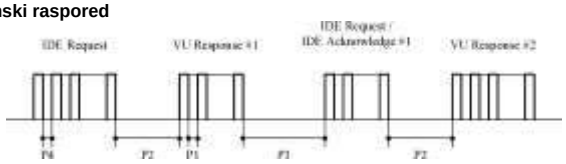
Tipičan tok poruke tokom redovnog postupka preuzimanja podataka sljedeći je:

IDE		**VU**
Zahtjev za početak komunikacije	⇨	
	⇦	Pozitivan odgovor
Zahtjev za početak dijagnostičke usluge	⇨	
	⇦	Pozitivan odgovor
Zahtjev za prihvat podataka	⇨	
	⇦	Pozitivan odgovor
Zahtjev za prenos pregleda podataka	⇨	
	⇦	Pozitivan odgovor
Zahtjev za prenos podataka #2	⇨	
	⇦	Pozitivan odgovor #1
Potvrda dijela poruke #1	⇨	
	⇦	Pozitivan odgovor #2
Potvrda dijela poruke #2	⇨	
	⇦	Pozitivan odgovor #m
Potvrda dijela poruke #m	⇨	
	⇦	Pozitivan odgovor (podatkovno polje < 255 bajtova)
Potvrda dijela poruke (neobvezno)	⇨	
…		
Zahtjev za prenos podataka #n	⇨	
	⇦	Pozitivan odgovor
Zahtjev za prekid prenosa podataka	⇨	
	⇦	Pozitivan odgovor
Zahtjev za prekid komunikacije	⇨	
	⇦	Pozitivan odgovor

2.2.4 *Vremenski raspored*

DDP_019 Tokom redovnog rada mjerodavni su vremenski parametri prikazani na sljedećoj slici:
Slika 1.

Tok poruke, vremenski raspored



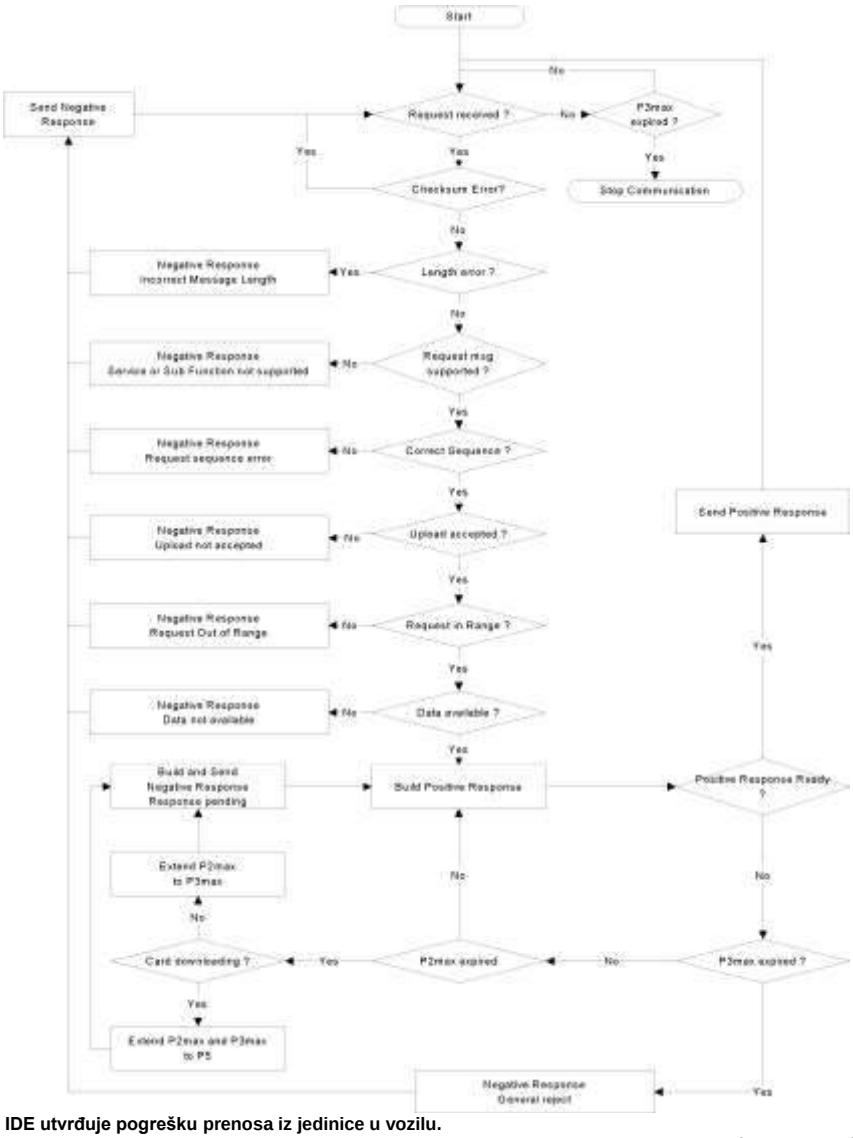
Gdje je:
P1=međubajtno vrijeme za odgovor jedinice u vozilu (VU),
P2=vrijeme između kraja zahtjeva IDE-a i početka odgovora jedinice u vozilu, ili između kraja potvrde IDE-a i početka sljedećeg odgovora jedinice u vozilu,
P3=vrijeme između kraja odgovora jedinice u vozilu i početka novog zahtjeva IDE-a ili između kraja odgovora jedinice u vozilu i početka potvrde IDE-a, ili između kraja zahtjeva IDE-a i početka novog zahtjeva IDE-a ako jedinica u vozilu ne odgovori,
P4=međubajtno vrijeme za zahtjev IDE-a,
P5=produžena vrijednost P3 za preuzimanje podataka s kartice.
Dopuštene vrijednosti vremenskih parametara prikazane su u sljedećoj tablici (prošireni niz vremenskih parametara KWP, upotrebljava se u slučaju fizičkog adresiranja za bržu komunikaciju).

Vremenski parametar	**Donja granična vrijednost (ms)**	**Gornja granična vrijednost (ms)**
P1	0	20
P2	20	1 000 ([1])
P3	10	5 000
P4	5	20
P5	10	20 minuta
([1]) Ako jedinica u vozilu pošalje negativan odgovor s kodom koji znači „zahtjev uredno primljen, čekanje na odgovor", ta se vrijednost proteže na istu gornju graničnu vrijednost P3.		

2.2.5 *Obrada pogrešaka*
Ako tokom razmjene poruka dođe do pogreške, shema toka poruke mijenja se zavisno o tome koja je oprema utvrdila pogrešku i o poruci koja uzrokuje pogrešku.
Na slikama 2. i 3. prikazani su postupci obrade pogrešaka za jedinicu u vozilu odnosno IDE.

2.2.5.1 Stadij početka komunikacije
DDP_020 Ako IDE utvrdi pogrešku u stadiju početka komunikacije u vezi s vremenom ili protokom bitova, čekat će u trajanju od najmanje P3 prije ponovnog izdavanja zahtjeva.
DDP_021 Ako jedinica u vozilu utvrdi pogrešku u slijedu koji dolazi iz IDE-a, ona neće poslati odgovor i čekat će u trajanju od najviše P3 drugu poruku sa zahtjevom za početak komunikacije.

2.2.5.2 Stadij komunikacije
Mogu se odrediti dva različita područja obrade pogrešaka:
1. **Jedinica u vozilu utvrđuje pogrešku prenosa iz IDE-a.**
DDP_022 Za svaku primljenu poruku jedinica u vozilu utvrđuje pogreške u vezi s vremenom, pogreške formata bajta (npr. kršenje početnog i zaustavnog bita) i greške pri upisu (pogrešan broj primljenih bajtova, pogrešan bajt kontrolnog zbira).
DDP_023 Ako jedinica u vozilu utvrdi jednu od prethodno navedenih pogrešaka, ona ne šalje nikakav odgovor i zanemaruje primljenu poruku.
DDP_024 Jedinica u vozilu može utvrditi ostale pogreške u formatu ili sadržaju primljene poruke (npr. poruka nije podržana) čak i ako poruka udovoljava zahtjevima dužine i kontrolnog zbira; u tom slučaju jedinica u vozilu odgovara IDE-u porukom s negativnim odgovorom u kojoj se navodi narav pogreške.



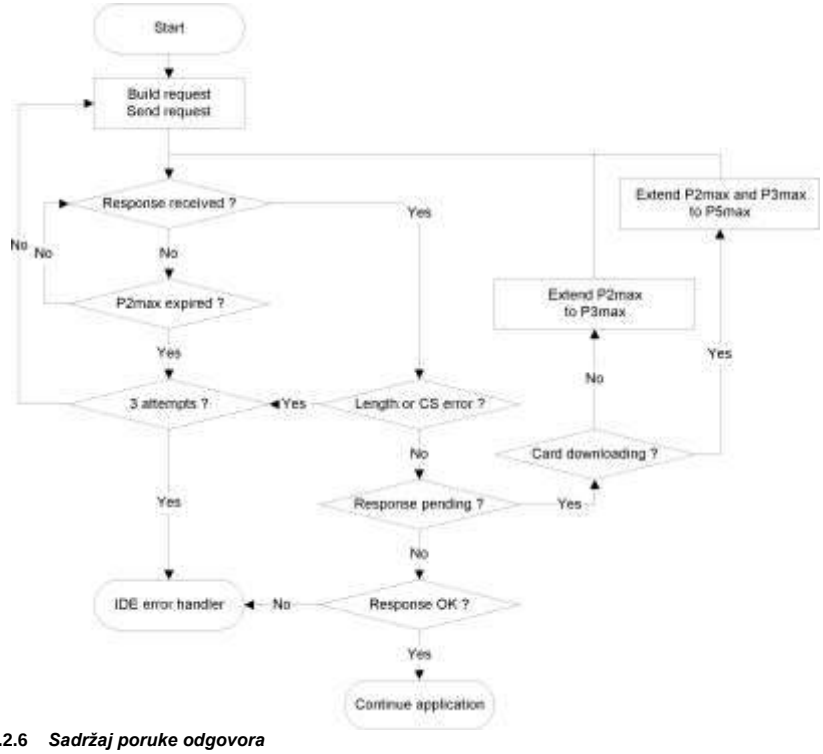
2. **IDE utvrđuje pogrešku prenosa iz jedinice u vozilu.**

DDP_025 Za svaku primljenu poruku IDE utvrđuje pogreške povezane s vremenom, pogreške formata bajta (npr. kršenje početnog i zaustavnog bita) i greške pri upisu (pogrešan broj primljenih bajtova, pogrešan bajt kontrolnog zbira).

DDP_026 IDE utvrđuje pogreške u slijedu, npr. neispravan korak povećanja brojača dijelova poruke za sljedeće primljene poruke.

DDP_027 Ako IDE utvrdi pogrešku ili nema odgovora iz jedinice u vozilu u trajanju od najviše P2, ponovo će poslati poruku sa zahtjevom za najviše tri prenosa ukupno. Za potrebe utvrđivanja te pogreške, potvrda dijela poruke smatrat će se zahtjevom upućenim jedinici u vozilu.

DDP_028 IDE mora čekati u trajanju od najmanje P3 prije početka svakog prenosa; period čekanja mjeri se od posljednjeg izračunanog javljanja zaustavnog bita nakon otkrivanja pogreške.



2.2.6 ***Sadržaj poruke odgovora***

U ovom se stavu navodi sadržaj podatkovnih polja različitih poruka s pozitivnim odgovorom.

Podatkovni elementi definisani su u rječniku podataka u Dodatku 1.

Napomena: Za preuzimanja podataka druge generacije, svaki podatkovni element gornje razine predstavlja se nizom zapisa (eng. *record array*), čak i ako sadrži samo jedan zapis. Niz zapisa počinje zaglavljem; to zaglavlje sadrži vrstu, veličinu i broj zapisa. Nizovi zapisa navode se kao „…niz zapisa" (sa zaglavljem) u tablicama u nastavu.

2.2.6.1 Pozitivan odgovor za prenos pregleda podataka

DDP_029 Podatkovno polje poruke „pozitivnog odgovora za prenos pregleda podataka" pruža sljedeće podatke sljedećim redom prema SID 76 Hex, TREP 01 ili 21 Hex te odgovarajućoj podjeli na dijelove i brojanju dijelova poruke:

Struktura podataka prve generacije (TREP 01 Hex)

Podatkovni element		Komentar
MemberStateCertificate		Sigurnosni certifikati jedinice u vozilu
VehicleIdentificationNumber VehicleRegistrationIdentification		Identifikacija vozila
CurrentDateTime		Trenutni datum i vrijeme jedinice u vozilu
VuDownloadablePeriod		Period u kojem je moguće preuzimati podatke
CardSlotsStatus		Vrsta kartica umetnutih u jedinicu u vozilu
VuDownloadActivityData		Prethodno preuzimanje podataka iz jedinice u vozilu
VuCompanyLocksData		Sve blokade preduzeće koje su arhivirane. Ako je odjeljak prazan, šalje se samo noOfLocks = 0.
VuControlActivityData		Svi kontrolni zapisi koji su arhivirani u jedinici u vozilu. Ako je odjeljak prazan, šalje se samo noOfControls = 0.
Signature		RSA potpis svih podataka (osim certifikata) od VehicleIdentificationNumber do posljednjeg bajta zadnjeg VuControlActivityData.

Struktura podataka druge generacije (TREP 21 Hex)

Podatkovni element		Komentar
MemberStateCertificateRecordArray		Certifikat države članice
VUCertificateRecordArray		Certifikat jedinice u vozilu
VehicleIdentificationNumberRecordArray		Identifikacija vozila
VehicleRegistrationNumberRecordArray		Registracijski broj vozila

CurrentDateTimeRecordArray		Trenutni datum i vrijeme jedinice u vozilu
VuDownloadablePeriodRecordArray		Period u kojem je moguće preuzimati podatke
CardSlotsStatusRecordArray		Vrsta kartica umetnutih u jedinicu u vozilu
VuDownloadActivityDataRecordArray		Prethodno preuzimanje podataka iz jedinice u vozilu
VuCompanyLocksRecordArray		Sve blokade preduzeće koje su arhivirane. Ako je odjeljak prazan, šalje se zaglavlje niza zapisa noOfRecords = 0.
VuControlActivityRecordArray		Svi kontrolni zapisi koji su arhivirani u jedinici u vozilu. Ako je odjeljak prazan, šalje se zaglavlje niza zapisa noOfRecords = 0.
SignatureRecordArray		ECC potpis svih prethodnih podataka osim certifikata.

2.2.6.2 Pozitivan odgovor za prenos podataka o aktivnostima

DDP_030 Podatkovno polje poruke „pozitivnog odgovora za prenos podataka o aktivnostima" pruža sljedeće podatke sljedećim redom prema SID 76 Hex, TREP 02 ili 22 Hex te odgovarajućoj podjeli na dijelove i brojanju dijelova poruke:

Struktura podataka prve generacije (TREP 02 Hex)

Podatkovni element		Komentar
TimeReal		Datum dana preuzimanja podataka.
OdometerValueMidnight		Stanje brojača kilometara na kraju dana preuzimanja podataka.
VuCardIWData		Podaci o broju ciklusa umetanja i izvlačenja kartice. — Ako je odjeljak prazan, šalje se samo noOfVuCardIWRecords = 0. — Kada se zapis VuCardIWRecord proteže preko 00:00 (umetanje kartice prethodnog dana) ili preko 24:00 (izvlačenje kartice sljedećeg dana), pojavljuje se u cijelosti u oba navedena dana.
VuActivityDailyData		Stanje otvora u 00:00 i promjene aktivnosti zabilježene na dan preuzimanja podataka.
VuPlaceDailyWorkPeriodData		Podaci koji se odnose na mjesta zabilježeni na dan preuzimanja podataka. Ako je odjeljak prazan, šalje se samo noOfPlaceRecords = 0.
VuSpecificConditionData		Podaci o posebnim stanjima zabilježeni na dan preuzimanja podataka. Ako je odjeljak prazan, šalje se samo noOfSpecificConditionRecords = 0.
Signature		RSA potpis svih podataka od TimeReal do posljednjeg bajta zadnjeg zapisa o posebnom stanju.

Struktura podataka druge generacije (TREP 22 Hex)

Podatkovni element		Komentar
DateOfDayDownloadedRecordArray		Datum dana preuzimanja podataka.
OdometerValueMidnightRecordArray		Stanje brojača kilometara na kraju dana preuzimanja podataka.
VuCardIWRecordArray		Podaci o broju ciklusa umetanja i izvlačenja kartice. — Ako je odjeljak prazan, šalje se zaglavlje niza zapisa noOfRecords = 0. — Kada se zapis VuCardIWRecord proteže preko 00:00 (umetanje kartice prethodnog dana) ili preko 24:00 (izvlačenje kartice sljedećeg dana), pojavljuje se u cijelosti u oba navedena dana.
VuActivityDailyRecordArray		Stanje otvora u 00:00 i promjene aktivnosti zabilježene na dan preuzimanja podataka.
VuPlaceDailyWorkPeriodRecordArray		Podaci koji se odnose na mjesta zabilježeni na dan preuzimanja podataka. Ako je odjeljak prazan, šalje se zaglavlje niza zapisa noOfRecords = 0.
VuGNSSADRecordArray		Položaji vozila GNSS-a ako akumulisano vrijeme vožnje vozila dostigne višekratnik tri sata. Ako je odjeljak prazan, šalje se zaglavlje niza zapisa noOfRecords = 0.
VuSpecificConditionRecordArray	Podaci o posebnim stanjima zabilježeni na dan preuzimanja podataka. Ako je odjeljak prazan, šalje se zaglavlje niza zapisa noOfRecords = 0.	
SignatureRecordArray	ECC potpis svih prethodnih podataka.	

2.2.6.3 Pozitivan odgovor za prenos podataka o događajima i pogreškama

DDP_031 Podatkovno polje poruke „pozitivnog odgovora za prenos podataka o događajima i pogreškama" pruža sljedeće podatke sljedećim redom prema SID 76h Hex, TREP 03 ili 23 Hex te odgovarajućoj podjeli na dijelove i brojanju dijelova poruke:

Struktura podataka prve generacije (TREP 03 Hex)

Podatkovni element		Komentar
VuFaultData		Sve pogreške koje su arhivirane ili još uvijek traju u jedinici u vozilu. Ako je odjeljak prazan, šalje se samo noOfVuFaults = 0.
VuEventData		Svi događaji (osim prekoračenja brzine) koji su arhivirani ili još uvijek traju u jedinici u vozilu. Ako je odjeljak prazan, šalje se samo noOfVuEvents = 0.
VuOverSpeedingControlData		Podaci koji se odnose na posljednju kontrolu prekoračenja brzine (standardna

		vrijednost ako nema podataka).
VuOverSpeedingEventData		Svi događaji u pogledu prekoračenja brzine koji su arhivirani u jedinici u vozilu. Ako je odjeljak prazan, šalje se samo noOfVuOverSpeedingEvents = 0.
VuTimeAdjustmentData		Svi događaji o prilagodbi vremena koji su arhivirani u jedinici u vozilu (izvan okvira pune kalibracije). Ako je odjeljak prazan, šalje se samo noOfVuTimeAdjRecords = 0.
Signature		RSA potpis svih podataka od noOfVuFaults do posljednjeg bajta zadnjeg zapisa o prilagodbi vremena.

Struktura podataka druge generacije (TREP 23 Hex)

Podatkovni element		Komentar
VuFaultRecordArray		Sve pogreške koje su arhivirane ili još uvijek traju u jedinici u vozilu. Ako je odjeljak prazan, šalje se zaglavlje niza zapisa noOfRecords = 0.
VuEventRecordArray		Svi događaji (osim prekoračenja brzine) koji su arhivirani ili još uvijek traju u jedinici u vozilu. Ako je odjeljak prazan, šalje se zaglavlje niza zapisa noOfRecords = 0.
VuOverSpeedingControlDataRecordArray		Podaci koji se odnose na posljednju kontrolu prekoračenja brzine (standardna vrijednost ako nema podataka).
VuOverSpeedingEventRecordArray		Svi događaji u pogledu prekoračenja brzine koji su arhivirani u jedinici u vozilu. Ako je odjeljak prazan, šalje se zaglavlje niza zapisa noOfRecords = 0.
VuTimeAdjustmentRecordArray		Svi događaji o prilagodbi vremena koji su arhivirani u jedinici u vozilu (izvan okvira pune kalibracije). Ako je odjeljak prazan, šalje se zaglavlje niza zapisa noOfRecords = 0.
SignatureRecordArray	ECC potpis svih prethodnih podataka.	

2.2.6.4 Pozitivan odgovor za prenos detaljnih podataka o brzini

DDP_032 Podatkovno polje poruke „pozitivan odgovor za prenos detaljnih podataka o brzini" pruža sljedeće podatke sljedećim redom prema SID 76 Hex, TREP 04 ili 24 Hex te odgovarajućoj podjeli na dijelove i brojanju dijelova poruke:

Struktura podataka prve generacije (TREP 04)

Podatkovni element		Komentar
VuDetailedSpeedData		Svi detaljni podaci o brzini koji su arhivirani u jedinici u vozilu (jedan blok brzine u minuti tokom koje se vozilo kretalo). 60 vrijednosti brzine u minuti (jedna u sekundi).
Signature		RSA potpis svih podataka od noOfSpeedBlocks do posljednjeg bajta zadnjeg bloka brzine.

Struktura podataka druge generacije (TREP 24)

Podatkovni element		Komentar
VuDetailedSpeedBlockRecordArray		Svi detaljni podaci o brzini koji su arhivirani u jedinici u vozilu (jedan blok brzine u minuti tokom koje se vozilo kretalo). 60 vrijednosti brzine u minuti (jedna u sekundi).
SignatureRecordArray		ECC potpis svih prethodnih podataka.

2.2.6.5 Pozitivan odgovor za prenos tehničkih podataka

DDP_033 Podatkovno polje „pozitivnog odgovora za prenos tehničkih podataka" pruža sljedeće podatke sljedećim redom prema SID 76 Hex, TREP 05 ili 25 Hex te odgovarajućoj podjeli na dijelove i brojanju dijelova poruke:

Struktura podataka prve generacije (TREP 05)

Podatkovni element		Komentar
VuIdentification		
SensorPaired		
VuCalibrationData		Svi zapisi o kalibraciji koji su arhivirani u jedinici u vozilu.
Signature		RSA potpis svih podataka od vuManufacturerName do posljednjeg bajta zadnjeg VuCalibrationRecord.

Struktura podataka druge generacije (TREP 25)

Podatkovni element		Komentar
VuIdentificationRecordArray		
VuSensorPairedRecordArray		Sva uparivanja država članica pohranjena u jedinici u vozilu.
VuSensorExternalGNSSCoupledRecordArray		Sva spajanja vanjskih uređaja GNSS-a pohranjena u jedinici u vozilu.
VuCalibrationRecordArray		Svi zapisi o kalibraciji koji su arhivirani u jedinici u vozilu.
VuCardRecordArray		Svi podaci o umetanju kartice koji su arhivirani u jedinici u vozilu.
VuITSConsentRecordArray		
VuPowerSupplyInterruptionRecordArray		
SignatureRecordArray		ECC potpis svih prethodnih podataka.

2.3. Spremanje datoteke ESM

DDP_034 Ako je proces preuzimanja podataka obuhvatio i prenos podataka iz jedinice u vozilu, IDE unutar jedne fizičke datoteke arhivira sve podatke primljene iz jedinice u vozilu tokom procesa preuzimanja podataka u okviru poruka s pozitivnim odgovorom na zahtjev za prenos podataka. Arhivirani podaci ne sadržiju zaglavlja poruka, brojače dijelova poruke, prazne dijelove poruka i kontrolne zbireve, ali obuhvaćaju SID i TREP (prvog dijela poruke samo ako ima više dijelova poruka).

3. PROTOKOL PREUZIMANJA PODATAKA S TAHOGRAFSKE KARTICE

3.1. Područje primjene

U ovom se stavu opisuje direktno preuzimanje podataka s tahografske kartice na IDE. IDE nije dio sigurnog okruženja; stoga se ne sprovodi nikakva autentifikacija između kartice i IDE-a.

3.2. Definicije

Proces preuzimanja podataka:svaki put kad se obavlja preuzimanje podataka s ICC-a. Proces obuhvaća cjelokupan postupak od povraćaja u početno stanje ICC-a od strane IFD-a do deaktivacije ICC-a (izvlačenje kartice ili sljedeći povraćaj u početno stanje).

Potpisana podatkovna datoteka:datoteka iz ICC-a. Datoteka se prenosi na IFD u običnom tekstu. Na ICC-u datoteka se raspršuje (hash) i potpisuje, a potpis se prenosi na IFD.

3.3. Preuzimanje podataka s kartice

▼M1

DDP_035 Preuzimanje podataka s tahografske kartice obuhvaća sljedeće korake:

— preuzimanje zajedničkih podataka kartice u EF-ovima [illegible] i [illegible]. Ti podaci nisu obvezni i nisu zaštićeni digitalnim potpisom.

— (za prvu i drugu generaciju tahografskih kartica) preuzimanje EF-ova unutar [illegible] DF:

— preuzimanje EF-ova Card_Certificate i CA_Certificate. Ovi podaci nisu zaštićeni digitalnim potpisom.

— Obvezno je preuzeti ove datoteke u svakom procesu preuzimanja podataka.

— preuzimanje EF-ova podataka drugih aplikacija (unutar [illegible] DF) osim EF-a [illegible] Ti su podaci zaštićeni digitalnim potpisom, u skladu s Dodatkom 11. „Zajednički sigurnosni mehanizmi”, dijelom A.

— u svakom je procesu preuzimanja podataka obvezno preuzeti barem EF-ove Application_Identification i Identification.

— prilikom preuzimanja podataka s kartice vozača isto je tako obvezno preuzeti sljedeće EF-ove:

— Driver_Activity_Data,
— Vehicles_Used,
— Places,
— Events_Data, — Control_Activity_Data,
— Faults_Data, — Specific_Conditions,

— (samo za drugu generaciju tahografskih kartica) osim kad preuzimanje podataka s kartice vozača umetnute u jedinicu u vozilu tokom kontrole vozača obavlja nadležno tijelo za kontrolu izvan EU-a, korištenjem kontrolne kartice prve generacije, preuzimanje EF-ova unutar Tachograph_G2 DF:

— preuzimanje EF-ova CardSignCertificate, CA_Certificate i Link_Certificate (ako ih ima). Ovi podaci nisu zaštićeni digitalnim potpisom.

— Obvezno je preuzeti ove datoteke u svakom procesu preuzimanja podataka.

— preuzimanje EF-ova podataka drugih aplikacija (unutar Tachograph_G2 DF) osim EF-a Card_Download. Ti su podaci zaštićeni digitalnim potpisom, u skladu s Dodatkom 11. „Zajednički sigurnosni mehanizmi”, dijelom B.

— u svakom je procesu preuzimanja podataka obvezno preuzeti barem EF-ove Application_Identification i Identification.

— prilikom preuzimanja podataka s kartice vozača isto je tako obvezno preuzeti sljedeće EF-ove:

— Events_Data,
— Faults_Data,
— Driver_Activity_Data,
— Vehicles_Used,
— Places,
— Control_Activity_Data,
— Specific_Conditions,
— Vehicleunits_Used,
— GNSS Places,

— prilikom preuzimanja podataka s kartice vozača, ažuriranje datuma LastCardDownload u EF-u Card_Download,u DF-u Tachograph i, ako je primjenjivo, DF-u Tachograph_G2.

— prilikom preuzimanja podataka s kartice radionice, povraćaj brojača kalibracija u početno stanje u EF-u Card_Download u DF-u Tachograph i, ako je primjenjivo, DF-u Tachograph_G2.

— prilikom preuzimanja podataka s kartice radionice ne preuzimaju se Sensor_Installation_Data u DF-u Tachograph i, ako je primjenjivo, DF-u Tachograph_G2.

3.3.1 *Slijed inicijalizacije*

DDP_036 IDE započinje sljedeći slijed:

Kartica	Smjer	IDE/IFD	Značenje/napomene
	⇦	Povraćaj hardvera u početno stanje	
ATR	⇨		

Za prelaz na višu brzinu prenosa podataka može se upotrijebiti PPS ako ICC to podržava.

3.3.2 *Slijed za nepotpisane podatkovne datoteke*

DDP_037 Slijed za preuzimanje EF-ova ICC, IC, Card_Certificate (ili CardSignCertificate za DF Tachograph_G2), CA_Certificate i Link_Certificate (samo za DF Tachograph_G2) je sljedeći:

Kartica	Smjer	IDE/IFD	Značenje/napomene
	⇦	**Odabir datoteke (*Select File*)**	Odabir s pomoću identifikatora datoteke
OK	⇨		
	⇦	**Čitanje datoteke (*Read Binary*)**	Ako datoteka sadrži više podataka nego što je veličina međumemorije čitača ili kartice, naredba se ponavlja dok se ne pročita cijela datoteka.
File Data OK	⇨	Arhiviranje podataka na ESM	prema **3.4.** Format za arhiviranje podataka

Napomena 1.: prije odabira EF-a Card_Certificate (ili CardSignCertificate), mora se odabrati tahografska aplikacija (odabir putem AID-a).
Napomena 2.: odabir i čitanje datoteke isto se tako može obaviti u jednom koraku naredbom READ BINARY (čitanje datoteke) s kratkim identifikatorom EF-a.

3.3.3 *Slijed za potpisane podatkovne datoteke*

DDP_038 Za svaku od sljedećih datoteka koje treba preuzeti s njihovim potpisom upotrebljava se sljedeći slijed:

Kartica	Smjer	IDE/IFD	Značenje/napomene
	⇦	**Odabir datoteke (Select File)**	
OK	⇨		
	⇦	**Raspršivanje datoteke (Perform Hash of File)**	— Izračunava vrijednost raspršivanja sadržaja podataka odabrane datoteke upotrebom propisanog algoritma raspršivanja u skladu s Dodatkom 11., dijelom A ili B. Ova naredba nije ISO-naredba.
Izračun vrijednost raspršivanja datoteke i privremeno arhiviranje vrijednosti raspršivanja			
OK	⇨		
	⇦	**Čitanje datoteke (Read Binary)**	Ako datoteka sadrži više podataka nego što međumemorija čitača ili kartice može primiti, naredba se mora ponoviti dok se ne pročita cijela datoteka.
Podaci o datoteci (File Data) OK	⇨	Arhiviranje primljenih podataka na ESM	u skladu s **3.4**. Format za arhiviranje podataka
	⇦	**PSO: Compute Digital Signature**	
Zaštitna radnja „izračuna digitalnog potpisa" upotrebom privremeno arhivirane vrijednosti raspršivanja (Hash)			
Potpis (Signature) OK	⇨	Podaci se pridodaju podacima koji su prethodno arhivirani na ESM	u skladu s **3.4**. Format za arhiviranje podataka

Napomena: odabir i čitanje datoteke isto se tako može obaviti u jednom koraku naredbom READ BINARY (čitanje datoteke) s kratkim identifikatorom EF-a. U tom se slučaju EF može odabrati i pročitati prije primjene naredbe PERFORM HASH OF FILE (raspršivanje datoteke).

3.3.4 *Slijed povraćaja brojača kalibracija u početno stanje*

DDP_039 Slijed povraćaja u početno stanje brojača NoOfCalibrationsSinceDownload u EF-u [illegible] na kartici radionice je sljedeći:

Kartica	Smjer	IDE/IFD	Značenje/napomene
	⇦	**Odabir datoteke (*Select File*)** EF Card_Download	Odabir s pomoću identifikatora datoteke
OK	⇨		
	⇦	**Ažuriranje datoteke (*Update Binary*)** NoOfCalibrationsSinceDownload = '00 00'	
Povraćaj u početno stanje broja preuzimanja podataka s kartice			
OK	⇨		

Napomena: odabir i ažuriranje datoteke isto se tako može obaviti u jednom koraku naredbom READ BINARY (čitanje datoteke) s kratkim identifikatorom EF-a.

3.4. Format za arhiviranje podataka

3.4.1 *Uvod*

DDP_040 Preuzeti podaci arhiviraju se u skladu sa sljedećim uslovima:
— podaci se arhiviraju transparentno. To znači da se poredak bajtova kao i poredak bitova unutar bajtova koji se prenose s kartice mora očuvati tokom arhiviranja,
— sve datoteke s kartice koje su preuzete tokom procesa preuzimanja podataka arhiviraju se u jednoj datoteci na ESM.

3.4.2 *Format datoteke*

DDP_041 Format datoteke lanac je više TLV objekata.
DDP_042 Oznaka za EF je FID plus dodatak „00".

DDP_043 Oznaka za potpis EF-a je FID datoteke plus dodatak „01”.
DDP_044 Dužina je dvobajtna vrijednost. Vrijednost određuje broj bajtova u polju vrijednosti. Vrijednost „FF FF” u polju dužine rezervisana je za buduću upotrebu.
DDP_045 Ako datoteka nije preuzeta, ništa što se odnosi na datoteku ne smije se arhivirati (nikakva oznaka i nikakva nulta dužina).
DDP_046 Potpis se arhivira kao sljedeći TLV objekt direktno nakon TLV objekta koji sadrži podatke datoteke.

Definicija	Značenje	Dužina
FID (2 bajta) || „00”	Oznaka za EF (FID) u [illegible] ili za zajedničke podatke na kartici	3 bajta
FID (2 bajta) || „01”	Oznaka za potpis EF-a (FID) u DF-u [illegible]	3 bajta
FID (2 bajta) || „02”	Oznaka za EF (FID) u DF-u [illegible]	3 bajta
FID (2 bajta) || „03”	Oznaka za potpis EF-a (FID) u DF-u [illegible]	3 bajta
xx xx	Dužina polja vrijednosti	2 bajta

Primjer podataka u datoteci preuzetoj na ESM

Oznaka	Dužina	Vrijednost
[illegible]	[illegible]	— Podaci EF-a ICC
[illegible]	[illegible]	- Podaci EF-a Card_Certificate
		— ...
[illegible]	[illegible]	Podaci EF-a [illegible] (u DF-u [illegible])
[illegible]	[illegible]	Potpis EF-a [illegible] (u DF-u [illegible])
[illegible]	[illegible]	Podaci EF-a [illegible] u DF-u [illegible]
[illegible]	[illegible]	Potpis EF-a [illegible] u DF-u [illegible]

4. PREUZIMANJE PODATAKA S TAHOGRAFSKE KARTICE PREKO JEDINICE U VOZILU

DDP_047 Jedinica u vozilu mora omogućiti preuzimanje sadržaja s kartice vozača umetnute u priključeni IDE.
DDP_048 IDE jedinici u vozilu šalje poruku „zahtjev za prenos podataka s kartice” za pokretanje tog načina rada (vidjeti 2.2.2.9).
DDP_049 Prva generacija kartica vozača: podaci se preuzimaju korištenjem protokola preuzimanja podataka prve generacije, a preuzeti podaci imaju isti format kao i podaci preuzeti s jedinice u vozilu prve generacije.
Druga generacija kartica vozača: jedinica u vozilu potom preuzima sve podatke s kartice, datoteku po datoteku, u skladu s protokolom preuzimanja s kartice definisanim u stavu 3 i dostavlja sve podatke primljene s kartice na IDE u odgovarajućem formatu datoteke TLV (vidjeti 3.4.2) i sažete unutar poruke ‚pozitivan odgovor za prenos podataka’.
DDP_050 IDE uzima podatke s kartice iz poruke „pozitivan odgovor za prenos podataka” (bez svih zaglavlja, SID-ova, TREP-ova, brojača dijelova poruke i kontrolnih zbireva) i arhivira ih u jednu fizičku datoteku kako je opisano u stavu 2.3.
DDP_051 Jedinica u vozilu nakon toga, prema potrebi, ažurira datoteku Control_Activity_Data ili [illegible] s kartice vozača.

Dodatak 8

PROTOKOL KALIBRACIJE

SADRŽAJ

1. UVOD

U ovom se Dodatku opisuje način razmjene podataka između jedinice u vozilu i ispitnog uređaja putem K-linije koja čini sastavni dio sučelja za kalibraciju opisanog u Dodatku 6. Isto se tako opisuje upravljanje linijom ulaznih/izlaznih signala na priključku za kalibraciju.

Uspostavljanje komunikacije putem K-linije opisano je u odjeljku 4. „Komunikacijske usluge”.

U ovom se Dodatku upotrebljava pojam dijagnostičkih „razmjena podataka” (eng. *session*) za određivanje obima upravljanja putem K-linije u različitim uslovima. Standardna je razmjena podataka „StandardDiagnosticSession” u kojoj se svi podaci mogu čitati s jedinice u vozilu, ali niti jedan podatak nije moguće upisati u jedinicu u vozilu.

Odabir dijagnostičke razmjene podataka opisan je u odjeljku 5. „Usluge upravljanja”.

Ovaj Dodatak smatra se relevantnim za obje generacije jedinica u vozilu i kartica radionica u skladu sa zahtjevima za interoperabilnost utvrđenima u ovoj Uredbi.

CPR_001 „ECUProgrammingSession” omogućava unos podataka u jedinicu u vozilu. Osim toga, u slučaju unosa podataka za kalibraciju, jedinica u vozilu mora biti u načinu rada KALIBRACIJA.

Prenos podataka putem K-linije opisan je u odjeljku 6. „Usluge prenosa podataka”. Formati prenesenih podataka detaljno su izloženi u odjeljku 8. „Formati dataRecords”.

CPR_002 „ECUAdjustmentSession” omogućava odabir U/I (ulazno/izlaznog) načina rada linije kalibracije U/I signala putem sučelja K-linije. Upravljanje linijom kalibracije U/I signala opisano je u odjeljku 7. „Upravljanje ispitnim impulsima – funkcionalna jedinica za upravljanje ulazom/izlazom”.

CPR_003 U ovom se dokumentu adresa ispitnog uređaja navodi kao ‘tt’. Iako mogu postojati preferirane adrese ispitnih uređaja, jedinica u vozilu ispravno odgovara na svaku adresu ispitnog uređaja. Fizička je adresa jedinice u vozilu 0xEE.

2. IZRAZI, DEFINICIJE I REFERENTNI DOKUMENTI

Protokoli, poruke i kodovi pogrešaka u načelu se temelje na nacrtu norme ISO 14229-1 (*Road vehicles – Diagnostic systems – Part 1*: *Diagnostic services*, verzija 6. od 22. februar 2001.).
Za identifikatore usluge, zahtjeve za usluge i odgovore te za standardne parametre upotrebljavaju se bajtno kodiranje i heksadecimalne vrijednosti.
Izraz „ispitni uređaj" odnosi se na uređaj koji se upotrebljava za unos podataka za programiranje/kalibraciju u jedinicu u vozilu (VU).
Izrazi „korisnik" i „poslužitelj" odnose se na ispitni uređaj odnosno jedinicu u vozilu.
Izraz ECU označava „elektroničku upravljačku jedinicu" i odnosi se na jedinicu u vozilu.
Referentni dokumenti:
ISO 14230-2: Road Vehicles -Diagnostic Systems — Keyword Protocol 2000- Part 2: Data Link Layer.
Prvo izdatje, 1999.

3. PREGLED USLUGA

3.1. Raspoložive usluge

U sljedećoj je tablici naveden pregled usluga koje će biti raspoložive u tahografu i koje su definisane u ovom dokumentu.
CPR_004 U tablici su prikazane usluge koje su raspoložive u aktiviranoj dijagnostičkoj razmjeni podataka.
— **U prvom koloni** navode se usluge koje su raspoložive,
— **u drugom koloni** navodi se broj odjeljka u ovom Dodatku u kojem je usluga detaljnije definisana,
— u **trećem koloni** pridružene su vrijednosti identifikatora usluge (SId) za poruke zahtjeva,
— **u četvrtom koloni** navode se usluge **„StandardDiagnosticSession" (SD)** koje se moraju primjenjivati u svakoj jedinici u vozilu,
— u **petom koloni** navode se usluge **„ECUAdjustmentSession" (ECUAS)** koje se moraju primjenjivati za omogućivanje upravljanja linijom U/I signala u priključku za kalibraciju na prednjoj stranici jedinice u vozilu,
— u **šestom koloni** navode se usluge **„ECUProgrammingSession" (ECUPS)** koje se moraju primjenjivati za omogućivanje programiranja parametara u jedinici u vozilu.

Tablica 1.
Sažetak vrijednosti identifikatora usluge

			Dijagnostička razmjena podataka		
Naziv dijagnostičke usluge	**Broj odjeljka**	**Zaht. vrijednost SId**	**SD**	**ECUAS**	**ECUPS**
StartCommunication	4.1	81	■	■	■
StopCommunication	4.2	82	■		
TesterPresent	4.3	3E	■	■	■
StartDiagnosticSession	5.1	10	■	■	■
SecurityAccess	5.2	27	■	■	■
ReadDataByIdentifier	6.1	22	■	■	■
WriteDataByIdentifier	6.2	2E			■
InputOutputControlByIdentifier	7.1	2F		■	
■ Ovaj simbol označava da je usluga obavezna u ovoj dijagnostičkoj razmjeni podataka. Izostanak simbola označava da ta usluga nije dopuštena u ovoj dijagnostičkoj razmjeni podataka.					

3.2. Kodovi odgovora

Za svaku su uslugu definisani kodovi odgovora.

4. KOMUNIKACIJSKE USLUGE

Neke su usluge potrebne za uspostavljanje i održavanje komunikacije. One se ne javljaju na aplikacijskoj nivou. Raspoložive usluge opisane su u sljedećoj tablici:

Tablica 2.
Komunikacijske usluge

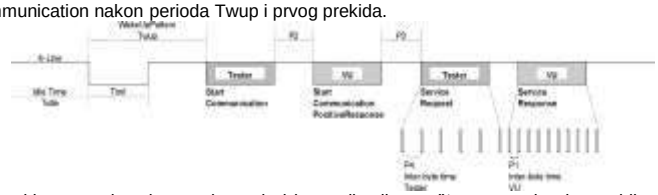
Naziv usluge	**Opis**
StartCommunication	Korisnik zahtijeva početak komunikacijske razmjene podataka s poslužiteljem (poslužiteljima).
StopCommunication	Korisnik zahtijeva prekid komunikacijske razmjene podataka koja je u toku.
TesterPresent	Korisnik ukazuje poslužitelju da je još uvijek prisutan.

CPR_005 Usluga StartCommunication upotrebljava se za početak komunikacije. Da bi se obavila neka usluga, komunikacija se mora pokrenuti, a komunikacijski parametri moraju biti primjereni željenom načinu rada.

4.1. Usluga StartCommunication

CPR_006 Po prijemu primitiva indikacije StartCommunication, jedinica u vozilu provjerava može li se zahtijevana komunikacijska veza pokrenuti u trenutnim uslovima. Važeći uslovi za početak komunikacijske veze opisani su u normi ISO 14230-2.
CPR_007 Potom jedinica u vozilu obavlja sve potrebne radnje za pokretanje (inicijalizaciju) komunikacijske veze i šalje primitiv odgovora StartCommunication s odabranim parametrima pozitivnog odgovora.
CPR_008 Ako jedinica u vozilu koja je već pokrenuta (i započela je dijagnostičku razmjenu podataka) primi novi zahtjev StartCommunication (npr. zbog ispravljanja pogreške u ispitnom uređaju), zahtjev se prihvaća i jedinica u vozilu se ponovno pokreće.
CPR_009 Ako se iz nekog razloga komunikacijska veza ne može pokrenuti, jedinica u vozilu nastavlja raditi kao i neposredno prije pokušaja pokretanja komunikacijske veze.
CPR_010 Poruka sa zahtjevom StartCommunication mora biti fizički naslovljena.
CPR_011 Pokretanje jedinice u vozilu za usluge obavlja se metodom „brzog pokretanja":
— prije svake aktivnosti postoji period neaktivnosti sabirnice,
— ispitni uređaj potom šalje obrazac za pokretanje,
— svi podaci koji su potrebni za uspostavljanje komunikacije sadržani su u odgovoru jedinice u vozilu.

CPR_012 Po završetku pokretanja:
— svi komunikacijski parametri postavljaju se na vrijednosti utvrđene u tablici 4. prema bajtovima ključa,
— jedinica u vozilu čeka na prvi zahtjev ispitnog uređaja,
— jedinica u vozilu u standardnom je dijagnostičkom načinu rada, tj. StandardDiagnosticSession,
— linija kalibracije U/I signala je u standardnom odnosno isključenom stanju.
CPR_014 Brzina prenosa podataka na K-liniji iznosi 10 400 bauda.
CPR_016 Brzo pokretanje započinje kada ispitni uređaj prenese obrazac pobude (Wup) na K-liniji. Obrazac započinje nakon vremena mirovanja na K-liniji u vremenu smanjene aktivnosti Tinil. Ispitni uređaj prenosi prvi bit usluge StartCommunication nakon perioda Twup i prvog prekida.



CPR_017 Vremenski raspored za brzo pokretanje i komunikaciju uopšteno naveden je u tablicama u nastavu. Postoje različite mogućnosti za period mirovanja:
— prvi prenos nakon uključivanja, Tidle = 300 ms,
— nakon okončanja usluge StopCommunication, Tidle = P3 min.,
— nakon prekida komunikacije zbog isteka vremena P3 maks., Tidle = 0.

Tablica 3.

Vremenski raspored za brzo pokretanje

Parametar		**najmanja vrijednost**	**najveća vrijednost**
Tinil	25 ± 1 ms	24 ms	26 ms
Twup	50 ± 1 ms	49 ms	51 ms

Tablica 4.

Vremenski raspored komunikacije

Vremenski parametar	**Opis parametra**	**Donje granične vrijednosti [ms]**	**Gornje granične vrijednosti [ms]**
		min.	**maks.**
P1	Međubajtno vrijeme za odgovor jedinice u vozilu	0	20
P2	Vrijeme između zahtjeva ispitnog uređaja i odgovora jedinice u vozilu ili dvaju odgovora jedinice u vozilu	25	250
P3	Vrijeme između kraja odgovora jedinice u vozilu i početka novog zahtjeva ispitnog uređaja	55	5 000
P4	Međubajtno vrijeme za zahtjev ispitnog uređaja	5	20

CPR_018 Format poruka za brzo pokretanje prikazan je u sljedećim tablicama:

Tablica 5.

Poruka zahtjeva StartCommunication

Bajt #	**Naziv parametra**	**Heksadecimalna vrijednost**	**Mnemonik**
#1	Formatni bajt – fizičko adresiranje	81	FMT
#2	Bajt ciljne adrese	EE	TGT
#3	Bajt izvorne adrese	tt	SRC
#4	**Identifikator usluge zahtjeva StartCommunication**	**81**	**SCR**
#5	Kontrolni zbir	00-FF	CS

Tablica 6.

Poruka StartCommunication s pozitivnim odgovorom

Bajt #	**Naziv parametra**	**Heksadecimalna vrijednost**	**Mnemonik**
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	tt	TGT
#3	Bajt izvorne adrese	EE	SRC
#4	Bajt za dodatnu dužinu	03	LEN
#5	**Identifikator usluge StartCommunication s pozitivnim odgovorom**	**C1**	**SCRPR**
#6	Bajt ključa 1	EA	KB1
#7	Bajt ključa 2	8F	KB2
#8	Kontrolni zbir	00-FF	CS

CPR_019 Nema negativnog odgovora na poruku zahtjeva StartCommunication; ako nema poruke s pozitivnim odgovorom za prenos, tada se jedinica u vozilu ne pokreće, ništa se ne prenosi i ona nastavlja s redovnim radom.

4.2. Usluga StopCommunication

4.2.1 *Opis poruka*

Svrha je ove usluge komunikacijske razine prekid komunikacijske razmjene podataka.
CPR_020 Po prijemu primitiva indikacije StopCommunication, jedinica u vozilu provjerava omogućuju li prevladavajući uslovi prekid ove komunikacije. U tom slučaju jedinica u vozilu obavlja sve radnje potrebne za okončanje ove komunikacije.

CPR_021 Ako je moguće prekinuti komunikaciju, jedinica u vozilu izdaje primitiv odgovora StopCommunication s odabranim parametrima pozitivnog odgovora prije prekida komunikacije.
CPR_022 Ako se komunikacija iz nekog razloga ne može prekinuti, jedinica u vozilu izdaje primitiv odgovora StopCommunication s odabranim parametrom negativnog odgovora.
CPR_023 Ako jedinica u vozilu utvrdi istek vremena P3 maks., komunikacija se prekida bez izdavanja primitiva bilo kakvog odgovora.

4.2.2 *Format poruka*

CPR_024 Formati poruke za primitive StopCommunication prikazani su u sljedećim tablicama:

Tablica 7.

Poruka zahtjeva StopCommunication

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	EE	TGT
#3	Bajt izvorne adrese	tt	SRC
#4	Bajt za dodatnu dužinu	01	LEN
#5	**StopCommunication Request Service Id**	**82**	**SPR**
#6	Kontrolni zbir	00-FF	CS

Tablica 8.

Poruka StopCommunication s pozitivnim odgovorom

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	tt	TGT
#3	Bajt izvorne adrese	EE	SRC
#4	Bajt za dodatnu dužinu	01	LEN
#5	**StopCommunication Positive Response Service Id**	**C2**	**SPRPR**
#6	Kontrolni zbir	00-FF	CS

Tablica 9.

Poruka StopCommunication s negativnim odgovorom

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	tt	TGT
#3	Bajt izvorne adrese	EE	SRC
#4	Bajt za dodatnu dužinu	03	LEN
#5	**negative Response Service Id**	**7F**	**NR**
#6	Identifikator usluge zahtjeva StopCommunication	82	SPR
#7	responseCode = generalReject	10	RC_GR
#8	Kontrolni zbir	00-FF	CS

4.2.3 *Opis parametara*

Ova usluga ne zahtijeva opis parametara.

4.3. Usluga TesterPresent

4.3.1 *Opis poruka*

Ispitni uređaj upotrebljava uslugu TesterPresent kako bi poslužitelju ukazao da je još uvijek prisutan, kako bi se spriječilo automatsko vraćanje poslužitelja u redovan rad i mogući prekid komunikacije. Ova usluga, koja se povremeno šalje, održava dijagnostičku razmjenu podataka / komunikaciju aktivnom ponovnim postavljanjem sata P3 prilikom svakog primitka zahtjeva za ovu uslugu.

4.3.2 *Format poruka*

CPR_079 Format poruka za primitive TesterPresent prikazan je u sljedećim tablicama:

Tablica 10.

Poruka zahtjeva TesterPresent

Bajt #	Naziv parametra		Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje		80	FMT
#2	Bajt ciljne adrese		EE	TGT
#3	Bajt izvorne adrese		tt	SRC
#4	Bajt za dodatnu dužinu		02	LEN
#5	**TesterPresent Request Service Id**		**3E**	**TP**
#6	Podfunkcija = responseRequired =	[da	01	RESPREQ_Y
		ne]	02	RESPREQ_NO
#7	Kontrolni zbir		00-FF	CS

CPR_080 Ako je parametar responseRequired postavljen na „da”, poslužitelj odgovara porukom sa sljedećim pozitivnim odgovorom. Ako je postavljen na „ne”, poslužitelj ne šalje nikakav odgovor.

Tablica 11.

Poruka TesterPresent s pozitivnim odgovorom

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	tt	TGT
#3	Bajt izvorne adrese	EE	SRC
#4	Bajt za dodatnu dužinu	01	LEN
#5	**TesterPresent Positive Response Service Id**	**7E**	**TPPR**
#6	Kontrolni zbir	00-FF	CS

CPR_081 Usluga podržava sljedeće kodove negativnih odgovora:

Tablica 12.

Poruka TesterPresent s negativnim odgovorom

Bajt #	Naziv parametra		Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje		80	FMT
#2	Bajt ciljne adrese		tt	TGT
#3	Bajt izvorne adrese		EE	SRC
#4	Bajt za dodatnu dužinu		03	LEN
#5	**negative Response Service Id**		**7F**	**NR**
#6	TesterPresent Request Service Identification		3E	TP
#7	responseCode =	[SubFunctionNotSupported-InvalidFormat	12	RC_SFNS_IF
		incorrectMessageLength]	13	RC_IML
#8	Kontrolni zbir		00-FF	CS

5. USLUGE UPRAVLJANJA

Raspoložive usluge opisane su u sljedećoj tablici:

Tablica 13.

Usluge upravljanja

Naziv usluge	Opis
StartDiagnosticSession	Korisnik zahtijeva početak dijagnostičke razmjene podataka s jedinicom u vozilu.
SecurityAccess	Korisnik zahtijeva pristup funkcijama koje su ograničene na ovlaštene korisnike.

5.1. Usluga StartDiagnosticSession

5.1.1 *Opis poruka*

CPR_025 Usluga StartDiagnosticSession upotrebljava se kako bi omogućila različite dijagnostičke razmjene podataka u poslužitelju. Dijagnostička razmjena podataka omogućava poseban skup usluga prema tablici 17. Razmjena podataka može proizvođačima vozila omogućiti posebne usluge koje nisu dio ovog dokumenta. Sprovedbena pravila ispunjavaju sljedeće zahtjeve:

— uvijek je samo jedna dijagnostička razmjena podataka aktivna u jedinici u vozilu,

— prilikom uključenja jedinica u vozilu uvijek pokreće StandardDiagnosticSession. Ako nije pokrenuta niti jedna druga dijagnostička razmjena podataka, StandardDiagnosticSession je aktivan sve dok je uključena jedinica u vozilu,

— ako je ispitni uređaj zatražio dijagnostičku razmjenu podataka koja je već aktivna, tada jedinica u vozilu šalje poruku s pozitivnim odgovorom,

— svaki put kada ispitni uređaj zatraži novu dijagnostičku razmjenu podataka, jedinica u vozilu najprije šalje poruku StartDiagnosticSession s pozitivnim odgovorom prije nego što novi proces postane aktivan u jedinici u vozilu. Ako nije u stanju započeti zatraženu novu dijagnostičku razmjenu podataka, jedinica u vozilu odgovara porukom StartDiagnosticSession s negativnim odgovorom te nastavlja tekuću razmjenu podataka.

CPR_026 Dijagnostička razmjena podataka započinje samo ako je uspostavljena komunikacija između korisnika i jedinice u vozilu.

CPR_027 Vremenski parametri utvrđeni u tablici 4. moraju biti aktivni nakon uspješne usluge StartDiagnosticSession s parametrom diagnosticSession postavljenim na „StandardDiagnosticSession” u poruci zahtjeva ako je prethodno bila aktivna druga dijagnostička razmjena podataka.

5.1.2 *Format poruka*

CPR_028 Formati poruka za primitive StartDiagnosticSession prikazani su u sljedećim tablicama:

Tablica 14.

Poruka zahtjeva StartDiagnosticSession

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	EE	TGT
#3	Bajt izvorne adrese	tt	SRC
#4	Bajt za dodatnu dužinu	02	LEN
#5	**StartDiagnosticSession Request Service Id**	**10**	**STDS**
#6	diagnosticSession = [jedna vrijednost iz tablice 17.]	xx	DS_…
#7	Kontrolni zbir	00-FF	CS

Tablica 15.

Poruka StartDiagnosticSession s pozitivnim odgovorom

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	tt	TGT
#3	Bajt izvorne adrese	EE	SRC
#4	Bajt za dodatnu dužinu	02	LEN
#5	**StartDiagnosticSession Positive Response Service Id**	**50**	**STDSPR**
#6	diagnosticSession = [ista vrijednost kao u bajtu #6 iz tablice 14.]	xx	DS_…
#7	Kontrolni zbir	00-FF	CS

Tablica 16.

Poruka StartDiagnosticSession s negativnim odgovorom

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	tt	TGT
#3	Bajt izvorne adrese	EE	SRC

#4	Bajt za dodatnu dužinu		03	LEN
#5	**Negative Response Service Id**		**7F**	**NR**
#6	StartDiagnosticSession Request Service Id		10	STDS
#7	ResponseCode =	[subFunctionNotSupported (1)	12	RC_SFNS
		incorrectMessageLength (2)	13	RC_IML
		conditionsNotCorrect (3)	22	RC_CNC
#8	Kontrolni zbir		00-FF	CS

(1) Vrijednost unesena u bajt #6 poruke zahtjeva ne podržava se, tj. nije u tablici 17.
(2) Dužina poruke pogrešna je.
(3) Kriteriji za zahtjev StartDiagnosticSession nisu ispunjeni.

5.1.3 *Opis parametara*

CPR_029 Usluga StartDiagnosticSession upotrebljava parametar diagnosticSession (DS_) za odabir posebnog postupka jednog ili više poslužitelja. U ovom su dokumentu opisane sljedeće dijagnostičke razmjene podataka:

Tablica 17.

Određivanje vrijednosti diagnosticSession

Heksadecimalna vrijednost	Opis	Mnemonik
81	**StandardDiagnosticSession** Ova dijagnostička razmjena podataka omogućava sve usluge navedene u **tablici 1. koloni 4. „SD"**. Te usluge omogućuju čitanje svih podataka s poslužitelja (jedinice u vozilu). Ova je dijagnostička razmjena podataka aktivna nakon što je uspješno obavljeno pokretanje između korisnika (ispitnog uređaja) i poslužitelja (jedinice u vozilu). Preko ove dijagnostičke razmjene podataka mogu se memorirati druge dijagnostičke razmjene podataka navedene u ovom odjeljku.	**SD**
85	**ECUProgrammingSession** Ova dijagnostička razmjena podataka omogućava sve usluge navedene u **tablici 1. koloni 6. „ECUPS"**. Te usluge podržavaju programiranje memorije poslužitelja (jedinice u vozilu). Preko ove dijagnostičke razmjene podataka mogu se memorirati druge dijagnostičke razmjene podataka navedene u ovom odjeljku.	**ECUPS**
87	**ECUAdjustmentSession** Ova dijagnostička razmjena podataka omogućava sve usluge navedene u **tablici 1. koloni 5. „ECUAS".** Te usluge podržavaju upravljanje ulazom/izlazom poslužitelja (jedinice u vozilu). Preko ove dijagnostičke razmjene podataka mogu se memorirati druge dijagnostičke razmjene podataka navedene u ovom odjeljku.	**ECUAS**

5.2. Usluga SecurityAccess

Upisivanje podataka kalibracije nije moguće osim ako je jedinica u vozilu u načinu rada KALIBRACIJA. Osim unošenja važeće kartice radionice u jedinicu u vozilu, u jedinicu u vozilu potrebno je upisati odgovarajući PIN prije dobivanja dopuštenja za pristup načinu rada KALIBRACIJA.

Kad je jedinica u vozilu u načinu rada KALIBRACIJA ili UPRAVLJANJE, moguć je pristup liniji kalibracije ulaznih/izlaznih signala.

Usluga SecurityAccess osigurava način unosa PIN-a i ukazivanje ispitnom uređaju je li jedinica u vozilu u načinu rada KALIBRACIJA.

Dopušten je unos PIN-a na neki drugi način.

5.2.1 *Opis poruka*

Uslugu SecurityAccess čine SecurityAccess poruke „requestSeed", nakon čega može slijediti SecurityAccess poruka „sendKey". Usluga SecurityAccess mora se provesti nakon usluge StartDiagnosticSession.

CPR_033 Ispitni uređaj može upotrebljavati SecurityAccess poruku „requestSeed" za provjeru je li jedinica u vozilu spremna za prihvaćanje PIN-a.

CPR_034 Ako je jedinica u vozilu već u načinu rada KALIBRACIJA, na zahtjev odgovara upućivanjem signala („seed") od 0x0000 upotrebom usluge SecurityAccess s pozitivnim odgovorom.

CPR_035 Ako je jedinica u vozilu spremna prihvatiti PIN za provjeru putem kartice radionice, na zahtjev odgovara slanjem signala („seed") većeg od 0x0000 upotrebom usluge SecurityAccess s pozitivnim odgovorom.

CPR_036 Ako jedinica u vozilu nije spremna prihvatiti PIN iz ispitnog uređaja, bilo zato što umetnuta kartica radionice nije važećia ili zato što kartica radionice nije umetnuta ili stoga što jedinica u vozilu očekuje PIN na neki drugi način, na zahtjev odgovara negativnim odgovorom s kodom odgovora koji je postavljen na conditionsNotCorrectOrRequestSequenceError.

CPR_037 Ispitni uređaj može potom upotrijebiti SecurityAccess poruku „sendKey" za slanje PIN-a jedinici u vozilu. Kako bi se dalo vremena za sprovođenje postupka autentifikacije kartice, jedinica u vozilu upotrebljava kod negativnog odgovora requestCorrectlyReceived-ResponsePending kako bi se produžilo vrijeme za davanje odgovora. Međutim, dopušteno vrijeme za davanje odgovora ne smije biti duže od pet minuta. Čim se zahtijevana usluga završi, jedinica u vozilu šalje poruku s pozitivnim odgovorom ili poruku s negativnim odgovorom s kodom odgovora koji je različit od navedenog. Jedinica u vozilu može ponavljati kod negativnog odgovora requestCorrectlyReceived-ResponsePending do završetka zahtijevane usluge i do upućivanja poruke s konačnim odgovorom.

CPR_038 Jedinica u vozilu odgovara na ovaj zahtjev upotrebom usluge SecurityAccess s pozitivnim odgovorom samo kada je u načinu rada KALIBRACIJA.

CPR_039 U sljedećim slučajevima, jedinica u vozilu odgovara na ovaj zahtjev negativnim odgovorom s kodom odgovora postavljenim na:

— subFunctionNotSupported: nepravilan format parametra podfunkcije (accessType),

— conditionsNotCorrectOrRequestSequenceError: jedinica u vozilu nije spremna za prihvaćanje unosa PIN-a,
— invalidKey: PIN nije važeći i broj pokušaja provjere PIN-a nije premašen,
— exceededNumberOfAttempts: PIN nije važeći i broj pokušaja provjere PIN-a je premašen,
— generalReject: ispravan PIN, ali uzajamna autentifikacija s karticom radionice nije uspjela.

5.2.2 *Format poruka – SecurityAccess – requestSeed*

CPR_040 Formati poruka za SecurityAccess primitive „requestSeed" prikazani su u sljedećim tablicama:

Tablica 18.

Zahtjev SecurityAccess – poruka requestSeed

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	EE	TGT
#3	Bajt izvorne adrese	tt	SRC
#4	Bajt za dodatnu dužinu	02	LEN
#5	**SecurityAccess Request Service Id**	**27**	**SA**
#6	accessType – requestSeed	7D	AT_RSD
#7	Kontrolni zbir	00-FF	CS

Tablica 19.

SecurityAccess – poruka requestSeed s pozitivnim odgovorom

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	tt	TGT
#3	Bajt izvorne adrese	EE	SRC
#4	Bajt za dodatnu dužinu	04	LEN
#5	**SecurityAccess Positive Response Service Id**	**67**	**SAPR**
#6	accessType – requestSeed	7D	AT_RSD
#7	SeedHigh	00-FF	SEEDH
#8	SeedLow	00-FF	SEEDL
#9	Kontrolni zbir	00-FF	CS

Tablica 20.

Poruka SecurityAccess s negativnim odgovorom

Bajt #	Naziv parametra		Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje		80	FMT
#2	Bajt ciljne adrese		tt	TGT
#3	Bajt izvorne adrese		EE	SRC
#4	Bajt za dodatnu dužinu		03	LEN
#5	**negativeResponse Service Id**		**7F**	**NR**
#6	Identifikator usluge zahtjeva SecurityAccess		27	SA
#7	responseCode =	[conditionsNotCorrectOrRequestSequenceError	22	RC_CNC
		incorrectMessageLength]	13	RC_IML
#8	Kontrolni zbir		00-FF	CS

5.2.3 *Format poruka – SecurityAccess – sendKey*

CPR_041 Formati poruka za SecurityAccess primitive „sendKey" prikazani su u sljedećim tablicama:

Tablica 21.

Zahtjev SecurityAccess – poruka sendKey

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	EE	TGT
#3	Bajt izvorne adrese	tt	SRC
#4	Bajt za dodatnu dužinu	m+2	LEN
#5	**SecurityAccess Request Service Id**	**27**	**SA**
#6	accessType – sendKey	7E	AT_SK
#7 do #m+6	Ključ #1 (viši)	xx	KEY
	…	…	
	Ključ #m (niži, m mora biti najmanje 4, a najviše 8)	xx	
#m+7	Kontrolni zbir	00-FF	CS

Tablica 22.

SecurityAccess – poruka sendKey s pozitivnim odgovorom

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	tt	TGT
#3	Bajt izvorne adrese	EE	SRC
#4	Bajt za dodatnu dužinu	02	LEN
#5	**SecurityAccess Positive Response Service Id**	**67**	**SAPR**
#6	accessType – sendKey	7E	AT_SK
#7	Kontrolni zbir	00-FF	CS

Tablica 23.

Poruka SecurityAccess s negativnim odgovorom

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	tt	TGT

#3	Bajt izvorne adrese		EE	SRC
#4	Bajt za dodatnu dužinu		03	LEN
#5	**NegativeResponse Service Id**		**7F**	**NR**
#6	SecurityAccess Request Service Id		27	SA
#7	ResponseCode =	[generalReject	10	RC_GR
		subFunctionNotSupported	12	RC_SFNS
		incorrectMessageLength	13	RC_IML
		conditionsNotCorrectOrRequestSequenceError	22	RC_CNC
		invalidKey	35	RC_IK
		exceededNumberOfAttempts	36	RC_ENA
		requestCorrectlyReceived-ResponsePending]	78	RC_RCR_RP
#8	Kontrolni zbir		00-FF	CS

6. USLUGE PRENOSA PODATAKA

Raspoložive usluge opisane su u sljedećoj tablici:

Tablica 24.

Usluge prenosa podataka

Naziv usluge	Opis
ReadDataByIdentifier	Korisnik zahtijeva prenos trenutne vrijednosti zapisa kojem recordDataIdentifier ima pristup.
WriteDataByIdentifier	Korisnik zahtijeva upisivanje zapisa kojem je recordDataIdentifier pristupio.

6.1. Usluga ReadDataByIdentifier

6.1.1 *Opis poruka*

CPR_050 Uslugu ReadDataByIdentifier korisnik upotrebljava za traženje vrijednosti podatkovnih zapisa iz poslužitelja. Podatke identificira recordDataIdentifier. Proizvođač jedinice u vozilu odgovoran je za ispunjavanje uvjeta poslužitelja prilikom obavljanja ove usluge.

6.1.2 *Format poruka*

CPR_051 Formati poruka za primitive ReadDataByIdentifier prikazani su u sljedećim tablicama:

Tablica 25.

Poruka zahtjeva ReadDataByIdentifier

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	EE	TGT
#3	Bajt izvorne adrese	tt	SRC
#4	Bajt za dodatnu dužinu	03	LEN
#5	**ReadDataByIdentifier Request Service Id**	**22**	**RDBI**
#6 do #7	recordDataIdentifier = [jedna vrijednost iz tablice 28.]	xxxx	RDI_…
#8	Kontrolni zbir	00-FF	CS

Tablica 26.

Poruka ReadDataByIdentifier s pozitivnim odgovorom

Bajt #	Naziv parametra		Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje		80	FMT
#2	Bajt ciljne adrese		tt	TGT
#3	Bajt izvorne adrese		EE	SRC
#4	Bajt za dodatnu dužinu		m+3	LEN
#5	**ReadDataByIdentifier Positive Response Service Id**		**62**	**RDBIPR**
#6 i #7	recordDataIdentifier = [ista vrijednost kao bajtovi #6 i #7 iz tablice 25.]		xxxx	RDI_…
#8 do #m+7	dataRecord[] =	[data#1	xx	DREC_DATA1
		:	:	.
		data#m]	xx	DREC_DATAm
#m+8	Kontrolni zbir		00-FF	CS

Tablica 27.

Poruka ReadDataByIdentifier s negativnim odgovorom

Bajt #	Naziv parametra		Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje		80	FMT
#2	Bajt ciljne adrese		tt	TGT
#3	Bajt izvorne adrese		EE	SRC
#4	Bajt za dodatnu dužinu		03	LEN
#5	**NegativeResponse Service Id**		**7F**	**NR**
#6	Identifikator usluge zahtjeva ReadDataByIdentifier		22	RDBI
#7	ResponseCode =	[requestOutOfRange	31	RC_ROOR
		incorrectMessageLength	13	RC_IML
		conditionsNotCorrect]	22	RC_CNC
#8	Kontrolni zbir		00-FF	CS

6.1.3 *Opis parametara*

CPR_052 Parametar ***recordDataIdentifier (RDI_)*** u poruci zahtjeva ReadDataByIdentifier identificira podatkovni zapis.

CPR_053 Vrijednosti recordDataIdentifier utvrđene u ovom dokumentu prikazane su u tablici u nastavu. Tablicu recordDataIdentifier čine četiri stupca i više redaka.

— **U prvom koloni (Heks.)** navodi se „heksadecimalna vrijednost" dodijeljena parametru recordDataIdentifier opisanom u trećem koloni.
— **U drugom koloni (Podatkovni element)** prikazan je podatkovni element iz Dodatka 1. na kojem se temelji recordDataIdentifier (ponekad je potrebno prekodiranje).
— **U trećem koloni (Opis)** navodi se odgovarajući naziv parametra recordDataIdentifier.
— **U četvrtom koloni (Mnemonik)** navodi se mnemonik tog parametra recordDataIdentifier.

Tablica 28.

Određivanje vrijednosti recordDataIdentifier

Heks.	Podatkovni element	Naziv parametra recordDataIdentifier (vidjeti format u odjeljku 8.2.)	Mnemonik
F90B	CurrentDateTime	TimeDate	RDI_TD
F912	HighResOdometer	HighResolutionTotalVehicleDistance	RDI_HRTVD
F918	K-ConstantOfRecordingEquipment	Kfactor	RDI_KF
F91C	L-TyreCircumference	LfactorTyreCircumference	RDI_LF
F91D	W-VehicleCharacteristicConstant	WvehicleCharacteristicFactor	RDI_WVCF
F921	TyreSize	TyreSize	RDI_TS
F922	NextCalibrationDate	NextCalibrationDate	RDI_NCD
F92C	SpeedAuthorised	SpeedAuthorised	RDI_SA
F97D	VehicleRegistrationNation	RegisteringMemberState	RDI_RMS
F97E	VehicleRegistrationNumber	VehicleRegistrationNumber	RDI_ VRN
F190	VehicleIdentificationNumber	VIN	RDI_ VIN

CPR_054 Parametar ***dataRecord (DREC_)*** upotrebljava poruka ReadDataByIdentifier s pozitivnim odgovorom za pružanje korisniku (ispitnom uređaju) vrijednosti podatkovnog zapisa koji je identifikovao recordDataIdentifier. Formati podataka navedeni su u odjeljku 8. Mogu se primijeniti dodatni korisnički neobvezni dataRecords, uključujući posebne ulazne, unutarnje i izlazne podatke jedinice u vozilu, no oni nisu definisani u ovom dokumentu.

6.2. Usluga WriteDataByIdentifier

6.2.1 *Opis poruka*

CPR_056 Uslugu WriteDataByIdentifier korisnik upotrebljava za upisivanje vrijednosti podatkovnih zapisa na poslužitelj. Podatke identificira parametar recordDataIdentifier. Proizvođač jedinice u vozilu odgovoran je za ispunjavanje uvjeta poslužitelja prilikom obavljanja ove usluge. Za ažuriranje parametara navedenih u tablici 28. jedinica u vozilu mora biti u načinu rada KALIBRACIJA.

6.2.2 *Format poruka*

CPR_057 Formati poruka za primitive WriteDataByIdentifier prikazani su u sljedećim tablicama:

Tablica 29.

Poruka zahtjeva WriteDataByIdentifier

Bajt #	Naziv parametra		Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje		80	FMT
#2	Bajt ciljne adrese		EE	TGT
#3	Bajt izvorne adrese		tt	SRC
#4	Bajt za dodatnu dužinu		m+3	LEN
#5	**WriteDataByIdentifier Request Service Id**		**2E**	**WDBI**
#6 do #7	recordDataIdentifier = [jedna vrijednost iz tablice 28.]		xxxx	RDI_…
#8 do m+7	dataRecord[] =	[data#1	xx	DREC_DATA1
		:	:	:
		data#m]	xx	DREC_DATAm
#m+8	Kontrolni zbir		00-FF	CS

Tablica 30.

Poruka WriteDataByIdentifier s pozitivnim odgovorom

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	tt	TGT
#3	Bajt izvorne adrese	EE	SRC
#4	Bajt za dodatnu dužinu	03	LEN
#5	**WriteDataByIdentifier Positive Response Service Id**	**6E**	**WDBIPR**
#6 do #7	recordDataIdentifier = [ista vrijednost kao bajtovi #6 i #7 iz tablice 25.]	xxxx	RDI_…
#8	Kontrolni zbir	00-FF	CS

Tablica 31.

Poruka WriteDataByIdentifier s negativnim odgovorom

Bajt #	Naziv parametra		Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje		80	FMT
#2	Bajt ciljne adrese		tt	TGT
#3	Bajt izvorne adrese		EE	SRC
#4	Bajt za dodatnu dužinu		03	LEN
#5	**NegativeResponse Service Id**		**7F**	**NR**
#6	WriteDataByIdentifier Request Service Id		2E	WDBI
#7	ResponseCode =	[requestOutOfRange	31	RC_ROOR
		incorrectMessageLength	13	RC_IML

		conditionsNotCorrect]	22	RC_CNC
#8	Kontrolni zbir		00-FF	CS

6.2.3 *Opis parametara*

Parametar ***recordDataIdentifier (RDI_)*** određen je u tablici 28.

Parametar ***dataRecord (DREC_)*** upotrebljava poruka zahtjeva WriteDataByIdentifier za davanje poslužitelju (jedinici u vozilu) vrijednosti podatkovnih zapisa koje je identifikovao recordDataIdentifier. Formati podataka navedeni su u odjeljku 8.

7. UPRAVLJANJE ISPITNIM IMPULSIMA – FUNKCIONALNA JEDINICA ZA UPRAVLJANJE ULAZOM/IZLAZOM

Raspoložive usluge opisane su u sljedećoj tablici:

Tablica 32.

Funkcionalna jedinica za upravljanje ulazom/izlazom

Naziv usluge	Opis
InputOutputControlByIdentifier	Korisnik zahtijeva upravljanje ulazom/izlazom specifično za poslužitelj

7.1. Usluga InputOutputControlByIdentifier

7.1.1 *Opis poruka*

Postoji veza putem priključka na prednjoj strani tahografa koja omogućava upravljanje ispitnim impulsima ili njihovo praćenje upotrebom odgovarajućeg ispitnog uređaja.

CPR_058 Ova linija kalibracije U/I signala može se konfigurirati naredbom iz K-linije putem usluge InputOutputControlByIdentifier za odabir zahtijevane funkcije ulaza ili izlaza za liniju. Raspoloživa su stanja linije:

— isključeno,

— speedSignalInput, pri čemu se linija kalibracije U/I signala upotrebljava za ulaz signala brzine (ispitni signal) koji nadomješta signal brzine senzora kretanja; ova funkcija nije moguća u kontrolnom načinu rada,

— realTimeSpeedSignalOutputSensor, pri čemu se linija kalibracije signala U/I upotrebljava za izlaz signala brzine senzora kretanja,

— RTCOutput, pri čemu se linija kalibracije U/I signala upotrebljava za izlaz signala UTC sata; ova funkcija nije moguća u kontrolnom načinu rada.

CPR_059 Jedinica u vozilu morala je pristupiti procesu podešavanja i mora biti u kalibracijskom ili kontrolnom načinu rada za konfiguraciju stanja linije. Kad je jedinica u vozilu u kalibracijskom načinu rada, dostupne su četiri linije stanja (isključeno, speedSignalInput, realTimeSpeedSignalOutputSensor, RTCOutput). Kad je jedinica u vozilu u kontrolnom načinu rada, dostupne su samo dvije linije stanja (isključeno, realTimeSpeedSignalOutputSensor). Prilikom izlaza iz procesa podešavanja ili kalibracijskog ili kontrolnog načina rada, jedinica u vozilu mora osigurati da se linija kalibracije U/I signala vrati u „isključeno" (standardno) stanje.

CPR_060 Ako se impulsi brzine u realnom vremenu primaju na liniju ulaza signala brzine jedinice u vozilu dok je linija kalibracije U/I signala postavljena na ulaz, tada se linija kalibracije U/I signala postavlja na izlaz ili vraća u isključeno stanje.

CPR_061 Redoslijed je sljedeći:

— uspostava komunikacije putem usluge StartCommunication,

— ulazak u proces podešavanja putem usluge StartDiagnosticSession i kalibracijski ili kontrolni način rada (redoslijed ovih dviju operacija nije bitan),

— promjena stanja izlaza putem usluge InputOutputControlByIdentifier.

7.1.2 *Format poruka*

CPR_062 Formati poruka za primitive InputOutputControlByIdentifier prikazani su u sljedećim tablicama:

Tablica 33.

Poruka zahtjeva InputOutputControlByIdentifier

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	EE	TGT
#3	Bajt izvorne adrese	tt	SRC
#4	Bajt za dodatnu dužinu	xx	LEN
#5	**InputOutputControlByIdentifier Request Sid**	**2F**	**IOCBI**
#6 i #7	InputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 ili #8 do #9	ControlOptionRecord = [		COR_…
	inputOutputControlParameter – jedna vrijednost iz tablice 36.	xx	IOCP_…
	controlState – jedna vrijednost iz tablice 37. (vidjeti napomenu u nastavu)]	xx	CS_…
#9 ili #10	Kontrolni zbir	00-FF	CS

Napomena: Parametar controlState prisutan je samo u nekim slučajevima (vidjeti tačku 7.1.3.).

Tablica 34.

Poruka InputOutputControlByIdentifier s pozitivnim odgovorom

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	tt	TGT
#3	Bajt izvorne adrese	EE	SRC
#4	Bajt za dodatnu dužinu	xx	LEN
#5	**inputOutputControlByIdentifier Positive Response SId**	**6F**	**IOCBIPR**
#6 i #7	inputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO

#8 ili #8 do #9	controlStatusRecord = [		CSR_
	inputOutputControlParameter = [ista vrijednost kao bajt #8 iz tablice 33.]	xx	IOCP_…
	controlState (ista vrijednost kao bajt #9 iz tablice 33.)(ako je primjenjivo)	xx	CS_…
#9 ili #10	Kontrolni zbir	00-FF	CS

Tablica 35.

Poruka InputOutputControlByIdentifier s negativnim odgovorom

Bajt #	Naziv parametra	Heksadecimalna vrijednost	Mnemonik
#1	Formatni bajt – fizičko adresiranje	80	FMT
#2	Bajt ciljne adrese	tt	TGT
#3	Bajt izvorne adrese	EE	SRC
#4	Bajt za dodatnu dužinu	03	LEN
#5	**negativeResponse Service Id**	**7F**	**NR**
#6	Identifikator usluge zahtjeva inputOutputControlByIdentifier	2F	IOCBI
#7	responseCode=[		
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrect	22	RC_CNC
	requestOutOfRange	31	RC_ROOR
	deviceControlLimitsExceeded]	7A	RC_DCLE
#8	Kontrolni zbir	00-FF	CS

7.1.3 *Opis parametara*

CPR_064 Parametar ***inputOutputControlParameter (IOCP_)*** određen je u sljedećoj tablici:

Tablica 36.

Određivanje vrijednosti inputOutputControlParameter

Heksadecimalna vrijednost	Opis	Mnemonik
00	**ReturnControlToECU** Ova vrijednost upozorava poslužitelja (jedinicu u vozilu) da ispitni uređaj više ne upravlja linijom kalibracije U/I signala.	RCTECU
01	**ResetToDefault** Ova vrijednost upozorava poslužitelja (jedinicu u vozilu) da se od njega zahtijeva povraćaj linije kalibracije U/I signala u standardno stanje.	RTD
03	**ShortTermAdjustment** Ova vrijednost upozorava poslužitelja (jedinicu u vozilu) da se od njega zahtijeva podešavanje linije kalibracije U/I signala s vrijednošću obuhvaćenom parametrom controlState.	STA

CPR_065 Parametar ***controlState*** prisutan je samo kada je inputOutputControlParameter postavljen na ShortTermAdjustment i definisan je u sljedećoj tablici:

Tablica 37.

Određivanje vrijednosti controlState

Način rada	Heksadecimalna vrijednost	Opis
Isključi	00	U/I linija je isključena (standardno stanje)
Uključi	01	Uključuje U/I liniju kalibracije kao speedSignalInput
Uključi	02	Uključuje U/I liniju kalibracije kao realTimeSpeedSignalOutputSensor
Uključi	03	Uključuje U/I liniju kalibracije kao RTCOutput

8. FORMATI DATARECORDS

U ovom se odjeljku opisuju:

— opća pravila koja se primjenjuju na raspon parametara koje jedinica u vozilu prenosi ispitnom uređaju,

— formati koji se upotrebljavaju za podatke koji se prenose putem usluga prenosa podataka opisanih u odjeljku 6.

CPR_067 Jedinica u vozilu podržava sve utvrđene parametre.

CPR_068 Podaci koje jedinica u vozilu prenosi ispitnom uređaju kao odgovor na poruku zahtjeva moraju biti izmjereni podaci (tj. trenutna vrijednost zahtijevanog parametra koji je jedinica u vozilu izmjerila ili uočila).

8.1. Rasponi prenesenih parametara

CPR_069 U tablici 38. određeni su rasponi koji se upotrebljavaju za utvrđivanje važnosti prenesenog parametra.

CPR_070 Vrijednosti u rasponu „indikator pogreške” omogućuju jedinici u vozilu da odmah upozori da važeći parametarski podatak trenutačno nije dostupan zbog neke pogreške u tahografu.

CPR_071 Vrijednosti u rasponu „nije dostupno” omogućuju jedinici u vozilu da prenese poruku koja sadrži parametar koji nije dostupan ili ga taj modul ne podržava. Vrijednosti u području „nije traženo” omogućuju uređaju da prenese poruku naredbe i odredi one parametre kod kojih se ne očekuje odgovor prijamnog uređaja.

CPR_072 Ako pogreška sastavnog dijela spriječi prenos važećiog podatka za parametar, umjesto podatka za takav parametar treba upotrijebiti indikator pogreške opisan u tablici 38. Međutim, ako izmjereni ili izračunani podatak daje važeću vrijednost, ali premašuje utvrđeni raspon parametra, ne smije se upotrebljavati indikator pogreške. Podatke treba prenositi upotrebljavajući odgovarajuću najmanju ili najveću vrijednost parametra.

Tablica 38.

Rasponi dataRecords

Naziv raspona	1 bajt (heksadecimalna vrijednost)	2 bajta (heksadecimalna vrijednost)	4 bajta (heksadecimalna vrijednost)	ASCII
Važeći signal	00 do FA	0000 do FAFF	00000000 do FAFFFFFF	1 do 254

Indikator specifičnog parametra	FB	FB00 do FBFF	FB000000 do FBFFFFFF	nema
Rezervisani raspon za bitove budućih indikatora	FC do FD	FC00 do FDFF	FC000000 do FDFFFFFF	nema
Indikator pogreške	FE	FE00 do FEFF	FE000000 do FEFFFFFF	0
Nije dostupno ili nije traženo	FF	FF00 do FFFF	FF000000 do FFFFFFFF	FF

CPR_073 Za parametre kodirane u ASCII, ASCII znak „*" rezervisan je kao razdjelnik.

8.2. Formati dataRecords

U tablicama 39. do 42. navedenima u nastavu detaljno su prikazani formati koji se upotrebljavaju putem usluga ReadDataByIdentifier i WriteDataByIdentifier.

CPR_074 U tablici 39. navedeni su dužina, rezolucija i radno područje za svaki parametar koji je identifikovao njegov recordDataIdentifier:

Tablica 39.

Format dataRecords

Naziv parametra	Dužina podatka (u bajtovima)	Rezolucija	Radno područje
TimeDate	8	Vidjeti pojedinosti u tablici 40.	
HighResolutionTotalVehicleDistance	4	uvećanje 5 m/bit, pomak 0 m	0 do + 21 055 406 km
Kfactor	2	uvećanje 0,001 impulsa/m/bit, pomak 0	0 do 64,255 impulsa/m
LfactorTyreCircumference	2	uvećanje 0,125 10^{-3} m /bit, pomak 0	0 do 8,031 m
WvehicleCharacteristicFactor	2	uvećanje 0,001 impulsa/m/bit, pomak 0	0 do 64,255 impulsa/m
TyreSize	15	ASCII	ASCII
NextCalibrationDate	3	Vidjeti pojedinosti u tablici 41.	
SpeedAuthorised	2	uvećanje 1/256 km/h/bit, pomak 0	0 do 250,996 km/h
RegisteringMemberState	3	ASCII	ASCII
VehicleRegistrationNumber	14	Vidjeti pojedinosti u tablici 42.	
VIN	17	ASCII	ASCII

CPR_075 U tablici 40. detaljno su opisani formati različitih bajtova parametra TimeDate:

Tablica 40.

Detaljni format TimeDate (vrijednost recordDataIdentifier # F90B)

Bajt	Opis parametara	Rezolucija	Radno područje
1	Sekunde	uvećanje 0,25 s/bit, pomak 0 s	0 do 59,75 s
2	Minute	uvećanje 1 min/bit, pomak 0 min	0 do 59 min
3	Sati	uvećanje 1 h/bit, pomak 0 h	0 do 23 h
4	Mjesec	uvećanje 1 mjesec/bit, pomak 0 mjeseci	1 do 12 mjeseci
5	Dan	uvećanje 0,25 dana/bit, pomak 0 dana (vidjeti napomenu ispod tablice 41.)	0,25 do 31,75 dana
6	Godina	uvećanje 1 godina/bit, pomak + 1985 godina (vidjeti napomenu ispod tablice 41.)	godina 1985. do 2235.
7	Pomak po minutama u lokalnom vremenu	uvećanje 1 min/bit, pomak – 125 min	– 59 do + 59 min
8	Pomak po satima u lokalnom vremenu	uvećanje 1 h/bit, pomak – 125 h	– 23 do + 23 h

CPR_076 U tablici 41. detaljno su opisani formati različitih bajtova parametra NextCalibrationDate:

Tablica 41.

Detaljni format NextCalibrationDate (vrijednost recordDataIdentifier # F922)

Bajt	Opis parametara	Rezolucija	Radno područje
1	Mjesec	uvećanje 1 mjesec/bit, pomak 0 mjeseci	1 do 12 mjeseci
2	Dan	uvećanje 0,25 dana/bit, pomak 0 dana (vidjeti napomenu u nastavu)	0,25 do 31,75 dana
3	Godina	uvećanje 1 godina/bit, pomak + 1985 godina (vidjeti napomenu u nastavu)	godina 1985. do 2235.

NAPOMENA povezana s upotrebom parametra „Dan":

1) Vrijednost 0 u datumu je prazna vrijednost. Vrijednosti 1, 2, 3 i 4 upotrebljavaju se za označivanje prvog dana u mjesecu; 5, 6, 7 i 8 određuju drugi dan u mjesecu itd.

2) Ovaj parametar ne utječe niti mijenja prethodno navedeni parametar sati.

NAPOMENA povezana s upotrebom parametra „Godina":

Vrijednost 0 za godinu označava 1985. godinu; vrijednost 1 označava 1986. itd.

CPR_078 U tablici 42. detaljno su opisani formati različitih bajtova parametra VehicleRegistrationNumber:

Tablica 42.

Detaljni format VehicleRegistrationNumber (vrijednost recordDataIdentifier # F97E)

Bajt	Opis parametara	Rezolucija	Radno područje
1	Kodna stranica (kako je utvrđena u Dodatku 1.)	ASCII	01 do 0A
2 – 14	Registracijski broj vozila (kako je utvrđen u Dodatku 1.)	ASCII	ASCII

Dodatak 9.

HOMOLOGACIJA POPIS OBVEZNIH ISPITIVANJA

SADRŽAJ

1. UVOD

1.1. Homologacija

EZ homologacija uređaja za bilježenje podataka (ili njegova sastavnog dijela) ili tahografske kartice temelji se na:

— **sigurnosnoj certifikaciji** koja se temelji na specifikacijama zajedničkih mjerila u odnosu na sigurnosni cilj koji je potpuno usklađen s Dodatkom 10. ovom Prilogu,

— **funkcionalnoj certifikaciji** koju sprovodi tijelo države članice koje potvrđuje da ispitivani predmet zadovoljava zahtjeve ovog Priloga u smislu izvršenih funkcija, tačnosti mjerenja i obilježja okruženja,

— **certifikaciji interoperabilnosti** koju obavlja nadležno tijelo koje potvrđuje da je uređaj za bilježenje podataka (ili tahografska kartica) u cijelosti interoperabilan sa zahtijevanim modelima tahografske kartice (ili uređaja za bilježenje podataka) (vidjeti poglavlje 8. ovog Priloga).

U ovom se Dodatku navode obavezna ispitivanja koja tijelo države članice mora obaviti tokom funkcionalnih ispitivanja te obavezna ispitivanja koja nadležno tijelo mora obaviti tokom ispitivanja interoperabilnosti. Postupci koji se provode za obavljanje ispitivanja ili vrsta ispitivanja nisu podrobnije opisani.

Ovim Dodatkom nisu obuhvaćeni aspekti sigurnosne certifikacije. Ako se neka ispitivanja zahtijevana za homologaciju obavljaju tokom sigurnosne procjene i postupka certifikacije, tada ta ispitivanja ne treba ponavljati. U tom se slučaju mogu samo pregledati rezultati tih ispitivanja sigurnosti. U informativne svrhe, zahtjevi za koje se očekuje da će biti ispitani (ili koji su blisko povezani s ispitivanjima za koja se očekuje da će biti obavljena) tokom sigurnosne certifikacije u ovom su Dodatku označeni znakom „*".

Numerisani zahtjevi odnose se na tekstove Priloga, dok se ostali zahtjevi odnose na ostale dodatke (npr. PIC_001 odnosi se na zahtjev PIC_001 piktograma iz Dodatka 3.).

U ovom se Dodatku razmatraju odvojeno homologacija senzora kretanja, jedinice u vozilu i vanjskog uređaja GNSS-a kao sastavnih dijelova uređaja za bilježenje podataka. Svaki sastavni dio dobiva vlastiti certifikat o homologaciji u kojem su naznačeni ostali kompatibilni sastavni dijelovi. Funkcionalno ispitivanje senzora kretanja (ili vanjskog uređaja GNSS-a) sprovodi se zajedno s jedinicom u vozilu i obrnuto.

Ne zahtijeva se interoperabilnost između svakog modela senzora kretanja (odnosno vanjskog uređaja GNSS-a) i svakog modela jedinice u vozilu. U tom slučaju homologacija senzora kretanja (odnosno vanjskog uređaja GNSS-a) može se dodijeliti samo u kombinaciji s homologacijom relevantne jedinice u vozilu i obrnuto.

1.2. Referentni dokumenti

U ovom su Dodatku upotrijebljeni sljedeći izvori:

IEC 60068-2-1:Environmental testing – Part 2-1: Tests – Test A: Cold;

IEC 60068-2-2:Basic environmental testing procedures; Part 2: Tests; Tests B: Dry heat (sinusoidal);

IEC 60068-2-6:Environmental testing – Part 2: Tests – Test Fc: Vibration;

IEC 60068-2-14:Environmental testing; Part 2-14: Tests; Test N: Change of temperature;

IEC 60068-2-27:Environmental testing. Part 2: Tests. Test Ea and guidance: Shock;

IEC 60068-2-30:Environmental testing – Part 2-30: Tests – Test Db: Damp heat, cyclic (12 h + 12 h cycle);

IEC 60068-2-64:Environmental testing – Part 2-64: Tests– Test Fh: Vibration, broadband random and guidance;

IEC 60068-2-78Environmental testing – Part 2-78: Tests – Test Cab: Damp heat, steady state;

ISO 16750-3 –Mechanical loads (2012-12);

ISO 16750-4 –Climatic loads (2010-04);

ISO 20653:Road vehicles – Degree of protection (IP code) – Protection of electrical equipment against foreign objects, water and access;

ISO 10605:2008 + Technical Corrigendum:2010 + AMD1:2014Road vehicles – Test methods for electrical disturbances from electrostatic discharge;

ISO 7637-1:2002 + AMD1: 2008Road vehicles – Electrical disturbances from conduction and coupling – Part 1: Definitions and general considerations;

ISO 7637-2Road vehicles – Electrical disturbances from conduction and coupling – Part 2: Electrical transient conduction along supply lines only;

ISO 7637-3Road vehicles – Electrical disturbances from conduction and coupling – Part 3: Electrical transient transmission by capacitive and inductive coupling via lines other than supply lines;

ISO/IEC 7816-1Identification cards – Integrated circuit(s) cards with contacts – Part 1: Physical characteristics;

ISO/IEC 7816-2Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 2: Dimensions and location of the contacts;

ISO/IEC 7816-3Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 3: Electronic signals and transmission protocol;

ISO/IEC 10373-1:2006 + AMD1:2012Identification cards – Test methods – Part 1: General characteristics;

ISO/IEC 10373-3:2010 + Technical Corrigendum:2013Identification cards – Test methods – Part 3: Integrated circuit cards with contacts and related interface devices;
ISO 16844-3:2004, Cor 1:2006Road vehicles – Tachograph systems – Part 3: Motion sensor interface (with vehicle units);
ISO 16844-4Road vehicles – Tachograph systems – Part 4: CAN interface;
ISO 16844-6Road vehicles – Tachograph systems – Part 6: Diagnostics;
ISO 16844-7Road vehicles – Tachograph systems – Part 7: Parameters;
ISO 534Paper and board – Determination of thickness, density and specific volume;
UN ECE R10Jedinstvene odredbe o homologaciji vozila s obzirom na elektromagnetsku kompatibilnost (Privredna komisija Ujedinjenih naroda za Evropu).

2. FUNKCIONALNA ISPITIVANJA JEDINICE U VOZILU

Br.	Ispitivanje	Opis	Povezani zahtjevi
1.	**Administrativni pregled**		
1.1	Dokumentacija	Ispravnost dokumentacije	
1.2	Rezultati ispitivanja proizvođača	Rezultati ispitivanja proizvođača provedenog tokom ugradnje. Osiguravanje dokumentacije.	88, 89, 91
2.	**Vizualni pregled**		
2.1	Shodnost s dokumentacijom		
2.2	Identifikacija/oznake		224 do 226
2.3	Materijali		219 do 223
2.4	Plombiranje		398, 401 do 405
2.5	Vanjska sučelja		
3.	**Funkcionalna ispitivanja**		
3.1	Predviđene funkcije		02, 03, 04, 05, 07, 382
3.2	Načini rada		09 do 11*, 134, 135
3.3	Funkcije i prava na pristup podacima		12* 13*, 382, 383, 386 do 389
3.4	Praćenje umetanja i uklanjanja kartica		15, 16, 17, 18, 19*, 20*, 134
3.5	Mjerenje brzine i udaljenosti		21 do 31
3.6	Mjerenje vremena (ispitivanje se obavlja na 20 °C)		38 do 43
3.7	Praćenje aktivnosti vozača		44 do 53, 134
3.8	Praćenje statusa vožnje		54, 55, 134
3.9	Ručni unosi		56 do 62
3.10	Upravljanje blokadama preduzeće		63 do 68
3.11	Praćenje aktivnosti nadzora		69, 70
3.12	Otkrivanje događaja i/ili pogrešaka		71 do 88, 134
3.13	Identifikacijski podaci o uređaju		93*, 94*, 97, 100
3.14	Podaci o umetanju i uklanjanju kartice vozača		102* do 104*
3.15	Podaci o aktivnosti vozača		105* do 107*
3.16	Podaci o mjestima i pozicijama		108* do 112*
3.17	Stanje brojača prijeđenih kilometara		113* do 115*
3.18	Detaljni podaci o brzini		116*
3.19	Podaci o događajima		117*
3.20	Podaci o pogreškama		118*
3.21	Podaci o kalibraciji		119* do 121*
3.22	Podaci o prilagodbi vremena		124*, 125*
3.23	Podaci o aktivnostima nadzora		126*, 127*
3.24	Podaci o blokadama preduzeće		128*
3.25	Podaci o aktivnostima preuzimanja podataka		129*
3.26	Podaci o posebnim stanjima		130*, 131*
3.27	Bilježenje i arhiviranje podataka na tahografske kartice		136, 137, 138*, 139*, 141*, 142, 143, 144, 145, 146*, 147*, 148*, 149, 150
3.28	Prikazivanje		90, 134, 151 do 168, PIC_001, DIS_001
3.29	Ispis		90, 134, 169 do 181, PIC_001, PRT_001 do PRT_014
3.30	Upozorenje		134, 182 do 191, PIC_001
3.31	Preuzimanje podataka na vanjske medije		90, 134, 192 do 196
3.32	Komunikacija na daljinu za ciljane provjere na putu		197 do 199
3.33	Izlaz podataka na dodatne vanjske uređaje		200, 201
3.34	Kalibracija		202 do 206*, 383, 384, 386 do 391
3.35	Provjera kalibracije na putu		207 do 209
3.36	Prilagodba vremena		210 do 212*
3.37	Neometanje dodatnih funkcija		06, 425
3.38	Sučelje senzora kretanja		02, 122
3.39	Vanjski uređaj GNSS-a		03, 123
3.40	Provjeriti otkriva li, bilježi i arhivira jedinica u vozilu događaj(e) i/ili pogrešku (pogreške) koje je definirao proizvođač jedinica u vozilu kad upareni senzor kretanja reagira na		217

	magnetska polja koja ometaju detekciju kretanja vozila.		
3.41	Slijed šifri (cypher suite) i normirani parametri domene		CSM_48, CSM_50
4.	**Ispitivanja utjecaja okoliša**		
4.1	Temperatura	Provjera funkcionalnosti putem: Ispitivanja u skladu s normom ISO 16750-4, poglavljem 5.1.1.2: ispitivanje rada pri niskoj temperaturi (72 h na –20 °C) Ovo se ispitivanje odnosi na normu IEC 60068-2-1: Environmental testing – Part 2-1: Tests – Test A: Cold. Ispitivanje u skladu s normom ISO 16750-4: poglavljem 5.1.2.2: ispitivanje rada pri visokoj temperaturi (72 h na 70 °C). Ovo se ispitivanje odnosi na normu IEC 60068-2-2: Basic environmental testing procedures; part 2: tests; tests B: dry heat. Ispitivanje u skladu s normom ISO 16750-4: poglavljem 5.3.2: Brze promjene temperature s određenim trajanjem prelaska (–20 °C/70 °C, 20 ciklusa, 2 h držanja pri svakoj temperaturi). Skraćeni niz ispitivanja (između onih utvrđenih u odjeljku 3. ove tablice) može se obaviti pri nižoj temperaturi, višoj temperaturi i tokom temperaturnih ciklusa.	213
4.2	Vlažnost	Provjeriti može li jedinica u vozilu izdržati cikličku vlažnost (ispitivanje toplinom) putem norme IEC IEC 60068-2-30, ispitivanje Db, šest ciklusa u trajanju od 24 sata, pri svakom promjena temperature od +25°C do +55°C i relativna vlažnost od 97 % pri +25°C te od 93 % pri +55°C.	214
4.3	Mehanička	1. Sinusne vibracije: provjeriti može li jedinica u vozilu izdržati sinusne vibracije sa sljedećim značajkama: konstantan pomak između 5 i 11 Hz: vršna amplituda 10 mm; konstantno ubrzanje između 11 i 300 Hz: 5 g. Ovaj se zahtjev provjerava putem norme IEC 60068-2-6, ispitivanje Fc, uz minimalno trajanje ispitivanja od 3 × 12 sati (12 sati po osi). Norma ISO 16750-3 ne zahtijeva ispitivanje na sinusne vibracije za uređaje smještene u odspojenoj kabini vozila. 2. Nasumične vibracije: Ispitivanje u skladu s normom ISO 16750-3: poglavljem 4.1.2.8: Test VIII: Commercial vehicle, decoupled vehicle cab. Ispitivanje na nasumične vibracije, 10...2 000 Hz, RMS okomito 21,3 m/s^2, RMS uzdužno 11,8 m/s^2, RMS bočno 13,1 m/s^2, 3 osi, 32 h po osi, uključujući temperaturni ciklus – 20…70 °C. Ovo se ispitivanje odnosi na normu IEC 60068-2-64: Environmental testing – Part 2–64: Tests– Test Fh: Vibration, broadband random and guidance. 3. Udarci: mehanički udarac s 3 g, polu-sinus, u skladu s normom ISO 16750. Prethodno opisana ispitivanja provode se na različitim uzorcima vrste opreme koja se ispituje.	219
4.4	Zaštita od vode i stranih tijela	Ispitivanje u skladu s normom ISO 20653: Road vehicles – Degree of protection (IP code) – Protection of electrical equipment against foreign objects, water and access (bez promjene parametara); minimalna vrijednost IP 40.	220, 221
4.5	Prenaponska zaštita	Provjeriti može li jedinica u vozilu izdržati snagu napajanja od: izvedbe od 24 V: 34 V pri +40 °C 1 sat, izvedbe od 12 V: 17 V pri +40 °C 1 sat (ISO 16750-2)	216
4.6	Zaštita od zamjene polariteta	Provjeriti može li jedinica u vozilu izdržati inverziju svojeg napajanja (ISO 16750-2)	216
4.7	Zaštita od kratkog spoja	Provjeriti jesu li ulazno/izlazni signali zaštićeni od kratkog spoja u odnosu na napajanje i uzemljenje (ISO 16750-2)	216
5.	**Ispitivanja elektromagnetske kompatibilnosti (EMC)**		
5.1	Emisije zračenja i osjetljivost	Shodnost s Pravilnikom ECE R10	218
5.2	Elektrostatičko pražnjenje	Shodnost s normom ISO 10605:2008 + Tehnički ispravak:2010 + AMD1:2014: +/–4 kV za kontakt i +/–8 kV za ispuštanje zraka	218
5.3	Osjetljivost napajanja na električne prelazne pojave	Za izvedbe od 24 V: shodnost s normom ISO 7637-2 + Pravilnik ECE-a br. 10, Rev. 3: impuls 1a: Vs = –450 V, Ri = 50 oma,	218

		impuls 2a: Vs = +37 V, Ri = 2 oma, impuls 2b: Vs = +20 V, Ri = 0,05 oma, impuls 3a: Vs = –150 V, Ri = 50 oma, impuls 3b: Vs = +150 V, Ri = 50 oma, impuls 4: Vs = –16 V, Va = –12 V, t6 = 100 ms, impuls 5: Vs = +120 V, Ri = 2,2 oma, td = 250 ms. Za izvedbe od 12 V: shodnost s normom ISO 7637-1 + Pravilnik ECE-a br. 10, Rev. 3: impuls 1: Vs = –75 V, Ri = 10 oma, impuls 2a: Vs = +37 V, Ri = 2 oma, impuls 2b: Vs = +10 V, Ri = 0,05 oma, impuls 3a: Vs = –112 V, Ri = 50 oma, impuls 3b: Vs = +75 V, Ri = 50 oma, impuls 4: Vs = –6 V, Va = –5 V, t6 = 15 ms, impuls 5: Vs = +65 V, Ri = 3 oma, td = 100 ms. Impuls 5 ispituje se samo za jedinice u vozilu namijenjene ugradnji u vozila na kojima se ne sprovodi jedinstvena vanjska zaštita od rasterećenja. Za prijedlog rasterećenja vidjeti normu ISO 16750-2, 4. izdatje, poglavlje 4.6.4.	

3. FUNKCIONALNA ISPITIVANJA SENZORA KRETANJA

Br.	Ispitivanje	Opis	Povezani zahtjevi
1.	**Administrativni pregled**		
1.1	Dokumentacija	Ispravnost dokumentacije	
2.	**Vizualni pregled**		
2.1.	Shodnost s dokumentacijom		
2.2.	Identifikacija/oznake		225, 226,
2.3	Materijali		219 do 223
2.4	Plombiranje		398, 401 do 405
3.	**Funkcionalna ispitivanja**		
3.1	Identifikacijski podaci senzora		95* do 97*
3.2	Uparivanje senzora kretanja i jedinice u vozilu		122*, 204
3.3	Detekcija kretanja Tačnost mjerenja kretanja		30 do 35
3.4	Sučelje jedinice u vozilu		02
3.5	Provjeriti je li senzor kretanja neosjetljiv na magnetsko polje. Alternativno, provjeriti reagira li senzor kretanja na konstantna magnetska polja koja ometaju detekciju kretanja vozila tako da spojena jedinica u vozilu može detektirati, zabilježiti i arhivirati pogreške senzora.		217
4.	**Ispitivanja utjecaja okoliša**		
4.1	Radna temperatura	Provjera funkcionalnosti (kako je određeno u ispitivanju br. 3.3) u temperaturnom rasponu [– 40 °C; + 135 °C] putem: IEC 60068-2-1, ispitivanje Ad, trajanje ispitivanja 96 sati pri najnižoj temperaturi To_{min}, IEC 60068-2-2, ispitivanje Bd, trajanje ispitivanja 96 sati pri najvišoj temperaturi To_{max}. Ispitivanje u skladu s ISO 16750-4, poglavlje 5.1.1.2.: ispitivanje rada pri niskoj temperaturi (24 h na – 40 °C). Ovo se ispitivanje odnosi na IEC 60068-2-1: Environmental testing – Part 2-1: Tests – Test A: Cold; IEC 68-2-2, ispitivanje Bd, trajanje ispitivanja 96 sati pri najnižoj temperaturi od – 40 °C. Ispitivanje u skladu s ISO 16750-4, poglavlje 5.1.2.2.: ispitivanje rada pri visokoj temperaturi (96 h na 135 °C). Ovo se ispitivanje odnosi na IEC 60068-2-2: Basic environmental testing procedures; Part 2: Tests; Tests B: Dry heat	213
4.2	Temperaturni ciklusi	Ispitivanje u skladu s ISO 16750-4, poglavlje 5.3.2.: brze promjene temperature s određenim trajanjem prelaska (– 40 °C/135 °C, 20 ciklusa, 30 min držanja pri svakoj temperaturi). IEC 60068-2-14: Environmental testing; Part 2-14: Tests; Test N: Change of temperature.	213
4.3	Ciklusi vlažnosti	Provjera funkcionalnosti (kako je određeno u ispitivanju br. 3.3) putem IEC 60068-2-30, ispitivanje Db, šest ciklusa u trajanju od 24 h, pri svakom primjena temperature od + 25°C do + 55°C i relativna vlažnost od 97 % pri + 25°C te od 93 % pri + 55°C.	214
4.4	Vibracije	ISO 16750-3, poglavlje 4.1.2.6., Test VI: Commercial vehicle, engine, gearbox. Ispitivanje na vibracije u mješovitom načinu, uključujući a) ispitivanje na sinusne vibracije, 20…520 Hz, 11,4 … 120 m/s^2, <= 0,5 okt/min; b) ispitivanje na nasumične vibracije, 10…2 000 Hz, RMS 177 m/s^2, 94 h po osi, uključujući temperaturni ciklus – 20…70 °C).	219

		Ovo se ispitivanje odnosi na IEC 60068-2-80: Environmental testing – Part 2-80: Tests – Test Fi: Vibration – Mixed mode.	
4.5	Mehanički udarac	ISO 16750-3, poglavlje 4.2.3., Test VI: Test for devices in or on the gearbox. Polu-sinusni udarac, ubrzanje treba dogovoriti u rasponu 3 000 …15 000 m/s^2, trajanje impulsa treba dogovoriti, međutim < 1 ms, broj udaraca: treba dogovoriti. Ovo se ispitivanje odnosi na IEC 60068-2-27: Environmental testing. Part 2: Tests. Test Ea and guidance: Shock.	219
4.6	Zaštita od vode i stranih tijela	Ispitivanje u skladu s ISO 20653: Road vehicles – Degree of protection (IP code) – Protection of electrical equipment against foreign objects, water and access (ciljana vrijednost IP 64)	220, 221
4.7	Zaštita od zamjene polariteta	Provjeriti može li senzor kretanja izdržati inverziju svojeg napajanja.	216
4.8	Zaštita od kratkog spoja	Provjeriti jesu li ulazno/izlazni signali zaštićeni od kratkog spoja u odnosu na napajanje i uzemljenje.	216
5.	**Elektromagnetska kompatibilnost (EMC)**		
5.1	Emisije zračenja i osjetljivost	Provjera shodnosti s Pravilnikom ECE R10	218
5.2	Elektrostatičko pražnjenje	Shodnost s ISO 10605:2008 + Tehnički ispravak:2010 + AMD1:2014: +/– 4 kV za kontakt i +/– 8 kV za ispuštanje zraka	218
5.3	Osjetljivost podatkovnih vodova na električne prelazne pojave	Za izvedbe od 24 V: shodnost s ISO 7637-2 + Pravilnik ECE-a br. 10, Rev. 3: impuls 1a: Vs = – 450V, Ri = 50 oma, impuls 2a: Vs = + 37V, Ri = 2 oma, impuls 2b: Vs = + 20V, Ri = 0,05 oma, impuls 3a: Vs = – 150V, Ri = 50 oma, impuls 3b: Vs = +150V, Ri = 50 oma, impuls 4: Vs = –16 V, Va = –12 V, t6 = 100 ms, impuls 5: Vs = + 120 V, Ri = 2,2 oma, td = 250 ms. Za izvedbe od 12V: shodnost s ISO 7637-1 + Pravilnik ECE-a br. 10, Rev. 3: impuls 1: Vs = – 75V, Ri = 10 oma, impuls 2a: Vs = + 37V, Ri = 2 oma, impuls 2b: Vs = + 10V, Ri = 0,05 oma, impuls 3a: Vs = – 112V, Ri = 50 oma, impuls 3b: Vs = +75V, Ri = 50 oma, impuls 4: Vs = – 6 V, Va = –5 V, t6 = 15 ms, impuls 5: Vs = + 65 V, Ri = 3 oma, td = 100 ms. Impuls 5 ispituje se samo za jedinice u vozilu namijenjene ugradnji u vozila na kojima se ne sprovodi jedinstvena vanjska zaštita od rasterećenja. Za prijedlog rasterećenja, vidjeti ISO 16750-2, 4. izdatje, poglavlje 4.6.4.	218

4. FUNKCIONALNA ISPITIVANJA TAHOGRAFSKIH KARTICA

Ispitivanja u skladu s ovim odjeljkom 4.,
br. 5 „Ispitivanja protokola”,
br. 6 „Struktura kartice” i
br. 7 „Funkcionalna ispitivanja”
može provesti osoba zadužena za evaluaciju ili certifikaciju tokom postupka sigurnosne certifikacije prema zajedničkim mjerilima (CC) za modul čipa.
Ispitivanja br. 2.3 i 4.2 jednaka su. To su mehanička ispitivanja kombinacije tijela kartice i modula čipa. Ako se jedan od tih sastavnih dijelova (tijelo kartice, modul čipa) promijeni, tada su potrebna ova ispitivanja.

Br.	**Ispitivanje**	**Opis**	**Povezani zahtjevi**
1.	**Administrativni pregled**		
1.1	Dokumentacija	Ispravnost dokumentacije	
2	**Tijelo kartice**		
2.1	Tiskani dizajn	Osigurati da su sva obilježja zaštite i vidljivi podaci ispravno ispisani na kartici i usklađeni. [Označitelj] Prilog 1.C, poglavlje 4.1. „Vidljivi podaci”, 227) Prednja stranica mora sadržiti: riječi „kartica vozača” ili „kontrolna kartica” ili „kartica radionice” ili „kartica preduzeće” tiskane velikim slovima na službenom jeziku ili jezicima države članice koja izdaje karticu, prema vrsti kartice; [Ime države članice] Prilog 1.C, poglavlje 4.1. „Vidljivi podaci”, 228) Prednja stranica mora sadržiti: ime države članice koja je izdala karticu (nije obvezno); [Razlikovna oznaka] Prilog 1.C, poglavlje 4.1. „Vidljivi podaci”, 229)	227 do 229, 232, 234 do 236

		Prednja stranica mora sadržiti: razlikovnu oznaku države članice koja izdaje karticu, tiskanu u negativu u plavom pravougaoniku i okruženu s 12 žutih zvijezda. [Numeriranje] Prilog 1.C, poglavlje 4.1. „Vidljivi podaci”, 232) Zadnja stranica mora sadržiti: objašnjenje numerisanih stavki na prednjoj stranici kartice. [Boja] Prilog 1.C, poglavlje 4.1. „Vidljivi podaci”, 234) Tahografske kartice moraju se štampati sa sljedećim prevladavajućim bojama pozadine: — kartica vozača: bijela, — kartica radionice: crvena, — kontrolna kartica: plava — kartica preduzeće: žuta. [Sigurnost] Prilog 1.C, poglavlje 4.1. „Vidljivi podaci”, 235) Tahografske kartice moraju imati barem sljedeća obilježja za zaštitu tijela kartice od krivotvorenja i neovlaštenog rukovanja: — sigurnosnu podlogu s tankim guilloche uzorcima i štampano s duginim efektom, — barem jednu dvobojnu liniju u mikrotisku. [Oznake] Prilog 1.C, poglavlje 4.1. „Vidljivi podaci”, 236) Države članice mogu dodavati boje i oznake kao što su nacionalni simboli i sigurnosna obilježja. [Homologacijska oznaka] Kartice tahografa moraju sadržiti homologacijsku oznaku. Homologacijsku oznaku čine: — pravougaonik, unutar kojeg se upisuje slovo „e”, nakon kojeg slijedi poznati broj ili slovo države koja je izdala homologaciju, — broj homologacije koji odgovara broju certifikata o homologaciji za tahografsku karticu, zapisan u neposrednoj blizini pravougaonika.	
2.2	Mehanička ispitivanja	[Veličina kartice] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7810 *Identification cards – Physical characteristics*, [5.] Dimenzije kartice, [5.1.] Veličina kartice, [5.1.1.] Dimenzije kartice i dopuštena odstepena, vrsta kartice ID-1 Neupotrijebljena kartica [Rubovi kartice] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7810 *Identification cards – Physical characteristics*, [5.] Dimenzije kartice, [5.1.] Veličina kartice, [5.1.2.] Rubovi kartice [Izrada kartice] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7810 *Identification cards – Physical characteristics*, [6.] Izrada kartice [Materijali kartice] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7810 *Identification cards – Physical characteristics*, [7.] Materijali kartice [Krutost pri savijanju] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7810 *Identification cards – Physical characteristics*, [8.] Karakteristike kartice, [8.1.] Krutost pri savijanju [Toksičnost] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7810 *Identification cards – Physical characteristics*, [8.] Karakteristike kartice, [8.3.] Toksičnost [Otpornost na kemikalije] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7810 *Identification cards – Physical characteristics*, [8.] Karakteristike kartice, [8.4.] Otpornost na kemikalije [Stabilnost kartice] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7810 *Identification cards – Physical characteristics*, [8.] Karakteristike kartice, [8.5.] Dimenzijska stabilnost kartice i izobličenje zbog temperature i vlage [Svjetlost]	240, 243 ISO/IEC 7810

		Tahografske kartice moraju biti u skladu s normom ISO/IEC 7810 *Identification cards – Physical characteristics*, [8.] Karakteristike kartice, [8.6.] Svjetlost [Trajnost] Prilog 1C, poglavlje 4.4. „Specifikacije okruženja i elektrotehničke specifikacije”, 241) Tahografske kartice moraju moći ispravno raditi tokom perioda od pet godina ako se upotrebljavaju u skladu sa specifikacijama okruženja i elektrotehničkim specifikacijama. [Čvrstoća ljuštenja] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7810 *Identification cards – Physical characteristics*, [8.] Karakteristike kartice, [8.8.] Čvrstoća ljuštenja [Prianjanje ili blokiranje] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7810 *Identification cards – Physical characteristics*, [8.] Karakteristike kartice, [8.9.] Prianjanje ili blokiranje [Izobličenje] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7810 *Identification cards – Physical characteristics*, [8.] Karakteristike kartice, [8.11.] Ukupno izobličenje kartice [Otpornost na toplinu] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7810 *Identification cards – Physical characteristics*, [8.] Karakteristike kartice, [8.12.] Otpornost na toplinu [Izobličenja površine] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7810 *Identification cards – Physical characteristics*, [8.] Karakteristike kartice, [8.13.] Izobličenja površine [Onečišćenje] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7810 *Identification cards – Physical characteristics*, [8.] Karakteristike kartice, [8.14.] Onečišćenje i međudjelovanje sastavnih dijelova kartice	
2.3	Mehanička ispitivanja s ugrađenim modulom čipa	[Savijanje] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7810:2003/Amd. 1:2009, *Identification cards – Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits*. [9.2.] Dinamičko opterećenje savijanjem Ukupni broj ciklusa savijanja: 4 000 . [Uvijanje (torzija)] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7810:2003/Amd. 1:2009, *Identification cards – Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits* [9.3.] Dinamičko opterećenje uvijanjem Ukupni broj ciklusa uvijanja: 4 000 .	ISO/IEC 7810
3	**Modul**		
3.1	Modul	Modul je kućište čipa i kontaktna pločica. [Profil površine] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7816-1:2011, *Identification cards – Integrated circuit cards – Part 1: Cards with contacts – Physical characteristics* [4.2.] Profil površine kontakata [Mehanička čvrstoća] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7816-1:2011, *Identification cards – Integrated circuit cards – Part 1: Cards with contacts – Physical characteristics* [4.3.] Mehanička čvrstoća (kartice i kontakata) [Električni otpor] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7816-1:2011, *Identification cards – Integrated circuit cards – Part 1: Cards with contacts – Physical characteristics* [4.4.] Električni otpor (kontakata) [Dimenzije] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7816-2:2007, *Identification cards – Integrated circuit cards – Part 2: Cards with contacts – Dimension and location of the contacts*	ISO/IEC 7816

		[3.] Dimenzije kontakata [Položaj] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7816-2:2007, *Identification cards – Integrated circuit cards – Part 2: Cards with contacts – Dimension and location of the contacts* [4.] Broj i položaj kontakata U slučaju modula sa šest kontakata, kontakti „C4" i „C8" nisu dio zahtjeva ovog ispitivanja.	
4	**Čip**		
4.1	Čip	[Radna temperatura] Čip tahografske kartice mora djelovati u rasponu temperature okoline između – 25 °C i + 85 °C. [Temperatura i vlažnost] Prilog 1C, poglavlje 4.4. „Specifikacije okruženja i elektrotehničke specifikacije", 241) Tahografske kartice moraju moći ispravno raditi u svim klimatskim uslovima uobičajenima na teritoriju Zajednice, pri temperaturnom rasponu od najmanje – 25 °C do + 70 °C s povremenim vršnim porastom do + 85 °C, pri čemu „povremeno" označava ne duže od 4 sata svaki puta i ne više od 100 puta tokom vijeka trajanja kartice. Tahografske kartice u uzastopnim se koracima izlažu sljedećim temperaturama i vlažnosti tokom određenog vremena. Nakon svakog koraka ispituje se električna funkcionalnost tahografskih kartica. 1. Temperatura od – 20 °C na 2 sata. 2. Temperatura od +/– 0 °C na 2 sata. 3. Temperatura od + 20 °C, relativna vlažnost 50 %, na 2 sata. 4. Temperatura od 50 °C, relativna vlažnost 50 %, na 2 sata. 5. Temperatura od + 70 °C, relativna vlažnost 50 %, na 2 sata. Temperatura se povremeno povećava na + 85 °C, relativna vlažnost 50 %, na 60 min. 6. Temperatura od + 70 °C, relativna vlažnost 85 %, na 2 sata. Temperatura se povremeno povećava na + 85 °C, relativna vlažnost 85 %, na 30 min. [Vlažnost] Prilog 1C, poglavlje 4.4. „Specifikacije okruženja i elektrotehničke specifikacije", 242) Tahografske kartice moraju moći ispravno raditi u rasponu vlažnosti između 10 % i 90 %. [Elektromagnetska kompatibilnost – EMC] Prilog 1C, poglavlje 4.4. „Specifikacije okruženja i elektrotehničke specifikacije", 244) Tokom rada, tahografske kartice moraju biti u skladu s Pravilnikom ECE R10 o elektromagnetskoj kompatibilnosti. [Statički elektricitet] Prilog 1C, poglavlje 4.4. „Specifikacije okruženja i elektrotehničke specifikacije", 244) Tokom rada, tahografske kartice moraju biti zaštićene od elektrostatičkih pražnjenja. Tahografske kartice moraju biti u skladu s normom ISO/IEC 7810:2003/Amd. 1:2009, *Identification cards – Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits* [9.4.] Statički elektricitet [9.4.1.] Elektroničke kartice s kontaktima Ispitni napon: 4 000 V. [Rendgenske zrake] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7810:2003/Amd. 1:2009, *Identification cards – Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits* [9.1.] Rendgenske zrake [Ultraljubičasto svjetlo] ISO/IEC 10373-1:2006, *Identification cards – Test methods – Part 1: General characteristics* [5.11.] Ultraljubičasto svjetlo [Uređaj za ispitivanje mehaničkog opterećenja kartice (*3-wheel*)] Tahografske kartice moraju biti u skladu s normom ISO/IEC 10373-1:2006/Amd. 1:2012, *Identification cards – Test methods – Part 1: General characteristics, Amendment 1.* [5.22.] ICC – Mehanička čvrstoća: *3-wheel* ispitivanje ICC-a s kontaktima [Savitljivost] Tahografske kartice moraju biti u skladu s normom MasterCard CQM V2.03:2013 [11.1.3.] R-L3-14-8: Ispitivanje izdržljivosti pri savijanju [13.2.1.32.] TM-422: Mehanička pouzdanost: Ispitivanje savitljivosti	241 do 244 ECE R10 ISO/IEC 7810 ISO/IEC 10373

4.2	Mehanička ispitivanja modula čipa ugrađenog u tijelo kartice -> isto kao 2.3.	[Savijanje] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7810:2003/Amd. 1:2009, *Identification cards – Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits*. [9.2.] Dinamičko opterećenje savijanjem Ukupni broj ciklusa savijanja: 4 000 . [Uvijanje (torzija)] Tahografske kartice moraju biti u skladu s normom ISO/IEC 7810:2003/Amd. 1:2009, *Identification cards – Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits*. [9.3] Dinamičko opterećenje uvijanjem Ukupni broj ciklusa uvijanja: 4 000 .	ISO/IEC 7810
5	**Ispitivanja protokola**		
5.1	ATR	Provjeriti shodnost ATR-a	ISO/IEC 7816-3 TCS_14, TCS_17, TCS_18
5.2	T = 0	Provjeriti shodnost protokola T = 0	ISO/IEC 7816-3 TCS_11, TCS_12, TCS_13, TCS_15
5.3	PTS	Provjeriti shodnost naredbe PTS postavljanjem s T = 0 na T = 1.	ISO/IEC 7816-3 TCS_12, TCS_19, TCS_20, TCS_21
5.4	T = 1	Provjeriti shodnost protokola T = 1	ISO/IEC 7816-3 TCS_11, TCS_13, TCS_16
6	**Struktura kartice**		
6.1		Ispitati shodnost strukture datoteke provjerom prisutnosti obveznih datoteka na kartici i uvjeta pristupa tim datotekama.	TCS_22 do TCS_28 TCS_140 do TCS_179
7	**Funkcionalna ispitivanja**		
7.1	Normalna obrada	Najmanje jednom ispitati svaku dopuštenu upotrebu svake naredbe (npr.: ispitivanje naredbe UPDATE BINARY (ažuriranje datoteke) s CLA = '00', CLA = '0C' s različitim parametrima P1, P2 i Lc). Provjeriti jesu li postupci doista provedeni na kartici (npr.: čitanjem datoteke za koju je izvršena naredba).	TCS_29 do TCS_139
7.2	Poruke o pogrešci	Najmanje jednom ispitati svaku poruku o pogrešci (kako je određeno u Dodatku 2.) za svaku naredbu. Najmanje jednom ispitati svaku generičku pogrešku (osim „**6400**" pogrešaka integriteta provjerenih tokom sigurnosne certifikacije).	
7.3	Slijed šifri (*cypher suite*) i normirani parametri domene		CSM_48, CSM_50
8	**Personalizacija**		
8.1	Optička personalizacija	Prilog 1C, poglavlje 4.1. „Vidljivi podaci", 230) Prednja stranica mora sadržiti: podatke karakteristične za izdatu karticu. Prilog 1C, poglavlje 4.1. „Vidljivi podaci", 231) Prednja stranica mora sadržiti: datume koji se pišu u obliku „dd/mm/gggg" ili „dd.mm.gggg." (dan, mjesec, godina). Prilog 1.C, poglavlje 4.1. „Vidljivi podaci", 235) Tahografske kartice moraju imati barem sljedeća obilježja za zaštitu tijela kartice od krivotvorenja i neovlaštenog rukovanja: — na prostoru za fotografiju, pozadina sa sigurnosnim uzorkom i fotografija moraju se preklapati.	230, 231, 235

5. ISPITIVANJA VANJSKOG UREĐAJA GNSS-A

Br.	**Ispitivanje**	**Opis**	**Povezani zahtjevi**
1.	**Administrativni pregled**		
1.1	Dokumentacija	Ispravnost dokumentacije	
2.	**Vizualna provjera vanjskog uređaja GNSS-a**		
2.1.	Shodnost s dokumentacijom		

2.2.	Identifikacija/oznake		224 do 226
2.3	Materijali		219 do 223
3.	**Funkcionalna ispitivanja**		
3.1	Identifikacijski podaci senzora		98.99
3.2	Povezivanje vanjskog uređaja GNSS-a i jedinice u vozilu		123, 205
3.3	Položaj GNSS-a		36, 37
3.4	Sučelje jedinice u vozilu kada je GNSS prijamnik vanjski u odnosu na jedinicu u vozilu		03
3.5	Slijed šifri (*cypher suite*) i normirani parametri domene		CSM_48, CSM_50
4.	**Ispitivanja utjecaja okoliša**		
4.1	Temperatura	Provjera funkcionalnost putem: ispitivanja u skladu s ISO 16750-4, poglavlje 5.1.1.2. Ispitivanje rada pri niskoj temperaturi (72 h na – 20 °C). Ovo se ispitivanje odnosi na IEC 60068-2-1: *Environmental testing – Part 2-1: Tests – Test A: Cold*. Ispitivanje u skladu s ISO 16750-4: poglavlje 5.1.2.2.: ispitivanje rada pri visokoj temperaturi (72 h na 70 °C). Ovo se ispitivanje odnosi na IEC 60068-2-2: *Basic environmental testing procedures; Part 2: Tests; Tests B: Dry heat.* Ispitivanje u skladu s ISO 16750-4, poglavlje 5.3.2.: brze promjene temperature s određenim trajanjem prelaska (– 20 °C/70 °C, 20 ciklusa, 1 h zadržavanja pri svakoj temperaturi). Skraćeni niz ispitivanja (između onih utvrđenih u odjeljku 3. ove tablice) može se obaviti pri nižoj temperaturi, višoj temperaturi i tokom temperaturnih ciklusa.	213
4.2	Vlažnost	Provjeriti može li jedinica u vozilu izdržati cikličnu vlažnost (ispitivanje toplinom) putem IEC 60068-2-30, ispitivanje Db, šest ciklusa u trajanju od 24 h, pri svakom promjena temperature od + 25°C do + 55°C i relativna vlažnost od 97 % pri + 25°C te od 93 % pri + 55°C.	214
4.3	Mehanički	1. Sinusne vibracije: provjeriti može li jedinica u vozilu izdržati sinusne vibracije sa sljedećim značajkama: konstantan pomak između 5 i 11 Hz: vršna amplituda 10 mm; konstantno ubrzanje između 11 i 300 Hz: 5 g. Ovaj se zahtjev provjerava putem IEC 60068-2-6, ispitivanje Fc, uz minimalno trajanje ispitivanja od 3 × 12 sati (12 sati po osi). Norma ISO 16750-3 ne zahtijeva ispitivanje na sinusne vibracije za uređaje smještene u odspojenoj kabini vozila. 2. Nasumične vibracije: Ispitivanje u skladu s ISO 16750-3, poglavlje 4.1.2.8., *Test VIII: Commercial vehicle, decoupled vehicle cab*. Ispitivanje na nasumične vibracije, 10…2 000 Hz, RMS vertikalno 21,3 m/s^2, RMS uzdužno 11,8 m/s^2, RMS bočno 13,1 m/s^2, 3 osi, 32 h po osi, uključujući temperaturni ciklus – 20…70 °C. Ovo se ispitivanje odnosi na IEC 60068-2-64: *Environmental testing – Part 2-64: Tests – Test Fh: Vibration, broadband random and guidance*. 3. Udarci: mehanički udarac s 3 g, polu-sinus, u skladu s ISO 16750. Prethodno opisana ispitivanja provode se na različitim uzorcima vrste opreme koja se ispituje.	219
4.4	Zaštita od vode i stranih tijela	Ispitivanje u skladu s ISO 20653: Road vehicles – Degree of protection (IP code) – Protection of electrical equipment against foreign objects, water and access (bez promjene parametara).	220, 221
4.5	Prenaponska zaštita	Provjeriti može li jedinica u vozilu izdržati snagu napajanja od: izvedbe od 24 V: 34 V pri + 40 °C 1 sat, izvedbe od 12 V: 17 V pri + 40 °C 1 sat. (ISO 16750-2, poglavlje 4.3.)	216
4.6	Zaštita od zamjene polariteta	Provjeriti može li jedinica u vozilu izdržati inverziju svojeg napajanja. (ISO 16750-2, poglavlje 4.7.)	216
4.7	Zaštita od kratkog spoja	Provjeriti jesu li ulazno/izlazni signali zaštićeni od kratkog spoja u odnosu na napajanje i uzemljenje. (ISO 16750-2, poglavlje 4.10.)	216
5	**Ispitivanja elektromagnetske kompatibilnosti (EMC)**		
5.1	Emisije zračenja i osjetljivosti	Shodnost s Pravilnikom ECE R10	218
5.2	Elektrostatičko pražnjenje	Shodnost s ISO 10605:2008 + Tehnički ispravak:2010 + AMD1:2014: +/– 4 kV za kontakt i +/– 8 kV za ispuštanje zraka	218
5.3	Osjetljivost napajanja na električne prelazne pojave	Za izvedbe od 24 V: shodnost s ISO 7637-2 + Pravilnik ECE-a br. 10, Rev. 3: impuls 1a: Vs = – 450V, Ri = 50 oma, impuls 2a: Vs = + 37V, Ri = 2 oma, impuls 2b: Vs = + 20V, Ri = 0,05 oma, impuls 3a: Vs = – 150V, Ri = 50 oma, impuls 3b: Vs = + 150V, Ri = 50 oma, impuls 4: Vs = – 16 V, Va = – 12 V, t6 = 100 ms,	218

		impuls 5: Vs = + 120 V, Ri = 2,2 oma, td = 250 ms. Za izvedbe od 12 V: shodnost s ISO 7637-1 + Pravilnik ECE-a br. 10, Rev. 3: impuls 1: Vs = – 75 V, Ri = 10 oma, impuls 2a: Vs = + 37 V, Ri = 2 oma, impuls 2b: Vs = + 10 V, Ri = 0,05 oma, impuls 3a: Vs = –112 V, Ri = 50 oma, impuls 3b: Vs = + 75 V, Ri = 50 oma, impuls 4: Vs = – 6 V, Va = – 5 V, t6 = 15 ms, impuls 5: Vs = + 65 V, Ri = 3 oma, td = 100 ms. Impuls 5 ispituje se samo za jedinice u vozilu namijenjene ugradnji u vozila na kojima se ne sprovodi jedinstvena vanjska zaštita od rasterećenja. Za prijedlog rasterećenja, vidjeti ISO 16750-2, 4. izdatje, poglavlje 4.6.4.	

6. ISPITIVANJE VANJSKIH UREĐAJA ZA KOMUNIKACIJU NA DALJINU

Br.	Ispitivanje	Opis	Povezani zahtjevi
1.	**Administrativni pregled**		
1.1	Dokumentacija	Ispravnost dokumentacije	
2.	**Vizualni pregled**		
2.1	Shodnost s dokumentacijom		
2.2	Identifikacija/oznake		225, 226
2.3	Materijali		219 do 223
3.	**Funkcionalna ispitivanja**		
3.1	Komunikacija na daljinu za ciljane provjere na putu		4, 197 do 199
3.2	Bilježenje i arhiviranje u podatkovnoj memoriji		91
3.3	Komunikacija s jedinicom u vozilu		Dodatak 14., DSC_66 do DSC_70, DSC_71 do DSC_76
4.	**Ispitivanja utjecaja okoliša**		
4.1	Temperatura	Provjera funkcionalnosti putem: Ispitivanja u skladu s normom ISO 16750-4, poglavljem 5.1.1.2: ispitivanje rada pri niskoj temperaturi (72 h na –20 °C) Ovo se ispitivanje odnosi na normu IEC 60068-2-1: Environmental testing – Part 2-1: Tests – Test A: Cold. Ispitivanje u skladu s normom ISO 16750-4: poglavljem 5.1.2.2: ispitivanje rada pri visokoj temperaturi (72 h na 70 °C). Ovo se ispitivanje odnosi na normu IEC 60068-2-2: Basic environmental testing procedures; part 2: tests; tests B: dry heat. Ispitivanje u skladu s normom ISO 16750-4: poglavljem 5.3.2: brze promjene temperature s određenim trajanjem prelaska (– 20 °C / 70 °C, 20 ciklusa, 1 h zadržavanja pri svakoj temperaturi). Skraćeni niz ispitivanja (između onih utvrđenih u odjeljku 3. ove tablice) može se obaviti pri nižoj temperaturi, višoj temperaturi i tokom temperaturnih ciklusa.	213
4.2	Zaštita od vode i stranih tijela	Ispitivanje u skladu s normom ISO 20653: Road vehicles – Degree of protection (IP code) – Protection of electrical equipment against foreign objects, water and access (targeted value IP40).	220, 221
5	**Ispitivanja elektromagnetske kompatibilnosti (EMC)**		
5.1	Emisije zračenja i osjetljivost	Shodnost s Pravilnikom ECE R10	218
5.2	Elektrostatičko pražnjenje	Shodnost s normom ISO 10605:2008 + Tehnički ispravak:2010 + AMD1:2014: +/–4 kV za kontakt i +/–8 kV za ispuštanje zraka	218
5.3	Osjetljivost napajanja na električne prelazne pojave	Za izvedbe od 24 V: shodnost s normom ISO 7637-2 + Pravilnik ECE-a br. 10, Rev. 3: impuls 1a: Vs = –450 V, Ri = 50 oma, impuls 2a: Vs = +37 V, Ri = 2 oma, impuls 2b: Vs = +20 V, Ri = 0,05 oma, impuls 3a: Vs = –150 V, Ri = 50 oma, impuls 3b: Vs = +150 V, Ri = 50 oma, impuls 4: Vs = –16 V, Va = –12 V, t6 = 100 ms, impuls 5: Vs = +120 V, Ri = 2,2 oma, td = 250 ms. Za izvedbe od 12 V: shodnost s normom ISO 7637-1 + Pravilnik ECE-a br. 10, Rev. 3: impuls 1: Vs = –75 V, Ri = 10 oma, impuls 2a: Vs = +37 V, Ri = 2 oma, impuls 2b: Vs = +10 V, Ri = 0,05 oma, impuls 3a: Vs = –112 V, Ri = 50 oma, impuls 3b: Vs = +75 V, Ri = 50 oma, impuls 4: Vs = –6 V, Va = –5 V, t6 = 15 ms, impuls 5: Vs = +65 V, Ri = 3 oma, td = 100 ms. Impuls 5 ispituje se samo za jedinice u vozilu namijenjene ugradnji u vozila na kojima se ne sprovodi jedinstvena vanjska zaštita od rasterećenja. Za prijedlog rasterećenja vidjeti normu ISO 16750-2, 4. izdatje,	218

		poglavlje 4.6.4.	

7. FUNKCIONALNA ISPITIVANJA PAPIRA

Br.	Ispitivanje	Opis	Povezani zahtjevi
1.	**Administrativni pregled**		
1.1	Dokumentacija	Ispravnost dokumentacije	
2	**Opća ispitivanja**		
2.1	Broj slovnih znakova po retku	Vizualni pregled ispisa.	172
2.2	Najmanja veličina znaka	Vizualni pregled ispisa i pregled znakova.	173
2.3	Podržani skupovi znakova	Pisač mora podržavati znakove navedene u Dodatku 1. poglavlju 4. „Skupovi znakova".	174
2.4	Određivanje ispisa	Provjera homologacije tahografa i vizualni pregled ispisa	174
2.5	Čitljivost i identifikacija ispisa	Pregled ispisa: dokazuje se izvješćima o ispitivanju i protokolima ispitivanja proizvođača. Svi homologacijski brojevi tahografa s kojima se može upotrebljavati papir pisača otisnuti su na papiru.	175, 177, 178
2.6	Dodavanje rukom pisanih napomena	Vizualni pregled: dostupno je polje za potpis vozača. Dostupna su polja za ostale dodatne rukom pisane unose.	180
2.7	Dodatne pojedinosti o stranicama papira	Prednja i zadnja stranica papira mogu uključivati dodatne pojedinosti i informacije. Ove dodatne pojedinosti i informacije ne smiju utjecati na čitljivost ispisa. Vizualni pregled.	177, 178
3	**Ispitivanja skladištenja**		
3.1	Suha toplina	Pretkondicioniranje: 16 sati pri temperaturi + 23 °C ± 2 °C i relativnoj vlažnosti 55 % ± 3 %. Ispitno okruženje: 72 sata pri + 70 °C ± 2 °C. Obnavljanje: 16 sati pri + 23 °C ± 2 °C i relativnoj vlažnosti 55 % ± 3 %.	176, 178 IEC 60068-2-2-Bb
2.2	Toplina s vlagom	Pretkondicioniranje: 16 sati pri temperaturi + 23 °C ± 2 °C i relativnoj vlažnosti 55 % ± 3 %. Ispitno okruženje: 144 sata pri + 55 °C ± 2 °C i relativnoj vlažnosti 93 % ± 3 %. Obnavljanje: 16 sati pri + 23 °C ± 2 °C i relativnoj vlažnosti 55 % ± 3 %.	176, 178 IEC 60068-2-78-Cab
4	**Ispitivanja papira u upotrebi**		
4.1	Otpornost podloge na vlagu (neispisani papir)	Pretkondicioniranje: 16 sati pri + 23 °C ± 2 °C i relativnoj vlažnosti 55 % ± 3 %. Ispitno okruženje: 144 sata pri + 55 °C ± 2 °C i relativnoj vlažnosti 93 % ± 3 %. Obnavljanje: 16 sati pri + 23 °C ± 2 °C i relativnoj vlažnosti 55 % ± 3 %.	176 do 178 IEC 60068-2-78-Cab
4.2	Kvaliteta ispisa	Pretkondicioniranje: 24 sata pri + 40 °C ± 2 °C i relativnoj vlažnosti 93 % ± 3 %. Ispitno okruženje: ispis izrađen pri + 23 °C ± 2 °C. Obnavljanje: 16 sati pri + 23 °C ± 2 °C i relativnoj vlažnosti 55 % ± 3 %.	176, 178
4.3	Otpornost na toplinu	Pretkondicioniranje: 16 sati pri + 23 °C ± 2 °C i relativnoj vlažnosti 55 % ± 3 %. Ispitno okruženje: 2 sata pri + 70 °C ± 2 °C, suha toplina. Obnavljanje: 16 sati pri + 23 °C ± 2 °C i relativnoj vlažnosti 55 % ± 3 %.	176, 178 IEC 60068-2-2-Bb
4.4	Otpornost na niske temperature	Pretkondicioniranje: 16 sati pri + 23 °C ± 2 °C i relativnoj vlažnosti 55 % ± 3 %. Ispitno okruženje: 24 sata – 20°C ± 3 °C, suha hladnoća. Obnavljanje: 16 sati pri + 23 °C ± 2 °C i relativnoj vlažnosti 55 % ± 3 %.	176 do 178 ISO 60068-2-1-Ab
4.5	Otpornost na svjetlo	Pretkondicioniranje: 16 sati pri + 23 °C ± 2 °C i relativnoj vlažnosti 55 % ± 3 %. Ispitno okruženje: 100 sati s osvijetljenošću od 5 000 luksa, pri + 23 °C ± 2 °C i relativnoj vlažnosti 55 % ± 3 %. Obnavljanje: 16 sati pri + 23 °C ± 2 °C i relativnoj vlažnosti 55 % ± 3 %.	176, 178

Mjerila čitljivosti za ispitivanja 3.x i 4.x:
Čitljivost ispisa osigurana je ako optičke gustoće ispunjavaju sljedeće granične vrijednosti:
ispisani znakovi: min. 1,0;
pozadina (neispisani papir): maks. 0,2.
Optičke gustoće dobivenih ispisa mjere se u skladu s DIN EN ISO 534.
Ispisi ne smiju pokazivati promjene dimenzija i moraju ostati jasno čitljivi.

8. ISPITIVANJA INTEROPERABILNOSTI

Br.	Ispitivanje	Opis
8.1.	Ispitivanja interoperabilnosti između jedinica u vozilu i tahografskih kartica	
1	Uzajamna autentifikacija	Provjeriti odvija li se uzajamna autentifikacija između jedinice u vozilu i kartice tahografa normalno.
2	Ispitivanja pisanja/čitanja	Na jedinici u vozilu izvršiti tipičan scenarij aktivnosti. Scenarij se prilagođava vrsti kartice koja se ispituje i uključuje upise u što je više moguće elementarnih datoteka (EF) na kartici. Na jedinici u vozilu koja preuzima podatke provjeriti jesu li svi odgovarajući zapisi ispravno zabilježeni.

		Na kartici koja preuzima podatke provjeriti jesu li svi odgovarajući zapisi ispravno zabilježeni. Putem dnevnih ispisa provjeriti mogu li se svi odgovarajući zapisi ispravno pročitati.
8.2. Ispitivanja interoperabilnosti između jedinica u vozilu i senzora kretanja		
1	Uparivanje	Provjeriti odvija li se uparivanje između jedinice u vozilu i senzora kretanja normalno.
2	Ispitivanja aktivnosti	Na senzoru kretanja izvršiti tipičan scenarij aktivnosti. Scenarij uključuje uobičajenu aktivnost i stvaranje što je moguće više događaja ili kvarova. Na jedinici u vozilu koja preuzima podatke provjeriti jesu li svi odgovarajući zapisi ispravno zabilježeni. Na kartici koja preuzima podatke provjeriti jesu li svi odgovarajući zapisi ispravno zabilježeni. Putem dnevnog ispisa provjeriti mogu li se svi odgovarajući zapisi ispravno pročitati.
8.3. Ispitivanja interoperabilnosti između jedinica u vozilu i vanjskih uređaja GNSS-a (ako je primjenjivo)		
1	Uzajamna autentifikacija	Provjeriti odvija li se uzajamna autentifikacija (povezivanje) između jedinice u vozilu i vanjskog uređaja GNSS-a normalno.
2	Ispitivanja aktivnosti	Na vanjskom uređaju GNSS-a izvršiti tipičan scenarij aktivnosti. Scenarij uključuje uobičajenu aktivnost i stvaranje što je moguće više događaja ili kvarova. Na jedinici u vozilu koja preuzima podatke provjeriti jesu li svi odgovarajući zapisi ispravno zabilježeni. Na kartici koja preuzima podatke provjeriti jesu li svi odgovarajući zapisi ispravno zabilježeni. Putem dnevnog ispisa provjeriti mogu li se svi odgovarajući zapisi ispravno pročitati.

Dodatak 10

SIGURNOSNI ZAHTJEVI

U ovom se Dodatku navode zahtjevi u pogledu informatičke sigurnosti za sastavne dijelove uređaja za bilježenje podataka.

SEC_001 Sljedeći sastavni dijelovi uređaja za bilježenje podataka podliježu sigurnosnoj certifikaciji u skladu sa šemom zajedničkih mjerila:

— jedinica u vozilu,

— tahografska kartica,

— senzor kretanja,

— vanjski uređaj GNSS-a.

SEC_002 Minimalni zahtjevi u pogledu informatičke sigurnosti koje treba ispuniti svaki sastavni dio koji podliježe sigurnosnoj certifikaciji utvrđuju se u profilu zaštite sastavnog dijela u skladu sa šemom zajedničkih mjerila.

SEC_003 Evropski komisija osigurava da su četiri profila zaštite usklađena s ovim Prilogom sponzorirana, razvijena i odobrena od strane državnih tijela nadležnih za certifikaciju informatičke sigurnosti organiziranih unutar Radne skupine za zajedničko tumačenje (eng. *Joint Interpretation Working Group*, JIWG) koja podržava uzajamno priznavanje certifikata u okviru evropskog Sporazuma o uzajamnom priznavanju certifikata o evaluaciji sigurnosti informacijske tehnologije, i da su ti profili registrirani:

— profil zaštite za jedinicu u vozilu,

— profil zaštite za tahografsku karticu,

— profil zaštite za senzor kretanja,

— profil zaštite za vanjski uređaj GNSS-a.

Profil zaštite za jedinicu u vozilu odnosi se na slučajeve kada je jedinica u vozilu (VU) namijenjena za upotrebu s vanjskim uređajem GNSS-a i kada nije. U prvom su slučaju sigurnosni zahtjevi za vanjski uređaj GNSS-a navedeni u posebnom profilu zaštite.

SEC_004 Proizvođači sastavnih dijelova prema potrebi dorađuju i dovršavaju profil zaštite za odgovarajući sastavni dio, bez izmjena ili brisanja postojećih opasnosti, ciljeva, načina postepena i propisanih funkcija za provedbu sigurnosti kako bi utvrdili sigurnosni cilj u odnosu na koji mogu zatražiti sigurnosnu certifikaciju sastavnog dijela.

SEC_005 Tokom postupka evaluacije mora se dati izjava o strogoj shodnosti takvog posebnog sigurnosnog cilja s odgovarajućim profilom zaštite.

SEC_006 Nivo osiguranja za svaki profil zaštite je nivo EAL4 pojačana s komponentama osiguranja ATE_DPT.2 i AVA_VAN.5.

Dodatak 11.

ZAJEDNIČKI SIGURNOSNI MEHANIZMI

SADRŽAJ

PREAMBULA

U ovom se Dodatku propisuju sigurnosni mehanizmi kojima se osiguravaju:

— uzajamna autentifikacija između različitih sastavnih dijelova opreme u sistemu tahografa;

— povjerljivost, integritet, autentičnost i/ili nepobitnost podataka koji se prenose između različitih sastavnih dijelova sistema tahografa ili koji se preuzimaju na vanjske medije za arhiviranje podataka.

Ovaj se Dodatak sastoji od dva dijela. U dijelu A utvrđeni su sigurnosni mehanizmi za sistem tahografa prve generacije (digitalni tahograf). U dijelu B utvrđeni su sigurnosni mehanizmi za sistem tahografa druge generacije (pametni tahograf).

Mehanizmi iz dijela A ovog Dodatka primjenjuju se ako najmanje jedan sastavni dio sistema tahografa uključenog u postupak uzajamne autentifikacije i/ili prenosa podataka pripada opremi prve generacije.

Mehanizmi iz dijela B ovog Dodatka primjenjuju se ako oba sastavna dijela sistema tahografa uključenog u postupak uzajamne autentifikacije i/ili prenosa podataka pripadaju opremi druge generacije.

U Dodatku 15. navedeno je više informacija o upotrebi sastavnih dijelova prve generacije u kombinaciji sa sastavnim dijelovima druge generacije.

DIO A

SISTEM TAHOGRAFA PRVE GENERACIJE

1. UVOD

1.1. Referentni dokumenti:

U ovom su Dodatku upotrijebljeni sljedeći izvori:

SHA-1 Nacionalni institut za norme i tehnologiju SAD-a (NIST), FIPS Publication 180-1 (Publikacija FIPS 180-1): Secure Hash Standard, travanj 1995.

PKCS1 Laboratoriji RSA. PKCS # 1: RSA Encryption Standard, verzija 2.0, listopad 1998.

TDES Nacionalni institut za norme i tehnologiju SAD-a (NIST), FIPS Publication 46-3 Data Encryption Standard, nacrt, 1999.

TDES-OP ANSI X9.52, Triple Data Encryption Algorithm Modes of Operation, 1998.

ISO/IEC 7816-4 Information Technology – Identification cards – Integrated circuit(s) cards with contacts – Part 4: Interindustry commands for interexchange. Prvo izdatje, 1995. + Izmjena 1.: 1997.

ISO/IEC 7816-6 Information Technology – Identification cards – Integrated circuit(s) cards with contacts – Part 6: Interindustry data elements. Prvo izdatje, 1996. + ispravak 1., 1998.

ISO/IEC 7816-8 Information Technology – Identification cards – Integrated circuit(s) cards with contacts – Part 8: Security related interindustry commands. Prvo izdatje, 1999.

ISO/IEC 9796-2 Information Technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Mechanisms using a hash function. Prvo izdatje, 1997.

ISO/IEC 9798-3 Information Technology – Security techniques – Entity authentication mechanisms – Part 3: Entity authentication using a public key algorithm. Drugo izdatje, 1998.

ISO 16844-3 Road vehicles – Tachograph systems – Part 3: Motion sensor interface.

1.2. Označivanje i skraćenice

U ovom se Dodatku upotrebljavaju sljedeće oznake i skraćenice:

(Ka, Kb, Kc) snop ključeva koji upotrebljava algoritam za trostruko šifriranje podataka,
CA certifikacijsko tijelo (eng. Certification Authority),
CAR upućivanje na certifikacijsko tijelo (eng. Certification Authority Reference),
CC kriptografski kontrolni zbir (eng. Cryptographic Checksum),
CG kriptogram (eng. Cryptogram),
CH zaglavlje naredbe (eng. Command Header),
CHA ovlaštenje nosioca certifikata (eng. Certificate Holder Authorisation),
CHR upućivanje na nosioca certifikata (eng. Certificate Holder Reference),
D() dešifriranje s pomoću DES-a,
DE podatkovni element (eng. Data Element),
DO podatkovni objekt (eng. Data Object),
d privatni ključ RSA, privatni eksponent,
e javni ključ RSA, javni eksponent,
E() šifriranje s pomoću DES-a,
EQT oprema (eng. Equipment),
Hash() vrijednost raspršene poruke, izlazni podatak Hash,
Hash funkcija raspršivanja (eng. hash),
KID identifikator ključa (eng. Key Identifier),
Km ključ TDES. Glavni ključ definisan u normi ISO 16844-3,
KmVU ključ TDES unesen u jedinice u vozilu,
KmWC ključ TDES unesen na kartice radionica,
m predstavnik poruke, cijeli broj između 0 i n–1,
n ključevi RSA, modul,
PB bajtovi za popunjenje (eng. Padding Bytes),
PI bajt indikatora popunjenja (za kriptograme povjerljivih podatkovnih objekata) (eng. Padding Indicator byte),
PV nešifrirana vrijednost (eng. Plain Value),
s predstavnik potpisa, cijeli broj između 0 i n–1,
SSC brojač redoslijeda slanja (eng. Send Sequence Counter),
SM siguran prenos poruka (eng. Secure Messaging),
TCBC način rada „ulančavanje šifriranih blokova TDEA" (eng. TDEA Cipher Block Chaining Mode of Operation),
TDEA algoritam trostrukog šifriranja podataka (eng. Triple Data Encryption Algorithm),
TLV vrijednost dužine oznake (eng. Tag Length Value),
VU jedinica u vozilu (eng. Vehicle Unit),
X.C certifikat korisnika X koji izdaje certifikacijsko tijelo,
X.CA certifikacijsko tijelo korisnika X,
X.CA.PK o X.C radnja otvaranja certifikata za izdvajanje javnog ključa. To je infiksni operator čiji je lijevi operand javni ključ certifikacijskog tijela, a desni operand je certifikat koji izdaje navedeno certifikacijsko tijelo. Ishod je javni ključ korisnika X čiji je certifikat desni operand,
X.PK privatni ključ RSA korisnika X,
X.PK[I] šifra RSA nekog podatka I, upotrebom javnog ključa korisnika X,
X.SK privatni ključ RSA korisnika X,
X.SK[I] šifra RSA nekog podatka I, upotrebom privatnog ključa korisnika X,
„xx" heksadecimalna vrijednost,
|| operator ulančavanja.

2. KRIPTOGRAFSKI SISTEMI I ALGORITMI

2.1. Kriptografski sistemi

CSM_001 U jedinicama u vozilu i tahografskim karticama upotrebljava se klasičan kriptografski sistem javnog ključa RSA kojim se osiguravaju sljedeći sigurnosni mehanizmi:

— autentifikacija između jedinica u vozilu i kartica,
— prenos ključeva trostrukog procesa DES između jedinica u vozilu i tahografskih kartica,
— digitalni potpis podataka preuzetih s jedinica u vozilu ili tahografskih kartica na vanjske medije.

CSM_002 U jedinicama u vozilu i tahografskim karticama upotrebljava se trostruki simetričan kriptografski sistem DES za osiguranje mehanizma integriteta podataka tokom razmjene korisničkih podataka između jedinica u vozilu i tahografskih kartica te za osiguranje, ako je primjereno, povjerljivosti razmjene podataka između jedinica u vozilu i tahografskih kartica.

2.2. Kriptografski algoritmi

2.2.1 *Algoritam RSA*

CSM_003 Algoritam RSA u potpunosti je definisan sljedećim odnosima:

$X.SK[m] = s = m^d \bmod n$

$X.PK[s] = m = s^e \bmod n$

Potpuniji opis funkcije RSA može se naći u izvoru [PKCS1]. Javni eksponent e za izračun RSA cijeli je broj između 3 i n–1 koji zadovoljava gcd(e, lcm(p–1, q–1)) = 1.

2.2.2 *Algoritam raspršivanja*

CSM_004 Mehanizmi digitalnog potpisa upotrebljavaju algoritam raspršivanja (*hash*) SHA-1 definisan u izvoru [SHA-1].

2.2.3 *Algoritam šifriranja podataka*

CSM_005 Algoritmi utemeljeni na DES-u upotrebljavaju se u načinu rada „ulančavanje šifriranih blokova”.

3. KLJUČEVI I CERTIFIKATI

3.1. Generisanje i raspodjela ključeva

3.1.1 *Generisanje i raspodjela ključeva RSA*

CSM_006 Ključevi RSA generišu se preko tri funkcionalne hijerarhijske razine:

— evropski nivo,

— nivo države članice,

— nivo opreme.

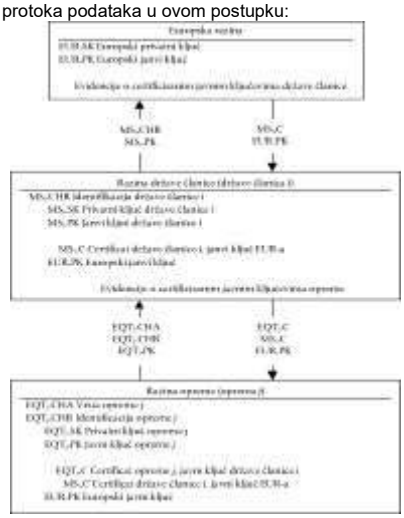
CSM_007 Na evropskoj se nivou generiše jedinstveni evropski par ključeva (EUR.SK i EUR.PK). Evropski privatni ključ upotrebljava se za certifikaciju javnih ključeva država članica. Potrebno je voditi evidenciju svih certificiranih ključeva. Te zadatke obavlja evropsko certifikacijsko tijelo, pod nadležnošću i odgovornosti Evropske komisije.

CSM_008 Na nivou države članice generiše se par ključeva države članice (MS.SK i MS.PK). Javne ključeve država članica certificira evropsko certifikacijsko tijelo. Privatni ključ države članice upotrebljava se za certificiranje javnih ključeva koji se unose u opremu (jedinica u vozilu ili tahografska kartica). Evidencija svih certificiranih javnih ključeva vodi se zajedno s identifikacijom opreme za koju su namijenjeni. Te zadatke obavlja certifikacijsko tijelo države članice. Država članica može redovito mijenjati svoj par ključeva.

CSM_009 Na nivou opreme generiše se jedan pojedinačni par ključeva (EQT.SK i EQT.PK) i unosi u svaki dio opreme. Javne ključeve opreme certificira certifikacijsko tijelo države članice. Te zadatke mogu obavljati proizvođači opreme, izvođači personalizacije opreme ili nadležna tijela države članice. Taj se par ključeva upotrebljava za usluge autentifikacije, digitalnog potpisa i šifriranja.

CSM_010 Povjerljivost privatnih ključeva održava se tokom generisanja, prenosa (ako postoji) i čuvanja.

Na sljedećoj je slici sažeti prikaz protoka podataka u ovom postupku:



3.1.2 *Ispitni ključevi RSA*

CSM_011 U svrhu ispitivanja opreme (uključujući ispitivanje interoperabilnosti) evropsko certifikacijsko tijelo generiše različit jedinstveni evropski par ispitnih ključeva i najmanje dva para ispitnih ključeva države članice, čiji se javni ključevi certificiraju evropskim privatnim ispitnim ključem. U opremu koja podliježe homologaciji proizvođači unose ispitne ključeve certifikovane jednim od tih ispitnih ključeva države članice.

3.1.3 *Ključevi senzora kretanja*

Povjerljivost triju ključeva trostrukog DES-a koji su opisani u nastavu održava se na odgovarajući način tokom generisanja, prenosa (ako postoji) i čuvanja.

Za podršku sastavnim dijelovima tahografa koji zadovoljavaju normu ISO 16844, evropsko certifikacijsko tijelo i certifikacijska tijela država članica dodatno osiguravaju sljedeće:

CSM_036 Evropsko certifikacijsko tijelo generiše KmVU i KmWC, dva neovisna i jedinstvena ključa trostrukog DES-a, te generiše Km kao:

$Km = Km_{VU}$ XOR Km_{WC}.

Evropsko certifikacijsko tijelo dostavlja navedene ključeve certifikacijskim tijelima država članica u odgovarajuće zaštićenim postupcima, na njihov zahtjev.

CSM_037 Certifikacijska tijela država članica:

— upotrebljavaju Km za šifriranje podataka senzora kretanja koje traže proizvođači senzora kretanja (podaci koji se šifriraju s Km definisani su u normi ISO 16844-3),
— u odgovarajuće zaštićenim postupcima proizvođačima jedinica u vozilu dostavljaju Km_{VU} za unošenje u jedinice u vozilu,
— osiguravaju unos ključa Km_{WC} u sve kartice radionica (SensorInstallationSecData u elementarnoj datoteci Sensor_Installation_Data) tokom personalizacije kartice.

3.1.4 ***Generisanje i raspodjela T-DES ključeva razmjene podataka***

CSM_012 Jedinice u vozilu i tahografske kartice, kao dio postupka uzajamne autentifikacije, generišu i razmjenjuju podatke potrebne za izradu zajedničkog ključa trostrukog procesa DES-a. Povjerljivost te razmjene podataka zaštićena je mehanizmom šifriranja RSA.

CSM_013 Ovaj se ključ upotrebljava za sve naredne kriptografske radnje koje upotrebljavaju siguran prenos poruka. Njegova važnost ističe na kraju razmjene podataka (povlačenje kartice ili povraćaj kartice u početno stanje) *i*/ili nakon 240 upotreba (jedna upotreba ključa = jedna naredba koja upotrebljava sigurni prenos poruka upućena kartici i odgovarajući odgovor).

3.2. Ključevi

CSM_014 Ključevi RSA imaju (bez obzira na razinu) sljedeće dužine: modul *n* 1 024 bita, javni eksponent *e* najviše 64 bita, privatni eksponent *d* 1 024 bita.

CSM_015 Ključevi trostrukog DES-a imaju oblik (K_a, K_b, K_a) pri čemu su K_a i K_b neovisni ključevi dužine 64 bita. Ne smiju biti namješteni bitovi koji utvrđuju paritetnu grešku.

3.3. Certifikati

CSM_016 Certifikati javnih ključeva su „nesamoopisni", „karticom provjerljivi" certifikati (izvor: ISO/IEC 7816-8).

3.3.1 ***Sadržaj certifikata***

CSM_017 Certifikati javnih ključeva RSA ugrađeni su u sljedeće podatke sljedećim redom:

Podaci	**Format**	**Bajtova**	**Opis**
CPI	CIJELI BROJ	1	Identifikator profila certifikata (u ovoj verziji „01")
CAR	OKTETNI NIZ	8	Upućivanje na certifikacijsko tijelo
CHA	OKTETNI NIZ	7	Ovlaštenje nosioca certifikata
EOV	TimeReal	4	Istek važnosti certifikata. Nije obvezno, popunjava se s „FF" ako se ne upotrebljava.
CHR	OKTETNI NIZ	8	Upućivanje na nosioca certifikata
n	OKTETNI NIZ	128	Javni ključ (modul)
e	OKTETNI NIZ	8	Javni ključ (javni eksponent)
		164	

Napomene:

1. „Identifikator profila certifikata" (CPI) označava tačnu strukturu autentifikacijskog certifikata. Može se upotrebljavati kao unutarnji identifikator opreme iz zaglavlja odgovarajućeg popisa koji opisuje ulančavanje podatkovnih elemenata unutar certifikata.

Zaglavlje popisa pridruženo sadržaju tog certifikata sljedeće je:

'4D'	'16'	'5F 29'	'01'	'42'	'08'	'5F 4B'	'07'	'5F 24'	'04'	'5F 20'	'08'	'7F 49'	'05'	'81'	'81 80'	'82'	'08'
Oznaka proširenog zaglavlja popisa	Duljina zaglavlja popisa	Oznaka CPI	Duljina CPI	Oznaka CAR	Duljina CAR	Oznaka CHA	Duljina CHA	Oznaka EOV	Duljina EOV	Oznaka CHR	Duljina CHR	Oznaka javnog ključa (kontruisana)	Duljina naredih DO-ova	Oznaka modula	Duljina modula	Oznaka javnog eksponenta	Dužina javnog eksponenta

2. „Upućivanje na certifikacijsko tijelo" (CAR) služi za identifikaciju certifikacijskog tijela (CA) koje je izdalo certifikat tako da se podatkovni element može istodobno upotrebljavati kao identifikator ključa tijela za upućivanje na javni ključ certifikacijskog tijela (za kodiranje vidjeti identifikator ključa u nastavu).

3. „Ovlaštenje nosioca certifikata" (CHA) upotrebljava se za identifikaciju prava nosioca certifikata. Ono se sastoji od identifikatora (ID) tahografske aplikacije i vrste opreme za koju je certifikat namijenjen (prema podatkovnom elementu [illegible], '00' za državu članicu).

4. „Upućivanje na nosioca certifikata" (CHR) služi za jedinstvenu identifikaciju nosioca certifikata tako da se podatkovni element može istodobno upotrebljavati kao identifikator ključa nosioca za upućivanje na javni ključ nosioca certifikata.

5. Identifikatori ključa na jedinstven način identificiraju nosioca certifikata ili certifikacijsko tijelo. Oni su kodirani kako slijedi:

5.1. Oprema (VU ili kartica):

Podaci	Serijski broj opreme	Datum	Tip	Proizvođač
Dužina	4 bajta	2 bajta	1 bajt	1 bajt
Vrijednost	cijeli broj	BCD kodiranje mm gg	specifičan za proizvođača	kôd proizvođača

U slučaju jedinice u vozilu proizvođač, prilikom traženja certifikata, može ili ne mora znati identifikaciju opreme u koju se unose ključevi.

U prvom slučaju proizvođač će tijelu svoje države članice na certifikaciju poslati identifikaciju opreme s javnim ključem. Certifikat će nakon toga sadržiti identifikaciju opreme, a proizvođač mora osigurati da se ključevi i certifikat unesu u opremu za koju su namijenjeni. Identifikator ključa ima prethodno prikazani oblik.
U posljednjem slučaju proizvođač mora na jedinstven način identifikovati svaki zahtjev za certifikat i poslati takvu identifikaciju s javnim ključem tijelu svoje države članice na certifikaciju. Certifikat će sadržiti identifikaciju zahtjeva. Proizvođač mora povraćajno obavještenjeiti tijelo svoje države članice o dodjeli ključa opremi (tj. identifikaciji zahtjeva za certifikat, identifikaciji opreme) nakon ugradnje ključa u opremu. Identifikator ključa ima sljedeći oblik:

Podaci	Serijski broj zahtjeva za certifikat	Datum	Tip	Proizvođač
Dužina	4 bajta	2 bajta	1 bajt	1 bajt
Vrijednost	cijeli broj	BCD kodiranje mm gg	'FF'	kôd proizvođača

5.2. Certifikacijsko tijelo:

Podaci	Identifikacija tijela	Serijski broj ključa	Dodatne informacije	Identifikator
Dužina	4 bajta	1 bajt	2 bajta	1 bajt
Vrijednost	1-bajtni numerički kod države 3-bajtni alfanumerički kod države	cijeli broj	dodatno kodiranje (specifično za CA); 'FF FF' ako nije upotrijebljeno	'01'

Serijski broj ključa upotrebljava se za raspoznavanje različitih ključeva države članice u slučaju da se ključ promijeni.
6. Osobe koje vrše provjeru certifikata implicitno znaju da je certificirani javni ključ RSA ključ koji se odnosi na autentifikaciju, provjeru digitalnog potpisa i šifriranje za usluge povjerljivosti (certifikat ne sadrži identifikator objekta koji bi to navodio).

3.3.2 *Izdati certifikati*

CSM_018 Izdati certifikat je digitalni potpis s djelomičnim obnavljanjem sadržaja certifikata u skladu s normom ISO/IEC 9796-2 (osim njezina priloga A4) s priloženim „upućivanjem na certifikacijsko tijelo".
X.C = X.CA.SK[‘6A’ || C_r || *Hash*(Cc) || ‘BC’] || C_n || X.CAR

Sa sadržajem certifikata = Cc =	C_r	||	C_n
	106 bajtova		58 bajtova

Napomene:
1. Dužina ovog certifikata je 194 bajta.
2. CAR, koji je skriven potpisom, isto je tako priložen potpisu tako da javni ključ certifikacijskog tijela može biti odabran za provjeru certifikata.
3. Osoba koja provjerava certifikat implicitno je upoznata s algoritmom koji je certifikacijsko tijelo upotrijebilo za potpisivanje certifikata.
4. Zaglavlje popisa pridruženo navedenom izdatom certifikatu sljedeće je:

'7F 21'	'09'	'5F 37'	'81 80'	'5F 38'	'3A'	'42'	'08'
Oznaka certifikata CV (kontruisana)	Dužina narednih DO-ova	Oznaka potpisa	Dužina potpisa	Oznaka ostatka	Dužina ostatka	Oznaka CAR	Dužina CAR

3.3.3 *Provjera i otvaranje certifikata*

Provjera i otvaranje certifikata sastoji se od provjere potpisa prema normi ISO/IEC 9796 2, preuzimanja sadržaja certifikata i sadržanog javnog ključa: X.PK = X.CA.PK $_o$ X.C, te provjere važnosti certifikata.
CSM_019 Obuhvaća sljedeće korake:
Provjeriti potpis i preuzeti sadržaj:

— iz X.C preuzeti Sign, C_n' i CAR':	X.C =	Sign	||	C_n'	||	CAR'
		128 bajtova		58 bajtova		8 bajtova,

— odabrati iz CAR' odgovarajući javni ključ certifikacijskog tijela (ako to nije učinjeno ranije na neki drugi način),
— otvoriti Sign s javnim ključem CA: Sr'= X.CA.PK [Sign],
— provjeriti da Sr' započinje sa '6A' i završava s 'BC',

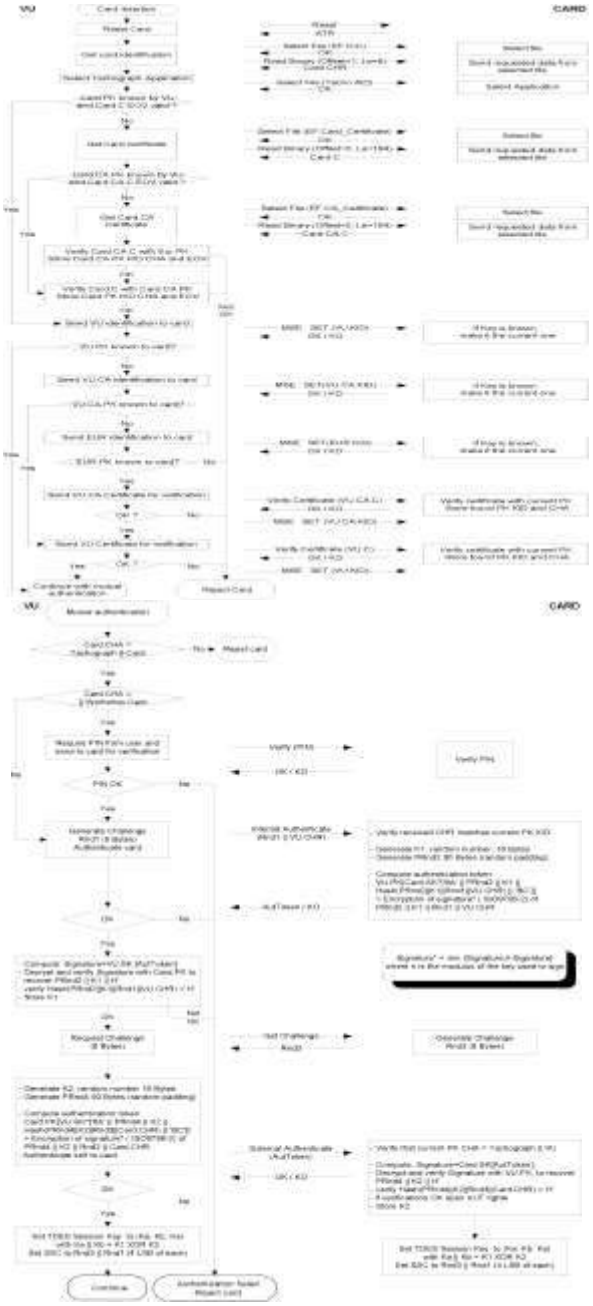
— izračunati C_r'i H' iz: Sr' =	'6A'	||	C_r'	||	H'	||	'BC'
			106 bajtova		20 bajtova,		

— ponovno učitati sadržaj certifikata C' = C_r'|| C_n',
— provjeriti *Hash*(C') = H'.
Ako su provjere u redu, certifikat je autentičan, njegov sadržaj je C'.
Provjeriti važnost. Iz C':
— prema potrebi, provjeriti datum isteka važnosti.
Preuzeti i arhivirati javni ključ, identifikator ključa, ovlaštenje nosioca certifikata i istek važnosti certifikata iz C':
— X.PK = *n* || *e*
— X.KID = CHR
— X.CHA = CHA
— X.EOV = EOV

4. MEHANIZAM UZAJAMNE AUTENTIFIKACIJE

Uzajamna autentifikacija između kartica i jedinica u vozilu (VU) temelji se na sljedećem načelu:
Svaka strana dokazuje drugoj strani da posjeduje važeći par ključeva čiji je javni ključ certifikovalo certifikacijsko tijelo države članice koje je certifikovalo evropsko certifikacijsko tijelo.
Dokazivanje se obavlja potpisivanjem privatnim ključem slučajnog broja koji je poslala druga strana koja mora obnoviti slučajni broj poslan prilikom provjere potpisa.

Mehanizam aktivira jedinica u vozilu pri umetanju kartice. On započinje razmjenom certifikata i otvaranjem javnih ključeva te završava postavljanjem ključa razmjene podataka.
CSM_020 Upotrebljava se sljedeći protokol (strelice ukazuju na naredbe i razmijenjene podatke (vidjeti Dodatak 2.)):



5. MEHANIZMI POVJERLJIVOSTI, INTEGRITETA I AUTENTIFIKACIJE PRENOSA PODATAKA IZMEĐU KARTICE I JEDINICE U VOZILU

5.1. Siguran prenos poruka

CSM_021 Integritet prenosa podataka između jedinice u vozilu i kartice zaštićen je sigurnim prenosom poruka u skladu s izvorima [ISO/IEC 7816-4] i [ISO/IEC 7816-8].

CSM_022 Kada podaci trebaju biti zaštićeni tokom prenosa, podatkovni objekt kriptografskog kontrolnog zbira dodaje se podatkovnim objektima koji se šalju u okviru naredbe ili odgovora. Kriptografski kontrolni zbir provjerava primatelj.

CSM_023 Kriptografski kontrolni zbir podataka koji se šalju u okviru naredbe objedinjuje zaglavlje naredbe i sve poslane podatkovne objekte (= > CLA = '0C', a svi podatkovni objekti moraju biti sažeti s oznakama u kojima je b1 = 1).

CSM_024 Bajtovi informacija o stanju odgovora zaštićeni su kriptografskim kontrolnim zbirem ako odgovor ne sadrži podatkovno polje.

CSM_025 Kriptografski kontrolni zbir ima dužinu od četiri bajta.

Struktura naredbi i odgovora pri sigurnom prenosu poruka stoga je sljedeća:

Upotrijebljeni DO-vi su parcijalni skup DO-ova za siguran prenos poruka opisan u normi ISO/IEC 7816-4:

Oznaka	Mnemonik	Značenje
'81'	T_{PV}	Nešifrirana vrijednost, podaci koji nisu kodirani u BER-TLV (zaštićena CC-om)
'97'	**T_{LE}**	Vrijednost Le u nezaštićenoj naredbi (zaštićena CC-om)
'99'	T_{SW}	Statusne informacije (zaštićene CC-om)
'8E'	T_{CC}	Kriptografski kontrolni zbir
'87'	$T_{PI\ CG}$	Bajt indikatora popunjenja || kriptogram (vrijednost koja nije kodirana u BER-TLV)

Pod pretpostavkom nezaštićenog para odgovora naredbe:

Zaglavlje naredbe				**Sadržaj naredbe**		
CLA	INS	P1	P2	[Polje L_c]	[Podatkovno polje]	[Polje L_e]
četiri bajta				Bajtovi L, označeni kao B_1 do B_L		

Sadržaj odgovora	**Nastavak odgovora**	
[Podatkovno polje]	SW1	SW2
L_r bajtova podataka	dva bajta	

Odgovarajući par zaštićenog odgovora naredbe je:

Zaštićena naredba:

Zaglavlje naredbe (CH)				**Sadržaj naredbe**										
CLA	INS	P1	P2	[Novo polje L_c]	[Novo podatkovno polje]									[Novo polje L_e]
'OC'				Dužina novog podatkovnog polja	T_{PV}	L_{PV}	PV	T_{LE}	L_{LE}	L_e	T_{CC}	L_{CC}	CC	'00'
					'81'	L_c	Podatkovno polje	'97'	'01'	L_e	'8E'	'04'	CC	

Podaci koje treba integrirati u kontrolni zbir = CH || PB || T_{PV} || L_{PV} || PV || T_{LE} || L_{LE} || L_e || PB

PB = bajtovi za popunjenje (80 .. 00) u skladu s normom ISO-IEC 7816-4 i metodom 2. iz norme ISO 9797.

DO PV i LE prisutni su samo kada postoje neki odgovarajući podaci u nezaštićenoj naredbi.

Zaštićeni odgovor:

1. Slučaj kada podatkovno polje odgovora nije prazno i ne treba ga zaštititi u pogledu povjerljivosti:

Sadržaj odgovora						**Nastavak odgovora**
[Novo podatkovno polje]						novi SW1 SW2
T_{PV}	L_{PV}	PV	T_{CC}	L_{CC}	CC	
'81'	L_r	podatkovno polje	'8E'	'04'	CC	

Podaci koje treba integrirati u kontrolni zbir = T_{PV} || L_{PV} || PV || PB

2. Slučaj kada podatkovno polje odgovora nije prazno i treba ga zaštititi u pogledu povjerljivosti:

Sadržaj odgovora						**Nastavak odgovora**
[Novo podatkovno polje]						novi SW1 SW2
$T_{PI\ CG}$	$L_{PI\ CG}$	PI CG	T_{CC}	L_{CC}	CC	
'87'		PI || CG	'8E'	'04'	CC	

Podaci koje prenosi CG: podaci koji nisu kodirani u BER-TLV i bajtovi za popunjenje.

Podaci koje treba integrirati u kontrolni zbir = $T_{PI\ CG}$ || $L_{PI\ CG}$ || PI CG || PB

3. Slučaj kada je podatkovno polje odgovora prazno:

Sadržaj odgovora						**Nastavak odgovora**
[Novo podatkovno polje]						novi SW1 SW2
T_{SW}	L_{SW}	SW	T_{CC}	L_{CC}	CC	
'99'	'02'	Novi SW1 SW2	'8E'	'04'	CC	

Podaci koje treba integrirati u kontrolni zbir = T_{SW} || L_{SW} || SW || PB

5.2. Postepene s pogreškama u sigurnom prenosu poruka

CSM_026 Kada tahografska kartica pri tumačenju naredbe prepozna pogrešku u sigurnom prenosu poruka (SM), tada se statusni bajtovi moraju vratiti bez SM-a. U skladu s normom ISO/IEC 7816-4, za označivanje pogrešaka u sigurnom prenosu poruka (SM) utvrđeni su sljedeći statusni bajtovi:

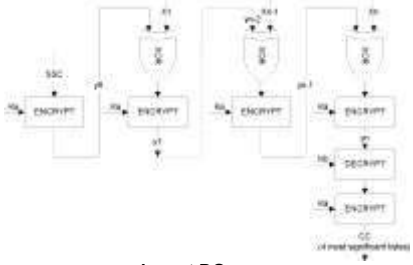
'66 88': neuspješna provjera kriptografskog kontrolnog zbira,

'69 87': nedostaju očekivani podatkovni objekti sigurnog prenosa poruka,

‘69 88’: neispravni podatkovni objekti sigurnog prenosa poruka.
CSM_027 Kada tahografska kartica vrati statusne bajtove bez SM DO ili s pogrešnim SM DO, jedinica u vozilu (VU) mora prekinuti razmjenu podataka.

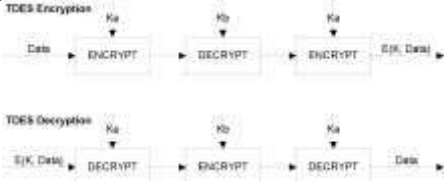
5.3. Algoritam izračuna kriptografskih kontrolnih zbireva

CSM_028 Kriptografski kontrolni zbirevi sastavljeni su upotrebom *retail* MAC-ova u skladu s ANSI X9.19 s DES-om:
— početni stadij: početni kontrolni blok y0 je E(Ka, SSC),
— naredni stadij: kontrolni blokovi y1, .., yn računaju se s pomoću Ka,
— konačni stadij: kriptografski kontrolni zbir izračunava se od posljednjeg kontrolnog bloka yn kako slijedi: E(Ka, D(Kb, yn)).
pri čemu E() označava šifriranje s pomoću DES-a, a D() označava dešifriranje s pomoću DES-a.
Četiri se najznačajnija bajta kriptografskog kontrolnog zbira prenose.
CSM_029 Brojač redoslijeda slanja (SSC) aktivira se u postupku dogovaranja ključa na:
početni SCC: Rnd3 (4 najmanje značajna bajta) || Rnd1 (4 najmanje značajna bajta).
CSM_030 Brojač redoslijeda slanja povećava se za 1 svaki put prije izračuna MAC-a (tj. SSC za prvu naredbu je početni SCC + 1, SCC za prvi odgovor je početni SCC + 2).
Na sljedećoj je slici prikazan izračun *retail* MAC-a:



5.4. Algoritam izračuna kriptograma za pouzdanost DO-ova

CSM_031 Kriptogrami se izračunavaju s pomoću TDEA u načinu rada TCBC u skladu s izvorima [TDES] i [TDES-OP] i s nultim vektorom kao blokom početne vrijednosti.
Na sljedećoj je slici prikazana primjena ključeva u TDES-u:



6. MEHANIZMI DIGITALNOG POTPISA KOD PREUZIMANJA PODATAKA

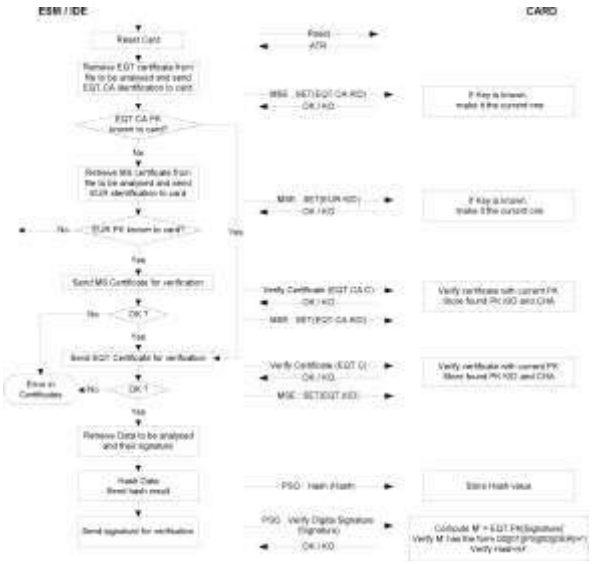
CSM_032 Posebna namjenska oprema (IDE) arhivira podatke primljene s opreme (jedinica u vozilu ili kartica) tokom jednog procesa preuzimanja podataka u jednoj fizičkoj podatkovnoj datoteci. Ta datoteka mora sadržiti certifikate MS_i.C i EQT.C. Datoteka sadrži digitalne potpise podatkovnih blokova navedenih u Dodatku 7. „Protokoli preuzimanja podataka”.
CSM_033 Digitalni potpisi preuzetih podataka upotrebljavaju šemu digitalnog potpisa s takvim dodatkom da se preuzeti podaci mogu čitati bez dešifriranja, ako se to želi.

6.1. Generisanje potpisa

CSM_034 Generisanje podatkovnog potpisa koje se sprovodi s pomoću opreme slijedi šemu potpisa s dodatkom koji je definisan u izvoru [PKCS1] s funkcijom raspršivanja (*hash*) SHA-1:
Potpis = EQT.SK[‘00’ || ‘01’ || *PS* || ‘00’ || DER(SHA-1(Podaci))]
PS = oktetni niz (eng. *octet string*) za popunjenje s takvom vrijednošću ‘FF’ da je dužina 128.
DER(SHA-1(*M*)) je kodiranje identifikatora (ID) algoritma za funkciju raspršivanja (*hash*) i vrijednost raspršivanja u vrijednosti ASN.1 tipa DigestInfo (posebna pravila kodiranja):
‘30’||‘21’||‘30’||‘09’||‘06’||‘05’||‘2B’||‘0E’||‘03’||‘02’||‘1A’||‘05’||‘00’||‘04’||‘14’||vrijednost raspršivanja (*hash*).

6.2. Provjera potpisa

CSM_035 Provjera potpisa na preuzetim podacima slijedi šemu potpisa s dodatkom koji je opisan u izvoru [PKCS1] s funkcijom raspršivanja (*hash*) SHA-1.
Verifikator mora nezavisno poznavati evropski javni ključ EUR.PK (i u njega imati povjerenja).
U sljedećoj je tablici prikazan protokol koji IDE s kontrolnom karticom može slijediti za provjeru integriteta podataka preuzetih i arhivirani na ESM (vanjski medij za arhiviranje podataka). Kontrolna kartica upotrebljava se za dešifriranje digitalnih potpisa. U tom slučaju takva funkcija ne mora biti ugrađena u IDE.
Oprema koja je preuzela i potpisala podatke koji se analiziraju označena je s EQT.



DIO B

SISTEM TAHOGRAFA DRUGE GENERACIJE

7. UVOD

7.1. Referentni dokumenti

U ovom su dijelu ovog Dodatka upotrijebljeni sljedeći izvori:

AES Nacionalni institut za norme i tehnologiju SAD-a (NIST), FIPS PUB 197: Advanced Encryption Standard (AES), 26. studenoga 2001.

DSS Nacionalni institut za norme i tehnologiju (NIST), FIPS PUB 186-4: Digital Signature Standard (DSS), srpanj 2013.

ISO 7816-4 ISO/IEC 7816-4, Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange, treće izdatje, 15.4.2013.

ISO 7816-8 ISO/IEC 7816-8, Identification cards – Integrated circuit cards – Part 8: Commands for security operations, drugo izdatje, 1.6.2004.

ISO 8825-1 ISO/IEC 8825-1, Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER), četvrto izdatje, 15.12.2008.

ISO 9797-1 ISO/IEC 9797-1, Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher, drugo izdatje, 1.3.2011.

ISO 10116 ISO/IEC 10116, Information technology – Security techniques – Modes of operation of an n-bit block cipher, treće izdatje, 1.2.2006.

ISO 16844-3 ISO/IEC 16844-3, Road vehicles – Tachograph systems – Part 3: Motion sensor interface, prvo izdatje, 2004., uključujući tehnički ispravak 1 2006.

RFC 5480 Elliptic Curve Cryptography Subject Public Key Information, ožujak 2009.

RFC 5639 Elliptic Curve Cryptography (ECC) – Brainpool Standard Curves and Curve Generation, 2010.

RFC 5869 HMAC-based Extract-and-Expand Key Derivation Function (HKDF), svibanj 2010.

SHS Nacionalni institut za norme i tehnologiju SAD-a (NIST), FIPS PUB 180-4: Secure Hash Standard, ožujak 2012.

SP 800-38B Nacionalni institut za norme i tehnologiju SAD-a (NIST), Posebno izdatje 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, 2005.

TR-03111 BSI Technical Guideline TR-03111, Elliptic Curve Cryptography, version 2.00, 28.6.2012.

7.2. Označivanje i skraćenice

U ovom se Dodatku upotrebljavaju sljedeće oznake i skraćenice:

AES norma naprednog šifriranja (eng. Advanced Encryption Standard)
CA certifikacijsko tijelo (eng. Certificate Authority)
CAR upućivanje na certifikacijsko tijelo (eng. Certificate Authority Reference)
CBC ulančavanje šifriranih blokova (eng. Cipher Block Chaining) (način rada)
CH zaglavlje naredbe (eng. Command Header)
CHA ovlaštenje nosioca certifikata (eng. Certificate Holder Authorisation)
CHR upućivanje na nosioca certifikata (eng. Certificate Holder Reference)
CV konstantni vektor (eng. Constant Vector)

DER posebna pravila kodiranja (eng. Distinguished Encoding Rules)
DO podatkovni objekt (eng. Data Object)
DSRC komunikacijski sistem kratkog dometa (eng. Dedicated Short Range Communication)
ECC kriptografija eliptičkih krivulja (eng. Elliptic Curve Cryptography)
ECDSA algoritam digitalnog potpisa na temelju eliptičkih krivulja (eng. Elliptic Curve Digital Signature Algorithm)
ECDH eliptička krivulja Diffie-Hellman (algoritam dogovaranja ključa)
EGF vanjski uređaj GNSS-a (eng. External GNSS Facility)
EQT oprema (eng. Equipment)
IDE posebna namjenska oprema (eng. Intelligent Dedicated Equipment)
KM glavni ključ senzora kretanja koji omogućava uparivanje jedinice u vozilu sa senzorom kretanja
KM-VU ključ unesen u jedinice u vozilu koji omogućava jedinici u vozilu (VU) da dobije glavni ključ senzora kretanja ako je kartica radionice umetnuta u VU
KM-WC ključ unesen u kartice radionice koji omogućava jedinici u vozilu (VU) da dobije glavni ključ senzora kretanja ako je kartica radionice umetnuta u VU
MAC kod za autentifikaciju poruke (eng. Message Authentication Code)
MoS senzor kretanja (eng. Motion Sensor)
MSB najznačajniji bit (eng. Most Significant Bit)
PKI infrastruktura javnih ključeva (eng. Public Key Infrastructure)
RCF uređaj za komunikaciju na daljinu (eng. Remote Communication Facility)
SSC brojač redoslijeda slanja (eng. Send Sequence Counter)
SM siguran prenos poruka (eng. Secure Messaging)
TDES norma trostrukog šifriranja podataka (eng. Triple Data Encryption Standard)
TLV vrijednost dužine oznake (eng. Tag Length Value)
VU jedinica u vozilu (eng. Vehicle Unit)
X.C certifikat javnog ključa korisnika X
X.CA certifikacijsko tijelo koje je izdalo certifikat korisniku X
X.CAR upućivanje na certifikacijsko tijelo koje je izdalo certifikat korisniku X
X.CHR upućivanje na nosioca certifikata navedenog u certifikatu korisnika X
X.PK javni ključ korisnika X
X.SK privatni ključ korisnika X
X.PKeph kratkotrajni javni ključ korisnika X
X.SKeph kratkotrajni privatni ključ korisnika X
'xx' heksadecimalna vrijednost
|| operator ulančavanja

7.3. Definicije

Definicije pojmova koji se upotrebljavaju u ovom Dodatku navedene su u odjeljku I. Priloga I.C.

8. KRIPTOGRAFSKI SISTEMI I ALGORITMI

8.1. Kriptografski sistemi

CSM_38 Jedinice u vozilu i tahografske kartice upotrebljavaju kriptografski sistem eliptičkih krivulja javnog ključa za pružanje sljedećih sigurnosnih usluga:
— uzajamna autentifikacija između jedinice u vozilu i kartice,
— dogovor AES ključeva razmjene podataka između jedinice u vozilu i kartice,
— osiguravanje autentičnosti, integriteta i nepobitnosti podataka preuzetih s jedinica u vozilu ili tahografskih kartica na vanjske medije.

CSM_39 Jedinice u vozilu i vanjski uređaji GNSS-a upotrebljavaju kriptografski sistem eliptičkih krivulja javnog ključa za pružanje sljedećih sigurnosnih usluga:
— povezivanje jedinice u vozilu i vanjskog uređaja GNSS-a,
— uzajamna autentifikacija između jedinice u vozilu i vanjskog uređaja GNSS-a,
— dogovor AES ključa razmjene podataka između jedinice u vozilu i vanjskog uređaja GNSS-a.

CSM_40 Jedinice u vozilu i tahografske kartice upotrebljavaju simetrični kriptografski sistem na temelju AES-a za pružanje sljedećih sigurnosnih usluga:
— osiguravanje autentičnosti i integriteta podataka razmijenjenih između jedinice u vozilu i tahografske kartice,
— ako je primjenjivo, osiguravanje povjerljivosti podataka razmijenjenih između jedinice u vozilu i tahografske kartice.

CSM_41 Jedinice u vozilu i vanjski uređaji GNSS-a upotrebljavaju simetrični kriptografski sistem na temelju AES-a za pružanje sljedećih sigurnosnih usluga:
— osiguravanje autentičnosti i integriteta podataka razmijenjenih između jedinice u vozilu i vanjskog uređaja GNSS-a.

CSM_42 Jedinice u vozilu i senzori kretanja upotrebljavaju simetrični kriptografski sistem na temelju AES-a za pružanje sljedećih sigurnosnih usluga:
— uparivanje jedinice u vozilu i senzora kretanja,
— uzajamna autentifikacija između jedinice u vozilu i senzora kretanja,
— osiguranje povjerljivosti podataka razmijenjenih između jedinice u vozilu i senzora kretanja.

CSM_43 Jedinice u vozilu i kontrolne kartice upotrebljavaju simetrični kriptografski sistem na temelju AES-a za pružanje sljedećih sigurnosnih usluga na sučelju za komunikaciju na daljinu:
— osiguranje povjerljivosti, autentičnosti i integriteta podataka koje jedinica u vozilu šalje kontrolnoj kartici.

Napomene:

— Konkretnije, podaci se iz jedinice u vozilu šalju uređaju za daljinsko ispitivanje (eng. *remote interrogator*) koji je pod kontrolom službenika za kontrolu s pomoću uređaja za komunikaciju na daljinu koji može biti vanjski ili unutarnji u odnosu na jedinicu u vozilu; vidjeti Dodatak 14. Međutim, uređaj za daljinsko ispitivanje šalje primljene podatke kontrolnoj kartici radi dešifriranja i potvrde autentičnosti. Što se tiče sigurnosti, uređaj za komunikaciju na daljinu i uređaj za daljinsko ispitivanje potpuno su transparentni.
— Kartica radionice pruža iste sigurnosne usluge za sučelje DSRC-a kao i kontrolna kartica. Time se radionici omogućava potvrda ispravnog funkcionisanja sučelja jedinice u vozilu za komunikaciju na daljinu, uključujući sigurnost. Za više informacija vidjeti odjeljak 9.2.2.

8.2. Kriptografski algoritmi

8.2.1 ***Simetrični algoritmi***

CSM_44 Jedinice u vozilu, tahografske kartice, senzori kretanja i vanjski uređaji GNSS-a podržavaju AES algoritam kako je definisano u [AES], s dužinama ključa od 128, 192 i 256 bitova.

8.2.2 ***Asimetrični algoritmi i normirani parametri domene***

CSM_45 Jedinice u vozilu, tahografske kartice i vanjski uređaji GNSS-a podržavaju kriptografiju eliptičkih krivulja s veličinom ključa od 256, 384 i 512/521 bitova.
CSM_46 Jedinice u vozilu, tahografske kartice i vanjski uređaji GNSS-a podržavaju algoritam potpisa ECDSA kako je navedeno u [DSS].
CSM_47 Jedinice u vozilu, tahografske kartice i vanjski uređaji GNSS-a podržavaju algoritam dogovaranja ključa ECKA-EG kako je navedeno u [TR 03111].
CSM_48 Jedinice u vozilu, tahografske kartice i vanjski uređaji GNSS-a podržavaju sve normirane parametre domene iz tablice 1. u nastavu za kriptografiju eliptičkih krivulja:

Tablica 1.

Normirani parametri domene

Naziv	Veličina (bitova)	Upućivanje	Identifikator objekta
NIST P-256	256	[DSS], [RFC 5480]	[illegible]
BrainpoolP256r1	256	[RFC 5639]	[illegible]
NIST P-384	384	[DSS], [RFC 5480]	[illegible]
BrainpoolP384r1	384	[RFC 5639]	[illegible]
BrainpoolP512r1	512	[RFC 5639]	[illegible]
NIST P-521	521	[DSS], [RFC 5480]	[illegible]

Napomena: identifikatori objekta u zadnjem koloni tablice 1. navedeni su u [RFC 5639] za krivulje Brainpool i u [RFC 5480] za krivulje NIST.

8.2.3 ***Algoritmi raspršivanja (hashing)***

CSM_49 Jedinice u vozilu, tahografske kartice i vanjski uređaji GNSS-a podržavaju algoritme SHA-256, SHA-384 i SHA-512 navedene u [SHS].

8.2.4 ***Sljedovi šifri (eng. Cipher Suites)***

CSM_50 U slučaju simetričnog algoritma, asimetrični algoritam i algoritam raspršivanja upotrebljavaju se zajedno kako bi oblikovali sigurnosni protokol; njihove su dužine ključeva i veličine raspršivanja (približno) jednake jakosti. U tablici 2. prikazani su dopušteni slijedovi šifri:

Tablica 2.

Dopušteni sljedovi šifri

ID slijeda šifri	Veličina ECC ključa (bitovi)	Dužina AES ključa (bitovi)	Algoritam kompresije	Dužina MAC (u bajtovima)
CS#1	256	128	SHA-256	8
CS#2	384	192	SHA-384	12
CS#3	512/521	256	SHA-512	16

Napomena: veličine ECC ključeva od 512 bitova odnosno 521 bita smatraju se jednakima po jakosti za sve namjene obuhvaćene ovim Dodatkom.

9. KLJUČEVI I CERTIFIKATI

9.1. Asimetrični parovi ključeva i certifikati javnih ključeva

9.1.1 ***Uopšteno***

Napomena: ključevi opisani u ovom odjeljku upotrebljavaju se za uzajamnu autentifikaciju i siguran prenos poruka između jedinica u vozilu i tahografskih kartica te između jedinica u vozilu i vanjskih uređaja GNSS-a. Ti su postupci detaljno opisani u poglavljima 10. i 11. ovog Dodatka.
CSM_51 U okviru Evropskog sistema pametnog tahografa, parovi ECC ključeva i odgovarajući certifikati generišu se i njima se upravlja preko tri funkcionalne hijerarhijske razine:
— evropski nivo,
— nivo države članice,
— nivo opreme.

CSM_52 U okviru cijelog Evropskog sistema pametnog tahografa, javni i privatni ključevi i certifikati generišu se, njima se upravlja te komuniciraju s pomoću normiranih i sigurnih metoda.

9.1.2 *Evropski nivo*

CSM_53 Na evropskoj se nivou generiše jedan jedinstveni par ECC ključeva označen kao EUR. Sastoji se od privatnog ključa (EUR.SK) i javnog ključa (EUR.PK). Taj par ključeva čini glavni (eng. *root*) par ključeva cijelog Evropskog pametnog tahografa PKI. Taj zadatak obavlja evropsko tijelo za izdavanje glavnog certifikata (eng. *European Root Certificate Authority*, ERCA), pod nadležnošću i odgovornošću Evropske komisije.

CSM_54 ERCA upotrebljava evropski privatni ključ za potpisivanje (samopotpisanog) glavnog certifikata evropskog javnog ključa te taj evropski glavni certifikat dostavlja svim državama članicama.

CSM_55 ERCA upotrebljava evropski privatni ključ za potpisivanje certifikata javnog ključa država članica na zahtjev. ERCA vodi evidenciju svih potpisanih certifikata javnih ključeva država članica.

CSM_56 Kako je prikazano na slici 1. u odjeljku 9.1.7., ERCA generiše novi evropski glavni par ključeva svakih 17 godina. Kada generiše novi evropski glavni par ključeva, ERCA stvara i novi samopotpisani glavni certifikat za novi evropski javni ključ. Rok važnosti evropskog glavnog certifikata je 34 godine uvećano za tri mjeseca.

Napomena: uvođenje novog glavnog para ključeva isto tako znači da će ERCA generišeti novi glavni ključ senzora kretanja i novi glavni ključ DSRC-a, vidjeti odjeljke 9.2.1.2. i 9.2.2.2.

CSM_57 Prije generisanja novog evropskog glavnog para ključeva, ERCA sprovodi analizu kriptografske jakosti koja je potrebna za novi par ključeva s obzirom na to da treba ostati zaštićen sljedeće 34 godine. Ako to smatra potrebnim, ERCA može prijeći na slijed šifri koji je jači od postojećeg, kako je navedeno u CSM_50.

CSM_58 Kada generiše novi evropski glavni par ključeva, ERCA stvara i certifikat o povezanosti za novi evropski javni ključ i potpisuje ga s prethodnim evropskim privatnim ključem. Rok važnosti certifikata o povezanosti je 17 godina uvećano za tri mjeseca. To je prikazano i na slici 1. u odjeljku 9.1.7.

Napomena: Budući da certifikat o povezanosti sadrži javni ključ ERCA generacije *X* koji je potpisan privatnim ključem ERCA generacije *X-1*, certifikat o povezanosti opremi izdatoj na temelju generacije *X-1* pruža metodu za uspostavu povjerenja u opremu izdatu na temelju generacije *X*.

CSM_59 ERCA ne upotrebljava privatni ključ glavnog para ključeva ni u koju svrhu od trenutka u kojem novi glavni certifikat ključa postane važeći.

CSM_60 ERCA u svakom trenutku ima na raspolaganju sljedeće kriptografske ključeve i certifikate:

— trenutni par EUR ključeva i odgovarajući certifikat,

— sve prethodne certifikate EUR koji se upotrebljavaju za provjeru certifikata MSCA koji su još uvijek važeći,

— certifikate o povezanosti za sve generacije certifikata EUR osim prve.

9.1.3 *Nivo države članice*

CSM_61 Na nivou države članice, sve države članice koje trebaju potpisivati certifikate tahografskih kartica generišu jedan ili više jedinstvenih parova ECC ključeva označenih kao MSCA_Card. Sve države članice koje trebaju potpisivati certifikate za jedinice u vozilu ili vanjske GNSS uređaje dodatno generišu jedan ili više jedinstvenih parova ECC ključeva označenih kao MSCA_VU-EGF.

CSM_62 Zadatak generisanja parova ključeva država članica obavlja certifikacijsko tijelo države članice (MSCA). Kada generiše par ključeva države članice, MSCA šalje javni ključ ERCA-i kako bi dobila odgovarajući certifikat države članice koji je potpisala ERCA.

CSM_63 MSCA odabire jakost para ključeva države članice jednaku jakosti evropskog glavnog para ključeva koji se upotrebljava za potpisivanje odgovarajućeg certifikata države članice.

CSM_64 Ako postoji, par ključeva MSCA_VU-EGF sastoji se od privatnog ključa MSCA_VU-EGF.SK i javnog ključa MSCA_VU-EGF.PK. MSCA upotrebljava privatni ključ MSCA_VU-EGF.SK isključivo za potpisivanje certifikata javnih ključeva jedinica u vozilu i vanjskih uređaja GNSS-a.

CSM_65 Par ključeva MSCA_Card sastoji se od privatnog ključa MSCA_Card.SK i javnog ključa MSCA_Card.PK. MSCA upotrebljava privatni ključ MSCA_Card.SK isključivo za potpisivanje certifikata javnih ključeva tahografskih kartica.

CSM_66 MSCA vodi evidenciju svih potpisanih certifikata jedinica u vozilu, certifikata vanjskih uređaja GNSS-a i certifikata kartica zajedno s identifikacijom opreme za koju je certifikat namijenjen.

CSM_67 Rok važnosti certifikata MSCA_VU-EGF je 17 godina uvećano za tri mjeseca. Rok važnosti certifikata MSCA_Card je sedam godina uvećano za jedan mjesec.

CSM_68 Kako je prikazano na slici 1. u odjeljku 9.1.7, period upotrebe privatnog ključa para ključeva MSCA_VU-EGF i privatnog ključa para ključeva MSCA_Card iznosi dvije godine.

CSM_69 MSCA ne upotrebljava privatni ključ para ključeva MSCA_VU-EGF ni u koju svrhu nakon što je isteklo njegovo period upotrebe. Nadalje, MSCA ne upotrebljava privatni ključ para ključeva MSCA_Card ni u koju svrhu nakon što je isteklo njegovo period upotrebe.

CSM_70 MSCA u svakom trenutku ima na raspolaganju sljedeće kriptografske ključeve i certifikate:

— trenutni par ključeva MSCA_Card i odgovarajući certifikat,

— sve prethodne certifikate MSCA_Card koji se upotrebljavaju za provjeru certifikata tahografskih kartica koji su još uvijek važeći,

— trenutni certifikat EUR potreban za provjeru trenutačnog certifikata MSCA,

— sve prethodne certifikate EUR potrebne za provjeru certifikata MSCA koji su još uvijek važeći.

CSM_71 Ako treba potpisivati certifikate za jedinice u vozilu ili vanjske uređaje GNSS-a, MSCA dodatno ima na raspolaganju sljedeće ključeve i certifikate:

— trenutni par ključeva MSCA_VU-EGF i odgovarajući certifikat,

— sve prethodne javne ključeve MSCA_VU-EGF koji se upotrebljavaju za provjeru certifikata jedinica u vozilu ili vanjskih uređaja GNSS-a koji su još uvijek važeći.

9.1.4 ***Nivo opreme: Jedinice u vozilu***

CSM_72 Za svaku se jedinicu u vozilu generišu dva jedinstvena para ECC ključeva označena kao VU_MA i VU_Sign. Taj zadatak obavljaju proizvođači jedinica u vozilu. Kada generiše par ključeva za jedinicu u vozilu, strana koja generiše ključ šalje javni ključ svojem MSCA-u kako bi dobila odgovarajući certifikat jedinice u vozilu koji je potpisao MSCA. Privatni ključ upotrebljava isključivo jedinica u vozilu.

CSM_73 Certifikati VU_MA i VU_Sign određene jedinice u vozilu imaju isti datum početka važnosti certifikata.

CSM_74 Proizvođač jedinica u vozilu odabire jakost para ključeva jedinice u vozilu jednaku jakosti para MSCA ključeva koji se upotrebljava za potpisivanje odgovarajućeg certifikata jedinice u vozilu.

CSM_75 Jedinica u vozilu upotrebljava svoj par VU_MA ključeva, koji se sastoji od privatnog ključa VU_MA.SK i javnog ključa VU_MA.PK, isključivo kako bi izvršila autentifikaciju jedinice u vozilu s obzirom na tahografske kartice i vanjske uređaje GNSS-a, kako je navedeno u odjeljcima 10.3. i 11.4. ovog Dodatka.

CSM_76 Jedinica u vozilu može generišeti kratkotrajne parove ECC ključeva, pri čemu kratkotrajni par ključeva upotrebljava isključivo za dogovaranje ključa razmjene podataka s tahografskom karticom ili vanjskim uređajem GNSS-a, kako je navedeno u odjeljcima 10.4. i 11.4. ovog Dodatka.

CSM_77 Jedinica u vozilu upotrebljava privatni ključ VU_Sign.SK iz svojeg para VU_Sign ključeva isključivo za potpisivanje preuzetih podatkovnih datoteka, kako je navedeno u poglavlju 14. ovog Dodatka. Odgovarajući javni ključ VU_Sign.PK upotrebljava se isključivo za provjeru potpisa koje stvara jedinica u vozilu.

CSM_78 Kako je prikazano na slici 1. u odjeljku 9.1.7., rok važnosti certifikata VU_MA je 15 godina i tri mjeseca. Rok važnosti certifikata VU_Sign je 15 godina i tri mjeseca.

Napomene:

— produženim se rokom važnosti certifikata VU_Sign jedinici u vozilu omogućava stvaranje važećiih potpisa za preuzete podatke tokom prva tri mjeseca nakon isteka važnosti certifikata u skladu s Uredbom (EU) br. 581/2010.

— Produženi je rok važnosti certifikata VU_MA potreban kako bi se jedinici u vozilu omogućila autentifikacija kontrolne kartice ili kartice preduzeće tokom prva tri mjeseca nakon isteka važnosti certifikata tako da može izvršiti preuzimanje podataka.

CSM_79 Jedinica u vozilu ne upotrebljava privatni ključ para ključeva jedinice u vozilu ni u koju svrhu od trenutka isteka odgovarajućeg certifikata.

CSM_80 Parovi ključeva jedinice u vozilu (osim kratkotrajnih parova ključeva) i odgovarajući certifikati određene jedinice u vozilu ne smiju se zamjenjivati ili obnavljati na terenu nakon što je jedinica u vozilu stavljena u upotrebu.

Napomene:

— kratkotrajni parovi ključeva nisu obuhvaćeni ovim zahtjevom jer jedinica u vozilu generiše kratkotrajni par ključeva svaki put kad se izvršava autentifikacija čipa ili dogovaranje ključa razmjene podataka,; vidjeti odjeljak 10.4. Potrebno je napomenuti da kratkotrajni parovi ključeva nemaju odgovarajuće certifikate.

— Ovim se zahtjevom ne zabranjuje mogućnost zamjene statičkih parova ključeva jedinice u vozilu tokom obnove ili popravka u sigurnom okruženju koje kontrolira proizvođač jedinice u vozilu.

CSM_81 Kada su stavljene u upotrebu, jedinice u vozilu sadržiju sljedeće kriptografske ključeve i certifikate:

— privatni ključ VU_MA i odgovarajući certifikat,

— privatni ključ VU_Sign i odgovarajući certifikat,

— certifikat MSCA_VU-EGF s javnim ključem MSCA_VU-EGF.PK koji se upotrebljava za provjeru VU_MA certifikata i VU_Sign certifikata,

— certifikat EUR s javnim ključem EUR.PK koji se upotrebljava za provjeru certifikata MSCA_VU-EGF,

— certifikat EUR čiji rok važnosti direktno prethodi roku važnosti certifikata EUR koji se upotrebljava za provjeru certifikata MSCA_VU-EGF, ako postoji,

— certifikat o povezanosti koji povezuje ta dva certifikata EUR, ako postoji.

CSM_82 Osim kriptografskih ključeva i certifikata navedenih u CSM_81, jedinice u vozilu isto tako sadržiju ključeve i certifikate iz dijela A ovog Dodatka kojima se jedinici u vozilu omogućava interakcija s tahografskim karticama prve generacije.

9.1.5 ***Nivo opreme: Tahografske kartice***

CSM_83 Za svaku tahografsku karticu generiše se jedan jedinstveni par ECC ključeva označen kao Card_MA. Za svaku se karticu vozača i svaku karticu radionice dodatno generiše drugi jedinstveni par ECC ključeva označen kao Card_Sign. Taj zadatak mogu obavljati proizvođači kartice ili izvođači personalizacije kartice. Kada generiše par ključeva kartica, strana koja generiše ključ šalje javni ključ svojem MSCA-u kako bi dobila odgovarajući certifikat kartice koji je potpisao MSCA. Privatni ključ upotrebljava isključivo tahografska kartica.

CSM_84 Certifikati Card_MA i Card_Sign određene kartice vozača ili kartice radionice imaju isti datum početka važnosti certifikata.

CSM_85 Proizvođač kartice ili izvođač personalizacije kartice odabire jakost para ključeva kartice jednaku jakosti para MSCA ključeva koji se upotrebljava za potpisivanje odgovarajućeg certifikata kartice.

CSM_86 Tahografska kartica upotrebljava svoj par VU_Card ključeva, koji se sastoji od privatnog ključa Card_MA.SK i javnog ključa Card_MA.PK, isključivo kako bi izvršila uzajamnu autentifikaciju i dogovaranje ključa razmjene podataka s obzirom na jedinice u vozilu, kako je navedeno u odjeljcima 10.3. i 10.4. ovog Dodatka.

CSM_87 Kartica vozača ili kartica radionice upotrebljava privatni ključ Card_Sign.SK iz svojeg para Card_Sign ključeva isključivo za potpisivanje preuzetih podatkovnih datoteka, kako je navedeno u poglavlju 14. ovog Dodatka. Odgovarajući javni ključ Card_Sign.PK upotrebljava se isključivo za provjeru potpisa koje stvara kartica.

CSM_88 Rok važnosti certifikata Card_MA sljedeći je:

— za kartice vozača: 5 godina

— za kartice preduzeće: 5 godina

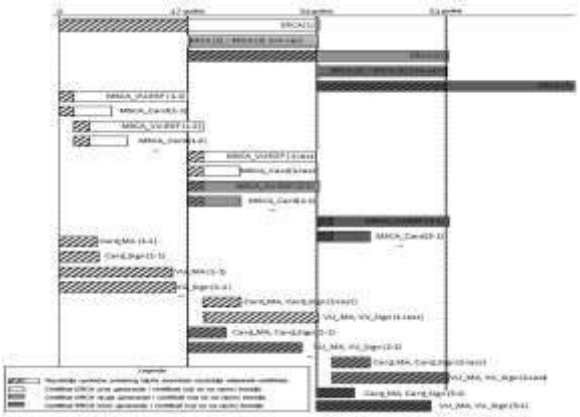
— za kontrolne kartice: 2 godine
— za kartice radionica: 1 godina
CSM_89 Rok važnosti certifikata Card_Sign sljedeći je:
— za kartice vozača: pet godina i jedan mjesec,
— za kartice radionica: jedna godina i jedan mjesec.
Napomena: produženim se rokom važnosti certifikata Card_Sign kartici vozača omogućava stvaranje važećiih potpisa za preuzete podatke tokom prvog mjeseca nakon isteka važnosti certifikata. To je potrebno s obzirom na Uredbu (EU) br. 581/2010 kojom se zahtijeva da preuzimanje podataka s kartice vozača mora biti moguće do 28 dana nakon posljednjeg zapisa podataka.
CSM_90 Parovi ključeva i odgovarajući certifikati određene tahografske kartice ne smiju se zamjenjivati ili obnavljati nakon izdavanja kartice.
CSM_91 Kada su izdate, tahografske kartice sadržiju sljedeće kriptografske ključeve i certifikate:
— privatni ključ Card_MA i odgovarajući certifikat,
— dodatno za kartice vozača i kartice radionica: privatni ključ Card_Sign i odgovarajući certifikat,
— certifikat MSCA_Card s javnim ključem MSCA_Card.PK koji se upotrebljava za provjeru certifikata Card_MA i certifikata Card_Sign,
— certifikat EUR s javnim ključem EUR.PK koji se upotrebljava za provjeru certifikata MSCA_Card,
— certifikat EUR čiji rok važnosti direktno prethodi roku važnosti certifikata EUR koji se upotrebljava za provjeru certifikata MSCA_Card, ako postoji,
— certifikat o povezanosti koji povezuje ta dva certifikata EUR, ako postoji,
— usto, samo za kontrolne kartice, kartice preduzeće i kartice radionica, te samo ako su takve kartice izdate tokom tri prva mjeseca perioda važnosti novog certifikata EUR: certifikat EUR koji je dvije generacije stariji, ako postoji.
Napomena: uz posljednju podtačku: na primjer, u prva tri mjeseca certifikata ERCA(3) (vidjeti sliku 1.), spomenute kartice sadrže certifikat ERCA(1). To je potrebno kako bi se osiguralo da se te kartice mogu koristiti za obavljanje preuzimanja podataka s jedinica u vozilu ERCA(1) čije uobičajeno vrijeme trajanja od 15 godina uz tromjesečno period preuzimanja podataka istječe tokom tih mjeseci; vidjeti posljednju podtačku zahtjeva 13) Priloga I.C.
CSM_92 Osim kriptografskih ključeva i certifikata navedenih u CSM_91, tahografske kartice sadržiju i ključeve i certifikate navedene u dijelu A ovog Dodatka koji tim karticama omogućuju interakciju s jedinicama u vozilu prve generacije.

9.1.6 ***Nivo opreme: Vanjski uređaji GNSS-a***

CSM_93 Za svaki vanjski uređaj GNSS-a generiše se jedan jedinstveni par ECC ključeva označen kao EGF_MA. Taj zadatak obavljaju proizvođači vanjskih uređaja GNSS-a. Kada generiše par ključeva EGF_MA, strana koja generiše ključ šalje javni ključ svojem MSCA-u kako bi dobila odgovarajući certifikat EFG_MA koji je potpisao MSCA. Privatni ključ upotrebljava isključivo vanjski uređaj GNSS-a.
CSM_94 Proizvođač vanjskog uređaja GNSS-a (EGF) odabire jakost para EGF_MA ključeva jednaku jakosti para MSCA ključeva koji se upotrebljava za potpisivanje odgovarajućeg certifikata EGF_MA.
CSM_95 Vanjski uređaj GNSS-a upotrebljava svoj par ključeva EGF_MA, koji se sastoji od privatnog ključa EGF_MA.SK i javnog ključa EGF_MA.PK, isključivo kako bi izvršio uzajamnu autentifikaciju i dogovaranje ključa razmjene podataka s obzirom na jedinice u vozilu, kako je navedeno u odjeljku 11.4. ovog Dodatka.
CSM_96 Rok važnosti certifikata EGF_MA je 15 godina.
CSM_97 Vanjski uređaj GNSS-a ne upotrebljava privatni ključ iz svojeg para EGF-MA ključeva za povezivanje s jedinicom u vozilu nakon isteka odgovarajućeg certifikata.
Napomena: kako je objašnjeno u odjeljku 11.3.3., EGF potencijalno može upotrijebiti svoj privatni ključ za uzajamnu autentifikaciju s obzirom na jedinicu u vozilu s kojom je već povezan čak i nakon isteka odgovarajućeg certifikata.
CSM_98 Par EGF_MA ključeva i odgovarajući certifikat određenog vanjskog uređaja GNSS-a ne smiju se zamjenjivati ili obnavljati na terenu nakon što je EGF stavljen u upotrebu.
Napomena: ovim se zahtjevom ne zabranjuje mogućnost zamjene parova EGF ključeva tokom obnove ili popravka u sigurnom okruženju koje kontrolira proizvođač EGF-a.
CSM_99 Kada je stavljen u upotrebu, vanjski uređaj GNSS-a sadrži sljedeće kriptografske ključeve i certifikate:
— privatni ključ EGF_MA i odgovarajući certifikat,
— certifikat MSCA_VU-EGF s javnim ključem MSCA_VU-EGF.PK koji se upotrebljava za provjeru certifikata EGF_MA,
— certifikat EUR s javnim ključem EUR.PK koji se upotrebljava za provjeru certifikata MSCA_VU-EGF,
— certifikat EUR čiji rok važnosti direktno prethodi roku važnosti certifikata EUR koji se upotrebljava za provjeru certifikata MSCA_VU-EGF, ako postoji,
— certifikat o povezanosti koji povezuje ta dva certifikata EUR, ako postoji.

9.1.7 ***Pregled: Zamjena certifikata***

Na slici 1. u nastavu prikazan je način izdavanja i upotrebe različitih generacija glavnih certifikata ERCA, certifikata o povezanosti ERCA, certifikata MSCA i certifikata opreme (jedinica u vozilu i kartica) tokom vremena:



1. različite generacije glavnog certifikata označene su brojem u zagradi. Npr. ERCA (1) znači prva generacija glavnog certifikata ERCA; ERCA (2) znači druga generacija itd.
2. Ostali su certifikati označeni s dva broja u zagradi, pri čemu prvi označava generaciju glavnog certifikata na temelju kojeg su izdati, a drugi generaciju samog certifikata. Npr. MSCA_Card (1-1) znači prvi certifikat MSCA_Card izdat na temelju ERCA (1); MSCA_Card (2-1) znači prvi certifikat MSCA_Card izdat na temelju ERCA (2); MSCA_Card (2-zadnji) znači zadnji certifikat MSCA_Card izdat na temelju ERCA (2); Card_MA(2-1) znači prvi certifikat kartice za uzajamnu autentifikaciju koji je izdat na temelju ERCA (2) itd.
3. Certifikati MSCA_Card (2-1) i MSCA_Card (1-zadnji) izdaju se na gotovo (ali ne potpuno) isti datum. Certifikat MSCA_Card (2-1) je prvi certifikat MSCA_Card izdat na temelju ERCA (2) i izdat će se malo kasnije od certifikata MSCA_Card (1-zadnji), zadnjeg certifikata MSCA_Card na temelju ERCA (1).
4. Kako je prikazano na slici, prvi certifikati jedinice u vozilu i kartica izdati na temelju ERCA (2) pojavit će se gotovo dvije godine prije pojave zadnjih certifikata jedinice u vozilu i kartica izdatih na temelju ERCA (1). To je zbog činjenice da se certifikati jedinice u vozilu i kartica izdaju na temelju certifikata MSCA, a ne direktno na temelju certifikata ERCA. Certifikat MSCA (2-1) izdaje se neposredno nakon što ERCA (2) postane važeći, ali certifikat MSCA (1-zadnji) izdaje se samo malo prije tog vremena, u posljednjem trenutku u kojem je certifikat ERCA (1) još uvijek važeći. Stoga će ta dva certifikata MSCA imati gotovo jednak rok važnosti unatoč činjenici da pripadaju različitim generacijama.
5. Rok važnosti prikazan za kartice odnosi se na kartice vozača (pet godina).
6. Radi uštede prostora razlika u roku važnosti između certifikata Card_MA i Card_Sign prikazana je samo za prvu generaciju.

9.2. Simetrični ključevi

9.2.1 *Ključevi za sigurnu komunikaciju između jedinice u vozilu i senzora kretanja*

9.2.1.1 *Uopšteno*

Napomena: čitatelji ovog odjeljka trebaju biti upoznati sa sadržajem norme [ISO 16844-3] u kojoj se opisuje sučelje između jedinice u vozilu i senzora kretanja. Postupak uparivanja između jedinice u vozilu i senzora kretanja detaljno je opisan u poglavlju 12. ovog Dodatka.

CSM_100 Za uparivanje jedinica u vozilu i senzora kretanja, uzajamnu autentifikaciju između jedinica u vozilu i senzora kretanja te šifriranje komunikacije između jedinica u vozilu i senzora kretanja potreban je niz simetričnih ključeva, kako je prikazano u tablici 3. Svi su ti ključevi AES ključevi, pri čemu je dužina ključa jednaka dužini glavnog ključa senzora kretanja, koji su povezani s duljinom (predviđenog) evropskog glavnog para ključeva kako je opisano u CSM_50.

Tablica 3.

Ključevi za sigurnu komunikaciju između jedinice u vozilu (VU) i senzora kretanja

Ključ	Simbol	Generiše	Metoda generisanja	Arhivira
Glavni ključ senzora kretanja – dio VU-a	K_{M-VU}	ERCA	Nasumično	ERCA, MSCA uključeni u izdavanje certifikata VU-ova, proizvođači VU-ova, jedinice u vozilu
Glavni ključ senzora kretanja – dio radionice	K_{M-WC}	ERCA	Nasumično	ERCA, MSCA, proizvođači kartica, kartice radionica
Glavni ključ senzora kretanja	K_M	Ne generiše se nezavisno	Izračunava se kao $K_M = K_{M-VU}$ XOR K_{M-WC}	ERCA, MSCA uključeni u izdavanje ključeva senzora kretanja (neobavezno) (*1)
Identifikacijski ključ	K_{ID}	Ne generiše se nezavisno	Izračunava se kao $K_{ID} = K_M$ XOR CV, pri čemu je CV navedeno u CSM_106	ERCA, MSCA uključeni u izdavanje ključeva senzora kretanja (neobavezno) (*1)
Ključ uparivanja	K_P	Proizvođač senzora kretanja	Nasumično	Jedan senzor kretanja
Ključ razmjene podataka	K_S	VU (tokom	Nasumično	Jedan VU i jedan senzor kretanja

		uparivanja VU-a i senzora kretanja)		
(*1) Arhiviranje K_M i K_{ID} nije obvezno jer se te ključeve može izvesti iz K_{M-VU}, K_{M-WC} i CV.				

CSM_101 Evropsko tijelo za izdavanje glavnog certifikata (ERCA) generiše K_{M-VU} i K_{M-WC}, dva nasumična i jedinstvena AES ključa, iz kojih se glavni ključ senzora kretanja K_M može izračunati kao K_{M-VU} XOR K_{M-WC}. ERCA dostavlja K_M, K_{M-VU} i K_{M-WC} certifikacijskim tijelima država članica na njihov zahtjev.

CSM_102 ERCA svakom glavnom ključu senzora kretanja K_M dodjeljuje jedinstveni broj verzije koji isto tako vrijedi za stvaranje ključeva K_{M-VU} i K_{M-WC} i povezanog identifikacijskog ključa K_{ID}. ERCA obavješćuje MSCA-ove o broju verzije kada im šalje K_{M-VU} i K_{M-WC}.

Napomena: Broj verzije upotrebljava se za razlikovanje različitih generacija tih ključeva, kako je detaljno objašnjeno u odjeljku 9.2.1.2.

CSM_103 Certifikacijsko tijelo države članice dostavlja K_{M-VU}, zajedno s brojem verzije proizvođačima jedinica u vozilu na njihov zahtjev. Proizvođači jedinica u vozilu unose K_{M-VU} i njegov broj verzije u sve proizvedene jedinice u vozilu.

CSM_104 Certifikacijsko tijelo države članice (MSCA) osigurava da je K_{M-WC}, zajedno s njegovim brojem verzije, unesen na svaku karticu radionice pod njegovom odgovornošću.

— vidjeti opis vrste podataka SensorInstallationSecData u Dodatku 2.

— Kako je objašnjeno u odjeljku 9.2.1.2., zapravo može biti potrebno unijeti više generacija K_{M-WC} na jednu karticu radionice.

CSM_105 Osim AES ključa navedenog u CSM_104, MSCA osigurava da je TDES ključ Km_{WC}, naveden u zahtjevu CSM_037 u dijelu A ovog Dodatka, unesen na svaku karticu radionice pod njezinom odgovornošću.

— Time se omogućava upotreba kartice radionice druge generacije za povezivanje s jedinicom u vozilu prve generacije.

— Kartica radionice druge generacije imat će dvije različite primjene, jednu koja je sukladna dijelu B ovog Dodatka i jednu koja je sukladna dijelu A. Potonja će sadržiti TDES ključ Km_{WC}.

CSM_106 MSCA uključena u izdavanje ključeva senzora kretanja izvodi identifikacijski ključ iz glavnog ključa senzora kretanja primjenom funkcije XOR na konstantni vektor CV. Vrijednost CV-a je sljedeća:

— za glavne ključeve senzora kretanja od 128 bitova:CV = ‘B6 44 2C 45 0E F8 D3 62 0B 7A 8A 97 91 E4 5D 83’,

— za glavne ključeve senzora kretanja od 192 bita: CV = ‘72 AD EA FA 00 BB F4 EE F4 99 15 70 5B 7E EE BB 1C 54 ED 46 8B 0E F8 25’,

— za glavne ključeve senzora kretanja od 256 bitova: CV = ‘1D 74 DB F0 34 C7 37 2F 65 55 DE D5 DC D1 9A C3 23 D6 A6 25 64 CD BE 2D 42 0D 85 D2 32 63 AD 60’.

Napomena: konstantni vektori generišu se kako slijedi:

Pi_10 = prvih 10 bajtova decimalnog dijela matematičke konstante π = ‘24 3F 6A 88 85 A3 08 D3 13 19’

CV_128-bits = prvih 16 bajtova SHA-256(Pi_10)

CV_192-bits = prva 24 bajta SHA-384(Pi_10)

CV_256-bits = prva 32 bajta SHA-512(Pi_10)

CSM_107 Svaki proizvođač senzora kretanja generiše nasumični i jedinstveni ključ uparivanja K_P za svaki senzor kretanja te svaki ključ uparivanja šalje certifikacijskom tijelu države članice. MSCA šifrira svaki ključ uparivanja s glavnim ključem senzora kretanja K_M i vraća šifrirani ključ proizvođaču senzora kretanja. Za svaki šifrirani ključ MSCA obavješćuje proizvođača senzora kretanja o broju verzije povezanog K_M.

Napomena: kako je objašnjeno u odjeljku 9.2.1.2., proizvođač senzora kretanja zapravo može trebati generišeti više jedinstvenih ključeva uparivanja za jedan senzor kretanja.

CSM_108 Svaki proizvođač senzora kretanja generiše jedinstveni serijski broj za svaki senzor kretanja te sve serijske brojeve šalje certifikacijskom tijelu države članice. MSCA šifrira svaki serijski broj odvojeno s identifikacijskim ključem K_{ID} te šifrirani serijski broj vraća proizvođaču senzora kretanja. Za svaki šifrirani serijski broj MSCA obavješćuje proizvođača senzora kretanja o broju verzije povezanog K_{ID}.

CSM_109 Za zahtjeve CSM_107 i CSM_108, MSCA upotrebljava AES algoritam u načinu rada „ulančavanje šifriranih blokova”, kako je utvrđeno u normi [ISO 10116], s parametrom preraspodjele (eng. *interleave parameter*) *m* = 1 i inicijalizacijskim vektorom (eng. *initialization vector*) SV = ‘00’ {16}, tj. 16 bajtova s binarnom vrijednošću 0. Prema potrebi, MSCA upotrebljava metodu popunjenja br. 2 iz norme [ISO 9797-1].

CSM_110 Proizvođač senzora kretanja arhivira šifrirani ključ uparivanja i šifrirani serijski broj u predviđeni senzor kretanja zajedno s odgovarajućim vrijednostima nešifriranog teksta i brojem verzije K_M i K_{ID} koji je upotrijebljen za šifriranje.

Napomena: kako je objašnjeno u odjeljku 9.2.1.2., proizvođač senzora kretanja zapravo može trebati unijeti više šifriranih ključeva uparivanja i šifriranih serijskih brojeva u jedan senzor kretanja.

CSM_111 Osim kriptografskog sadržaja na temelju AES-a utvrđenog u CSM_110, proizvođač senzora kretanja isto tako može u svaki senzor kretanja arhivirati kriptografski sadržaj na temelju TDES-a naveden u zahtjevu CSM_037 u dijelu A ovog Dodatka.

Napomena: time se omogućava povezivanje senzora kretanja druge generacije s jedinicom u vozilu prve generacije.

CSM_112 Dužina ključa razmjene podataka K_S koji generiše jedinica u vozilu (VU) tokom uparivanja sa senzorom kretanja povezana je s duljinom njezinog K_{M-VU}, kako je opisano u CSM_50.

9.2.1.2 ***Zamjena glavnog ključa senzora kretanja kod opreme druge generacije***

CSM_113 Svaki glavni ključ senzora kretanja i svi povezani ključevi (vidjeti tablicu 3.) povezani su s određenom generacijom glavnog para ključeva ERCA. Stoga se ti ključevi zamjenjuju svakih 17 godina. Rok važnosti svake

generacije glavnog ključa senzora kretanja počinje godinu dana prije nego što povezani glavni par ključeva ERCA postane važeći te završava kad istekne povezani glavni par ključeva ERCA. To je prikazano na slici 2.

CSM_114 Najmanje godinu dana prije generisanja novog evropskog glavnog para ključeva, kako je opisano u CSM_56, ERCA generiše novi glavni ključ senzora kretanja K_M generisanjem novih $K_{M\text{-}VU}$ i $K_{M\text{-}WC}$. Dužina glavnog ključa senzora kretanja povezana je s predviđenom jakošću novog evropskog glavnog para ključeva u skladu s CSM_50. ERCA dostavlja nove K_M, $K_{M\text{-}VU}$ i $K_{M\text{-}WC}$ MSCA-ovima na njihov zahtjev, zajedno s njihovim brojem verzije.

CSM_115 MSCA osigurava da su sve važeće generacije $K_{M\text{-}WC}$ arhivirane u svakoj kartici radionice izdatoj pod njezinom nadležnošću zajedno s njihovim brojevima verzije, kako je prikazano na slici 2.

Napomena: to znači da će u posljednjoj godini roka važnosti certifikata ERCA kartice radionica biti izdate s tri različite generacije $K_{M\text{-}WC}$, kako je prikazano na slici 2.

CSM_116 U odnosu na postupak opisan u prethodnim CSM_107 i CSM_108: MSCA šifrira svaki ključ uparivanja K_P koji primi od proizvođača senzora kretanja posebno za svaku važeću generaciju glavnog ključa senzora kretanja K_M. Osim toga, MSCA šifrira svaki serijski broj koji primi od proizvođača senzora kretanja posebno za svaku važeću generaciju identifikacijskog ključa K_{ID}. Proizvođač senzora kretanja arhivira sva šifriranja ključa uparivanja i sva šifriranja serijskog broja u predviđeni senzor kretanja zajedno s odgovarajućim vrijednostima nešifriranog teksta i brojem (brojevima) verzije K_M i K_{ID} koji je upotrijebljen za šifriranje.

Napomena: to znači da će u posljednjoj godini roka važnosti certifikata ERCA senzori kretanja biti izdati sa šifriranim podacima na temelju tri različite generacije K_M, kako je prikazano na slici 2.

CSM_117 U odnosu na postupak opisan u prethodnom CSM_107: budući da je dužina ključa uparivanja K_P povezana s duljinom K_M (vidjeti CSM_100), proizvođač senzora kretanja može trebati generišeti do tri različita ključa uparivanja (različitih dužina) za jedan senzor kretanja u slučaju da naredne generacije K_M imaju različite dužine. U takvom slučaju proizvođač svaki ključ uparivanja šalje MSCA-u. MSCA osigurava da je svaki ključ uparivanja šifriran s ispravnom generacijom glavnog ključa senzora kretanja tj. onom jednake dužine.

Napomena: ako proizvođač senzora kretanja izabere generisanje ključa uparivanja na temelju TDES-a za senzor kretanja druge generacije (vidjeti CSM_111), proizvođač MSCA-u navodi da se za šifriranje tog ključa uparivanja mora upotrijebiti glavni ključ senzora kretanja na temelju TDES-a. To je stoga što dužina TDES ključa može biti jednaka dužini AES ključa, a MSCA ne može zaključiti o kojem se ključu radi samo na osnovi dužine ključa.

CSM_118 Proizvođači jedinica u vozilu unose samo jednu generaciju $K_{M\text{-}VU}$ u svaku jedinicu u vozilu zajedno s njegovim brojem verzije. Generacija $K_{M\text{-}VU}$ povezana je s certifikatom ERCA na kojem se temelje certifikati jedinice u vozilu.

— Jedinica u vozilu na temelju generacije *X* certifikata ERCA sadrži samo generaciju *X* $K_{M\text{-}VU,}$ čak i ako je izdata nakon početka roka važnosti generacije *X+1* certifikata ERCA. To je prikazano na slici 2.

— Jedinica u vozilu generacije *X* ne može se upariti sa senzorom kretanja generacije *X-1*.

— Budući da kartice radionica imaju rok važnosti od jedne godine, rezultat CSM_113 – CSM_118 je taj da će sve kartice radionica sadržiti novi $K_{M\text{-}WC}$ u trenutku izdavanja prve jedinice u vozilu s novim $K_{M\text{-}VU}$. Stoga će takva jedinica u vozilu uvijek moći izračunati novi K_M. Nadalje, do tog će trenutka većina novih senzora kretanja isto tako sadržiti šifrirane podatke na temelju $K_{M.}$

9.2.2 *Ključevi za sigurnu komunikaciju preko DSRC-a*

9.2.2.1 *Uopšteno*

CSM_119 Autentičnost i povjerljivost podataka poslanih s jedinice u vozilu nadzornom tijelu putem kanala za komunikaciju na daljinu DSRC-a osigurava se skupom AES ključeva specifičnih za jedinicu u vozilu (VU), koji se izvode iz jedinstvenog DSRC glavnog ključa, KM_{DSRC}.

CSM_120 Glavni ključ DSRC-a KM_{DSRC} je AES ključ koji ERCA generiše, arhivira i distribuira na siguran način. Dužina ključa može biti 128, 192 ili 256 bitova i povezana je s duljinom evropskog glavnog para ključeva, kako je opisano u CSM_50.

CSM_121 ERCA na siguran način dostavlja glavni ključ DSRC-a certifikacijskim tijelima država članica na njihov zahtjev, kako bi im omogućila izvođenje ključeva DSRC-a specifičnih za jedinicu u vozilu i kako bi osigurala da je glavni ključ DSRC-a unesen u sve kontrolne kartice i kartice radionica izdate pod njihovom odgovornošću.

CSM_122 ERCA svakom glavnom ključu DSRC-a dodjeljuje jedinstveni broj verzije. ERCA obavješćuje MSCA-ove o broju verzije kada im šalje glavni ključ DSRC-a.

Napomena: broj verzije upotrebljava se za razlikovanje različitih generacija glavnog ključa DSRC-a, kako je detaljno objašnjeno u odjeljku 9.2.2.2.

CSM_123 Proizvođač jedinica u vozilu za svaku jedinicu u vozilu stvara jedinstveni serijski broj jedinice u vozilu te taj broj šalje svojem certifikacijskom tijelu države članice u zahtjevu za dobivanje skupa od dvaju ključeva DSRC-a specifičnih za jedinicu u vozilu. Serijski broj jedinice u vozilu sadrži vrstu podataka `VuSerialNumber`.

— Taj će serijski broj jedinice u vozilu biti jednak elementu vuSerialNumber informacija VuIdentification, vidjeti Dodatak 1. i upućivanju na nosioca certifikata u certifikatima jedinice u vozilu.

— Serijski broj jedinice u vozilu možda ne bude poznat u trenutku kada proizvođač jedinice u vozilu zatraži ključeve DSRC-a specifične za jedinicu u vozilu. U tom slučaju proizvođač jedinice u vozilu umjesto toga šalje jedinstveni identifikator zahtjeva za certifikat koji je koristio pri podnošenju zahtjeva za certifikat jedinica u vozilu; vidjeti CSM_153. Taj identifikator zahtjeva za certifikat zbog toga je jednak upućivanju na nosioca certifikata u certifikatima jedinica u vozilu.

CSM_124 Po primitku zahtjeva za ključeve DSRC-a specifične za VU, MSCA izvodi dva AES ključa za jedinicu u vozilu, koji se nazivaju K_VU_{DSRC}_ENC i K_VU_{DSRC}_MAC. Ti ključevi specifični za jedinicu u vozilu imaju jednaku dužinu kao glavni ključ DSRC-a. MSCA upotrebljava funkciju izvođenja ključeva utvrđenu u [RFC 5869]. Funkcija raspršivanja (eng. *hash*) koja je potrebna za funkciju HMAC-Hash povezana je s duljinom glavnog ključa DSRC-a, kako je opisano u CSM_50. Funkcija izvođenja ključeva [RFC 5869] upotrebljava se kako slijedi:

Korak 1. (Extract):

— *PRK* = HMAC-Hash (*salt, IKM*), pri čemu je *salt* prazni niz (eng. *empty string*), a *IKM* je KM_{DSRC}.

Korak 2. (Expand):

— *OKM* = *T(1)*, pri čemu je

— *T(1)* = HMAC-Hash (*PRK*, *T(0)* || *info* || '01'), gdje je

— *T(0)* = prazni niz (''),

— 'info = serijski broj jedinice u vozilu ili identifikator zahtjeva za certifikat kako je navedeno u CSM_123

— K_VU_{DSRC}_ENC = prvi *L* okteti *OKM*-a i

— K_VU_{DSRC}_MAC = posljednji *L* okteti *OKM*-a

— gdje je *L* zahtijevana dužina K_VU_{DSRC}_ENC i K_VU_{DSRC}_MAC u oktetima.

CSM_125 MSCA dostavlja K_VU_{DSRC}_ENC i K_VU_{DSRC}_MAC proizvođaču jedinice u vozilu na siguran način za unos u predviđenu jedinicu u vozilu.

CSM_126 Kad je izdata, jedinica u vozilu u svojoj sigurnoj memoriji ima arhivirane K_VU_{DSRC}_ENC i K_VU_{DSRC}_MAC radi osiguravanja integriteta, autentičnosti i povjerljivosti podataka koji se šalju kanalom za komunikaciju na daljinu. Jedinica u vozilu isto tako arhivira broj verzije glavnog ključa DSRC-a koji je upotrijebljen za izvođenje tih ključeva specifičnih za jedinicu u vozilu.

CSM_127 Kad su izdate, kontrolne kartice i kartice radionica u svojoj sigurnoj memoriji imaju pohranjen KM_{DSRC} kako bi mogle provjeriti integritet i autentičnost podataka koje je jedinica u vozilu poslala kanalom za komunikaciju na daljinu te za dešifriranje tih podataka. Kontrolne kartice i kartice radionica arhiviraju i broj verzije glavnog ključa DSRC-a.

Napomena: kako je objašnjeno u odjeljku 9.2.2.2., zapravo može biti potrebno unijeti više generacija K_{DSRC} na jednu karticu radionice ili kontrolnu karticu.

CSM_128 MSCA vodi evidenciju svih ključeva DSRC-a specifičnih za jedinicu u vozilu koje je generišela, njihova broja verzije te serijskog broja jedinice u vozilu ili identifikatora zahtjeva za certifikat koji je korišten za njihovo izvođenje.

9.2.2.2 *Zamjena glavnog ključa DSRC-a*

CSM_129 Svaki glavni ključ DSRC-a povezan je s određenom generacijom glavnog para ključeva ERCA. Stoga ERCA zamjenjuje glavni ključ DSRC-a svakih 17 godina. Rok važnosti svake generacije glavnog ključa DSRC-a počinje dvije godine prije nego što povezani glavni par ključeva ERCA postane važeći te završava kada istekne povezani glavni par ključeva ERCA. To je prikazano na slici 3.

CSM_130 Najmanje dvije godine prije generisanja novog evropskog glavnog para ključeva, kako je opisano u CSM_56, ERCA generiše novi glavni ključ DSRC-a. Dužina glavnog ključa DSRC-a povezana je s predviđenom jakošću novog evropskog glavnog para ključeva u skladu s CSM_50. ERCA dostavlja novi glavni ključ DSRC-a MSCA-ovima na njihov zahtjev, zajedno s njegovim brojem verzije.
CSM_131 MSCA osigurava da su sve važeće generacije K_{DSRC} arhivirane u svakoj kontrolnoj kartici izdatoj pod njezinom nadležnošću zajedno s njihovim brojevima verzije, kako je prikazano na slici 3.
Napomena: to znači da će u posljednje dvije godine roka važnosti certifikata ERCA kontrolne kartice biti izdate s tri različite generacije K_{DSRC}, kako je prikazano na slici 3.
CSM_132 MSCA osigurava da su sve generacije K_{DSRC}, koje su bile važeće najmanje godinu dana i još su uvijek važeće, arhivirane u svakoj kartici radionice izdatoj pod njezinom nadležnošću zajedno s njihovim brojevima verzije, kako je prikazano na slici 3.
Napomena: to znači da će u posljednjoj godini roka važnosti certifikata ERCA kartice radionica biti izdate s tri različite generacije K_{DSRC}, kako je prikazano na slici 3.
CSM_133 Proizvođači jedinica u vozilu unose samo jedan skup ključeva DSRC-a specifičnih za jedinicu u vozilu u svaku jedinicu u vozilu zajedno s njegovim brojem verzije. Taj se skup ključeva izvodi iz generacije KM_{DSRC} povezane s certifikatom ERCA na kojem se temelje certifikati jedinica u vozilu.
— To znači da jedinica u vozilu na temelju generacije *X* certifikata ERCA sadrži samo generaciju *X* K_VU_{DSRC}_ENC i K_VU_{DSRC}_MAC, čak i ako je VU izdat nakon početka roka važnosti generacije *X+1* certifikata ERCA. To je prikazano na slici 3.
— Budući da kartice radionica imaju rok važnosti od jedne godine, a kontrolne kartice od dvije godine, rezultat CSM_131 – CSM_133 je taj da će sve kartice radionica i kontrolne kartice sadržiti novi glavni ključ DSRC-a u trenutku izdavanja prve jedinice u vozilu s novim ključevima specifičnima za jedinicu u vozilu na temelju tog glavnog ključa.

9.3. Certifikati

9.3.1 *Uopšteno*

CSM_134 Svi su certifikati u Evropskom sistemu pametnog tahografa samoopisni, karticom provjerljivi (eng. *card-verifiable*, CV) certifikati u skladu s normama [ISO 7816-4] i [ISO 7816-8].
CSM_135 Za kodiranje podatkovnih objekata u certifikatima upotrebljavaju se posebna pravila kodiranja (DER) u skladu s normom [ISO 8825-1]. Tablica 4. prikazuje potpuno kodiranje certifikata, uključujući sve oznake i dužine bajtova.
Napomena: takvo kodiranje daje sljedeću strukturu vrijednosti dužine oznake (eng. *Tag-Length-Value*, TLV):
oznaka : Oznaka je kodirana u jednom ili dva okteta i označava sadržaj.
dužina : Dužina je kodirana kao nepotpisani cijeli broj u jednom, dva ili tri okteta, što dovodi do najveće dužine od 65 535 okteta. Upotrebljava se najmanji broj okteta.
vrijednost : Vrijednost je kodirana u nula ili više okteta.

9.3.2 *Sadržaj certifikata*

CSM_136 Svi certifikati imaju strukturu prikazanu u profilu certifikata u tablici 4.

Tablica 4.

Profil certifikata – verzija 1

Polje	ID polja	Oznaka	Dužina (bajtova)	Vrsta podataka ASN.1 (vidjeti Dodatak 1.)
ECC certifikat	C	'7F 21'	var	
Tijelo ECC certifikata	B	'7F 4E'	var	
Identifikator profila certifikata	CPI	'5F 29'	'01'	[illegible]
Upućivanje na certifikacijsko tijelo	CAR	'42'	'08'	[illegible]
Ovlaštenje nosioca certifikata	CHA	'5F 4C'	'07'	CertificateHolder[illegible]
Javni ključ	PK	'7F 49'	var	
Parametri domene	DP	'06'	var	OBJECT IDENTIFIER
Javna tačka	PP	'86'	var	[illegible]
Upućivanje na nosioca certifikata	CHR	'5F 20'	'08'	[illegible]
Datum početka važnosti certifikata	CEfD	'5F 25'	'04'	[illegible]
Datum isteka važnosti certifikata	CExD	'5F 24'	'04'	[illegible]
Potpis ECC certifikata	S	'5F 37'	var	[illegible]

Napomena: ID polja upotrebljavat će se u kasnijim odjeljcima ovog Dodatka za označivanje pojedinačnih polja certifikata, npr. X.CAR je upućivanje na certifikacijsko tijelo navedeno u certifikatu korisnika X.

9.3.2.1 Identifikator profila certifikata

CSM_137 Certifikati upotrebljavaju identifikator profila certifikata za označivanje upotrijebljenog profila certifikata. Verzija 1, kako je navedena u tablici 4., identificira se vrijednošću '00'.

9.3.2.2 Upućivanje na certifikacijsko tijelo

CSM_138 Upućivanje na certifikacijsko tijelo upotrebljava se za identifikaciju javnog ključa koji treba upotrijebiti za provjeru potpisa certifikata. Upućivanje na certifikacijsko tijelo stoga je jednako upućivanju na nosioca certifikata u certifikatu odgovarajućeg certifikacijskog tijela.
CSM_139 Glavni certifikat ERCA samopotpisan je, tj. upućivanje na certifikacijsko tijelo i upućivanje na nosioca certifikata u certifikatu jednaki su.
CSM_140 Za certifikat o povezanosti ERCA, upućivanje na nosioca certifikata jednako je CHR-u novog glavnog certifikata ERCA. Upućivanje na certifikacijsko tijelo za certifikat o povezanosti jednako je CHR-u prethodnog glavnog certifikata ERCA.

9.3.2.3 Ovlaštenje nosioca certifikata

CSM_141 Ovlaštenje nosioca certifikata upotrebljava se za identifikaciju vrste certifikata. Sastoji se od šest najznačajnijih bajtova identifikatora (ID) tahografske aplikacije, ulančanih s vrstom opreme, koji označavaju vrstu opreme za koju je certifikat namijenjen. U slučaju certifikata jedinice u vozilu, certifikata kartice vozača ili certifikata kartice radionice, vrsta opreme također se koristi za razlikovanje između certifikata za uzajamnu autentifikaciju i certifikata za stvaranje digitalnih potpisa (vidjeti odjeljak 9.1 i Dodatak 1., vrsta podataka EquipmentType).

9.3.2.4 Javni ključ

Javni ključ sadrži dva podatkovna elementa: normirane parametre domene koji se upotrebljavaju s javnim ključem u certifikatu i vrijednosti javne točke (eng. *public point*).

CSM_142 Podatkovni element parametara domene sadrži jedan od identifikatora objekta navedenih u tablici 1. za upućivanje na skup normiranih parametara domene.

CSM_143 Podatkovni element javne točke sadrži javnu tačku. Javne točke eliptičke krivulje pretvaraju se u oktetne nizove kako je navedeno u [TR-03111]. Upotrebljava se nekomprimirani format kodiranja. Pri obnavljanju točke eliptičke krivulje iz njezina kodiranog formata uvijek se provode potvrde opisane u [TR-03111].

9.3.2.5 Upućivanje na nosioca certifikata

CSM_144 Upućivanje na nosioca certifikata je identifikator za javni ključ osiguran u certifikatu. Upotrebljava se za upućivanje na taj javni ključ u drugim certifikatima.

CSM_145 Za certifikate kartica i certifikate vanjskih uređaja GNSS-a, upućivanje na nosioca certifikata sadrži vrstu podataka ExtendedSerialNumber navedenu u Dodatku 1.

CSM_146 Za jedinice u vozilu proizvođač pri podnošenju zahtjeva za certifikat može, ali ne mora, znati serijski broj jedinice u vozilu, specifičan za proizvođača, za koju su taj certifikat i povezani privatni ključ namijenjeni. U prvom slučaju, upućivanje na nosioca certifikata sadrži vrstu podataka ExtendedSerialNumber navedenu u Dodatku 1. U drugom slučaju, upućivanje na nosioca certifikata sadrži vrstu podataka CertificateRequestID navedenu u Dodatku 1.

Napomena: za certifikat kartice vrijednost CHR-a jednaka je vrijednosti cardExtendedSerialNumber u EF_ICC-u; vidjeti Dodatak 2. Za certifikat EGF vrijednost CHR-a jednaka je vrijednosti sensorGNSSSerialNumber u EF_ICC-u; vidjeti Dodatak 14. Za certifikat jedinice u vozilu vrijednost CHR-a jednaka je elementu vuSerialNumber informacija VuIdentification, vidjeti Dodatak 1., osim ako proizvođač ne zna serijski broj specifičan za proizvođača u trenutku podnošenja zahtjeva za certifikat.

CSM_147 Za certifikate ERCA i MSCA, upućivanje na nosioca certifikata sadrži vrstu podataka CertificationAuthorityKID navedenu u Dodatku 1.

9.3.2.6 Datum početka važnosti certifikata

CSM_148 Datum početka važnosti certifikata označava datum i vrijeme početka roka važnosti certifikata.

9.3.2.7 Datum isteka važnosti certifikata

CSM_149 Datum isteka važnosti certifikata označava datum i vrijeme isteka roka važnosti certifikata.

9.3.2.8 Potpis certifikata

CSM_150 Potpis certifikata stvara se za kodirano tijelo certifikata, uključujući oznaku i dužinu tijela certifikata. Algoritam potpisa je ECDSA, kako je utvrđeno u [DSS], upotrebom algoritma raspršivanja (*hash*) povezanog s veličinom ključa nadležnog tijela potpisnika, kako je navedeno u CSM_50. Format potpisa je nešifriran, kako je navedeno u [TR-03111].

9.3.3 *Podnošenje zahtjeva za certifikate*

CSM_151 Prilikom podnošenja zahtjeva za certifikat, MSCA šalje sljedeće podatke ERCA-u:

— identifikator profila certifikata zahtijevanog certifikata,

— upućivanje na certifikacijsko tijelo za koje se očekuje da će se upotrebljavati za potpisivanje certifikata,

— javni ključ koji treba potpisati.

CSM_152 Osim podataka iz CSM_151, MSCA šalje sljedeće podatke u zahtjevu za certifikat ERCA-i, čime ERCA-i omogućava stvaranje upućivanja na nosioca certifikata novog certifikata MSCA:

— numerički kod države certifikacijskog tijela (vrsta podataka [illegible] utvrđena u Dodatku 1.),

— alfanumerički kod države certifikacijskog tijela (vrsta podataka [illegible] utvrđena u Dodatku 1.),

— Jednobajtni serijski broj za razlikovanje različitih ključeva certifikacijskog tijela u slučaju promjene ključeva,

— Dvobajtno polje koje sadrži posebne dodatne informacije o certifikacijskom tijelu.

CSM_153 Proizvođač opreme šalje sljedeće podatke u zahtjevu za certifikat MSCA-u, čime MSCA-u omogućava stvaranje upućivanja na nosioca certifikata novog certifikata opreme:

— ako je poznat (vidjeti CSM_154), serijski broj opreme, jedinstven za proizvođača, vrstu opreme te mjesec proizvodnje. U protivnom, jedinstveni identifikator zahtjeva za certifikat,

— mjesec i godinu proizvodnje opreme ili zahtjeva za certifikat.

Proizvođač osigurava da su ti podaci točni i da je certifikat koji je MSCA vratio unesen u predviđenu opremu.

CSM_154 U slučaju jedinice u vozilu, proizvođač pri podnošenju zahtjeva za certifikat može, ali ne mora, znati serijski broj jedinice u vozilu, specifičan za proizvođača, za koju su taj certifikat i povezani privatni ključ namijenjeni. Ako je poznat, proizvođač jedinice u vozilu šalje serijski broj MSCA-i. Ako nije poznat, proizvođač na jedinstveni način identificira svaki zahtjev za certifikat te taj serijski broj zahtjeva za certifikat šalje MSCA-i. Dobiveni certifikat nakon toga sadrži serijski broj zahtjeva za certifikat. Nakon unošenja certifikata u specifičnu jedinicu u vozilu, proizvođač MSCA-i šalje vezu između serijskog broja zahtjeva za certifikat i identifikacije jedinice u vozilu.

10. UZAJAMNA AUTENTIFIKACIJA I SIGURAN PRENOS PORUKA IZMEĐU JEDINICA U VOZILU I KARTICA

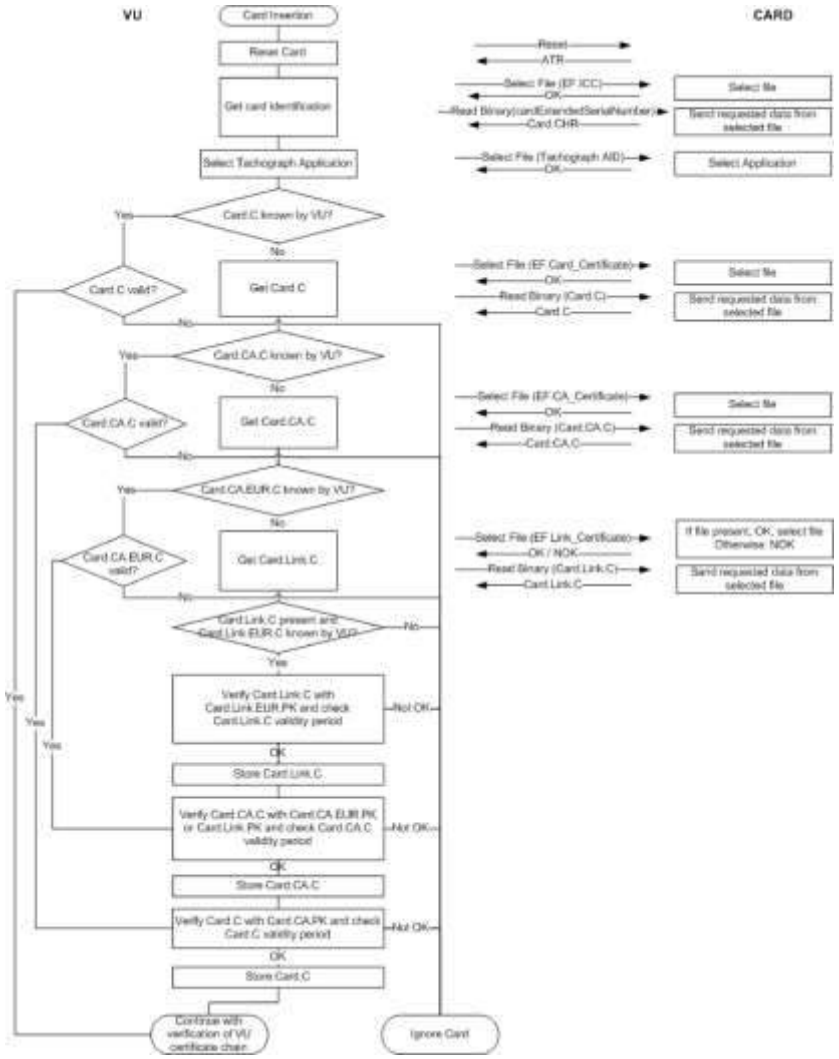
10.1. Uopšteno

CSM_155 Na visokoj se nivou sigurna komunikacija između jedinice u vozilu i tahografske kartice temelji na sljedećim koracima:
— Prvo, svaka strana drugoj strani dokazuje da je vlasnik važećiog certifikata javnog ključa koji je potpisalo certifikacijsko tijelo države članice. Zauzvrat, certifikat javnog ključa MSCA mora potpisati evropsko tijelo za izdavanje glavnog certifikata. Taj se korak naziva provjera lanca certifikata te su njegove pojedinosti navedene u odjeljku 10.2.
— Drugo, jedinica u vozilu dokazuje kartici da posjeduje privatni ključ koji odgovara javnom ključu u predočenom certifikatu. To radi tako da potpiše slučajni broj koji je poslala kartica. Kartica provjerava potpis tog slučajnog broja. Ako je ta provjera uspješna, jedinica u vozilu je autentificirana. Taj se korak naziva autentifikacija jedinice u vozilu te su njegove pojedinosti navedene u odjeljku 10.3.
— Treće, obje strane samostalno izračunavaju dva AES ključa razmjene podataka s pomoću asimetričnog algoritma dogovaranja ključa. Upotrebom jednog od tih ključeva razmjene podataka, kartica stvara kod za autentifikaciju poruke (MAC) za određene podatke koje je poslala jedinica u vozilu. Jedinica u vozilu provjerava MAC. Ako je ta provjera uspješna, kartica je autentificirana. Taj se korak naziva autentifikacija kartice te su njegove pojedinosti navedene u odjeljku 10.4.
— Četvrto, jedinica u vozilu i kartica upotrebljavaju dogovorene ključeve razmjene podataka kako bi osigurale povjerljivost, integritet i autentičnost svih razmijenjenih poruka. Taj se korak naziva siguran prenos poruka te su njegove pojedinosti navedene u odjeljku 10.5.
CSM_156 Mehanizam opisan u CSM_155 aktivira jedinica u vozilu svaki put kad je kartica umetnuta u jedan od njezinih otvora za kartice.

10.2. Uzajamna provjera lanca certifikata

10.2.1 ***Provjera lanca certifikata kartice koju sprovodi jedinica u vozilu***

CSM_157 Za provjeru lanca certifikata tahografske kartice, jedinice u vozilu upotrebljavaju protokol prikazan na slici 4. Za svaki certifikat koji očita s kartice, jedinica u vozilu potvrđuje da je polje ovlaštenja nosioca certifikata (CHA) ispravno:
— u polju CHA certifikata kartice navodi se certifikat kartice za uzajamnu autentifikaciju (vidjeti Dodatak 1., vrstu podataka EquipmentType),
— u polju CHA certifikata Card.CA navodi se MSCA,
— u polju CHA certifikata Card.Link navodi se ERCA.
Napomene za sliku 4.:
— Certifikati Card i javni ključevi prikazani na slici oni su za uzajamnu autentifikaciju. U odjeljku 9.1.5. označeni su kao Card_MA,
— Certifikati Card.CA i javni ključevi prikazani na slici oni su za potpisivanje certifikata kartica navedeni u CAR-u certifikata Card. U odjeljku 9.1.3. označeni su kao MSCA_Card,
— Certifikat Card.CA.EUR prikazan na slici je evropski glavni certifikat koji je naveden u CAR certifikata Card.CA,
— Certifikat Card.Link prikazan na slici je certifikat o povezanosti kartice, ako postoji. Kako je navedeno u odjeljku 9.1.2., to je certifikat o povezanosti za novi evropski glavni par ključeva koji je ERCA stvorila i potpisala prethodnim evropskim privatnim ključem,
— Certifikat Card.Link.EUR je evropski glavni certifikat koji je naveden u CAR certifikata Card.Link,
CSM_158 Kako je prikazano na slici 4., provjera lanca certifikata kartice počinje nakon umetanja kartice. Jedinica u vozilu čita upućivanje na nosioca kartice (cardExtendedSerialNumber) iz elementarne datoteke (EF) ICC. Jedinica u vozilu provjerava poznaje li karticu, tj. je li u prošlosti uspješno provjerila certifikat kartice i pohranila ga za buduću upotrebu. Ako poznaje karticu te je certifikat kartice još uvijek važeći, postupak se nastavlja provjerom lanca certifikata jedinice u vozilu. U protivnom, jedinica u vozilu uzastopno s kartice čita certifikat MSCA_Card koji se upotrebljava za provjeru certifikata kartice, certifikat Card.CA.EUR koji se upotrebljava za provjeru certifikata MSCA_Card te eventualno certifikat o povezanosti koji se upotrebljava za provjeru certifikata EUR dok ne nađe certifikat koji poznaje ili može provjeriti. Ako nađe takav certifikat, jedinica u vozilu upotrebljava taj certifikat za provjeru temeljnih certifikata kartice koje je pročitala s kartice. Ako je provjera uspješna, postupak se nastavlja provjerom lanca certifikata jedinice u vozilu. Ako provjera nije uspješna, jedinica u vozilu zanemaruje karticu.
Napomena: Postoje tri načina na koje jedinica u vozilu može prepoznati certifikat Card.CA.EUR:
— certifikat Card.CA.EUR isti je certifikat kao i vlastiti certifikat EUR jedinice u vozilu;
— certifikat Card.CA.EUR prethodi vlastitom certifikatu EUR jedinice u vozilu te je jedinica u vozilu već sadržila taj certifikat pri izdavanju (vidjeti CSM_81);
— certifikat Card.CA.EUR nasljeđuje vlastiti certifikat EUR jedinice u vozilu te je jedinica u vozilu u prošlosti primila certifikat o povezanosti od druge tahografske kartice, provjerila ga i pohranila za buduću upotrebu.
CSM_159 Kako je prikazano na slici 4., kad je jedinica u vozilu provjerila autentičnost i važnost prethodno nepoznatog certifikata, taj certifikat može arhivirati za buduću upotrebu tako da ne mora ponovno provjeravati autentičnost tog certifikata ako je ponovno predočen jedinici u vozilu. Osim arhiviranja cijelog certifikata, jedinica u vozilu može odabrati arhivirati samo sadržaj tijela certifikata, kako je navedeno u odjeljku 9.3.2. Dok je arhiviranje svih drugih vrsta certifikata neobvezno, jedinica u vozilu mora arhivirati novi certifikat o povezanosti koji predoči kartica.
CSM_160 Jedinica u vozilu provjerava vremensku važnost svakog certifikata pročitanog s kartice ili pohranjenog u memoriji jedinice u vozilu te odbija certifikate koji su istekli. Jedinica u vozilu za provjeru vremenske važnosti certifikata koji je predočila kartica upotrebljava svoj unutarnji sat.



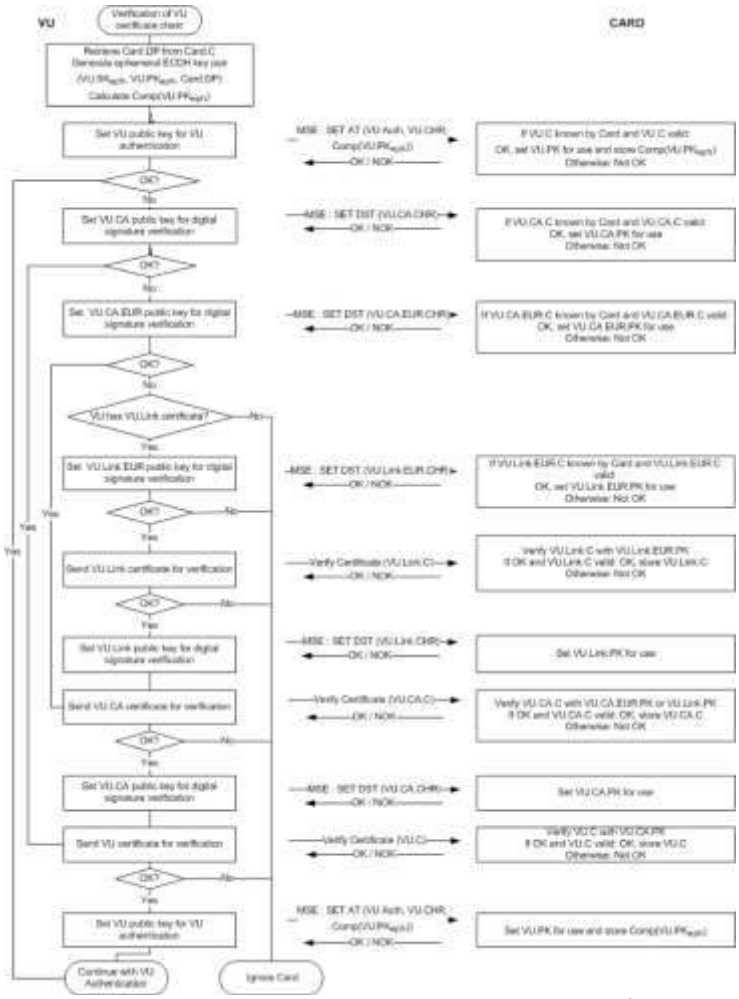
10.2.2 ***Provjera lanca certifikata jedinice u vozilu koju sprovodi kartica***

CSM_161 Za provjeru lanca certifikata jedinice u vozilu, tahografske kartice upotrebljavaju protokol prikazan na slici 5. Za svaki certifikat koji predoči jedinica u vozilu, kartica potvrđuje da je polje ovlaštenja nosioca certifikata (CHA) ispravno:

— u polju CHA certifikata VU.Link navodi se ERCA,

— u polju CHA certifikata VU.CA navodi se MSCA,

— u polju CHA certifikata jedinice u vozilu navodi se certifikat jedinice u vozilu za uzajamnu autentifikaciju (vidjeti Dodatak 1., vrstu podataka EquipmentType).



— Certifikati jedinice u vozilu i javni ključevi prikazani na slici oni su za uzajamnu autentifikaciju. U odjeljku 9.1.4. označeni su kao VU_MA,

— Certifikati VU.CA i javni ključevi prikazani na slici oni su za potpisivanje certifikata jedinica u vozilu i vanjskih uređaja GNSS-a. U odjeljku 9.1.3. označeni su kao MSCA_VU-EGF.

— Certifikat VU.CA.EUR prikazan na slici je evropski glavni certifikat koji je naveden u CAR certifikata VU.CA,

— Certifikat VU.Link prikazan na slici je certifikat o povezanosti jedinice u vozilu, ako postoji. Kako je navedeno u odjeljku 9.1.2., to je certifikat o povezanosti za novi evropski glavni par ključeva koji je ERCA stvorila i potpisala prethodnim evropskim privatnim ključem.

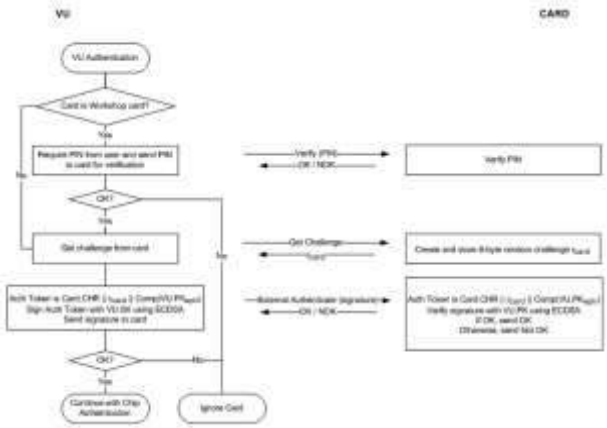
— Certifikat VU.Link.EUR je evropski glavni certifikat koji je naveden u CAR certifikata VU.Link.

CSM_162 Kako je prikazano na slici 5., provjera lanca certifikata jedinice u vozilu počinje tako da jedinica u vozilu pokuša postaviti svoj vlastiti javni ključ za upotrebu u tahografskoj kartici. Ako u tome uspije, znači da je kartica u prošlosti uspješno provjerila lanac certifikata jedinice u vozilu i pohranila certifikat jedinice u vozilu za buduću upotrebu. U tom se slučaju certifikat jedinice u vozilu postavlja za upotrebu i postupak se nastavlja autentifikacijom jedinice u vozilu. Ako kartica ne prepoznaje jedinicu u vozilu, jedinica u vozilu uzastopno predočuje certifikat MSCA_VU koji se upotrebljava za provjeru njezina certifikata jedinice u vozilu, certifikat VU.CA.EUR koji se upotrebljava za provjeru certifikata MSCA_VU te potencijalno certifikat o povezanosti, kako bi se pronašao certifikat koji kartica prepoznaje ili može provjeriti. Ako je takav certifikat pronađen, kartica upotrebljava taj certifikat za provjeru temeljnih certifikata jedinice u vozilu koji su joj predočeni. Ako je uspješna,

jedinica u vozilu konačno postavlja svoj javni ključ za upotrebu u tahografskoj kartici. Ako provjera nije uspješna, jedinica u vozilu zanemaruje karticu.
Napomena: Postoje tri načina na koje kartica može prepoznati certifikat VU.CA.EUR:
— certifikat VU.CA.EUR isti je certifikat kao i vlastiti certifikat EUR kartice;
— certifikat VU.CA.EUR prethodi vlastitom certifikatu EUR kartice te je kartica već sadržila taj certifikat pri izdavanju (vidjeti CSM_91);
— certifikat VU.CA.EUR nasljeđuje vlastiti certifikat EUR kartice te je kartica u prošlosti primila certifikat o povezanosti od druge jedinice u vozilu, provjerila ga i pohranila za buduću upotrebu.
CSM_163 VU upotrebljava naredbu MSE: SET AT za postavljanje svojeg javnog ključa za upotrebu u tahografskoj kartici. Kako je navedeno u Dodatku 2., ta naredba sadrži oznaku kriptografskog mehanizma koji će se upotrebljavati s postavljenim ključem. Taj je mehanizam „autentifikacija jedinice u vozilu upotrebom algoritma ECDSA u kombinaciji s algoritmom raspršivanja (*hash*) povezanim s veličinom ključa para VU_MA ključeva jedinice u vozilu, kako je navedeno u CSM_50".
CSM_164 Naredba MSE: SET AT isto tako sadrži oznaku kratkotrajnog para ključeva koje jedinica u vozilu upotrebljava tokom dogovaranja ključa razmjene podataka (vidjeti odjeljak 10.4.). Stoga prije slanja naredbe MSE: SET AT jedinica u vozilu generiše kratkotrajni par ECC ključeva. Za generisanje kratkotrajnog para ključeva VU upotrebljava normirane parametre domene navedene u certifikatu kartice. Kratkotrajni par ključeva označava se kao ($VU.SK_{eph}$, $VU.PK_{eph}$, Card.DP). Jedinica u vozilu uzima x-koordinatu ECDH kratkotrajne javne točke kao identifikaciju ključa; to se naziva komprimirano predstavljanje javnog ključa i označava se kao $Comp(VU.PK_{eph})$.
CSM_165 Ako je naredba MSE: Set AT uspješna, kartica postavlja navedeni VU.PK za kasniju upotrebu tokom autentifikacije vozila te privremeno arhivira Comp(VU.PKeph). U slučaju slanja jedne ili više uspješnih naredbi MSE: Set AT prije provedbe dogovaranja ključa razmjene podataka, kartica arhivira samo zadnji primljeni Comp(VU.PKeph). Nakon uspješne naredbe GENERAL AUTHENTICATE kartica će vratiti Comp(VU.PKeph) u početno stanje.
CSM_166 Kartica provjerava vremensku važnost svakog certifikata koji jedinica u vozilu predočava ili na njega upućuje dok je pohranjen u memoriji kartice te odbija certifikate koji su istekli.
CSM_167 Za provjeru vremenske važnosti certifikata koji je predočila jedinica u vozilu, svaka tahografska kartica interno arhivira određene podatke koji predstavljaju trenutačno vrijeme. Jedinica u vozilu te podatke ne smije moći direktno ažurirati. Pri izdavanju trenutačno se vrijeme kartice postavlja tako da je jednako datumu početka važnosti certifikata kartice Card_MA. Kartica ažurira svoje trenutačno vrijeme ako je datum početka važnosti autentičnog certifikata „važećiog izvora vremena" koji je predočila jedinica u vozilu noviji od trenutačnog vremena kartice. U tom slučaju kartica postavlja svoje trenutačno vrijeme na datum početka važnosti tog certifikata. Kartica kao važećii izvor vremena prihvaća samo sljedeće certifikate:
— certifikate o povezanosti ERCA druge generacije,
— certifikate MSCA druge generacije,
— certifikate jedinice u vozilu druge generacije koje je izdala ista država kao i vlastiti certifikat (certifikate) kartice.
Napomena: posljednji zahtjev znači da kartica može prepoznati CAR certifikata jedinice u vozilu, tj. certifikat MSCA_VU-EGF. On nije jednak CAR-u njezina vlastitog certifikata, odnosno certifikata MSCA_Card.
CSM_168 Kako je prikazano na slici 5., kada je kartica provjerila autentičnost i važnost prethodno nepoznatog certifikata, taj certifikat može arhivirati za buduću upotrebu tako da ne mora ponovno provjeravati autentičnost tog certifikata ako je ponovno predočen kartici. Osim arhiviranja cijelog certifikata, kartica može odabrati arhivirati samo sadržaj tijela certifikata, kako je navedeno u odjeljku 9.3.2.

10.3. Autentifikacija jedinice u vozilu

CSM_169 Jedinice u vozilu i kartice upotrebljavaju protokol autentifikacije jedinice u vozilu prikazan na slici 6. za autentifikaciju jedinice u vozilu s obzirom na karticu. Autentifikacija jedinice u vozilu omogućava tahografskoj kartici da izričito provjeri autentičnost jedinice u vozilu. Kako bi to učinila, jedinica u vozilu upotrebljava svoj privatni ključ za potpisivanje zahtjeva za ključnu riječ koji generiše kartica.
CSM_170 Uz zahtjev kartice za ključnu riječ, jedinica u vozilu u potpis uključuje upućivanje na nosioca certifikata preuzeto iz certifikata kartice.
Napomena: time se osigurava da je kartica koju jedinica u vozilu sama autentificira ista kartica čiji je lanac certifikata jedinica u vozilu prethodno provjerila.
CSM_171 Osim toga, jedinica u vozilu u potpis uključuje identifikator kratkotrajnog javnog ključa $Comp(VU.PK_{eph})$ koji jedinica u vozilu upotrebljava za uspostavu sigurnog prenosa poruka tokom postupka autentifikacije čipa navedenog u odjeljku 10.4.
Napomena: time se osigurava da je jedinica u vozilu s kojom kartica komunicira tokom procesa sigurnog prenosa poruka ista jedinica u vozilu koju je autentificirala kartica.
Slika 6.
Protokol za autentifikaciju jedinice u vozilu



CSM_172 Ako jedinica u vozilu tokom autentifikacije jedinice u vozilu pošalje više naredbi GET CHALLENGE, kartica svaki put vraća novi 8-bajtni nasumični zahtjev za ključnu riječ, ali arhivira samo posljednji zahtjev za ključnu riječ.

CSM_173 Algoritam potpisivanja koji jedinica u vozilu upotrebljava za autentifikaciju jedinice u vozilu je ECDSA, kako je navedeno u [DSS], upotrebom algoritma raspršivanja (*hashing*) povezanog s veličinom ključa para VU_MA ključeva jedinice u vozilu, kako je navedeno u CSM_50. Format potpisa je nešifriran, kako je navedeno u [TR-03111]. Dobiveni potpis jedinica u vozilu šalje kartici.

CSM_174 Nakon što primi potpis jedinice u vozilu u naredbi EXTERNAL AUTHENTICATE, kartica:

— izračunava token autentifikacije ulančavanjem Card.CHR, zahtjeva kartice za ključnu riječ rcard i identifikatora kratkotrajnog javnog ključa jedinice u vozilu Comp(VU.PKeph),

— provjerava potpis jedinice u vozilu koristeći algoritam ECDSA, koristeći algoritam raspršivanja (hashing) povezan s veličinom ključa para VU_MA ključeva jedinice u vozilu u skladu sa stavkom CSM_50, u kombinaciji s VU.PK i izračunanim tokenom autentifikacije.

10.4. Autentifikacija čipa i dogovaranje ključa razmjene podataka

CSM_175 Jedinice u vozilu i kartice upotrebljavaju protokol autentifikacije čipa prikazan na **slici 7.** za autentifikaciju kartice u odnosu na jedinicu u vozilu. Autentifikacija čipa omogućava jedinici u vozilu da izričito provjeri autentičnost kartice.

Slika 7.

Autentifikacija čipa i dogovaranje ključa razmjene podataka

CSM_176 Jedinica u vozilu i kartica poduzimaju sljedeće korake:

1. Jedinica u vozilu započinje postupak autentifikacije čipa slanjem naredbe MSE: SET AT u kojoj se navodi „autentifikacija čipa s pomoću algoritma ECDSA kojim se dobiva dužina AES ključa razmjene podataka povezana s veličinom ključa para Card_MA ključeva kartice, kako je navedeno u CSM_50". Jedinica u vozilu utvrđuje veličinu ključa para ključeva kartice iz certifikata kartice.

2. Jedinica u vozilu kartici šalje javnu tačku $VU.PK_{eph}$ svojeg kratkotrajnog para ključeva. Javna tačka pretvara se u oktetni niz kako je navedeno u [TR-03111]. Upotrebljava se nekomprimirani format kodiranja. Kako je objašnjeno u stavu CSM_164, jedinica u vozilu taj kratkotrajni par ključeva generiše prije provjere lanca

certifikata jedinice u vozilu. Jedinica u vozilu poslala je identifikator kratkotrajnog javnog ključa Comp($VU.PK_{eph}$) kartici te ga je kartica pohranila.
3. Kartica izračunava Comp($VU.PK_{eph}$) iz $VU.PK_{eph}$ i uspoređuje ga s pohranjenom vrijednošću Comp(VU.PKeph).
4. Primjenom algoritma ECDH u kombinaciji sa statičkim privatnim ključem i kratkotrajnim javnim ključem jedinice u vozilu, kartica izračunava tajni K.
5. Kartica odabire nasumični 8-bajtni broj za jednokratnu upotrebu (eng. *number used only once*, *nonce*) N_{PICC} i upotrebljava ga za izvođenje dvaju AES ključeva razmjene podataka K_{MAC} i K_{ENC} iz K. Vidjeti CSM_179.
6. Koristeći K_{MAC} kartica izračunava token autentifikacije preko kratkotrajne javne točke jedinice u vozilu: T_{PICC} = CMAC(K_{MAC}, $VU.PK_{eph}$). Javna tačka mora biti u formatu koji koristi jedinica u vozilu (vidjeti prethodno navedenu podtačku 2.). Kartica šalje N_{PICC} i T_{PICC} jedinici vozila.
7. Primjenom algoritma ECDH u kombinaciji sa statičkim javnim ključem i kratkotrajnim javnim ključem jedinice u vozilu, jedinica u vozilu izračunava isti tajni K kao kartica u koraku 4.
8. Jedinica u vozilu izvodi ključeve razmjene podataka K_{MAC} i K_{ENC} iz K i N_{PICC}. Vidjeti CSM_179.
9. Jedinica u vozilu provjerava token autentifikacije T_{PICC}.
CSM_177 U prethodnom koraku 3. kartica izračunava Comp($VU.PK_{eph}$) kao x-koordinatu javne točke u $VU.PK_{eph}$.
CSM_178 U prethodnim koracima 4. i 7. kartica i jedinica u vozilu upotrebljavaju algoritam ECKA-EG kako je utvrđeno u [TR-03111].
CSM_179 U prethodnim koracima 5. i 8. kartica i jedinica u vozilu upotrebljavaju funkciju izvođenja ključeva za AES ključeve razmjene podataka utvrđene u [TR-03111] sa sljedećim preciznostima i promjenama:
— vrijednost brojača iznosi '00 00 00 01' za K_{ENC} i '00 00 00 02'za K_{MAC},.
— upotrebljava se neobavezni broj za jednokratnu upotrebu (*nonce*) r koji je jednak N_{PICC}.
— Za izvođenje AES ključeva od 128 bitova upotrebljava se algoritam raspršivanja (*hashing*) SHA-256,
— Za izvođenje AES ključeva od 192 bita upotrebljava se algoritam raspršivanja (*hashing*) SHA-384,
— Za izvođenje AES ključeva od 256 bitova upotrebljava se algoritam raspršivanja (*hashing*) SHA-512.
Dužina ključeva razmjene podataka (tj. dužina na koju je *hash* skraćen) povezana je s veličinom para Card_MA ključeva, kako je navedeno u CSM_50.
CSM_180 U prethodnim koracima 6. i 9. kartica i jedinica u vozilu upotrebljavaju AES algoritam u načinu rada CMAC, kako je navedeno u [SP 800-38B]. Dužina T_{PICC} povezana je s duljinom AES ključeva razmjene podataka, kako je navedeno u CSM_50.

10.5. Siguran prenos poruka

10.5.1 *Uopšteno*

CSM_181 Sve naredbe i odgovori razmijenjeni između jedinice u vozilu i tahografske kartice nakon uspješne autentifikacije čipa i do završetka razmjene podataka zaštićeni su sigurnim prenosom poruka.
CSM_182 Osim pri čitanju iz datoteke s uslovom pristupa SM-R-ENC-MAC-G2 (vidjeti Dodatak 2., odjeljak 4.), siguran prenos poruka upotrebljava se u načinu rada namijenjenom isključivo autentifikaciji. U tom se načinu rada kriptografski kontrolni zbir (odnosno MAC) dodaje svim naredbama i odgovorima u svrhu osiguranja autentičnosti i integriteta poruke.
CSM_183 Pri čitanju podataka iz datoteke s uslovom pristupa SM-R-ENC-MAC-G2, siguran prenos poruka upotrebljava se u načinu rada namijenjenom šifriranju i zatim autentifikaciji, tj. podaci odgovora prvo se šifriraju u svrhu osiguranja povjerljivosti poruke, a zatim se izračunava MAC za formatirane šifrirane podatke u svrhu osiguranja autentičnosti i integriteta.
CSM_184 Siguran prenos poruka upotrebljava AES kako je utvrđen u [AES] s ključevima razmjene podataka K_{MAC} i K_{ENC} koji su dogovoreni tokom autentifikacije čipa.
CSM_185 Kao brojač redoslijeda slanja (SSC) upotrebljava se nepotpisani cijeli broj u svrhu sprječavanja napada reprodukcijom. Veličina SSC-a jednaka je veličini AES bloka, tj. 128 bitova. SSC je u formatu MSB-first. Brojač redoslijeda slanja (SSC) postavlja se na nulu (tj. '00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00') prilikom početka sigurnog prenosa poruka. SSC se povećava svaki put prije generisanja naredbe ili odgovora APDU, tj. budući da je početna vrijednost SSC-a u procesu sigurnog prenosa poruke (SM) 0, u prvoj će naredbi vrijednost SSC-a biti 1. Vrijednost SSC-a za prvi odgovor bit će 2.
CSM_186 Za šifriranje poruka upotrebljava se K_{ENC} s AES-om u načinu rada „ulančavanje šifriranih blokova" (CBC), kako je utvrđeno u [ISO 10116], s parametrom preraspodjele (eng. *interleave parameter*) *m* = 1 i inicijalizacijskim vektorom (eng. *initialization vector*) SV = E(K_{ENC}, SSC), tj. trenutačnom vrijednošću brojača redoslijeda slanja šifriranom s K_{ENC}.
CSM_187 Za autentifikaciju poruka upotrebljava se K_{MAC} s AES-om u načinu rada CMAC kako je navedeno u [SP 800-38B]. Dužina MAC povezana je s duljinom AES ključeva razmjene podataka, kako je navedeno u CSM_50. Brojač redoslijeda slanja (SSC) uključuje se u MAC njegovim dodavanjem na početak prije bloka podataka (eng. *datagram*) koji se autentificira.

10.5.2 *Struktura sigurne poruke*

CSM_188 Siguran prenos poruka upotrebljava samo podatkovne objekte sigurnog prenosa poruka (vidjeti normu [ISO 7816-4]) navedene u tablici 5. U svakoj se poruci ti podatkovni objekti upotrebljavaju redoslijedom navedenim u sljedećoj tablici:

Tablica 5.
Podatkovni objekti sigurnog prenosa poruka

Naziv podatkovnog objekta	Oznaka	Prisutnost obavezna (O), uvjetna (U) ili zabranjena (Z) u	
		naredbama	odgovorima

Vrijednost koja nije kodirana u BER-TLV	'81'	U	U
Vrijednost koja je kodirana u BER-TLV, ali ne uključujući SM DO-ove	'B3'	U	U
Indikator popunjenja sadržaja nakon kojeg slijedi kriptogram, vrijednost koja nije kodirana u BER-TLV	'87'	U	U
Zaštićena Le	'97'	U	Z
Status obrade	'99'	Z	O
Kriptografski kontrolni zbir	'8E'	O	O

Napomena: kako je navedeno u Dodatku 2., tahografske kartice mogu podržavati naredbe READ BINARY (čitanje datoteke) i UPDATE BINARY (ažuriranje datoteke) s neparnim INS bajtom ('B1' odnosno 'D7'). Te varijante naredbi trebaju čitati i ažurirati datoteke s više od 32 768 bajtova. U slučaju upotrebe takve varijante, podatkovni objekt s oznakom 'B3' upotrebljava se umjesto objekta s oznakom '81'. Za više informacija vidjeti Dodatak 2.

CSM_189 Svi podatkovni objekti sigurnog prenosa poruka (SM) kodirani su u DER TLV kako je navedeno u normi [ISO 8825-1]. To kodiranje daje sljedeću strukturu vrijednosti dužine oznake (TLV):

Oznaka : Oznaka je kodirana u jednom ili dva okteta i označava sadržaj.

Dužina : Dužina je kodirana kao nepotpisani cijeli broj u jednom, dva ili tri okteta, što dovodi do najveće dužine od 65 535 okteta. Upotrebljava se najmanji broj okteta.

Vrijednost : Vrijednost je kodirana u nula ili više okteta.

CSM_190 APDU-ovi zaštićeni sigurnim prenosom poruka stvaraju se kako slijedi:

— Zaglavlje naredbe uključeno je u izračun MAC-a, stoga se upotrebljava vrijednost '0C' za bajt razreda CLA.

— Kako je navedeno u Dodatku 2., svi INS bajtovi su parni, s mogućim izuzetkom neparnih INS bajtova za naredbe READ BINARY i UPDATE BINARY.

— Stvarna vrijednost Lc preinačuje se u Lc' nakon primjene sigurnog prenosa poruka.

— Podatkovno polje sastoji se od podatkovnih objekata sigurnog prenosa poruka (SM).

— U zaštićenoj APDU naredbi novi bajt Le postavlja se na '00'. Ako je potrebno, podatkovni objekt '97' uključuje se u podatkovno polje kako bi proslijedio izvornu vrijednost Le.

CSM_191 Bilo koji podatkovni objekt koji se šifrira popunjuje se u skladu s normom [ISO 7816-4] upotrebom indikatora popunjenja sadržaja ‚01'. Za izračun MAC-a, podatkovni objekti APDU popunjuju se u skladu s normom [ISO 7816-4].

Napomena: popunjenje za siguran prenos poruka uvijek se sprovodi na nivou sigurnog prenosa poruka, a ne s pomoću algoritama CMAC ili CBC.

Naredba APDU s primjenom sigurnog prenosa poruka imat će sljedeću strukturu, zavisno o slučaju odgovarajuće nezaštićene naredbe (DO je podatkovni objekt):

Slučaj 1. : CLA INS P1 P2 || Lc' || DO '8E' || Le

Slučaj 2. : CLA INS P1 P2 || Lc' || DO '97' || DO'8E' || Le

Slučaj 3. (parni INS bajt) : CLA INS P1 P2 || Lc' || DO '81' || DO'8E' || Le

Slučaj 3. (neparni INS bajt): CLA INS P1 P2 || Lc' || DO 'B3' || DO'8E' || Le

Slučaj 4. (parni INS bajt) : CLA INS P1 P2 || Lc' || DO '81' || DO'97' || DO'8E' || Le

Slučaj 4. (neparni INS bajt): CLA INS P1 P2 || Lc' || DO 'B3' || DO'97' || DO'8E' || Le

gdje je Le = '00' ili '00 00', zavisno o tome upotrebljavaju li se kratka polja (eng. short length fields) ili produžena polja (eng. extended length fields); vidjeti normu [ISO 7816-4].

Odgovor APDU s primjenom sigurnog prenosa poruka ima sljedeću strukturu, zavisno o slučaju odgovarajućeg nezaštićenog odgovora:

Slučaj 1. ili 3.: DO '99' || DO '8E' || SW1SW2

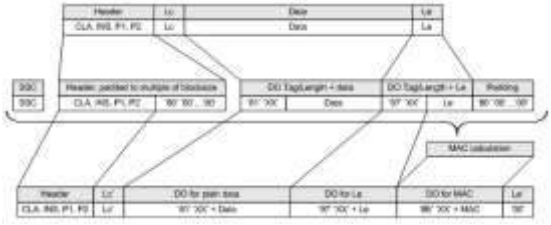
Slučaj 2. ili 4. (parni INS bajt) bez šifriranja: DO '81' || DO '99' || DO '8E' || SW1SW2

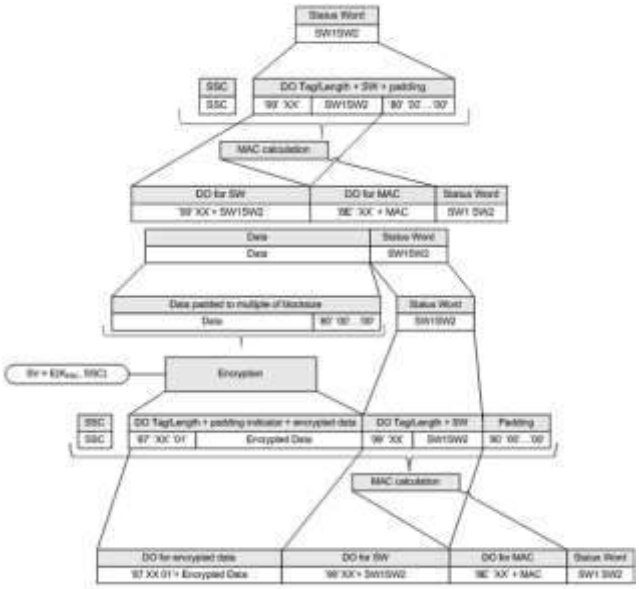
Slučaj 2. ili 4. (parni INS bajt) sa šifriranjem: DO '87' || DO '99' || DO '8E' || SW1SW2

Slučaj 2. ili 4. (neparni INS bajt) bez šifriranja: DO 'B3' || DO '99' || DO '8E' || SW1SW2

Napomena: slučaj 2. ili 4. (neparni INS bajt) sa šifriranjem nikad se ne upotrebljava za komunikaciju između jedinice u vozilu i kartice.

U nastavu su navedena tri primjera transformacije APDU za naredbe s parnim INS kodom. Slika 8. prikazuje autentificiranu naredbu APDU u slučaju 4., slika 9. prikazuje autentificirani odgovor APDU u slučaju 1./slučaju 3., a slika 10. prikazuje šifrirani i autentificirani odgovor APDU u slučaju 2./slučaju 4.





10.5.3 ***Prekid procesa sigurnog prenosa poruka***

CSM_192 Jedinica u vozilu prekida proces sigurnog prenosa poruka koji je u toku ako i samo ako nastupi jedno od sljedećih stanja:

— ako primi nešifrirani odgovor APDU,

— ako u odgovoru APDU otkrije pogrešku u sigurnom prenosu poruka:

— nedostaje očekivani podatkovni objekt sigurnog prenosa poruka, redoslijed podatkovnih objekata netočan je ili je uključen nepoznati podatkovni objekt,

— podatkovni objekt sigurnog prenosa poruka netočan je, npr. netačna je vrijednost MAC, netačna je struktura TLV ili indikator popunjenja u oznaci '87' nije jednak '01',

— ako je kartica poslala statusni bajt kojim javlja da je otkrila pogrešku u sigurnom prenosu poruka (SM) (vidjeti CSM_194),

— ako je dosegnuta granica za broj naredbi i povezanih odgovora u razmjeni podataka koja je u toku. Tu granicu za određenu jedinicu u vozilu utvrđuje proizvođač, uzimajući u obzir sigurnosne zahtjeve korištenog hardvera s najvećom vrijednošću od 240 SM naredbi i povezanih odgovora u jednoj razmjeni podataka.

CSM_193 Tahografska kartica prekida proces sigurnog prenosa poruka koji je u toku ako i samo ako nastupi jedno od sljedećih stanja:

— ako primi nešifriranu naredbu APDU,

— ako u naredbi APDU otkrije pogrešku u sigurnom prenosu poruka,

— nedostaje očekivani podatkovni objekt sigurnog prenosa poruka, redoslijed podatkovnih objekata netočan je ili je uključen nepoznati podatkovni objekt,

— podatkovni objekt sigurnog prenosa poruka netočan je, npr. netačna vrijednost MAC, netačna struktura TLV,

— ako je kartica isključena ili vraćena u početno stanje,

— ako jedinica u vozilu započne postupak autentifikacije jedinice u vozilu,

— ako je dosegnuta granica za broj naredbi i povezanih odgovora u procesu razmjene podataka koja je u toku. Tu granicu za određenu karticu utvrđuje njezin proizvođač uzimajući u obzir sigurnosne zahtjeve korištenog hardvera s najvećom vrijednošću od 240 SM naredbi i povezanih odgovora u jednom procesu.

CSM_194 U vezi s obradom SM pogrešaka koju sprovodi tahografska kartica:

— ako u naredbi APDU nedostaju neki očekivani podatkovni objekti sigurnog prenosa poruka, redoslijed podatkovnih objekata netočan je ili je uključen nepoznati podatkovni objekt, tahografska kartica odgovara statusnim bajtovima '69 87',

— ako je podatkovni objekt sigurnog prenosa poruka u naredbi APDU netočan, tahografska kartica odgovara statusnim bajtovima '69 88'.

U takvom se slučaju statusni bajtovi vraćaju bez upotrebe sigurnog prenosa poruka.

CSM_195 U slučaju prekida procesa sigurnog prenosa poruka između jedinice u vozilu i tahografske kartice, jedinica u vozilu i tahografska kartica:

— na siguran način uništavaju arhivirane ključeve razmjene podataka,

— odmah uspostavljaju novi proces sigurne razmjene poruka, kako je opisano u odjeljcima od 10.2. do 10.5.

CSM_196 Ako zbog nekog razloga jedinica u vozilu odluči ponovno pokrenuti uzajamnu autentifikaciju s obzirom na umetnutu karticu, postupak počinje ponovno s provjerom lanca certifikata kartice, kako je opisano u odjeljku 10.2., i nastavlja se kako je opisano u odjeljcima od 10.2. do 10.5.

11. POVEZIVANJE, UZAJAMNA AUTENTIFIKACIJA I SIGURAN PRENOS PORUKA IZMEĐU JEDINICE U VOZILU I VANJSKOG UREĐAJA GNSS-a

11.1. Uopšteno

CSM_197 Uređaj GNSS-a koji jedinica u vozilu upotrebljava za utvrđivanje svojeg položaja može biti unutarnji (tj. ugrađen u jedinicu i neodvojiv) ili to može biti vanjski modul. U prvom slučaju nema potrebe za standardizacijom unutarnje komunikacije između uređaja GNSS-a i jedinice u vozilu te se zahtjevi ovog poglavlja ne primjenjuju. U posljednjem slučaju, komunikacija između jedinice u vozilu i vanjskog uređaja GNSS-a standardizirana je i zaštićena kako je opisano u ovom poglavlju.

CSM_198 Sigurna komunikacija između jedinice u vozilu i vanjskog uređaja GNSS-a odvija se na isti način kao i sigurna komunikacija između jedinice u vozilu i tahografske kartice, pri čemu vanjski uređaj GNSS-a (EGF) ima ulogu kartice. Za EGF moraju biti ispunjeni svi zahtjevi navedeni u poglavlju 10. za tahografske kartice, uzimajući u obzir odstepena, pojašnjenja i dodatke navedene u ovom poglavlju. Posebno se uzajamna provjera lanca certifikata, autentifikacija jedinice u vozilu i autentifikacija čipa provode na način opisan u odjeljcima 11.3. i 11.4.

CSM_199 Komunikacija između jedinice u vozilu i EGF-a razlikuje se od komunikacije između jedinice u vozilu i kartice u činjenici da se jedinica u vozilu i EGF moraju povezati kada su u radionici, prije nego što jedinica u vozilu može s EGF-om razmijeniti podatke na temelju GNSS-a tokom redovnog rada. Postupak povezivanja opisan je u odjeljku 11.2.

CSM_200 Za komunikaciju između jedinice u vozilu i EGF-a upotrebljavaju se naredbe i odgovori APDU u skladu s normama [ISO 7816-4] i [ISO 7816-8]. Tačna je struktura tih APDU-ova definisana u Dodatku 2. ovom Prilogu.

11.2. Povezivanje jedinice u vozilu i vanjskog uređaja GNSS-a (EGF-a)

CSM_201 Povezivanje jedinice u vozilu i EGF-a u vozilu sprovodi radionica. Jedinica u vozilu i EGF mogu komunicirati tokom redovnog rada samo ako su povezani.

CSM_202 Povezivanje jedinice u vozilu i EGF-a moguće je ako je jedinica u vozilu u kalibracijskom načinu rada. Povezivanje pokreće jedinica u vozilu.

CSM_203 Radionica može u bilo kojem trenutku ponovno povezati jedinicu u vozilu s drugim EGF-om ili s istim EGF-om. Tokom ponovnog uparivanja jedinica u vozilu na siguran način uništava postojeći certifikat EGF_MA u svojoj memoriji te arhivira certifikat EGF_MA na EGF s kojim se povezuje.

CSM_204 Radionica može u bilo kojem trenutku ponovno povezati vanjski uređaj GNSS-a s drugom jedinicom u vozilu ili s istom jedinicom u vozilu. Tokom ponovnog povezivanja EGF na siguran način uništava postojeći certifikat VU_MA u svojoj memoriji te arhivira certifikat VU_MA na jedinicu u vozilu s kojom se povezuje.

11.3. Uzajamna provjera lanca certifikata

11.3.1 *Uopšteno*

CSM_205 Uzajamna provjera lanca certifikata između jedinice u vozilu i EGF-a odvija se samo tokom povezivanja jedinice u vozilu i EGF-a koje sprovodi radionica. Tokom redovnog rada povezanih jedinice u vozilu i EGF-a ne provjeravaju se certifikati. Umjesto toga, jedinica u vozilu i EGF imaju povjerenja u certifikate koje su pohranili tokom povezivanja, nakon provjere vremenske važnosti tih certifikata. Jedinica u vozilu i EGF nemaju povjerenja u druge certifikate za zaštitu komunikacije jedinica u vozilu – EGF tokom redovnog rada.

11.3.2 *Tokom povezivanja jedinica u vozilu (VU) – EGF*

CSM_206 Tokom povezivanja na EGF, jedinica u vozilu upotrebljava protokol prikazan na slici 4. (odjeljak 10.2.1.) za provjeru lanca certifikata vanjskog uređaja GNSS-a.

Napomene za sliku 4. u tom kontekstu:

— Upravljanje komunikacijom nije u području primjene ovog Dodatka. Međutim, EGF nije pametna kartica te stoga jedinica u vozilu vjerojatno neće poslati naredbu vraćanja u početno stanje (eng. *reset*) za pokretanje komunikacije te neće primiti ATR.

— Certifikati Card i javni ključevi prikazani na slici tumače se kao certifikati EGF i javni ključevi za uzajamnu autentifikaciju. U odjeljku 9.1.6. označeni su kao EGF_MA.

— Certifikati Card:CA i javni ključevi prikazani na slici tumače se kao certifikati MSCA i javni ključevi za potpisivanje certifikata EGF. U odjeljku 9.1.3. označeni su kao MSCA_VU-EGF.

— Certifikat Card.CA.EUR prikazan na slici tumači se kao evropski glavni certifikat koji je naveden u CAR certifikata MSCA_VU-EGF.

— Certifikat Card.Link prikazan na slici tumači se kao certifikat o povezanosti EGF-a, ako postoji. Kako je navedeno u odjeljku 9.1.2., to je certifikat o povezanosti za novi evropski glavni par ključeva koji je ERCA stvorila i potpisala prethodnim evropskim privatnim ključem.

— Certifikat Card.Link.EUR je evropski glavni certifikat koji je naveden u CAR certifikata Card.Link.

— Umjesto `cardExtendedSerialNumber`, jedinica u vozilu čita `sensorGNSSserialNumber` iz elementarne datoteke (EF) ICC.

— Umjesto odabira AID tahografa, jedinica u vozilu odabire AID EGF-a.

— „Ignore Card" tumači se kao „Ignore EGF".

CSM_207 Jednom kad je provjerila certifikat EGF_MA, jedinica u vozilu arhivira taj certifikat za upotrebu tokom redovnog rada; vidjeti odjeljak 11.3.3.

CSM_208 Tokom povezivanja na jedinicu u vozilu, vanjski uređaj GNSS-a upotrebljava protokol prikazan na slici 5. (odjeljak 10.2.2) za provjeru lanca certifikata jedinice u vozilu.

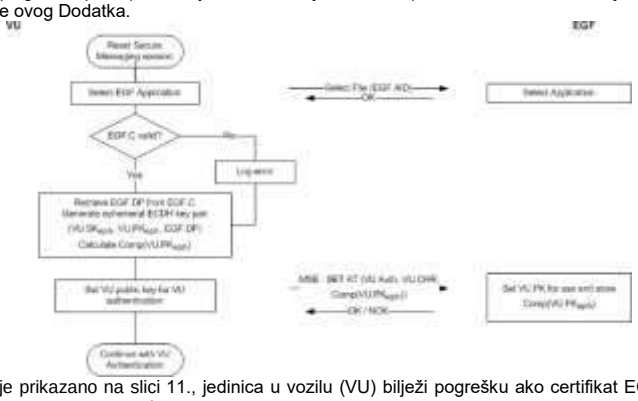
Napomene za sliku 5. u tom kontekstu:

— Jedinica u vozilu generiše novi kratkotrajni par ključeva s pomoću parametara domene u certifikatu EGF.

— Certifikati jedinice u vozilu i javni ključevi prikazani na slici oni su za uzajamnu autentifikaciju. U odjeljku 9.1.4. označeni su kao VU_MA,
— Certifikati VU.CA i javni ključevi prikazani na slici oni su za potpisivanje certifikata jedinica u vozilu i vanjskih uređaja GNSS-a. U odjeljku 9.1.3. označeni su kao MSCA_VU-EGF.
— Certifikat VU.CA.EUR prikazan na slici je evropski glavni certifikat koji je naveden u CAR certifikata VU.CA.
— Certifikat VU.Link prikazan na slici je certifikat o povezanosti jedinice u vozilu, ako postoji. Kako je navedeno u odjeljku 9.1.2., to je certifikat o povezanosti za novi evropski glavni par ključeva koji je ERCA stvorila i potpisala prethodnim evropskim privatnim ključem.
— Certifikat VU.Link.EUR je evropski glavni certifikat koji je naveden u CAR certifikata VU.Link.
CSM_209 Odstupajući od zahtjeva CSM_167, EGF upotrebljava vrijeme GNSS-a za provjeru vremenske važnosti svakog predočenog certifikata.
CSM_210 Jednom kada je provjerio certifikat VU_MA, vanjski uređaj GNSS-a arhivira taj certifikat za upotrebu tokom redovnog rada; vidjeti odjeljak 11.3.3.

11.3.3 *Tokom redovnog rada*

CSM_211 Tokom redovnog rada jedinica u vozilu i EGF upotrebljavaju protokol prikazan na slici 11. za provjeru vremenske važnosti pohranjenog certifikata EGF_MA te za postavljanje javnog ključa VU_MA za kasniju autentifikaciju jedinice u vozilu. Tokom redovnog rada ne odvija se nikakva daljnja uzajamna provjera lanca certifikata.
Treba napomenuti da se slika 11. zapravo sastoji od prvih koraka prikazanih na slikama 4. i 5. Nadalje, treba uzeti u obzir da EGF nije pametna kartica te da jedinica u vozilu vjerojatno neće poslati naredbu vraćanja u početno stanje (eng. *reset*) za pokretanje komunikacije te neće primiti ATR. U svakom je slučaju to izvan područja primjene ovog Dodatka.



CSM_212 Kako je prikazano na slici 11., jedinica u vozilu (VU) bilježi pogrešku ako certifikat EGF_MA više nije važeći. Međutim, uzajamna autentifikacija, dogovaranje ključa i kasnija komunikacija sigurnim prenosom poruka normalno se nastavljaju.

11.4. Autentifikacija jedinice u vozilu, autentifikacija čipa i dogovaranje ključa razmjene podataka

CSM_213 Autentifikacija jedinice u vozilu, autentifikacija čipa i dogovaranje ključa razmjene podataka između jedinice u vozilu i EGF-a odvijaju se tokom povezivanja i svaki put kad je proces sigurnog prenosa poruka ponovno uspostavljen tokom redovnog rada. Jedinica u vozilu i EGF provode postupke opisane u odjeljcima 10.3. i 10.4. Primjenjuju se svi zahtjevi iz tih odjeljaka.

11.5. Siguran prenos poruka

CSM_214 Sve naredbe i odgovori razmijenjeni između jedinice u vozilu i vanjskog uređaja GNSS-a nakon uspješne autentifikacije čipa i do završetka razmjene podataka zaštićeni su sigurnim prenosom poruka u načinu rada namijenjenom isključivo autentifikaciji. Primjenjuju se svi zahtjevi iz odjeljka 10.5.
CSM_215 U slučaju prekida procesa sigurnog prenosa poruka između jedinice u vozilu i EGF-a, jedinica u vozilu odmah uspostavlja novi proces sigurnog prenosa poruka, kako je opisano u odjeljcima 11.3.3. i 11.4.

12. UPARIVANJE I KOMUNIKACIJA IZMEĐU JEDINICE U VOZILU I SENZORA KRETANJA

12.1. Uopšteno

CSM_216 Jedinica u vozilu i senzor kretanja komuniciraju upotrebom protokola sučelja navedenog u normi [ISO 16844-3] tokom uparivanja i redovnog rada, uz promjene navedene u ovom poglavlju i odjeljku 9.2.1.
Napomena: čitatelji ovog poglavlja trebaju biti upoznati sa sadržajem norme [ISO 16844-3].

12.2. Uparivanje jedinice u vozilu i senzora kretanja upotrebom različitih generacija ključeva

Kako je objašnjeno u odjeljku 9.2.1., glavni ključ senzora kretanja i svi povezani ključevi redovito se zamjenjuju. To dovodi do prisutnosti najviše triju AES ključeva $K_{M\text{-}WC}$ (uzastopnih generacija ključeva) povezanih sa senzorom kretanja na karticama radionica. Jednako tako, u senzorima kretanja mogu biti prisutna do tri različita šifriranja podataka na temelju AES (na temelju uzastopnih generacija glavnog ključa senzora kretanja K_M). Jedinica u vozilu sadrži samo jedan ključ $K_{M\text{-}VU}$ povezan sa senzorom kretanja.
CSM_217 Jedinica u vozilu druge generacije i senzor kretanja druge generacije uparuju se kako slijedi (usporediti s tablicom 6. u normi [ISO 16844-3]):

1. u jedinicu u vozilu umeće se kartica radionice druge generacije te se jedinica u vozilu povezuje sa senzorom kretanja;
2. Jedinica u vozilu čita sve dostupne ključeve K_{M-WC} s kartice radionice, pregledava njihove brojeve verzija ključa i odabire onaj koji odgovara broju verzije ključa K_{M-VU} jedinice u vozilu. Ako na kartici radionice nije prisutan odgovarajući ključ K_{M-WC}, jedinica u vozilu prekida postupak uparivanja te nositelju kartice radionice prikazuje odgovarajuću poruku o pogrešci.
3. Jedinica u vozilu izračunava glavni ključ senzora kretanja K_M iz K_{M-VU} i $K_{M-WC,}$ te identifikacijski ključ K_{ID} iz K_M, kako je navedeno u odjeljku 9.2.1.
4. Jedinica u vozilu šalje uputu za pokretanje postupka uparivanja s obzirom na senzor kretanja, kako je opisano u normi [ISO 16844-3], te šifrira serijski broj koji je primila od senzora kretanja s identifikacijskim ključem $K_{ID.}$ Jedinica u vozilu šalje šifrirani serijski broj senzoru kretanja.
5. Senzor kretanja uzastopno uspoređuje šifrirani serijski broj sa svakim šifriranjem serijskog broja koje je interno pohranio. Ako nađe odgovarajući broj, jedinica u vozilu je autentificirana. Senzor kretanja bilježi generaciju K_{ID} koju upotrebljava jedinica u vozilu i vraća odgovarajuću šifriranu vrijednost svojeg ključa uparivanja; tj. šifriranje je stvoreno upotrebom iste generacije K_M.
6. Jedinica u vozilu dešifrira ključ uparivanja s pomoću K_M, generiše ključ razmjene podataka $K_{S,}$ šifrira ga s ključem uparivanja i rezultat šalje senzoru kretanja. Senzor kretanja dešifrira K_S.
7. Jedinica u vozilu prikuplja informacije za uparivanje, kako je utvrđeno u normi [ISO 16844-3], šifrira informacije s ključem uparivanja i rezultat šalje senzoru kretanja. Senzor kretanja dešifrira informacije za uparivanje.
8. Senzor kretanja šifrira primljene informacije za uparivanje s primljenim K_S i to vraća jedinici u vozilu. Jedinica u vozilu provjerava da su informacije za uparivanje iste informacije koje je jedinica u vozilu poslala senzoru kretanja u prethodnom koraku. Ako jest, to dokazuje da je senzor kretanja upotrijebio isti K_S kao jedinica u vozilu te je stoga u koraku 5. poslao svoj ključ uparivanja šifriran s ispravnom generacijom K_M. Slijedom toga, senzor kretanja je autentificiran.
Treba napomenuti da se koraci 2. i 5. razlikuju od standardnog postupka u normi [ISO 16844-3]; ostali su koraci standardni.
Primjer: pretpostavimo da se uparivanje odvija u prvoj godini važnosti certifikata ERCA (3); vidjeti sliku 2. u odjeljku 9.2.1.2. Nadalje,
— pretpostavimo da je senzor kretanja izdat u posljednjoj godini važnosti certifikata ERCA (1). Stoga će sadržiti sljedeće ključeve i podatke:
— N_S[1]: vlastiti serijski broj šifriran s prvom generacijom K_{ID},
— N_S[2]: vlastiti serijski broj šifriran s drugom generacijom K_{ID},
— N_S[3]: vlastiti serijski broj šifriran s trećom generacijom K_{ID},
— K_P[1]: vlastiti ključ uparivanja prve generacije ([18]), šifriran s prvom generacijom K_M,
— K_P[2]: vlastiti ključ uparivanja druge generacije, šifriran s drugom generacijom K_M,
— K_P[3]: vlastiti ključ uparivanja treće generacije, šifriran s trećom generacijom K_M;
— pretpostavimo da je kartica radionice izdata u prvoj godini važnosti certifikata ERCA (3). Zato će sadržiti drugu generaciju i treću generaciju ključa K_{M-WC};
— pretpostavimo da je VU jedinica u vozilu druge generacije i sadrži drugu generaciju $K_{M-VU.}$
U tom se slučaju u koracima od 2. do 5. događa sljedeće:
— 2. korak: VU čita drugu generaciju i treću generaciju K_{M-WC} s kartice radionice i pregledava njihove brojeve verzija.
— 3. korak: VU kombinira drugu generaciju K_{M-WC} sa svojim K_{M-VU} za izračun K_M i $K_{ID.}$
— 4. korak: VU šifrira serijski broj koji je primila od senzora kretanja s $K_{ID.}$
— 5. korak: senzor kretanja uspoređuje primljene podatke s N_S[1] i ne nalazi odgovarajući broj. Nakon toga, uspoređuje primljene podatke s N_S[2] i nalazi odgovarajući broj. Zaključuje da je ta VU jedinica u vozilu druge generacije i stoga nazad šalje K_P[2].

12.3. Uparivanje i komunikacija između jedinice u vozilu i senzora kretanja upotrebom AES

CSM_218 Kako je navedeno u tablici 3. odjeljka 9.2.1., svi su ključevi uključeni u uparivanje jedinice u vozilu (druge generacije) i senzora kretanja te u kasniju komunikaciju AES ključevi, a ne TDES ključevi dvostruke dužine kako je navedeno u normi [ISO 16844-3]. Ti AES ključevi mogu biti dužine 128, 192 ili 256 bitova. Budući da je veličina AES bloka 16 bajtova, dužina šifrirane poruke mora biti višekratnik 16 bajtova u usporedbi s 8 bajtova za TDES. Nadalje, neke će se od tih poruka upotrebljavati za prenos AES ključeva, čija dužina može biti 128, 192 ili 256 bitova. Stoga se broj bajtova podataka po uputi u tablici 5. iz norme [ISO 16844-3] mijenja kako je prikazano u tablici 6.:

Tablica 6.

Broj bajtova nešifriranih i šifriranih podataka prema uputi utvrđenoj u normi [ISO 16844-3]

Upute	Zahtjev /odgovor	Opis podataka	# bajtova nešifriranih podataka u skladu s [ISO 16844-3]	# bajtova nešifriranih podataka upotrebom AES ključeva	# bajtova šifriranih podataka upotrebom AES ključeva dužine bitova od		
					128	192	256
10	zahtjev	podaci za autentifikaciju + broj datoteke	8	8	16	16	16
11	odgovor	podaci za autentifikaciju + sadržaj datoteke	16 ili 32, zavisno o datoteci	16 ili 32, zavisno o datoteci	32 / 48	32 / 48	32 / 48
41	zahtjev	serijski broj senzora kretanja (MoS)	8	8	16	16	16

41	odgovor	ključ uparivanja	16	16 / 24 / 32	16	32	32
42	zahtjev	ključ razmjene podataka	16	16 / 24 / 32	16	32	32
43	zahtjev	informacije za uparivanje	24	24	32	32	32
50	odgovor	informacije za uparivanje	24	24	32	32	32
70	zahtjev	podaci za autentifikaciju	8	8	16	16	16
80	odgovor	vrijednost brojača MoS + podaci za autentifikaciju	8	8	16	16	16

CSM_219 Informacije za uparivanje koje se šalju u uputama 43. (zahtjev VU) i 50. (odgovor MoS) prikupljaju se kako je navedeno u odjeljku 7.6.10. norme [ISO 16844-3], osim što se u shemi šifriranja podataka za uparivanje upotrebljava AES algoritam umjesto TDES algoritma, čime nastaju dva AES šifriranja te se popunjenje navedeno u CSM_220 primjenjuje za usklađivanje s veličinom AES bloka. Ključ K'_p koji se upotrebljava za to šifriranje generiše se kako slijedi:

— u slučaju da je ključ uparivanja K_P dužine 16 bajtova: $K'_p = K_P \text{ XOR } (N_s||N_s)$,
— u slučaju da je ključ uparivanja K_P dužine 24 bajta: $K'_p = K_P \text{ XOR } (N_s||N_s||N_s)$,
— u slučaju da je ključ uparivanja K_P dužine 32 bajta: $K'_p = K_P \text{ XOR } (N_s||N_s||N_s||N_s)$,
pri čemu je N_s 8-bajtni serijski broj senzora kretanja.

CSM_220 U slučaju da dužina nešifriranih podataka (upotrebom AES ključeva) nije višekratnik 16 bajtova, upotrebljava se metoda popunjenja br. 2 iz norme [ISO 9797-1].

Napomena: u normi [ISO 16844-3] broj bajtova nešifriranih podataka uvijek je višekratnik broja 8 tako da popunjenje nije potrebno pri upotrebi TDES. Definicija podataka i poruka iz norme [ISO 16844-3] ne mijenja se ovim dijelom ovog Dodatka te je stoga potrebna primjena popunjenja.

CSM_221 Za uputu 11. i u slučaju da se mora šifrirati više od jednog bloka podataka, upotrebljava se način rada „ulančavanje šifriranih blokova" (CBC), kako je utvrđeno u normi [ISO 10116], s parametrom preraspodjele *m* = 1. Inicijalizacijski vektor upotrebljava se:

— za uputu 11.: 8-bajtni blok autentifikacije naveden u odjeljku 7.6.3.3. norme [ISO 16844-3], popunjen upotrebom metode popunjenja br. 2 iz norme [ISO 9797-1]; vidjeti i odjeljke 7.6.5. i 7.6.6. u normi [ISO 16844-3],
— za sve ostale upute u kojima se prenosi više od 16 bajtova, kako je navedeno u tablici 6.: '00' {16}, tj. šesnaest bajtova s binarnom vrijednošću 0.

Napomena: kako je prikazano u odjeljcima 7.6.5. i 7.6.6. norme [ISO 16844-3], kada MoS šifrira podatkovne datoteke za uključivanje u uputu 11. blok autentifikacije se:

— upotrebljava kao inicijalizacijski vektor za šifriranje podatkovnih datoteka u načinu rada CBC,
— šifrira i uključuje u prvi blok u podacima koji se šalju u jedinicu u vozilu.

12.4. Uparivanje jedinice u vozilu i senzora kretanja za različite generacije opreme

CSM_222 Kako je objašnjeno u odjeljku 9.2.1., senzor kretanja druge generacije može sadržiti šifriranje podataka za uparivanje na temelju TDES (kako je utvrđeno u dijelu A ovog Dodatka), koje omogućava da senzor kretanja bude uparen s jedinicom u vozilu prve generacije. U tom se slučaju jedinica u vozilu prve generacije i senzor kretanja druge generacije uparuju kako je opisano u dijelu A ovog Dodatka i u normi [ISO 16844-3]. Za postupak uparivanja može se upotrijebiti kartica radionice prve ili druge generacije.

Napomene:

— Nije moguće upariti jedinicu u vozilu druge generacije sa senzorom kretanja prve generacije.
— Nije moguće upotrijebiti karticu radionice prve generacije za povezivanje VU druge generacije sa senzorom kretanja.

13. SIGURNOST KOMUNIKACIJE NA DALJINU PUTEM DSRC-a

13.1. Uopšteno

Kako je navedeno u Dodatku 14., jedinica u vozilu redovito generiše podatke za praćenje tahografa na daljinu (eng. *Remote Tachograph Monitoring*, RTM) i te podatke šalje (unutarnjem ili vanjskom) uređaju za komunikaciju na daljinu (eng. *Remote Communication Facility*, RCF). Uređaj za komunikaciju na daljinu odgovoran je za slanje tih podataka uređaju za ispitivanje na daljinu putem sučelja DSRC-a opisanog u Dodatku 14. U Dodatku 1. utvrđeno je da podaci RTM-a čine ulančavanje:

šifriranog prenosa podataka iz tahografa (eng. *encrypted tachograph payload*) – šifriranje nešifriranog prenosa podataka iz tahografa,
sigurnosnih podataka DSRC-a (eng. *DSRC security data*) – opisani u nastavu.

Format nešifriranog prenosa podataka iz tahografa naveden je u Dodatku 1. te detaljnije opisan u Dodatku 14. U ovom se odjeljku opisuje struktura sigurnosnih podataka DSRC-a; službena je specifikacija navedena u Dodatku 1.

CSM_223 Nešifrirani podaci tachographPayload koje jedinica u vozilu (VU) dostavlja uređaju za komunikaciju na daljinu (ako je RCF vanjski u odnosu na VU) ili ih VU putem sučelja DSRC-a dostavlja uređaju za ispitivanje na daljinu (ako je RCF unutarnji u odnosu na VU) zaštićuju se u načinu rada namijenjenom šifriranju i zatim autentifikaciji, tj. podaci iz tahografa prvo se šifriraju u svrhu osiguranja povjerljivosti poruke te se nakon toga izračunava MAC u svrhu osiguranja autentičnosti i integriteta.

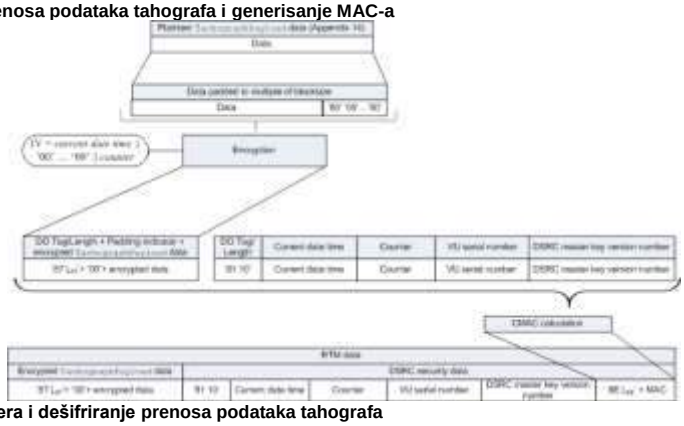
CSM_224 Sigurnosni podaci DSRC-a sastoje se od ulančavanja sljedećih podatkovnih elemenata sljedećim redoslijedom; vidjeti i sliku 12.:

trenutni datum i vrijeme – trenutni datum i vrijeme jedinice u vozilu (vrsta podataka),
brojač – 3-bajtni brojač, vidjeti CSM_225,
serijski broj jedinice u vozilu – serijski broj jedinice u vozilu ili identifikator zahtjeva za certifikat (vrsta podataka VuSerialNumber ili CertificateRequestID) – vidjeti CSM_123,

broj verzije glavnog ključa DSRC-a – 1-bajtni broj verzije glavnog ključa DSRC-a iz kojeg su izvedeni ključevi DSRC-a specifični za jedinicu u vozilu; vidjeti odjeljak 9.2.2.,
MAC – MAC izračunan za sve prethodne bajtove u podacima RTM-a.
CSM_225 Trobajtni brojač u sigurnosnim podacima DSRC-a je u formatu MSB-first. Kad jedinica u vozilu prvi put otkad je stavljena u upotrebu izračunava niz podataka RTM-a, postavlja vrijednost brojača na 0. Jedinica u vozilu povećava vrijednost podataka brojača za 1 svaki put prije nego što izračuna sljedeći niz podataka RTM-a.

13.2. Šifriranje prenosa podataka tahografa i generisanje MAC-a

CSM_226 S obzirom na nešifrirani podatkovni element s vrstom podataka `TachographPayload`, kako je opisan u Dodatku 14., jedinica u vozilu šifrira te podatke kako je prikazano na slici 12.: ključ DSRC-a jedinice u vozilu za šifriranje K_VU$_{DSRC}$_ENC (vidjeti odjeljak 9.2.2.) upotrebljava se s AES-om u načinu rada „ulančavanje šifriranih blokova" (CBS), kako je utvrđeno u normi [ISO 10116], s parametrom preraspodjele *m* = 1. Inicijalizacijski vektor jednak je *IV = trenutni datum i vrijeme*|| *'00 00 00 00 00 00 00 00'* || *brojač*, pri čemu su *trenutni datum i vrijeme* i *brojač* navedeni u CSM_224. Podaci za šifriranje popunjavaju se metodom br. 2 iz norme [ISO 9797-1].
CSM_227 Jedinica u vozilu izračunava MAC u sigurnosnim podacima DSRC-a kako je prikazano na slici 12.: MAC se izračunava za sve prethodne bajtove u RTM podacima, do broja verzije glavnog ključa DSRC-a i uključujući taj broj te uključujući oznake i dužine podatkovnih objekata. Jedinica u vozilu upotrebljava svoj ključ DSRC-a za autentičnost K_VU$_{DSRC}$_MAC (vidjeti odjeljak 9.2.2.) s AES algoritmom u načinu rada CMAC, kako je navedeno u [SP 800-38B]. Dužina MAC-a povezana je s duljinom ključeva DSRC-a specifičnih za jedinicu u vozilu, kako je navedeno u CSM_50.
Slika 12.
Šifriranje prenosa podataka tahografa i generisanje MAC-a



13.3. Provjera i dešifriranje prenosa podataka tahografa

CSM_228 Kada primi RTM podatke iz jedinice u vozilu, uređaj za daljinsko ispitivanje šalje sve RTM podatke na kontrolnu karticu u podatkovnom polju naredbe PROCESS DSRC MESSAGE, kako je opisano u Dodatku 2. Zatim:
1. kontrolna kartica pregledava broj verzije glavnog ključa DSRC-a u sigurnosnim podacima DSRC-a. Ako ne prepoznaje navedeni glavni ključ DSRC-a, kontrolna kartica javlja pogrešku navedenu u Dodatku 2. i prekida postupak;
2. kontrolna kartica upotrebljava navedeni glavni ključ DSRC-a u kombinaciji sa serijskim brojem jedinice u vozilu ili identifikatorom zahtjeva za certifikat u sigurnosnim podacima DSRC-a za izvođenje ključeva DSRC-a K_VU$_{DSRC}$_ENC i K_VU$_{DSRC}$_MAC specifičnih za jedinicu u vozilu, u skladu sa stavkom CSM_124;
3. kontrolna kartica upotrebljava K_VU$_{DSRC}$_MAC za provjeru MAC-a u sigurnosnim podacima DSRC-a, kako je navedeno u CSM_227. Ako je MAC netočan, kontrolna kartica javlja pogrešku navedenu u Dodatku 2. i prekida postupak;
4. kontrolna kartica upotrebljava K_VU$_{DSRC}$_ENC za dešifriranje šifriranog prenosa podataka tahografa, kako je navedeno u CSM_226. Kontrolna kartica uklanja popunjenje i uređaju za daljinsko ispitivanje vraća dešifrirani prenos podataka tahografa.
CSM_229 U svrhu sprječavanja napada reprodukcijom, uređaj za daljinsko ispitivanje provjerava aktualnost (eng. *freshness*) RTM podataka provjerom da *trenutni datum i vrijeme* u sigurnosnim podacima DSRC-a ne odstupa previše od trenutačnog vremena uređaja za daljinsko ispitivanje.
Napomene:
— To zahtijeva da uređaj za daljinsko ispitivanje ima točan i pouzdan izvor vremena.
— Budući da se u Dodatku 14. od jedinice u vozilu zahtijeva novi niz RTM podataka svakih 60 sekundi te je dopušteno da sat jedinice u vozilu odstupa jednu minutu od realnog vremena, donja granica za aktualnost RTM podataka je dvije minute. Stvarna aktualnost podataka koja se zahtijeva ovisi i o tačnosti sata uređaja za daljinsko ispitivanje.
CSM_230 Nakon što provjeri pravilan rad funkcije DSRC-a jedinice u vozilu, radionica šalje sve RTM podatke primljene iz jedinice u vozilu na karticu radionice u podatkovnom polju naredbe PROCESS DSRC MESSAGE, kako je opisano u Dodatku 2. Kartica radionice obavlja sve provjere i radnje navedene u CSM_228.

14. POTPISIVANJE PREUZIMANJA PODATAKA I PROVJERA POTPISA

14.1. Uopšteno

CSM_231 Posebna namjenska oprema (IDE) arhivira podatke primljene s jedinice u vozilu ili kartice tokom jednog procesa preuzimanja podataka u jednoj fizičkoj podatkovnoj datoteci. Podaci se mogu arhivirati na ESM (vanjski medij za arhiviranje podataka). Ta datoteka sadrži digitalne potpise podatkovnih blokova navedenih u Dodatku 7. Ta datoteka sadrži i sljedeće certifikate (vidjeti odjeljak 9.1.):

— u slučaju preuzimanja podataka iz jedinice u vozilu:
— certifikat VU_Sign,
— certifikat MSCA_VU-EGF s javnim ključem koji se upotrebljava za provjeru certifikata VU_Sign;
— u slučaju preuzimanja podataka s kartice:
— certifikat Card_Sign,
— certifikat MSCA_Card s javnim ključem koji se upotrebljava za provjeru certifikata Card_Sign.

CSM_232 IDE na raspolaganju ima i sljedeće:

— u slučaju da za provjeru potpisa upotrebljava kontrolnu karticu, kako je prikazano na slici 13.: certifikat o povezanosti koji povezuje najnoviji certifikat EUR s certifikatom EUR čiji mu rok važnosti direktno prethodi, ako postoji,
— u slučaju da sam provjerava potpis: sve važeće evropske glavne certifikate.

Napomena: metoda koju IDE upotrebljava za preuzimanje tih certifikata nije utvrđena u ovom Dodatku.

14.2. Generisanje potpisa

CSM_233 Algoritam potpisivanja za stvaranje digitalnih potpisa preuzetih podataka je ECDSA, kako je utvrđeno u [DSS], upotrebom algoritma raspršivanja (*hashing*) povezanog s veličinom ključa jedinice u vozilu ili kartice, kako je navedeno u CSM_50. Format potpisa je nešifriran, kako je navedeno u [TR-03111].

14.3. Provjera potpisa

CSM_234 IDE provjeru potpisa preuzetih podataka može provesti sam ili za to može upotrijebiti kontrolnu karticu. U slučaju da upotrebljava kontrolnu karticu, provjera potpisa odvija se na način prikazan na slici 13. Kontrolna kartica za provjeru vremenske važnosti certifikata koji je predočio IDE upotrebljava svoje unutarnje trenutačno vrijeme, u skladu sa stavkom CSM_167. Kontrolna kartica ažurira svoje trenutačno vrijeme ako je datum početka važnosti autentičnog certifikata „važećiog izvora vremena" noviji od trenutačnog vremena kartice. Kartica kao važećii izvor vremena prihvaća samo sljedeće certifikate:

— certifikate o povezanosti ERCA druge generacije,
— certifikate MSCA druge generacije,
— certifikate VU_Sign ili Card_Sign druge generacije koje je izdala ista država kao i certifikat kontrolne kartice.

U slučaju da provjeru potpisa sprovodi sam, IDE provjerava autentičnost i važnost svih certifikata u lancu certifikata u podatkovnoj datoteci te provjerava potpis podataka u skladu sa šemom potpisa utvrđenom u [DSS]. U oba slučaja za svaki je certifikat očitan s podatkovne datoteke potrebno provjeriti je li polje ovlaštenja nosioca certifikata (CHA) tačno:

— u polju CHA certifikata EQT navodi se certifikat jedinice u vozilu ili kartice (kako je primjenjivo) za potpisivanje (vidjeti Dodatak 1., vrstu podataka EquipmentType).
— u polju CHA certifikata EQT.CA navodi se MSCA.
— u polju CHA certifikata EQT.Link navodi se ERCA.

Napomene za sliku 13.:

— Oprema koja je potpisala podatke koji se analiziraju označena je s EQT.
— Certifikati EQT i javni ključevi prikazani na slici su oni za potpisivanje, tj. VU_Sign ili Card_Sign.
— Certifikati EQT.CA i javni ključevi prikazani na slici oni su za potpisivanje certifikata jedinice u vozilu ili kartice, kako je primjenjivo.
— Certifikat EQT.CA.EUR prikazan na slici je evropski glavni certifikat koji je naveden u CAR certifikata EQT.CA.
— Certifikat EQT.Link prikazan na slici je certifikat o povezanosti EQT, ako postoji. Kako je navedeno u odjeljku 9.1.2., to je certifikat o povezanosti za novi evropski glavni par ključeva koji je ERCA stvorila i potpisala prethodnim evropskim privatnim ključem,
— Certifikat EQT.Link.EUR je evropski glavni certifikat koji je naveden u CAR certifikata EQT.Link.

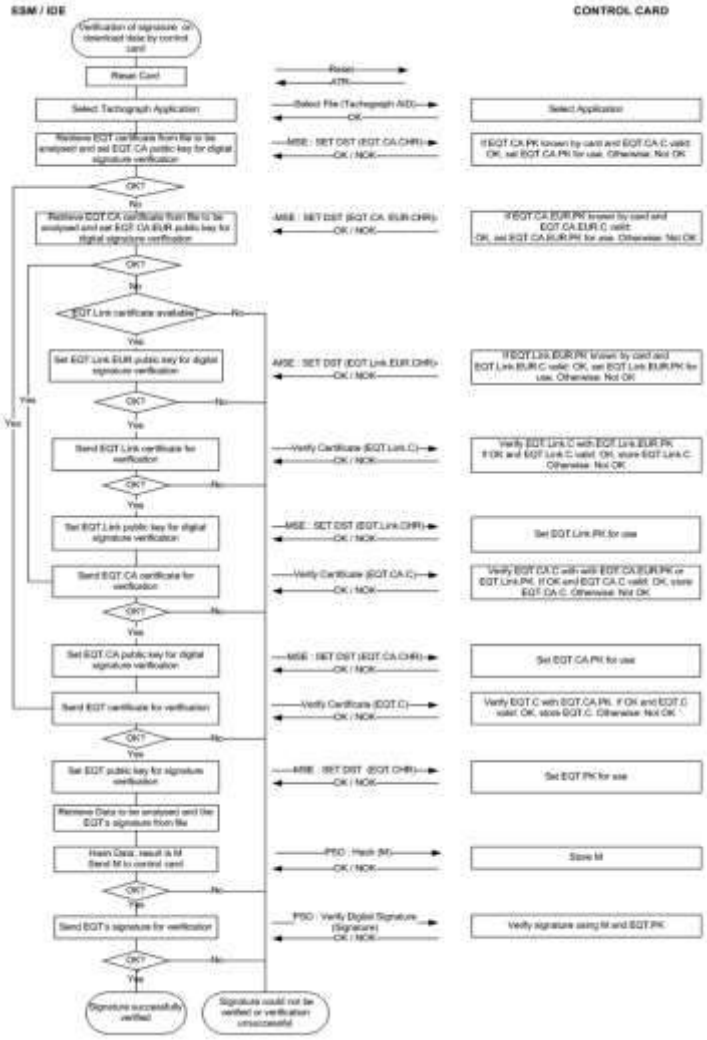
CSM_235 Za izračun raspršivanja (*hash*) M poslanog kontrolnoj kartici u naredbi PSO:Hash, IDE upotrebljava algoritam raspršivanja (*hashing*) povezan s veličinom ključa jedinice u vozilu ili kartice s koje se preuzimaju podaci, kako je navedeno u CSM_50.

CSM_236 Za provjeru potpisa EQT kontrolna kartica slijedi šemu potpisa utvrđenu u [DSS].

Napomena: ovim se dokumentom ne određuju bilo kakve mjere koje treba poduzeti ako se potpis preuzete podatkovne datoteke ne može provjeriti ili je provjera neuspješna.

Slika 13.

Protokol za provjeru potpisa preuzete podatkovne datoteke


ESM / IDE
CONTROL CARD
Verification of signature on download data by control card
Reset Card
Reset
ATR
Select Tachograph Application
Select File (Tachograph AID)
OK
Select Application
Retrieve EQT certificate from file to be analysed and set EQT CA public key for digital signature verification
MSE : SET DST (EQT CA CHR)
OK / NOK
If EQT CA PK known by card and EQT CA C valid: OK, set EQT CA PK for use. Otherwise: Not OK
OK?
No
Retrieve EQT CA certificate from file to be analysed and set EQT CA EUR public key for digital signature verification
MSE : SET DST (EQT CA EUR CHR)
OK / NOK
If EQT CA EUR PK known by card and EQT CA EUR C valid: OK, set EQT CA EUR PK for use. Otherwise: Not OK
OK?
No
EQT Link certificate available?
No
Yes
Set EQT Link EUR public key for digital signature verification
MSE : SET DST (EQT Link EUR CHR)
OK / NOK
If EQT Link EUR PK known by card and EQT Link EUR C valid: OK, set EQT Link EUR PK for use. Otherwise: Not OK
OK?
No
Yes
Yes
Send EQT Link certificate for verification
Verify Certificate (EQT Link C)
OK / NOK
Verify EQT Link C with EQT Link EUR PK If OK and EQT Link C valid: OK, store EQT Link C. Otherwise: Not OK
OK?
No
Yes
Set EQT Link public key for digital signature verification
MSE : SET DST (EQT Link CHR)
OK / NOK
Set EQT Link PK for use
Send EQT CA certificate for verification
Verify Certificate (EQT CA C)
OK / NOK
Verify EQT CA C with with EQT CA EUR PK or EQT Link PK. If OK and EQT CA C valid: OK, store EQT CA C. Otherwise: Not OK
OK?
No
Yes
Set EQT CA public key for digital signature verification
MSE : SET DST (EQT CA CHR)
OK / NOK
Set EQT CA PK for use
Send EQT certificate for verification
Verify Certificate (EQT C)
OK / NOK
Verify EQT C with EQT CA PK. If OK and EQT C valid: OK, store EQT C. Otherwise: Not OK
OK?
No
Yes
Set EQT public key for signature verification
MSE : SET DST (EQT CHR)
OK / NOK
Set EQT PK for use
Retrieve Data to be analysed and the EQT's signature from file
Hash Data, result is M
Send M to control card
PSO : Hash (M)
OK / NOK
Store M
OK?
No
Yes
Send EQT's signature for verification
PSO : Verify Digital Signature (Signature)
OK / NOK
Verify signature using M and EQT PK
OK?
No
Yes
Signature successfully verified
Signature could not be verified or verification unsuccessful

Dodatak 12.

UTVRĐIVANJE POLOŽAJA NA TEMELJU GLOBALNOG SATELITSKOG NAVIGACIJSKOG SISTEMA (GNSS)

SADRŽAJ

1. UVOD

U ovom su Dodatku navedeni tehnički zahtjevi za podatke GNSS-a koje upotrebljava jedinica u vozilu, uključujući protokole koji se moraju sprovoditi kako bi se osigurao zaštićen i točan podatkovni prenos informacija za utvrđivanje položaja.

Glavni članci Uredbe (EZ) br. 165/2014 na kojima se temelje ti zahtjevi su: članak 8., Bilježenje položaja vozila na određenim mjestima tokom dnevnog radnog vremena, članak 10., Povezanost s inteligentnim prijevoznim sistemima i članak 11., Detaljne odredbe za pametni tahograf.

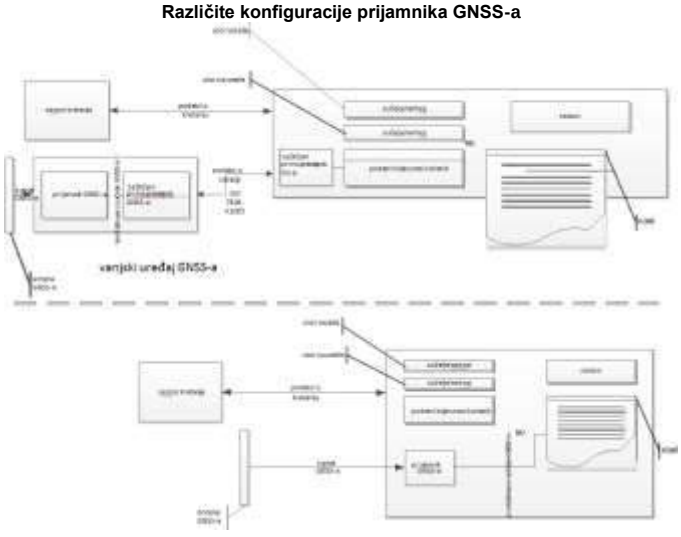
1.1. Područje primjene

GNS_1 Jedinica u vozilu prikuplja podatke o lokaciji iz barem jednog GNSS-a kako bi se pružila potpora sprovođenju člana 8.

Jedinica u vozilu može, ali ne mora, imati vanjski uređaj GNSS-a kako je prikazano na slici 1.:

Slika 1.

Različite konfiguracije prijamnika GNSS-a



1.2. Skraćenice i bilješke

U ovom se Dodatku upotrebljavaju sljedeće skraćenice:

DOP slabljenje preciznosti (eng. Dilution of Precision)
EGF elementarna datoteka uređaja GNSS-a (eng. Elementary file GNSS Facility)
EGNOS Evropski geostacionarni navigacijski sistem (eng. European Geostationary Navigation Overlay Service)
GNSS globalni satelitski navigacijski sistem (eng. Global Navigation Satellite System)
GSA GPS DOP (slabljenje preciznosti GPS-a) i aktivni sateliti (eng. GPS DOP and active satellites)
HDOP horizontalno slabljenje preciznosti (eng. Horizontal Dilution of Precision)
ICD dokument upravljanja sučeljem (eng. Interface Control Document)
NMEA Nacionalno udruženje za pomorsku elektroniku (eng. National Marine Electronics Association)
PDOP slabljenje preciznosti položaja (eng. Position Dilution of Precision)
RMC preporučena minimalna određenost (eng. Recommended Minimum Specific)
SIS signal u svemiru (eng. Signal in Space)
VDOP vertikalno slabljenje preciznosti (eng. Vertical Dilution of Precision)
VU jedinica u vozilu (eng. Vehicle Unit)

2. SPECIFIKACIJE PRIJAMNIKA GNSS-A

Bez obzira na konfiguraciju pametnog tahografa s vanjskim uređajem GNSS-a ili bez njega, pružanje tačnih i pouzdanih informacija za utvrđivanje položaja ključan je element učinkovitog rada pametnog tahografa. Stoga je primjereno zahtijevati njegovu kompatibilnost s uslugama koje pružaju programi Galileo i Evropski geostacionarni navigacijski sistem (EGNOS), kako je navedeno u Uredbi (EU) br. 1285/2013 Evropskog parlamenta i Vijeća ([19]). Sistem uveden u okviru programa Galileo nezavisni je globalni satelitski navigacijski sistem, dok je sistem uveden u okviru programa EGNOS regionalni satelitski navigacijski sistem kojim se poboljšava kvaliteta signala globalnog sistema za utvrđivanje položaja.

GNS_2 Proizvođači osiguravaju da su prijamnici GNSS-a u pametnim tahografima kompatibilni s uslugama utvrđivanja položaja koje pružaju sistemi Galileo i EGNOS. Proizvođači se također mogu odlučiti i na kompatibilnost s drugim satelitskim navigacijskim sistemima.

GNS_3 Prijamnik GNSS-a mora imati mogućnost autentifikacije za otvorenu uslugu programa Galileo ako takvu uslugu pruža sistem Galileo i ako je podržavaju proizvođači prijamnika GNSS-a. Međutim, za pametne tahografe koji su stavljeni na tržište prije ispunjenja gore navedenih zahtjeva i koji nemaju mogućnosti autentifikacije za otvorenu uslugu programa Galileo neće se zahtijevati nikakva prilagodba.

3. NMEA REČENICE

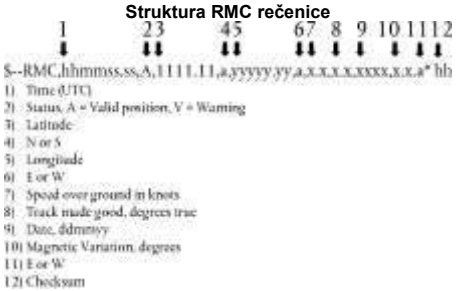
U ovom su odjeljku opisane NMEA rečenice koje se upotrebljavaju u radu pametnog tahografa. Ovaj se odjeljak primjenjuje na konfiguraciju pametnih tahografa s vanjskim uređajem GNSS-a ili bez njega.

GNS_4 Podaci o lokaciji temelje se na NMEA rečenici *Recommended Minimum Specific* (RMC) *GNSS Data*, koja sadrži informacije o položaju (zemljopisna širina, zemljopisna dužina), vrijeme u UTC formatu (hhmmss.ss) te brzinu preko dna u čvorovima uz dodatne vrijednosti.

Format RMC rečenice glasi kako slijedi (prema normi NMEA V4.1):

Slika 2.

Struktura RMC rečenice



Status označava je li signal GNSS-a dostupan. Sve dok se vrijednost statusa ne postavi na A, primljeni podaci (npr. o vremenu ili zemljopisnoj dužini/širini) ne mogu se upotrijebiti za bilježenje položaja vozila u jedinici u vozilu.

Rezolucija položaja temelji se na formatu prethodno opisane RMC rečenice. Prvi dijelovi polja 3) i 5) upotrebljavaju se za prikaz stupnjeva. Ostatak se upotrebljava za prikaz minuta s tri decimale. Stoga rezolucija iznosi 1/1 000 minute ili 1/60 000 stupnja (jer jedna minuta iznosi 1/60 stupnja).

GNS_5 Jedinica u vozilu sprema u svojoj bazi podataka informacije o položaju za zemljopisnu dužinu i zemljopisnu širinu pri rezolucijai od 1/10 minute ili 1/600 stupnja, kako je opisano u Dodatku 1. za vrstu GeoCoordinates.

Jedinica u vozilu može upotrebljavati naredbu GPS DOP and active satellites (GSA) za određivanje i bilježenje dostupnosti i preciznosti signala. HDOP se posebno upotrebljava za ukazivanje na razinu preciznosti zabilježenih podataka o lokaciji (vidjeti tačku 4.2.2). Jedinica u vozilu spremit će vrijednost horizontalnog slabljenja preciznosti (HDOP) izračunanu kao minimum HDOP vrijednosti prikupljenih na raspoloživim sistemima GNSS-a.

GNSS Id. označava odgovarajući NMEA Id. za svaku konfiguraciju GNSS-a i satelitski sistem proširivanja (SBAS).

Slika 3.
Struktura GSA rečenice

GNS_6 *GSA* rečenica sprema se pod brojem zapisa '02' do '06'.
GNS_7 Maksimalna veličina NMEA rečenice (npr. RMC, GSA ili druge) koja se može upotrijebiti za određivanje veličine naredbe za čitanje zapisa iznosi 85 bajtova (vidjeti tablicu 1).

4. JEDINICA U VOZILU S VANJSKIM UREĐAJEM GNSS-A

4.1. Konfiguracija

4.1.1 *Glavni sastavni dijelovi i sučelja*

U ovoj je konfiguraciji prijamnik GNSS-a sastavni dio vanjskog uređaja GNSS-a.
GNS_8 Vanjski uređaj GNSS-a mora se napajati putem specifičnog sučelja vozila.
GNS_9 Vanjski uređaj GNSS-a sastoji se od sljedećih sastavnih dijelova (vidjeti sliku 4.):
a) komercijalnog prijamnika GNSS-a koji pruža podatke o položaju putem podatkovnog sučelja GNSS-a. Primjerice, podatkovno sučelje GNSS-a može upotrebljavati normu NMEA V4.10 pri čemu prijamnik GNSS-a služi kao odašiljač i prenosi NMEA rečenice zaštićenom primopredajniku GNSS-a pri frekvenciji od 1 Hz za predefinisani niz NMEA rečenica, koji mora sadržiti barem RMC i GSA rečenice. Proizvođači vanjskog uređaja GNSS-a odabiru način provedbe podatkovnog sučelja GNSS-a;
b) primopredajne jedinice (zaštićenog primopredajnika GNSS-a) koja može podržati standard ISO/IEC 7816-4:2013 (vidjeti 4.2.1) za komunikaciju s jedinicom u vozilu te podržati podatkovno sučelje GNSS-a do prijamnika GNSS-a. Jedinica je opremljena memorijom za spremanje identifikacijskih podataka prijamnika GNSS-a i vanjskog uređaja GNSS-a;
c) kućišta s funkcijom otkrivanja neovlaštenog rukovanja u kojem se nalaze prijamnik GNSS-a i zaštićeni primopredajnik GNSS-a. Funkcijom otkrivanja neovlaštenog rukovanja provode se sigurnosne mjere zaštite navedene u profilu zaštite pametnih tahografa;
d) antene GNSS-a ugrađene na vozilo i spojene na prijamnik GNSS-a kroz kućište.
GNS_10 Vanjski uređaj GNSS-a sadrži barem sljedeća vanjska sučelja:
a) sučelje prema anteni GNSS-a ugrađenoj na vozilo, ako se upotrebljava vanjska antena;
b) sučelje prema jedinici u vozilu.
GNS_11 U jedinici u vozilu zaštićeni primopredajnik jedinice u vozilu predstavlja drugi kraj zaštićene komunikacije sa zaštićenim primopredajnikom GNSS-a te mora podržavati normu ISO/IEC 7816-4:2013 za spajanje s vanjskim uređajem GNSS-a.
GNS_12 Za fizički dio komunikacije s vanjskim uređajem GNSS-a jedinica u vozilu podržava normu ISO/IEC 7816-12:2005 ili neku drugu normu koja može podržavati normu ISO/IEC 7816-4:2013. (vidjeti odjeljak 4.2.1).

4.1.2 *Stanje vanjskog uređaja GNSS-a na kraju proizvodnog procesa*

GNS_13 Vanjski uređaj GNSS-a pri izlasku iz tvornice sprema sljedeće vrijednosti u neizbrisivu memoriju zaštićenog primopredajnika GNSS-a:
— par ključeva EGF_MA i odgovarajući certifikat;
— certifikat MSCA_VU-EGF koji sadrži javni ključ MSCA_VU-EGF.PK koji se upotrebljava za provjeravanje certifikata EGF_MA;
— EUR certifikat koji sadrži javni ključ EUR.PK koji se upotrebljava za provjeravanje certifikata MSCA_VU-EGF;
— EUR certifikat čije period važnosti direktno prethodi razdoblju važnosti EUR certifikata koji se upotrebljava za provjeravanje certifikata MSCA_VU-EGF, ako postoji;
— certifikat o povezanosti koji povezuje ta dva EUR certifikata, ako postoji;
— prošireni serijski broj vanjskog uređaja GNSS-a;
— identifikator operativnog sistema uređaja GNSS-a;
— homologacijski broj vanjskog uređaja GNSS-a;
— identifikator sigurnosne komponente vanjskog uređaja GNSS-a.

4.2. Komunikacija između vanjskog uređaja GNSS-a i jedinice u vozilu

4.2.1 *Komunikacijski protokol*

GNS_14 Komunikacijski protokol između vanjskog uređaja GNSS-a i jedinice u vozilu podržava tri funkcije:
1. prikupljanje i distribuciju podataka GNSS-a (npr. položaj, vrijeme, brzinu);
2. prikupljanje konfiguracijskih podataka vanjskog uređaja GNSS-a;
3. upravljački protokol za podršku spajanju, međusobnoj autentifikaciji i dogovoru o ključu za razmjenu podataka između vanjskog uređaja GNSS-a i jedinice u vozilu.
GNS_15 Komunikacijski protokol temelji se na normi ISO/IEC 7816 4:2013, pri čemu zaštićeni primopredajnik jedinice u vozilu ima nadređenu, a zaštićeni primopredajnik GNSS-a podređenu ulogu. Fizička veza između

vanjskog uređaja GNSS-a i jedinice u vozilu temelji se na normi ISO/IEC 7816-12:2005 ili nekoj drugoj normi koja može podržavati zahtjeve norme ISO/IEC 7816-4:2013.
GNS_16 Polja proširene dužine ne moraju biti podržana u komunikacijskom protokolu.
GNS_17 Komunikacijski protokol norme ISO 7816 (*-4:2013 i *-12:2005) između vanjskog uređaja GNSS-a i jedinice u vozilu ima vrijednost T=1.
GNS_18 S obzirom na funkcije 1) prikupljanja i distribucije podataka GNSS-a, 2) prikupljanja konfiguracijskih podataka vanjskog uređaja GNSS-a i 3) upravljačkog protokola, zaštićeni primopredajnik GNSS-a simulira pametnu karticu čija se arhitektura sistema datoteka sastoji od glavne datoteke (eng. Master File, MF), namjenske datoteke (eng. Dedicated File, DF) s identifikatorom aplikacije određenim u poglavlju 6.2. Dodatka 1. („FF 44 54 45 47 4D") te tri elementarne datoteke (eng. Elementary File, EF) koje sadržiju certifikate i jedne elementarne datoteke (EF.EGF) s identifikatorom datoteke koji odgovara vrijednosti „2F2F" kako je opisano u tablici 1.
GNS_19 Zaštićeni primopredajnik GNSS-a sprema podatke iz prijamnika GNSS-a i konfiguraciju u datoteku EF.EGF. To je linearna datoteka zapisa promjenjive dužine čiji identifikator odgovara vrijednosti '2F2F' u heksadecimalnom formatu.
GNS_20 Zaštićeni primopredajnik GNSS-a upotrebljava memoriju za spremanje podataka i može izvršiti najmanje 20 milijuna ciklusa čitanja/pisanja. Osim ovoga, interno projektiranje i implementacija zaštićenog primopredajnika GNSS-a prepušta se proizvođačima.
Mapiranje brojeva i podataka zapisa prikazano je u tablici 1. Napominjemo da postoji pet GSA rečenica za konfiguracije GNSS-a i satelitski sistem proširivanja (SBAS).
GNS_21 Struktura datoteka navedena je u tablici 1. Za uslove pristupa (ALW, NEV, SM-MAC) vidjeti poglavlje 3.5. Dodatka 2.

Tablica 1.
Struktura datoteke

		Uslovi pristupa		
Datoteka	**Identifikacija datoteke**	**Čitanje**	**Ažuriranje**	**Šifrirano**
MF	3F00			
EF.ICC	0002	ALW	NEV (sprovodi ga jedinica u vozilu)	Ne
DF uređaja GNSS-a	0501	ALW	NEV	Ne
EF EGF_MACertificate	C100	ALW	NEV	Ne
EF CA_Certificate	C108	ALW	NEV	Ne
EF Link_Certificate	C109	ALW	NEV	Ne
EF.EGF	2F2F	SM-MAC	NEV (sprovodi ga jedinica u vozilu)	Ne

Datoteka / podatkovni element	**Broj zapisa**	**Veličina (u bajtovima)**		**Zadane vrijednosti**
		min.	**maks.**	
MF		552	1 031	
EF.ICC				
sensorGNSSSerialNumber		8	8	
DF uređaja GNSS-a		*612*	*1 023*	
EF EGF_MACertificate		*204*	*341*	
EGFCertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF.EGF				
RMC NMEA rečenica	'01'	85	85	
prva GSA NMEA rečenica	'02'	85	85	
druga GSA NMEA rečenica	'03'	85	85	
treća GSA NMEA rečenica	'04'	85	85	
četvrta GSA NMEA rečenica	'05'	85	85	
peta GSA NMEA rečenica	'06'	85	85	
prošireni serijski broj vanjskog uređaja GNSS-a definisan u Dodatku 1. kao SensorGNSSSerialNumber.	'07'	8	8	
identifikator operativnog sistema GNSS-a zaštićeni primopredajnik definisan u Dodatku 1. kao SensorOSIdentifier.	'08'	2	2	
homologacijski broj vanjskog uređaja GNSS-a definisan u Dodatku 1. kao SensorExternalGNSSApprovalNumber.	'09'	16	16	
identifikator sigurnosne komponente vanjskog uređaja GNSS-a definisan u Dodatku 1. kao SensorExternalGNSSSCIdentifier	'10'	8	8	
RFU – rezervisano za buduću upotrebu	Od '11' do 'FD'			

4.2.2 *Zaštićeni prenos podataka GNSS-a*

GNS_22 Zaštićeni prenos podataka o položaju GNSS-a dopušta se samo u sljedećim okolnostima:

1. proces spajanja izvršen je kako je opisano u Dodatku 11., Zajednički sigurnosni mehanizmi;
2. povremena međusobna autentifikacija i dogovor o ključu za razmjenu podataka između jedinice u vozilu i vanjskog uređaja GNSS-a, isto tako opisani u Dodatku 11., Zajednički sigurnosni mehanizmi, izvršeni su prema naznačenoj učestalosti.

GNS_23 Svakih T sekundi, pri čemu je T vrijednost niža od 10 ili jednaka 10, osim ako dođe do spajanja ili međusobne autentifikacije i dogovora o ključu za razmjenu podataka, jedinica u vozilu traži od vanjskog uređaja GNSS-a informacije o položaju na temelju sljedećeg toka:

1. Jedinica u vozilu traži podatke o lokaciji od vanjskog uređaja GNSS-a zajedno s podacima o slabljenju preciznosti (iz GSA NMEA rečenice). Zaštićeni primopredajnik jedinice u vozilu upotrebljava normu ISO/IEC 7816-4:2013, naredbu *SELECT and READ RECORD(S)* u sigurnom prenosu poruka u načinu rada namijenjenom isključivo autentifikaciji, kako je opisano u odjeljku 11.5. Dodatka 11., s identifikatorom datoteke '2F2F' te RECORD brojem koji ima vrijednost '01' za RMC NMEA rečenice te vrijednosti '02', '03', '04', '05', '06' za GSA NMEA rečenice.
2. Zadnji zaprimljeni podaci o lokaciji spremaju se u EF-u s identifikatorom '2F2F' i zapisima opisanima u tablici
1. u zaštićeni primopredajnik GNSS-a kada zaštićeni primopredajnik GNSS-a zaprimi NMEA podatke pri frekvenciji od najmanje 1 Hz od prijamnika GNSS-a putem podatkovnog sučelja GNSS-a.
3. Zaštićeni primopredajnik GNSS-a šalje odgovor zaštićenom primopredajniku jedinice u vozilu koristeći se APDU odgovorom u sigurnom prenosu poruka u načinu rada namijenjenom isključivo autentifikaciji, kako je opisano u odjeljku 11.5. Dodatka 11.
4. Zaštićeni primopredajnik jedinice u vozilu provjerava autentičnost i integritet primljenog odgovora. U slučaju pozitivnog rezultata podaci o lokaciji šalju se u procesor jedinice u vozilu putem podatkovnog sučelja GNSS-a.
5. Procesor jedinice u vozilu provjerava primljene podatke, dobivajući podatke (npr. zemljopisna širina, zemljopisna dužina, vrijeme) iz RMC NMEA rečenice. RMC NMEA rečenica uključuje informacije o važnosti položaja. Ako položaj nije važeći, podaci o lokaciji još nisu dostupni i ne mogu se upotrijebiti za bilježenje položaja vozila. Ako je položaj važeći, procesor jedinice u vozilu isto tako dobiva HDOP vrijednosti iz GSA NMEA rečenica i računa najmanju vrijednost na dostupnom satelitskom sistemu (to jest, kada je lociranje dostupno).
6. Procesor jedinice u vozilu sprema primljene i obrađene informacije, poput zemljopisne širine, zemljopisne dužine, vremena i brzine, u jedinici u vozilu u formatu definisanom u Dodatku 1., Rječnik s podacima, kao *GeoCoordinates* zajedno s HDOP vrijednošću izračunanom kao minimum HDOP vrijednosti prikupljenih na dostupnim sistemima GNSS-a.

4.2.3 *Struktura naredbe Read Record*

U ovom odjeljku detaljno je opisana struktura naredbe *Read Record* (čitanje zapisa). Sigurni prenos poruka (u načinu rada namijenjenom isključivo autentifikaciji) dodaje se kako je opisano u Dodatku 11., Zajednički sigurnosni mehanizmi.

GNS_24 Naredba podržava sigurni prenos poruka u načinu rada namijenjenom isključivo autentifikaciji; vidjeti Dodatak 11.

GNS_25 Poruka naredbe

Bajt	Dužina	Vrijednost	Opis
CLA	1	'0Ch'	Zahtjev za sigurni prenos poruka.
INS	1	'B2h'	Čitanje zapisa
P1	1	'XXh'	Broj zapisa ('00' označava da se radi o trenutnom zapisu)
P2	1	'04h'	Čitanje zapisa čiji je broj zapisa naveden u P1
Le	1	'XXh'	Očekivana dužina podataka. Broj bajtova koji se očitava.

GNS_26 Zapis naveden u P1 postaje trenutni zapis.

Bajt	Dužina	Vrijednost	Opis
#1-#X	X	'XX..XXh'	Očitani podaci
SW	2	'XXXXh'	Statusne riječi (SW1,SW2)

— Ako je naredba uspješna, zaštićeni primopredajnik GNSS-a uzvraća '**9000**'.
— Ako trenutna datoteka nije postavljena za zapis, zaštićeni primopredajnik GNSS-a uzvraća '**6981**'.
— Ako se naredba koristi s P1 = '00', no ne postoji trenutni EF, zaštićeni primopredajnik GNSS-a uzvraća '**6986**' (naredba nije dozvoljena).
— Ako zapis nije pronađen, zaštićeni primopredajnik GNSS-a uzvraća '**6A 83**'.
— Ako je vanjski uređaj GNSS-a otkrio neovlašteno rukovanje, uzvraća statusne riječi '**66 90**'.

GNS_27 Zaštićeni primopredajnik GNSS-a podržava sljedeće naredbe druge generacije tahografa, navedene u Dodatku 2.:

Naredba	Upućivanje
Select	poglavlje 3.5.1. Dodatka 2.
Read Binary	poglavlje 3.5.2. Dodatka 2.
Get Challenge	poglavlje 3.5.4. Dodatka 2.
PSO: Verify Certificate	poglavlje 3.5.7. Dodatka 2.
External Authenticate	poglavlje 3.5.9. Dodatka 2.
General Authenticate	poglavlje 3.5.10. Dodatka 2.
MSE:SET	poglavlje 3.5.11. Dodatka 2.

4.3. Spajanje, međusobna autentifikacija i dogovor o ključu za razmjenu podataka između vanjskog uređaja GNSS-a i jedinice u vozilu

Spajanje, međusobna autentifikacija i dogovor o ključu za razmjenu podataka između vanjskog uređaja GNSS-a i jedinice u vozilu opisani su u poglavlju 11. Dodatka 11., Zajednički sigurnosni mehanizmi.

4.4. Upravljanje greškama

U ovom odjeljku opisano je kako se moguća stanja greške vanjskog uređaja GNSS-a obrađuju i zapisuju u jedinici u vozilu.

4.4.1 *Greška u komunikaciji s vanjskim uređajem GNSS-a*

GNS_28 Ako jedinica u vozilu ne može uspostaviti komunikaciju sa spojenim vanjskim uređajem GNSS-a duže od 20 uzastopnih minuta, jedinica u vozilu generiše i bilježi u jedinici u vozilu događaj vrste EventFaultType with koji ima vrijednost enumerirane vrste '0E'H Communication error with the external GNSS facility te oznaku vremena koja navodi trenutačno vrijeme. Događaj će se generišeti samo ako su ispunjena sljedeća dva uvjeta: a) pametni tahograf nije u načinu rada za kalibraciju i b) vozilo se kreće. U ovom kontekstu, greška u komunikaciji nastaje kada zaštićeni primopredajnik jedinice u vozilu ne primi odgovor nakon zahtjeva kako je opisano u 4.2.

4.4.2 *Proboj fizičkog integriteta vanjskog uređaja GNSS-a*

▼M1

GNS_29 Ako je došlo do proboja vanjskog uređaja GNSS-a, zaštićeni primopredajnik GNSS-a briše cijelu svoju memoriju, uključujući kriptografski materijal. Kako je opisano u stavcima GNS_25 i GNS_26, jedinica u vozilu otkriva neovlašteno rukovanje ako odgovor ima status ‚6690'. Jedinica u vozilu tada generiše događaj vrste EventFaultType, enumerirane vrste ‚19'H Tamper detection of GNSS (otkriveno neovlašteno rukovanje GNSS-om). U suprotnom, vanjski uređaj GNSS-a više ne može odgovoriti ni na koji vanjski zahtjev.

4.4.3 *Izostanak podataka o položaju iz prijamnika GNSS-a*

GNS_30 Ako zaštićeni primopredajnik GNSS-a ne zaprimi podatke od prijamnika GNSS-a duže od tri uzastopna sata, zaštićeni primopredajnik GNSS-a generiše odgovor na naredbu READ RECORD s brojem RECORD koji ima vrijednost ‚01', s podatkovnim poljem (eng. Data Field) od 12 bajtova od kojih svi imaju vrijednost ‚0xFF'. Po zaprimanju odgovora čije podatkovno polje ima tu vrijednost, jedinica u vozilu generiše i bilježi događaj vrste EventFaultType, enumerirane vrste '0D'H Absence of position information from GNSS receiver (izostanak podataka o položaju iz prijamnika GNSS-a) s oznakom vremena koja navodi vrijeme u tom trenutku, samo pod uslovom da su ispunjena sljedeća dva uvjeta: a) pametni tahograf nije u načinu rada za kalibraciju i b) vozilo se kreće.

4.4.4 *Istekla je važnost certifikata vanjskog uređaja GNSS-a*

GNS_31 Ako jedinica u vozilu otkrije da certifikat EGF koji se upotrebljava za međusobnu autentifikaciju nije više važeći, jedinica u vozilu generiše i bilježi događaj uređaja za bilježenje podataka vrste EventFaultType, enumerirane vrste *'1B'H External GNSS facility certificate expired (certifikat vanjskog uređaja GNSS-a istekao)* s oznakom vremena koja navodi vrijeme u tom trenutku. Jedinica u vozilu i dalje upotrebljava zaprimljene podatke o položaju GNSS-a.

Slika 4

Nacrt vanjskog uređaja GNSS-a

5. JEDINICA U VOZILU BEZ VANJSKOG UREĐAJA GNSS-A

5.1. Konfiguracija

U ovoj se konfiguraciji prijamnik GNSS-a nalazi unutar jedinice u vozilu kako je opisano na slici 1.

GNS_32 Prijamnik GNSS-a ima ulogu odašiljača i prenosi NMEA rečenice procesoru jedinice u vozilu, koji ima ulogu prijamnika s frekvencijom od 1/10 Hz ili bržom za predefinisani niz NMEA rečenica, koje uključuju barem RMC i GSA rečenice.

GNS_33 Na jedinicu u vozilu spaja se vanjska antena GNSS-a ugrađena na vozilo ili interna antena GNSS-a.

5.2. Upravljanje greškama

5.2.1 *Izostanak podataka o položaju iz prijamnika GNSS-a*

GNS_34 Ako jedinica u vozilu ne primi podatke iz prijamnika GNSS-a duže od tri uzastopna sata, jedinica u vozilu generiše i bilježi događaj vrste EventFaultType, enumerirane vrste '0D'H Absence of position information from GNSS receiver (izostanak podataka o položaju iz prijamnika GNSS) s oznakom vremena koja navodi vrijeme u tom trenutku, pod uslovom da su ispunjena sljedeća dva uvjeta: a) pametni tahograf nije u načinu rada za kalibraciju i b) vozilo se kreće.

6. VREMENSKI KONFLIKT GNSS-A

Ako jedinica u vozilu otkrije nepodudarnost dulju od jedne minute između vremena koje je izmjerila funkcija mjerenja vremena jedinice u vozilu i vremena koje je izmjerio prijamnik GNSS-a, jedinica u vozilu zabilježit će događaj vrste EventFaultType, enumerirane vrste *'0B'H Time conflict (GNSS versus VU internal clock) (vremenski konflikt između GNSS-a i unutarnjeg sata jedinice u vozilu)*. Nakon što se aktivira vremenski konflikt, jedinica u vozilu neće provjeravati nepodudarnost vremena sljedećih 12 sati. Taj se događaj neće aktivirati ako prijamnik GNSS-a nije mogao otkriti važećii signal GNSS-a u posljednjih 30 dana.

7. KONFLIKT U KRETANJU VOZILA

GNS_35 Jedinica u vozilu pokreće i bilježi događaj konflikta u kretanju vozila (vidjeti zahtjev 84 u Prilogu I.C) s oznakom vremena koja odgovara trenutačnom vremenu, u slučaju da su informacije o kretanju izračunane s pomoću senzora kretanja proturječne informacijama o kretanju dobivenima iz unutarnjeg prijamnika GNSS-a ili iz vanjskog uređaja GNSS-a. U svrhu otkrivanja takvih protivrječnosti upotrebljava se srednja vrijednost razlika u brzini između tih izvora, kako je navedeno u nastavu:

— najviše svakih deset sekundi izračunava se apsolutna vrijednost razlike između brzine vozila koju je procijenio GNSS i one koju je procijenio senzor kretanja,

— sve se vrijednosti izračunane u razdoblju koje se odnosi na posljednjih pet minuta kretanja upotrebljavaju za izračunavanje srednje vrijednosti,

— srednja se vrijednost izračunava kao prosjek od 80 % preostalih vrijednosti, nakon eliminiranja onih najviših u apsolutnim vrijednostima.

Događaj konflikta u kretanju vozila nastaje ako je srednja vrijednost viša od 10 km/h tokom pet neprekidnih minuta kretanja vozila. Mogu se upotrebljavati i drugi neovisni izvori otkrivanja kretanja vozila kako bi se omogućilo pouzdanije otkrivanje manipuliranja tahografom. (Napomena: upotreba srednje vrijednosti posljednjih pet minuta primjenjuje se radi ublažavanja rizika od netipičnih vrijednosti mjerenja i prelaznih vrijednosti). Ovaj se događaj neće aktivirati u sljedećim uslovima: a) tokom vožnje trajektom/vozom, b) kada podaci o položaju iz prijamnika GNSS-a nisu raspoloživi i c) kada je u načinu rada za kalibraciju.

Dodatak 13

ITS SUČELJE

SADRŽAJ

1. UVOD

U ovom se Dodatku utvrđuju izrada i postupci koje treba slijediti za provedbu sučelja s inteligentnim prijevoznim sistemima (ITS) u skladu sa zahtjevima iz člana 10. Uredbe (EU) br. 165/2014 (u daljnjem tekstu: Uredba).

Uredbom se utvrđuje da tahografi vozila mogu biti opremljeni standardizovanim sučeljima putem kojih podatke koje je tahograf zabilježio ili generisao može upotrebljavati vanjski uređaj u operativnom načinu rada ako su ispunjeni sljedeći uslovi:

(a) sučelje ne utječe na ispravnost i integritet podataka koje je zabilježio tahograf;

(b) sučelje je usklađeno s detaljnim odredbama iz člana 11. Uredbe;

(c) vanjski uređaj povezan sa sučeljem ima pristup ličnim podacima, uključujući podatke o geografskom položaju, samo nakon prethodnog odobrenja vozača na kojeg se podaci odnose.

2. PODRUČJE PRIMJENE

U okviru područja primjene ovog Dodatka utvrđuje se kako aplikacije na vanjskim uređajima preko Bluetooth® veze dobivaju podatke (u daljnjem tekstu: podaci) iz tahografa.

Podaci dostupni preko tog sučelja opisani su u Prilogu 1. ovom dokumentu. Sučelje ne zabranjuje provedbu drugih sučelja (npr. preko CAN sabirnice) za prenos podataka iz jedinice u vozilu u druge procesorske jedinice u vozilu.

U ovom se Dodatku utvrđuju:

— podaci dostupni preko ITS sučelja,

— Bluetooth® profil koji se upotrebljava za prenos podataka,

— postupci povezani s upitima i preuzimanjem podataka te slijed operacija,

— mehanizam uparivanja tahografa i vanjskog uređaja,

— mehanizam za davanje saglasnosti koji je dostupan vozaču.

Radi pojašnjenja, u ovom se Dodatku ne utvrđuju:

— prikupljanje *podataka* i upravljanje prikupljanjem podatka unutar jedinice u vozilu (oni se utvrđuju drugdje u *Uredbi* ili su funkcija izvedbe proizvoda),

— oblik prikaza prikupljenih podataka u aplikaciji na vanjskom uređaju,

— odredbe o sigurnosti podataka izvan onoga što osigurava Bluetooth® (kao što je šifriranje) u vezi sa sadržajem *podataka* (one će biti utvrđene drugdje u *Uredbi* [Dodatak 11. „Zajednički sigurnosni mehanizmi"]),

— Bluetooth® protokoli koje primjenjuje ITS sučelje.

2.1. Skraćenice, definicije i zapisi

U ovom se Dodatku upotrebljavaju sljedeće skraćenice i definicije specifične za ovaj Dodatak:

komunikacija razmjena informacija/podataka između glavne jedinice (tj. tahografa) i vanjske jedinice preko ITS sučelja primjenom Bluetootha®.

podaci skupovi podataka kako je utvrđeno u Prilogu 1.

Uredba Uredba (EU) br. 165/2014 Evropskog parlamenta i Vijeća od 4. februar 2014. o tahografima u drumskom prometu, stavljanju izvan snage Uredbe Vijeća (EEZ) br. 3821/85 o tahografu u drumskom prometu i izmjeni Uredbe (EZ) br. 561/2006 Evropskog parlamenta i Vijeća o usklađivanju određenog socijalnog zakonodavstva koje se odnosi na drumski promet.

BR osnovna brzina (eng. Basic Rate)
EDR povećana brzina prenosa podataka (eng. Enhanced Data Rate)
GNSS globalni satelitski navigacijski sistem (eng. Global Navigation Satellite System)
IRK ključ za utvrđivanje identiteta (eng. Identity Resolution Key)
ITS inteligentni prijevozni sistem (eng. Intelligent Transport System)
LE niska energija (eng. Low Energy)
PIN lični identifikacijski broj (eng. Personal Identification Number)
PUC osobna šifra za deblokadu (eng. Personal Unblocking Code)
SID identifikator usluge (eng. Service Identifier)
SPP profil serijskog ulaza (eng. Serial Port Profile)

SSP sigurno jednostavno uparivanje (eng. Secure Simple Pairing)
TRTP parametar zahtjeva za prenos (eng. Transfer Request Parameter)
TREP parametar odgovora na prenos (eng. Transfer Response Parameter)
VU jedinica u vozilu (eng. Vehicle Unit)

3. UPUĆIVANJA NA UREDBE I NORME

Specifikacija utvrđena u ovom Dodatku odnosi se na sve sljedeće uredbe i norme ili njihove dijelove te o njima ovisi. U klauzulama ovog Dodatka navedene su relevantne norme ili njihove relevantne klauzule. U slučaju bilo kakve protivrječnosti, prednost imaju klauzule ovog Dodatka.

U ovom se Dodatku upućuje na sljedeće uredbe i norme:

— Uredbu (EU) br. 165/2014 Evropskog parlamenta i Vijeća od 4. februar 2014. o tahografima u drumskom prometu, stavljanju izvan snage Uredbe Vijeća (EEZ) br. 3821/85 o tahografu u drumskom prometu i izmjeni Uredbe (EZ) br. 561/2006 Evropskog parlamenta i Vijeća o usklađivanju određenog socijalnog zakonodavstva koje se odnosi na drumski promet,

— Uredbu (EZ) br. 561/2006 Evropskog parlamenta i Vijeća od 15. ožujka 2006. o usklađivanju određenog socijalnog zakonodavstva koje se odnosi na drumski promet i o izmjeni uredbi Vijeća (EEZ) br. 3821/85 i (EZ) br. 2135/98 te o stavljanju izvan snage Uredbe Vijeća (EEZ) br. 3820/85,

— ISO 16844 – 4: *Road vehicles – Tachograph systems – Part 4: Can interface*,

— ISO 16844 – 7: *Road vehicles – Tachograph systems – Part 7: Parameters*,

— Bluetooth® – Serial Port Profile – V1.2,

— *Bluetooth® – Core Version 4.2*,

— protokol NMEA 0183 V4.1.

4. NAČELA RADA SUČELJA

4.1. Preduslovi za prenos podataka ITS sučeljem

Jedinica u vozilu odgovorna je za ažuriranje i održavanje podataka koji se arhiviraju na jedinici u vozilu bez uključivanja ITS sučelja. To se postiže na način svojstven jedinici u vozilu koji nije utvrđen u ovom Dodatku, već drugdje u Uredbi.

4.1.1 *Podaci dostupni preko ITS sučelja*

Jedinica u vozilu odgovorna je za ažuriranje podataka koji će biti dostupni putem ITS sučelja učestalošću koja se utvrđuje u okviru postupaka jedinice u vozilu, bez uključivanja ITS sučelja. Podaci iz jedinice u vozilu upotrebljavaju se kao osnova za dopunjavanje i ažuriranje podataka; način na koji se to ostvaruje utvrđen je drugdje u Uredbi, a ako takva specifikacija ne postoji, taj je način funkcija izvedbe proizvoda i nije utvrđen u ovom Dodatku.

4.1.2 *Sadržaj podataka*

Sadržaj podataka utvrđen je u Prilogu 1. ovom Dodatku.

4.1.3 *ITS aplikacije*

ITS aplikacije upotrebljavat će podatke koji su stavljeni na raspolaganje preko ITS sučelja za, na primjer, optimizaciju upravljanja aktivnostima vozača u skladu s Uredbom, otkrivanje mogućih kvarova tahografa ili upotrebu podataka GNSS-a. Specifikacija aplikacija nije obuhvaćena područjem primjene ovog Dodatka.

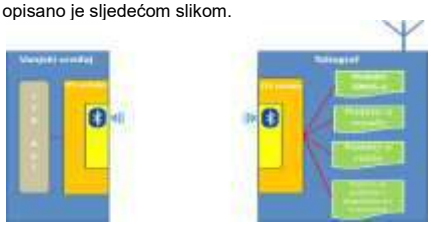
4.2. Komunikacijska tehnologija

Podaci se razmjenjuju primjenom ITS sučelja preko Bluetooth® sučelja koje je kompatibilno s verzijom 4.2 ili kasnijom verzijom. Bluetooth® radi u nelicenciranom pojasu od 2,4 do 2,485 GHz za industrijsku, znanstvenu i medicinsku primjenu (ISM). Bluetooth® 4.2 nudi unaprijeđene mehanizme za zaštitu privatnosti i sigurnosne mehanizme te veću brzinu i pouzdanost prenosa podataka. U smislu ove specifikacije, primjenjuje se Bluetooth® radio drugog razreda s dometom od najviše 10 metara. Više informacija o Bluetoothu® 4.2 dostupno je na stranici www.bluetooth.com (https://www.bluetooth.org/en-us/specification/adopted-specifications?_ga=1.215147412.2083380574.1435305676).

Komunikacija se uspostavlja komunikacijskom opremom nakon što odobreni uređaj završi proces uparivanja. Budući da Bluetooth® upotrebljava model nadređenog/podređenog uređaja kojim nadzire kada i kako uređaji mogu slati podatke, tahograf će imati nadređenu ulogu, dok će vanjski uređaji imati podređenu ulogu.

Proces uparivanja putem Bluetootha® može započeti kada vanjski uređaj prvi put dođe u domet jedinice u vozilu (vidjeti i Prilog 2.). Uređaji dijele adrese, nazive i profile te zajednički tajni ključ kojim im se omogućava povezivanje pri svakom budućem susretu. Tim je korakom uspostavljeno povjerenje u odnosu na vanjski uređaj te je on u stanju pokrenuti zahtjeve za preuzimanje podataka iz tahografa. Nije predviđeno dodavanje mehanizama za šifriranje povrh onih koje pruža Bluetooth®. Međutim, ako su potrebni dodatni sigurnosni mehanizmi, oni se osiguravaju u skladu s Dodatkom 11. „Zajednički sigurnosni mehanizmi".

Opšte komunikacijsko načelo opisano je sljedećom slikom.



SPP (profil serijskog ulaza) profil Bluetootha® upotrebljava se za prenos podataka iz jedinice u vozilu na vanjski uređaj.

4.3. Aotvorizacija PIN-om

Iz sigurnosnih razloga jedinica u vozilu zahtijevat će sistem za aotvorizaciju PIN lozinkom odvojen od uparivanja Bluetoothom. Svaka jedinica u vozilu mora moći generišeti PIN lozinke za autentifikaciju koje se sastoje od najmanje četiri znamenke. Pri svakom uparivanju vanjskog uređaja s jedinicom u vozilu vanjski uređaj mora osigurati tačnu PIN lozinku prije zaprimanja podataka.

Nakon uspješnog unosa PIN-a uređaj se stavlja na popis dopuštenih uređaja. Na popisu dopuštenih uređaja nalazi se najmanje 64 uređaja uparenih s određenom jedinicom u vozilu.

U slučaju unosa netačne PIN lozinke tri puta zaredom, uređaj se privremeno stavlja na popis zabranjenih uređaja. Svaki pokušaj uređaja odbija se sve dok se uređaj nalazi na popisu zabranjenih uređaja. Ponovni unos netačne PIN lozinke tri puta zaredom za posljedicu ima duže trajanje zabrane (vidjeti tablicu 1.). Unosom točne PIN lozinke poništava se trajanje zabrane i broj pokušaja. Na slici 1. u Prilogu 2. prikazan je dijagram slijeda za pokušaj potvrde PIN-a.

Tablica 1

Trajanje zabrane zavisno o broju uzastopnih neuspješnih pokušaja unosa točne PIN lozinke

Broj uzastopnih neuspješnih pokušaja	Trajanje zabrane
3	30 sekundi
6	5 minuta
9	1 sat
12	24 sata
15	trajno

U slučaju unosa netačne PIN lozinke petnaest puta (5 x 3) zaredom ITS jedinica trajno se uvrštava na popis zabranjenih uređaja. Trajna se zabrana ukida samo unosom točne PUC lozinke.

PUC lozinku, koja se sastoji od osam cifara, dostavlja proizvođač zajedno s jedinicom u vozilu. U slučaju unosa netačne PUC lozinke deset puta zaredom ITS jedinica neopozivo se stavlja na popis zabranjenih uređaja.

Proizvođač može ponuditi mogućnost promjene PIN lozinke direktno putem jedinice u vozilu, no PUC lozinka nepromjenjiva je. Za eventualnu promjenu PIN lozinke potrebno je unijeti trenutačnu PIN lozinku direktno u jedinicu u vozilu.

Nadalje, svi uređaji navedeni na popisu dopuštenih uređaja čuvaju se dok ih ručno ne ukloni korisnik (npr. preko sučelja čovjek – stroj jedinice u vozilu ili drugim sredstvima). Time se izgubljene ili ukradene ITS jedinice mogu ukloniti s popisa dopuštenih uređaja. Nadalje, svaka ITS jedinica koja izađe izvan dometa Bluetooth veze u trajanju dužem od 24 sata automatski se uklanja s popisa dopuštenih uređaja za jedinicu u vozilu i mora ponovno osigurati tačnu PIN lozinku pri ponovnom uspostavljanju veze.

Format poruka između sučelja jedinice u vozilu i jedinice u vozilu nije predviđen, već ga po vlastitom nahođenju određuje proizvođač. Međutim, predmetni proizvođač osigurava da se poštuje format poruka između ITS jedinice i sučelja jedinice u vozilu (vidjeti specifikacije za ASN.1).

Stoga se na svaki zahtjev za podatke odgovara prikladnom provjerom ovlaštenja pošiljatelja prije bilo kakvog oblika obrade. Na slici 2. u Prilogu 2. prikazan je dijagram slijeda za taj postupak. Svaki uređaj uvršten na popis zabranjenih uređaja automatski se odbija, dok svaki uređaj koji nije uvršten na popis zabranjenih uređaja ni na popis dopuštenih uređaja dobiva zahtjev za PIN koji treba ispuniti prije ponovnog slanja zahtjeva za podatke.

4.4. Format poruke

Sve poruke koje razmjenjuju ITS jedinica i sučelje jedinice u vozilu po svojem formatu imaju strukturu koja se sastoji od triju dijelova: zaglavlja koje se sastoji od ciljanog bajta (TGT), izvornog bajta (SRC) i bajta dužine (LEN);

podatkovnog polja koje se sastoji od bajta identifikatora usluge (SID) i promjenjivog iznosa podatkovnih bajtova (najviše 255) te

bajta kontrolnog zbira koji je jedna serija zbira bajtova modulo 256 svih bajtova poruke osim samog kontrolnog zbira (CS).

Poruka prati redoslijed zapisa big endian.

Tablica 2

Opći format poruke

Zaglavlje			Podatkovno polje					Kontrolni zbir
TGT	SRC	LEN	SID	TRTP	CC	CM	DATA	CS
3 bajta			Najviše 255 bajtova					1 bajt

Zaglavlje

TGT i SRC: identifikator ciljnih (TGT) i izvornih (SRC) uređaja poruke. Sučelje jedinice u vozilu ima standardni identifikator „EE”. Taj identifikator nije moguće promijeniti. ITS jedinica upotrebljava standardni identifikator „A0” za svoju prvu poruku u komunikacijskoj razmjeni podataka. Sučelje jedinice u vozilu zatim ITS jedinici dodjeljuje jedinstveni identifikator i obavješćuje ju o tom identifikatoru za buduće poruke tokom razmjene podataka.

LEN bajt uzima u obzir samo dio „DATA” podatkovnog polja (vidjeti tablicu 2.); implicitna su prva četiri bajta.

Sučelje jedinice u vozilu potvrđuje autentičnost pošiljatelja poruke usporedbom svojeg popisa identifikatora s Bluetooth podacima tako što provjerava je li ITS jedinica navedena uz dostavljeni identifikator trenutačno u dometu Bluetooth veze.

Podatkovno polje

Osim SID-a, podatkovno polje sadrži i druge parametre: parametar zahtjeva za prenos (TRTP) i bajtove brojača.

Ako su podaci koji se obrađuju dulji od raspoloživog prostora u jednoj poruci, oni se dijele u nekoliko potporuka. Svaka potporuka ima jednako zaglavlje i SID, ali sadrži brojač od dva bajta, trenutni brojač (CC) i maksimalni brojač (CM) za označavanje broja potporuke. Kako bi se omogućili provjera grešaka i prekid, uređaj koji prima podatke potvrđuje svaku potporuku. Uređaj koji prima podatke može prihvatiti potporuku, zatražiti njezino ponovno slanje i zatražiti od uređaja koji šalje podatke da ponovno započne ili prekine prenos.
Ako se ne upotrebljavaju, za CC i CM određuje se vrijednost 0 x FF.
Na primjer, sljedeća poruka

ZAGLAVLJE (eng. *HEADER*)	**SID**	**TRTP**	**CC**	**CM**	**DATA**	**CS**
3 bajta	više od 255 bajtova					1 bajt

prenosi se kao:

ZAGLAVLJE	**SID**	**TRTP**	**01**	**n**	**DATA**	**CS**
3 bajta	255 bajtova					1 bajt

ZAGLAVLJE	**SID**	**TRTP**	**02**	**n**	**DATA**	**CS**
3 bajta	255 bajtova					1 bajt

…

ZAGLAVLJE (eng. *HEADER*)	**SID**	**TRTP**	**N**	**N**	**DATA**	**CS**
3 bajta	najviše 255 bajtova					1 bajt

Tablica 3. sadrži poruke koje mogu razmjenjivati jedinica u vozilu i ITS jedinica. Sadržaj svakog parametra naveden je u heksadecimalnom zapisu. U tablici radi jasnoće nisu navedeni CC i CM; za potpuni format vidjeti prethodno.

Tablica 3
Detaljan sadržaj poruke

Poruka	**Zaglavlje**			**DATA**			**Kontrolni zbir**
	TGT	**SRC**	**LEN**	**SID**	**TRTP**	**DATA**	
RequestPIN	*ITSID*	EE	00	01	FF		
SendITSID	*ITSID*	EE	01	02	FF	*ITSID*	
SendPIN	EE	*ITSID*	04	03	FF	4*INTEGER (0..9)	
PairingResult	*ITSID*	EE	01	04	FF	BOOLEAN (T/F)	
SendPUC	EE	*ITSID*	08	05	FF	8*INTEGER (0..9)	
BanLiftingResult	*ITSID*	EE	01	06	FF	BOOLEAN (T/F)	
RequestRejected	*ITSID*	EE	08	07	FF	vrijeme (*Time*)	
RequestData							
standardTachData	EE	*ITSID*	01	08	01		
personalTachData	EE	*ITSID*	01	08	02		
gnssData	EE	*ITSID*	01	08	03		
standardEventData	EE	*ITSID*	01	08	04		
personalEventData	EE	*ITSID*	01	08	05		
standardFaultData	EE	*ITSID*	01	08	06		
manufacturerData	EE	*ITSID*	01	08	07		
ResquestAccepted	*ITSID*	EE	Len	09	TREP	podaci (*Data*)	
DataUnavailable							
Podaci nisu dostupni	*ITSID*	EE	02	0A	TREP	10	
Lični se podaci ne dijele	*ITSID*	EE	02	0A	TREP	11	
NegativeAnswer							
Opšte odbijanje	*ITSID*	EE	02	0B	SID Req	10	
Usluga nije podržana	*ITSID*	EE	02	0B	SID Req	11	
Podfunkcija nije podržana	*ITSID*	EE	02	0B	SID Req	12	
Nepravilna dužina poruke	*ITSID*	EE	02	0B	SID Req	13	
Nepravilni uslovi ili greška u slijedu zahtjeva	*ITSID*	EE	02	0B	SID Req	22	
Zahtjev izvan dometa	*ITSID*	EE	02	0B	SID Req	31	
Čeka se odgovor	*ITSID*	EE	02	0B	SID Req	78	
Neusklađenost ITSID-a	*ITSID*	EE	02	0B	SID Req	FC	
Nije pronađen ITSID	*ITSID*	EE	02	0B	SID Req	FB	

RequestPIN (SID 01)
Poruku šalje sučelje jedinice u vozilu ako ITS jedinica koja nije na popisu zabranjenih uređaja, ali ni na popisu dopuštenih uređaja, pošalje bilo kakav zahtjev za podatke.
SendITSID (SID 02)
Poruku šalje sučelje jedinice u vozilu svaki put kada novi uređaj pošalje zahtjev. Taj uređaj upotrebljava standardni identifikator „A0" prije no što mu se dodijeli jedinstveni identifikator za buduću komunikacijsku razmjenu podataka.
SendPIN (SID 03)
Poruku šalje ITS jedinica koju sučelje jedinice u vozilu treba uvrstiti na popis dopuštenih uređaja. Sadržaj je poruke kod od četiri cijela broja (4 INTEGER) između nula i devet.
PairingResult (SID 04)
Poruku šalje sučelje jedinice u vozilu kako bi obavještenjeilo ITS jedinicu da je PIN lozinka koju je poslala tačna. Sadržaj je poruke Booleov izraz s vrijednošću „tačno" („True") ako je PIN lozinka bila tačna ili „netačno" („False") ako je PIN lozinka bila netačna.
SendPUC (SID 05)

Poruku šalje ITS jedinica kako bi se sučelje jedinice u vozilu uklonilo s popisa zabranjenih uređaja. Sadržaj je poruke kod od četiri cijela broja (8 INTEGER) između nula i devet.

BanLiftingResult (SID 06)

Poruku šalje sučelje jedinice u vozilu kako bi obavještenjeilo ITS jedinicu da je PUC lozinka koju je poslala tačna. Sadržaj je poruke Booleov izraz s vrijednošću „tačno" („True") ako je PUC lozinka bila tačna ili „netačno" („False") ako je PUC lozinka bila netačna.

RequestRejected (SID 07)

Poruku šalje sučelje jedinice u vozilu kao odgovor na bilo koju poruku koju je poslala ITS jedinica uvrštena na popis zabranjenih uređaja osim poruke „SendPUC". Poruka sadrži preostalo vrijeme tokom kojeg je ITS jedinica uvrštena na popis zabranjenih uređaja u skladu s formatom slijeda „Time" kako je utvrđeno u Prilogu 3.

RequestData (SID 08)

Poruku za pristup podacima šalje ITS jedinica. Parametrom zahtjeva za prenos od jednog bajta (TRTP) označena je vrsta traženih podataka. Nekoliko je vrsta podataka:

— standardTachData (TRTP 01): podaci dostupni iz tahografa koji su klasificirani kao nelični,
— personalTachData (TRTP 02): podaci dostupni iz tahografa koji su klasificirani kao lični,
— gnssData (TRTP 03): podaci GNSS-a, koji su uvijek lični,
— standardEventData (TRTP 04): zabilježeni podaci o događaju koji su klasificirani kao nelični,
— personalEventData (TRTP 05): zabilježeni podaci o događaju koji su klasificirani kao lični,
— standardFaultData (TRTP 06): zabilježeni kvarovi koji su klasificirani kao nelični,
— manufacturerData (TRTP 07): podaci koje je na raspolaganje stavio proizvođač.

Vidjeti Prilog 3. ovom Dodatku za više informacija o sadržaju svake vrste podataka.
Vidjeti Dodatak 12. za više informacija o formatu i sadržaju podataka GNSS-a.
Vidjeti priloge I.B i I.C za više informacija o kodu podataka o događaju i o kvarovima.

ResquestAccepted (SID 09)

Poruku šalje sučelje jedinice u vozilu ako je prihvatilo poruku „RequestData" ITS jedinice. Poruka sadrži TREP od jednog bajta, koji je TRTP bajt povezane poruke „RequestData", i sve podatke zatražene vrste.

DataUnavailable (SID 0A)

Poruku šalje sučelje jedinice u vozilu ako iz nekog razloga zatraženi podaci nisu dostupni za slanje ITS jedinici s popisa dopuštenih uređaja. Poruka sadrži TREP od jednog bajta, koji je TRTP zatraženih podataka, i kod greške od jednog bajta kako je navedeno u tablici 3. Dostupni su sljedeći kodovi:

— Podaci nisu dostupni (10): Sučelje jedinice u vozilu ne može pristupiti podacima jedinice u vozilu iz neutvrđenih razloga.
— Lični se podaci ne dijele (11): ITS jedinica pokušava učitati osobne podatke ako se oni ne dijele.

NegativeAnswer (SID 0B)

Poruke šalje sučelje jedinice u vozilu ako zahtjev ne može biti ispunjen iz bilo kojeg drugog razloga osim nedostupnosti podataka. Poruke su obično posljedica nepravilnog formata zahtjeva (dužina, SID, ITSID…), ali razlozi nisu ograničeni na to. TRTP u podatkovnom polju sadrži SID zahtjeva. Podatkovno polje sadrži kod na temelju kojeg se utvrđuje razlog negativnog odgovora. Dostupni su sljedeći kodovi:

— Opšte odbijanje (kôd 10)
— Radnja se ne može provesti zbog razloga koji nije naveden u nastavu ili u odjeljku (unos broja odjeljka *DataUnavailable*).
— Usluga nije podržana (kôd 11)
— Nerazumljiv SID zahtjeva.
— Podfunkcija nije podržana (kôd 12)
— Nerazumljiv TRTP zahtjeva. To, na primjer, može biti vrijednost koja nedostaje ili neprihvatljiva vrijednost.
— Nepravilna dužina poruke (kôd 13)
— Dužina primljene poruke pogrešna je (neusklađenost LEN bajta i stvarne dužine poruke).
— Nepravilni uslovi ili greška u slijedu zahtjeva (kôd 22)
— Zatražena usluga nije aktivna ili slijed poruka zahtjeva nije točan.
— Zahtjev izvan dometa (kôd 33)
— Zapis parametra zahtjeva (podatkovno polje) nije važeći.
— Čeka se odgovor (kôd 78)
— Zatražena se radnja ne može provesti na vrijeme i jedinica u vozilu nije spremna prihvatiti drugi zahtjev.
— Neusklađenost ITSID-a (kôd FB)
— SRC *ITSID* nije usklađen s povezanim uređajem nakon usporedbe s Bluetooth informacijama.
— Nije pronađen *ITSID* (kôd FC)
— SRC *ITSID* nije povezan ni s jednim uređajem.

U redcima od 1. do 72. (**FormatMessageModule**) ASN.1 koda u Prilogu 3. utvrđen je format poruka kako je opisano u tablici 3. Više pojedinosti o sadržaju poruka navedeno je u nastavu.

4.5. Saglasnost vozača

Svi dostupni podaci klasificirani su kao standardni ili kao lični. Lični su podaci dostupni samo ako je vozač dao saglasnost i prihvatio da se njegovi lični podaci iz tahografa mogu prenositi izvan mreže vozila aplikacijama trećih strana.

Vozač saglasnost daje pri prvom umetanju određene kartice vozača ili kartice radionice koja je trenutačno nepoznata jedinici u vozilu; nosioca kartice poziva se da dâ svoju saglasnost za prenos ličnih podataka iz tahografa preko neobveznog ITS sučelja. (Vidjeti i Prilog I.C stavak 3.6.2.).

Stanje saglasnosti (omogućeno/onemogućeno) bilježi se u memoriji tahografa.

U slučaju više vozača, s ITS sučeljem dijele se samo lični podaci vozača koji su dali svoju saglasnost. Na primjer, ako su u vozilu dva vozača i ako je samo prvi vozač pristao dijeliti svoje osobne podatke, podaci koji se odnose na drugog vozača ne dijele se.

4.6. Učitavanje standardnih podataka

Na slici 3. u Prilogu 2. prikazani su dijagrami slijeda za važeći zahtjev za pristup standardnim podacima koji je poslala ITS jedinica. Ako je ITS jedinica pravilno uvrštena na popis dopuštenih uređaja i ne traži osobne podatke, dodatna provjera nije potrebna. U dijagramima se smatra da se poštovao pravilan postupak prikazan na slici 2. u Prilogu 2. Dijagrami mogu biti izjednačeni sa sivim poljem *REQUEST TREATMENT* na slici 2.

Od dostupnih se podataka standardnima smatraju sljedeći:

— standardTachData (TRTP 01),

— StandardEventData (TRTP 04),

— standardFaultData (TRTP 06).

4.7. Učitavanje ličnih podataka

Na slici 4. u Prilogu 2. prikazan je dijagram slijeda za obradu zahtjeva za osobne podatke. Kako je ranije navedeno, sučelje jedinice u vozilu šalje osobne podatke samo ako je vozač dao izričitu saglasnost (vidjeti i 4.5.). U suprotnom zahtjev se mora automatski odbiti.

Od dostupnih se podataka ličnima smatraju sljedeći:

— personalTachData (TRTP 02),

— gnssData (TRTP 03),

— personalEventData (TRTP 05),

— manufacturerData (TRTP 07).

4.8. Učitavanje podataka o događajima i kvarovima

ITS jedinice moraju moći zatražiti podatke o događajima koji sadržiju popis svih neočekivanih događaja. Ti se podaci smatraju standardnima ili ličnima; vidjeti Prilog 3. Sadržaj svakog događaja u skladu je s dokumentacijom iz Priloga 1. ovom Dodatku.

PRILOG 1.

1) POPIS PODATAKA DOSTUPNIH PREKO ITS SUČELJA

Podaci	**Izvor**	**Preporučena klasifikacija (lični/nelični)**
VehicleIdentificationNumber	Jedinica u vozilu	**nelični**
CalibrationDate	Jedinica u vozilu	**nelični**
TachographVehicleSpeed speed instant t	Jedinica u vozilu	lični
Driver1WorkingState Selector driver	Jedinica u vozilu	lični
Driver2WorkingState	Jedinica u vozilu	lični
DriveRecognize Speed Threshold detected	Jedinica u vozilu	**nelični**
Driver1TimeRelatedStates Weekly day time	Kartica vozača	lični
Driver2TimeRelatedStates	Kartica vozača	lični
DriverCardDriver1	Jedinica u vozilu	**nelični**
DriverCardDriver2	Jedinica u vozilu	**nelični**
OverSpeed	Jedinica u vozilu	lični
TimeDate	Jedinica u vozilu	**nelični**
HighResolutionTotalVehicleDistance	Jedinica u vozilu	**nelični**
ServiceComponentIdentification	Jedinica u vozilu	**nelični**
ServiceDelayCalendarTimeBased	Jedinica u vozilu	**nelični**
Driver1Identification	Kartica vozača	lični
Driver2Identification	Kartica vozača	lični
NextCalibrationDate	Jedinica u vozilu	**nelični**
Driver1ContinuousDrivingTime	Kartica vozača	lični
Driver2ContinuousDrivingTime	Kartica vozača	lični
Driver1CumulativeBreakTime	Kartica vozača	lični
Driver2CumulativeBreakTime	Kartica vozača	lični
Driver1CurrentDurationOfSelectedActivity	Kartica vozača	lični
Driver2CurrentDurationOfSelectedActivity	Kartica vozača	lični
SpeedAuthorised	Jedinica u vozilu	**nelični**
TachographCardSlot1	Kartica vozača	**nelični**
TachographCardSlot2	Kartica vozača	**nelični**
Driver1Name	Kartica vozača	lični
Driver2Name	Kartica vozača	lični
OutOfScopeCondition	Jedinica u vozilu	**nelični**
ModeOfOperation	Jedinica u vozilu	**nelični**
Driver1CumulatedDrivingTimePreviousAndCurrentWeek	Kartica vozača	lični
Driver2CumulatedDrivingTimePreviousAndCurrentWeek	Kartica vozača	lični
EngineSpeed	Jedinica u vozilu	lični
RegisteringMemberState	Jedinica u vozilu	**nelični**
VehicleRegistrationNumber	Jedinica u vozilu	**nelični**
Driver1EndOfLastDailyRestPeriod	Kartica vozača	lični
Driver2EndOfLastDailyRestPeriod	Kartica vozača	lični
Driver1EndOfLastWeeklyRestPeriod	Kartica vozača	lični

Driver2EndOfLastWeeklyRestPeriod	Kartica vozača	lični
Driver1EndOfSecondLastWeeklyRestPeriod	Kartica vozača	lični
Driver2EndOfSecondLastWeeklyRestPeriod	Kartica vozača	lični
Driver1CurrentDailyDrivingTime	Kartica vozača	lični
Driver2CurrentDailyDrivingTime	Kartica vozača	lični
Driver1CurrentWeeklyDrivingTime	Kartica vozača	lični
Driver2CurrentWeeklyDrivingTime	Kartica vozača	lični
Driver1TimeLeftUntilNewDailyRestPeriod	Kartica vozača	lični
Driver2TimeLeftUntilNewDailyRestPeriod	Kartica vozača	lični
Driver1CardExpiryDate	Kartica vozača	lični
Driver2CardExpiryDate	Kartica vozača	lični
Driver1CardNextMandatoryDownloadDate	Kartica vozača	lični
Driver2CardNextMandatoryDownloadDate	Kartica vozača	lični
TachographNextMandatoryDownloadDate	Jedinica u vozilu	**nelični**
Driver1TimeLeftUntilNewWeeklyRestPeriod	Kartica vozača	lični
Driver2TimeLeftUntilNewWeeklyRestPeriod	Kartica vozača	lični
Driver1NumberOfTimes9hDailyDrivingTimesExceeded	Kartica vozača	lični
Driver2NumberOfTimes9hDailyDrivingTimesExceeced	Kartica vozača	lični
Driver1CumulativeUninterruptedRestTime	Kartica vozača	lični
Driver2CumulativeUninterruptedRestTime	Kartica vozača	lični
Driver1MinimumDailyRest	Kartica vozača	lični
Driver2MinimumDailyRest	Kartica vozača	lični
Driver1MinimumWeeklyRest	Kartica vozača	lični
Driver2MinimumWeeklyRest	Kartica vozača	lični
Driver1MaximumDailyPeriod	Kartica vozača	lični
Driver2MaximumDailyPeriod	Kartica vozača	lični
Driver1MaximumDailyDrivingTime	Kartica vozača	lični
Driver2MaximumDailyDrivingTime	Kartica vozača	lični
Driver1NumberOfUsedReducedDailyRestPeriods	Kartica vozača	lični
Driver2NumberOfUsedReducedDailyRestPeriods	Kartica vozača	lični
Driver1RemainingCurrentDrivingTime	Kartica vozača	lični
Driver2RemainingCurrentDrivingTime	Kartica vozača	lični
GNSS position	Jedinica u vozilu	lični

2) KONTINUIRANI PODACI GNSS-A DOSTUPNI NAKON SAGLASNOSTI VOZAČA

Vidjeti Dodatak 12. – GNSS.

3) KODOVI DOGAĐAJA DOSTUPNI BEZ SAGLASNOSTI VOZAČA

Događaj	**Pravila arhiviranje**	**Podaci koje je potrebno bilježiti po događaju**
Umetanje nevažeće kartice	— deset najnovijih događaja.	— datum i vrijeme događaja, — vrstu i broj kartice, državu članicu koja je izdala karticu i generaciju kartice kojom je stvoren događaj, — broj sličnih događaja tog dana.
Konflikt kartica	— deset najnovijih događaja.	— datum i vrijeme početka događaja, — datum i vrijeme završetka događaja, — vrstu i broj kartice, državu članicu koja je izdala karticu i generaciju dviju kartica zbog kojih je nastao sukob.
Posljednja razmjena podataka s karticom koja nije ispravno zatvorena	— deset najnovijih događaja.	— datum i vrijeme umetanja kartice, — vrstu i broj kartice, državu članicu koje je izdala karticu i generaciju kartice, — posljednju razmjenu podataka očitanih s kartice: — datum i vrijeme umetanja kartice, — VRN, državu članicu registracije i generaciju jedinice u vozilu.
Prekid napajanja (2)	— najduži događaj za svaki od deset posljednjih dana pojave, — pet najdužih događaja u posljednjih 365 dana.	— datum i vrijeme početka događaja, — datum i vrijeme završetka događaja, — vrstu i broj kartice, državu članicu koja je izdala karticu i generaciju bilo koje kartice umetnute na početku i/ili završetku događaja, — broj sličnih događaja tog dana.
Greška u komunikaciji s uređajem za komunikaciju na daljinu	— najduži događaj za svaki od deset posljednjih dana pojave, — pet najdužih događaja u posljednjih 365 dana.	— datum i vrijeme početka događaja, — datum i vrijeme završetka događaja, — vrstu i broj kartice, državu članicu koja je izdala karticu i generaciju bilo koje kartice umetnute na početku i/ili završetku događaja, — broj sličnih događaja tog dana.
Izostanak podataka o položaju iz prijamnika GNSS-a	— najduži događaj za svaki od deset posljednjih dana pojave, — pet najdužih događaja u posljednjih 365 dana.	— datum i vrijeme početka događaja, — datum i vrijeme završetka događaja, — vrstu i broj kartice, državu članicu koja je izdala karticu i generaciju bilo koje kartice umetnute na početku i/ili završetku događaja, — broj sličnih događaja tog dana.
Greška u komunikaciji s vanjskim uređajem GNSS-a	— najduži događaj za svaki od deset posljednjih dana pojave, — pet najdužih događaja u	— datum i vrijeme početka događaja, — datum i vrijeme završetka događaja, — vrstu, broj, državu članicu koja je izdala karticu i

	zadnjih 365 dana	generaciju bilo koje kartice umetnute na početku i/ili završetku događaja, — broj sličnih događaja tog dana.
Greška u podacima o kretanju	— najduži događaj za svaki od deset posljednjih dana pojave, — pet najdužih događaja u posljednjih 365 dana.	— datum i vrijeme početka događaja, — datum i vrijeme završetka događaja, — vrstu i broj kartice, državu članicu koja je izdala karticu i generaciju bilo koje kartice umetnute na početku i/ili završetku događaja, — broj sličnih događaja tog dana.
Konflikt u kretanju vozila	— najduži događaj za svaki od deset posljednjih dana pojave, — pet najdužih događaja u posljednjih 365 dana.	— datum i vrijeme početka događaja, — datum i vrijeme završetka događaja, — vrstu i broj kartice, državu članicu koja je izdala karticu i generaciju bilo koje kartice umetnute na početku i/ili završetku događaja, — broj sličnih događaja tog dana.
Pokušaji povrede sigurnosti	deset najnovijih događaja po vrsti događaja.	— datum i vrijeme početka događaja, — datum i vrijeme završetka događaja (ako je relevantno), — vrstu i broj kartice, državu članicu koja je izdala karticu i generaciju bilo koje kartice umetnute na početku i/ili završetku događaja, — vrstu događaja.
Vremenski konflikt	— najduži događaj za svaki od deset posljednjih dana pojave, — pet najdužih događaja u posljednjih 365 dana.	— datum i vrijeme iz uređaja za bilježenje podataka, — datum i vrijeme GNSS-a, — vrstu i broj kartice, državu članicu koja je izdala karticu i generaciju bilo koje kartice umetnute na početku i/ili završetku događaja, — broj sličnih događaja tog dana.

4) KODOVI DOGAĐAJA DOSTUPNI UZ SAGLASNOST VOZAČA

Događaj	Pravila arhiviranje	Podaci koje je potrebno bilježiti po događaju
Vožnja bez odgovarajuće kartice	— najduži događaj za svaki od deset posljednjih dana pojave, — pet najdužih događaja u posljednjih 365 dana.	— datum i vrijeme početka događaja, — datum i vrijeme završetka događaja, — vrstu i broj kartice, državu članicu koja je izdala karticu i generaciju bilo koje kartice umetnute na početku i/ili završetku događaja, — broj sličnih događaja tog dana.
Umetanje kartice tokom vožnje	— posljednji događaj za svaki od deset posljednjih dana pojave,	— datum i vrijeme događaja, — vrstu i broj kartice, državu članicu koje je izdala karticu i generaciju kartice, — broj sličnih događaja tog dana.
Prekoračenje brzine (1)	— najozbiljniji događaj za svaki od deset posljednjih dana pojave (tj. događaj s najvećom prosječnom brzinom), — pet najozbiljnijih događaja u posljednjih 365 dana. — prvi događaj koji se dogodio nakon posljednje kalibracije.	— datum i vrijeme početka događaja, — datum i vrijeme završetka događaja, — najveću brzinu izmjerenu tokom događaja, — aritmetički prosjek brzine izmjerene tokom događaja, — vrstu i broj kartice, državu članicu koja je izdala karticu i generaciju kartice vozača (ako je primjereno), — broj sličnih događaja tog dana.

5) KODOVI ZA PODATKE O KVARU DOSTUPNI BEZ SAGLASNOSTI VOZAČA

Kvar	Pravila arhiviranje	Podaci koje je potrebno bilježiti po kvaru
Kvar kartice	— deset najnovijih kvarova kartice vozača.	— datum i vrijeme početka kvara, — datum i vrijeme završetka kvara, — vrstu i broj kartice, državu članicu koja je izdala karticu i generaciju kartice.
Kvar uređaja za bilježenje podataka	— deset najnovijih kvarova po vrsti kvara, — prvi kvar koji se dogodio nakon posljednje kalibracije.	— datum i vrijeme početka kvara, — datum i vrijeme završetka kvara, — vrstu kvara, — vrstu i broj kartice, državu članicu koja je izdala karticu i generaciju bilo koje kartice umetnute na početku i/ili završetku kvara.

Taj se kvar aktivira za neku od sljedećih grešaka dok nije u kalibracijskom načinu:
— unutarnji kvar jedinice u vozilu,
— kvar pisača,
— kvar zaslona,
— kvar pri preuzimanju podataka,
— kvar senzora,
— kvar prijamnika GNSS-a ili vanjskog uređaja GNSS-a,
— kvar uređaja za komunikaciju na daljinu,
— kvar povezan s ITS sučeljem (ako je primjenjivo).

6) DOGAĐAJI I KVAROVI SPECIFIČNI ZA PROIZVOĐAČA BEZ SAGLASNOSTI VOZAČA

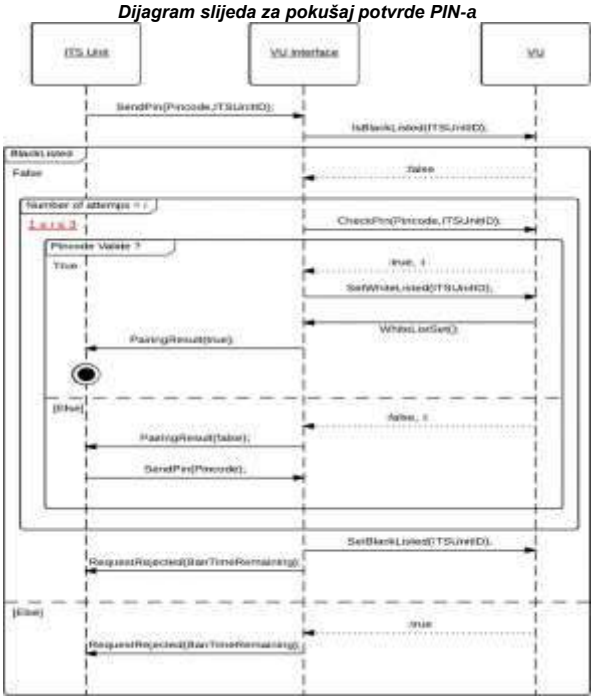
Događaj ili kvar	Pravila arhiviranje	Podaci koje je potrebno bilježiti po događaju
Utvrđuje proizvođač.	Utvrđuje proizvođač.	Utvrđuje proizvođač.

PRILOG 2.

DIJAGRAMI SLIJEDA RAZMJENA PORUKA S ITS JEDINICOM

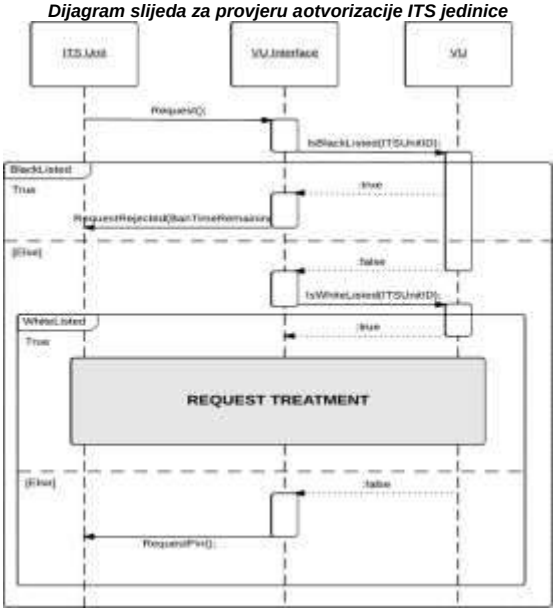
Slika 1

Dijagram slijeda za pokušaj potvrde PIN-a



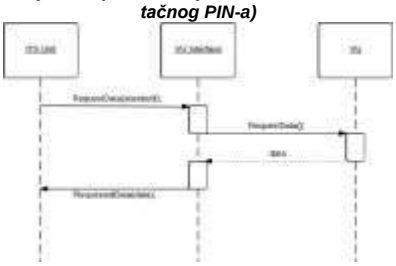
Slika 2

Dijagram slijeda za provjeru aotvorizacije ITS jedinice



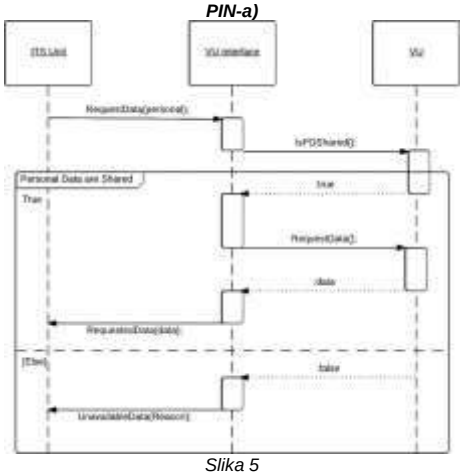
Slika 3

Dijagram slijeda za obradu zahtjeva za podatke koji su klasificirani kao nelični (pristup nakon unosa tačnog PIN-a)



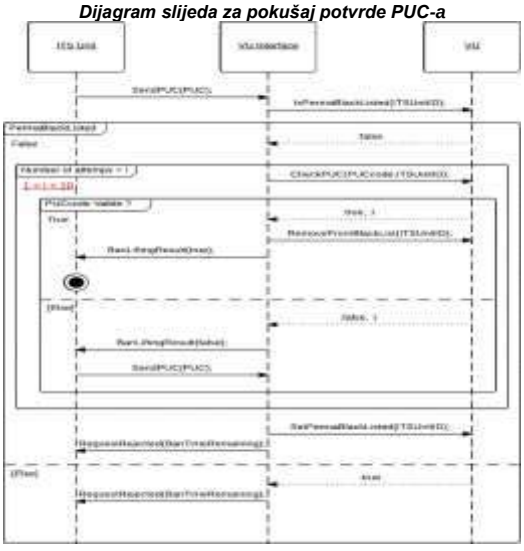
Slika 4

Dijagram slijeda za obradu zahtjeva za podatke koji su klasificirani kao lični (pristup nakon unosa tačnog PIN-a)



Slika 5

Dijagram slijeda za pokušaj potvrde PUC-a



PRILOG 3.

ASN.1 – SPECIFIKACIJE

```
FormatMessageModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
EXPORTS ;
IMPORTS SendPIN, SendPUC, PairingResult, RequestPIN, RequestRejected,
        BanLiftingResult FROM PINPUCDataFieldsModule
        RequestAccepted,RequestData, DataUnavailable FROM
        RequestDataFieldsModule
        SendITSID, NegativeAnswer FROM OtherDataFieldsModule;

        CompleteMessage ::=SEQUENCE{
              header Header,
              data DataField,
              checksum Checksum
        }

        ----------------
        --HEADER TYPES--
        ----------------


        Header::=SEQUENCE{
              tgt IDList,
              src IDList,
              len BIT STRING (1..255)
        }

        vuID BIT STRING ::= 'EE'H
        IDList ::=CHOICE{
              vu BIT STRING (vuID),
              itsUnits SEQUENCE OF BIT STRING,
                    --Default hex Value:A0, redefined after first message exchange--
                    --Each ID will be linked to the Bluetooth ID of the device--
              ...
        }

        --------------------
        --DATAFIELDS TYPES--
        --------------------
        DataField ::=SEQUENCE{
              sId BIT STRING,
              trtp BIT STRING,
              subMBytes SubMessageBytes,
              dataField Content,
              ...
        }

        SubMessageBytes ::= SEQUENCE{
              currentSubM BIT STRING,
              totalSubM BIT STRING
        }

        Content ::= CHOICE{
              requestPIN RequestPIN,
              sendITSID SendITSID,
              sendPin SendPIN,
             pairRslt PairingResult,
             sendPUC SendPUC,
             banlift BanLiftingResult,
             requestRejected RequestRejected,
             requestData RequestData,
             requestOK RequestAccepted,
             dataUnavailable DataUnavailable,
             negAns NegativeAnswer
        }

        ----------------
        --CHECKSUM TYPES--
        ----------------

        Checksum ::= SEQUENCE{
              --SHA2 checksum
        }
END

```

```
PINPUCDataFieldsModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
EXPORTS SendPIN, SendPUC, PairingResult, RequestPIN, RequestRejected,
BanLiftingResult;
IMPORTS ;

      ----------
      ---Utils--
      ----------

      PUC ::= SEQUENCE (SIZE(8)) OF
      INTEGER (SIZE(0..9))

      PIN ::=      SEQUENCE (SIZE(4)) OF
            INTEGER (SIZE(0..9))

      --------------------------
      --Messages From ITS Unit--
      --------------------------

      SendPIN {PIN:pin} ::= SEQUENCE {
            sid BIT STRING ('03'H),
            pin PIN (pin)
      }

      SendPUC {PUC:puc} ::= SEQUENCE {
            sid BIT STRING ('05'H),
            puc PUC (puc)
      }
      --------------------
      --Messages From VU--
      --------------------

      PairingResult ::= SEQUENCE{
            sid BIT STRING ('04'H),
            result BOOLEAN
      }

      RequestPIN {MType:receivedRequest}::= SEQUENCE{
            sid BIT STRING ('01'H)
      }

      RequestRejected ::= SEQUENCE{
            sid BIT STRING ('07'H),
            banTimeRemaining GeneralizedTime, --PermaBan == 1k years-- }

      BanLiftingResult ::= SEQUENCE{
            sid BIT STRING ('06'H),
            result BOOLEAN
      }
END
```

```
RequestDataFields DEFINITIONS AUTOMATIC TAGS ::= BEGIN
	EXPORTS RequestAccepted,RequestData, DataUnavailable ;
	IMPORTS StandardEvent, PersonalEvent, StandardFault FROM EventsModule;

	------------------
	---From ITS Unit--
	------------------
	RequestData ::= SEQUENCE{
		sid BIT STRING ('08'H),
		requestedData DataTypeCode,
		...
	}

	-----------
	--From VU--
	-----------
	RequestAccepted ::=SEQUENCE{
		sid BIT STRING ('09'H),
		trtp DataTypeCode,
		dataSheet CHOICE{
			standardData StandardTachDataContent,
			personalData PersonalTachDataContent,
			gnss GNSSDataContent,
			standardEvent StandardEventContent,
			personalEvent PersonalEventContent,
			standardFault StandardFaultContent,
			manufacturerdata ManufacturerDataContent,
			...
		}
	}

	DataTypeCode ::=CHOICE{
		standardTachData BIT STRING ('01'H),
		personalTachData BIT STRING ('02'H),
		gnssData BIT STRING ('03'H),
		standardEventData BIT STRING ('04'H),
		personalEventData BIT STRING ('05'H),
		standardFaultData BIT STRING ('06'H),
		manufacturerData BIT STRING ('07'H),
		...
	}

	DataUnavailable ::=SEQUENCE{
		sid BIT STRING ('0A'H),
		trtp DataTypeCode,
		reason UnavailableDataCodes
	}

	UnavailableDataCodes ::= CHOICE{
		noDataAvailable BIT STRING ('10'H),
		personalDataNotShared BIT STRING ('11'H),
		...
	}
	---------------------------
	--Complete Tachograph Data--
	---------------------------
	--The format of the data was taken from the ISO16844-7 norm, more information
available in this ISO document-
```

```
Time ::= SEQUENCE{
	seconds INTEGER (0..59.75), --increment: 0.25s--
	minutes INTEGER (0..59), --increment: 1min--
	hours INTEGER (0..23), --increment: 1h--
	day INTEGER (0.25.. 31.75), --increment: 0.25d--
	month INTEGER (1..12), --increment: 1month--
	year INTEGER (1985..2235), --increment: 1year--
	locMinOffset INTEGER (-59..59), --increment: 1min--
	locHouroffset INTEGER (-23..23)--increment: 1h--
}

Date ::= SEQUENCE{
	month INTEGER (1..12), --increment: 1month--
	day INTEGER (0.25.. 31.75), --increment: 0.25d--
	year INTEGER (1985..2235) --increment: 1year--
}

DriverName ::=SEQUENCE{
	codePageSurname UTF8String, --See ISO/IEC 8859--
	surname UTF8String,
	codePageFirstname UTF8String, --See ISO/IEC 8859--
	firstname UTF8String,
}

DriverID ::= SEQUENCE{
issuingMemberState OCTET STRING (SIZE(3)),
cardNumber OCTET STRING (SIZE(16))
}

--------------------
--Message Content--
--------------------

StandardTachDataContent ::= SEQUENCE{
	trtp DataTypeCode (DataTypeCode.&standardTachData),
	personal BOOLEAN (FALSE),
	data StandardTachyDataSheet,
}

PersonalTachDataContent ::= SEQUENCE{
	trtp DataTypeCode (DataTypeCode.&personalTachData),
	personal BOOLEAN (TRUE),
	data PersonalTachyDataSheet
}

GNSSDataContent ::= SEQUENCE{
	trtp DataTypeCode (DataTypeCode.&gnssData),
	personal BOOLEAN (TRUE),
	data GNSSDataSheet
}

StandardEventContent ::= SEQUENCE{
	trtp DataTypeCode (DataTypeCode.&standardEventData),
	personal BOOLEAN (FALSE),
	data StandardEventDataSheet
}

PersonalEventContent ::= SEQUENCE{
	trtp DataTypeCode (DataTypeCode.&personalEventData),
	personal BOOLEAN (TRUE),
	data PersonalEventDataSheet
}

StandardFaultContent ::= SEQUENCE{
```

```
243                 trtp DataTypeCode (DataTypeCode.&standardFaultDat
244                 personal BOOLEAN (FALSE),
245                 data StandardFault
246         }
247
248         ManufacturerDataContent ::= SEQUENCE{
249                 trtp DataTypeCode (DataTypeCode.&manufacturerDat
250                 personal BOOLEAN (TRUE),
251                 ...
252         }
253
254         ---------------
255         --DATA SHEETS--
256         ---------------
257
258         --Data sheet format follows ISO 16844-7.--
259         StandardTachyDataSheet ::= SEQUENCE{
260                 vin UTF8String (SIZE(17)),
261                 calibrationDate Date,
262   driveRecognize BIT STRING ('00'B UNION '01'B),
263   driverCardDriver1 BIT STRING ('00'B UNION '01'B),
264   driverCardDriver2 BIT STRING ('00'B UNION '01'B),
265                 timeDate Time,
266                 highResolutionTotalVehicleDistance INTEGER (0..21055406), --increment:
267   5m--
268                 serviceComponentIdentification INTEGER (0..255),
269                 serviceDelayCalendarTimeBased INTEGER (-125..125), --increment: 1week-
270   -
271                 nextCalibrationDate Date,
272                 speedAuthorised INTEGER (0..250.996), --increment 1/256km/h--
273                 tachographCardSlot1 INTEGER (0..4...), --Maximum 250--
274                 tachographCardSlot2 INTEGER (0..4...), --Maximum 250--
275   outOfScopeCondition BIT STRING ('00'B UNION '01'B),
276                 modeOfOperation INTEGER (0..4...), --Maximum 250--
277                 registeringMemberState UTF8String,
278         vehicleRegistrationNumber SEQUENCE {
279                         codePageVRN INTEGER (0..255),
280                         vrn OCTET STRING (SIZE(13)),
281                 },
282                 tachographNextMandatoryDownloadDate Date,
283                 ...
284         }
285
286         PersonalTachyDataSheet ::= SEQUENCE{
287                 tachographVehicleSpeed INTEGER (0..250.996), --increment 1/256km/h--
288   driver1WorkingState BIT STRING ('000'B UNION '001'B UNION '010'B UNIO
289   '011'B UNION '100'B UNION '101'B …),
290   driver2WorkingState BIT STRING ('000'B UNION '001'B UNION '010'B UNIO
291   '011'B UNION '100'B UNION '101'B …),
292
293   driver1TimeRelatedStates BIT STRING ('0000'B UNION '0001'B
294   UNION '0010'B UNION '0011'B UNION '0100'B UNION '0101'B UNION
295   '0110'B UNION '0111'B UNION '1000'B UNION '1001'B UNION '1010'B
296   UNION '1011'B UNION '1100'B UNION '1101'B …),
297
298
299   driver2TimeRelatedStates BIT STRING ('0000'B UNION '0001'B
300   UNION '0010'B UNION '0011'B UNION '0100'B UNION '0101'B UNION
```

```
    '0110'B UNION '0111'B UNION '1000'B UNION '1001'B UNION '1010'B
    UNION '1011'B UNION '1100'B UNION '1101'B …),



    overSpeed BIT STRING ('00 'B UNION '01 'B),
    driver1Identification DriverID,
    driver2Identification DriverID,


                driver1ContinuousDrivingTime INTEGER (0.. 64255), --increment: 1min--
                driver2ContinuousDrivingTime INTEGER (0.. 64255), --increment: 1min--
                driver1CurrentDurationOfSelectedActivity INTEGER (0.. 64255), --
    increment: 1min--
                driver2CurrentDurationOfSelectedActivity INTEGER (0.. 64255), --
    increment: 1min--
                driver1Name DriverName,
                driver2Name DriverName,
                driver1CumulatedDrivingTimePreviousAndCurrentWeek INTEGER (0.. 64255),
    --increment: 1min--
                driver2CumulatedDrivingTimePreviousAndCurrentWeek INTEGER (0.. 64255),
    --increment: 1min--
                engineSpeed INTEGER(0..8031.875), --increment: 0,125r/min--
                driver1EndOfLastDailyRestPeriod Time,
                driver2EndOfLastDailyRestPeriod Time,
                driver1EndOfLastWeeklyRestPeriod Time,
                driver2EndOfLastWeeklyRestPeriod Time,
                driver1EndOfSecondLastWeeklyRestPeriod Time,
                driver2EndOfSecondLastWeeklyRestPeriod Time,
                driver1CurrentDailyDrivingTime INTEGER (0.. 64255), --increment: 1min-
    -
                driver2CurrentDailyDrivingTime INTEGER (0.. 64255), --increment: 1min-
    -
                driver1CurrentWeeklyDrivingTime INTEGER (0.. 64255), --increment:
    1min--
                driver2CurrentWeeklyDrivingTime INTEGER (0.. 64255), --increment:
    1min--
                driver1TimeLeftUntilNewDailyRestPeriod INTEGER (0.. 64255), --
    increment: 1min--
                driver2TimeLeftUntilNewDailyRestPeriod INTEGER (0.. 64255), --
    increment: 1min--
                driver1CardExpiryDate Date,
                driver2CardExpiryDate Date,
                driver1CardNextMandatoryDownloadDate Date,
                driver2CardNextMandatoryDownloadDate Date,
                driver1TimeLeftUntilNewWeeklyRestPeriod INTEGER (0.. 64255), --
    increment: 1min--
                driver2TimeLeftUntilNewWeeklyRestPeriod INTEGER (0.. 64255), --
    increment: 1min--
                driver1NumberOfTimes9hDailyDrivingTimesExceeded INTEGER (0..13),
                driver2NumberOfTimes9hDailyDrivingTimesExceeced INTEGER (0..13),
                driver1CumulativeUninterruptedRestTime INTEGER (0.. 64255), --
    increment: 1min--
                driver2CumulativeUninterruptedRestTime INTEGER (0.. 64255), --
    increment: 1min--
                driver1MinimumDailyRest INTEGER (0.. 64255), --increment: 1min--
                driver2MinimumDailyRest INTEGER (0.. 64255), --increment: 1min--
                driver1MinimumWeeklyRest INTEGER (0.. 64255), --increment: 1min--
                driver2MinimumWeeklyRest INTEGER (0.. 64255), --increment: 1min--
```

```
360                 driver1MaximumDailyPeriod INTEGER (0..250), --increment: 1h--
361                 driver2MaximumDailyPeriod INTEGER (0..250), --increment: 1h--
362   driver1MaximumDailyDrivingTime BIT STRING (SIZE(4)),
363   driver2MaximumDailyDrivingTime BIT STRING (SIZE(4)),
364                 driver1NumberOfUsedReducedDailyRestPeriods INTEGER (0..13),
365                 driver2NumberOfUsedReducedDailyRestPeriods INTEGER (0..13),
366                 driver1RemainingCurrentDrivingTime INTEGER (0.. 64255), --increment:
367   1min--
368                 driver2RemainingCurrentDrivingTime INTEGER (0.. 64255), --increment:
369   1min--
370                 ...
371           }
372
373           GNSSDataSheet ::=  SEQUENCE {
374           gnssPosition GeoCoordinates
375                 --See Appendix 1 for definition of GeoCoordinates--
376           }
377
378           StandardEventDataSheet ::= SEQUENCE{
379                 events SEQUENCE OF StandardEvent
380           }
381
382           PersonalEventDataSheet ::= SEQUENCE{
383                 events SEQUENCE OF PersonalEvent
384           }
385   END
386
387   EventsModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
388           EXPORTS ALL;
389           IMPORTS NationAlpha FROM Appendix1; --See Appendix 1 for more information
390   about NationAlpha--
391
392                 SecurityBreachEvent ::=SEQUENCE{
393                       --See Annex 1B for more information--
394                 }
395
396                 RecordingEquipmentFaultType ::= SEQUENCE{
397                       --See Annex 1B for more information--
398                 }
399
400                 StandardEvent::= CHOICE{
401                       insertionInvalidCard InsertionOfANonValidCard,
402                       cardConflict CardConflict,
403                       timeOverlap TimeOverlap,
404                       previousSessionNotClosed LastCardSessionNotCorrectlyClosed,
405                       overSpeeding OverSpeeding,
406                       powerSupplyInterruption PowerSupplyInterruption,
407                       comErrorWithRemoteFacility
408   CommunicationErrorWithTheRemoteCommunicationFacility,
409                       absenceGNSSPosition
410   AbsenceOfPositionInformationFromGNSSReceiver,
410a  comErrorWithExternalGNSSFacility
410b  CommunicationErrorWithTheExternalGNSSFacility,
411                       positionDataError PositionDataError,
412                       motionDataError MotionDataError,
413                       vehicleMotionConflict VehicleMotionConflict,
414                       securityBreachAttempt SecurityBreachAttempt,
415                       timeConflict TimeConflict,
416                       ...
417                 }
418
```

```
PersonalEvent ::= CHOICE{
	lackOfAppropriateCard DrivingWithoutAnAppropriateCard,
	cardInsertionWhileDriving CardInsertionWhileDriving,
	overSpeeding OverSpeeding,
	...
}

StandardFault ::= CHOICE{
	cardFault CardFault,
	recordingEquipementFault RecordingEquipmentFault,
...
}

---------------
--EVENTS LIST--
---------------

InsertionOfANonValidCard::=SEQUENCE{
	beginDate GeneralizedTime,
	endDate GeneralizedTime,
	carsdType SEQUENCE OF UTF8String,
	cardsNumber SEQUENCE OF INTEGER,
	issuingMemberState SEQUENCE OF NationAlpha,
	cardsGeneration SEQUENCE OF INTEGER
}

CardConflict ::= SEQUENCE{
	beginDate GeneralizedTime,
	endDate GeneralizedTime,
	carsdType SEQUENCE OF UTF8String,
	cardsNumber SEQUENCE OF INTEGER,
	issuingMemberState SEQUENCE OF NationAlpha,
	cardsGeneration SEQUENCE OF INTEGER
}

TimeOverlap ::=SEQUENCE{
	beginDate GeneralizedTime,
	endDate GeneralizedTime,
	carsdType SEQUENCE OF UTF8String,
	cardsNumber SEQUENCE OF INTEGER,
	issuingMemberState SEQUENCE OF NationAlpha,
	cardsGeneration SEQUENCE OF INTEGER,
	numberSimilarEvent INTEGER
}

DrivingWithoutAnAppropriateCard ::= SEQUENCE{
	beginDate GeneralizedTime,
	endDate GeneralizedTime,
	carsdType SEQUENCE OF UTF8String,
	cardsNumber SEQUENCE OF INTEGER,
	issuingMemberState SEQUENCE OF NationAlpha,
	cardsGeneration SEQUENCE OF INTEGER,
	numberOfSimilarEvent INTEGER
}

CardInsertionWhileDriving ::= SEQUENCE{
	date GeneralizedTime,
	carsdType SEQUENCE OF UTF8String,
	cardsNumber SEQUENCE OF INTEGER,
```

```
478                     issuingMemberState SEQUENCE OF NationAlpha,
479                     numberOfSimilarEvents INTEGER
480             }
481
482             LastCardSessionNotCorrectlyClosed ::=SEQUENCE{
483                     beginDate GeneralizedTime,
484                     endDate GeneralizedTime,
485                     carsdType SEQUENCE OF UTF8String,
486                     cardsNumber SEQUENCE OF INTEGER,
487                     issuingMemberState SEQUENCE OF NationAlpha,
488                     cardsGeneration SEQUENCE OF INTEGER,
489                     oldSession SEQUENCE{
490                             beginDate GeneralizedTime,
491                             endDate GeneralizedTime,
492                             vrn UTF8String,
493                             issuingMemberState NationAlpha,
494                             cardsGeneration INTEGER,
495                     }
496             }
497
498             OverSpeeding ::=SEQUENCE{
499                     beginDate GeneralizedTime,
500                     endDate GeneralizedTime,
501                     maximumSpeed INTEGER,
502                     averageSpeed INTEGER,
503                     cardType UTF8String,
504                     cardNumber INTEGER,
505                     issuingMemberState NationAlpha,
506                     cardGeneration INTEGER,
507                     numberOfSimilarEvents INTEGER
508             }
509
510             PowerSupplyInterruption ::=SEQUENCE{
511                     beginDate GeneralizedTime,
512                     endDate GeneralizedTime,
513                     carsdType SEQUENCE OF UTF8String,
514                     cardsNumber SEQUENCE OF INTEGER,
515                     issuingMemberState SEQUENCE OF NationAlpha,
516                     cardsGeneration SEQUENCE OF INTEGER,
517                     numberOfSimilarEvent INTEGER
518             }
519
520             CommunicationErrorWithTheRemoteCommunicationFacility ::=SEQUENCE{
521                     beginDate GeneralizedTime,
522                     endDate GeneralizedTime,
523                     carsdType SEQUENCE OF UTF8String,
524                     cardsNumber SEQUENCE OF INTEGER,
525                     issuingMemberState SEQUENCE OF NationAlpha,
526                     cardsGeneration SEQUENCE OF INTEGER,
527                     numberOfSimilarEvent INTEGER
528             }
529
530             AbsenceOfPositionInformationFromGNSSReceiver ::= SEQUENCE{
531                     beginDate GeneralizedTime,
532                     endDate GeneralizedTime,
533                     carsdType SEQUENCE OF UTF8String,
534                     cardsNumber SEQUENCE OF INTEGER,
535                     issuingMemberState SEQUENCE OF NationAlpha,
536                     cardsGeneration SEQUENCE OF INTEGER,
```

```
                        numberOfSimilarEvent INTEGER
                }

CommunicationErrorWithTheExternalGNSSFacility ::= SEQUENCE{
beginDate GeneralizedTime,
endDate GeneralizedTime,
cardsType SEQUENCE OF UTF8String,
cardsNumber SEQUENCE OF INTEGER,
issuingMemberState SEQUENCE OF NationAlpha,
cardsGeneration SEQUENCE OF INTEGER,
numberOfSimilarEvent INTEGER
        }

                PositionDataError ::= SEQUENCE{
                        beginDate GeneralizedTime,
                        endDate GeneralizedTime,
                        carsdType SEQUENCE OF UTF8String,
                        cardsNumber SEQUENCE OF INTEGER,
                        issuingMemberState SEQUENCE OF NationAlpha,
                        cardsGeneration SEQUENCE OF INTEGER,
                        numberOfSimilarEvent INTEGER
                }

                MotionDataError ::= SEQUENCE{
                        beginDate GeneralizedTime,
                        endDate GeneralizedTime,
                        carsdType SEQUENCE OF UTF8String,
                        cardsNumber SEQUENCE OF INTEGER,
                        issuingMemberState SEQUENCE OF NationAlpha,
                        cardsGeneration SEQUENCE OF INTEGER,
                        numberOfSimilarEvent INTEGER
                }

                VehicleMotionConflict ::= SEQUENCE{
                        beginDate GeneralizedTime,
                        endDate GeneralizedTime,
                        carsdType SEQUENCE OF UTF8String,
                        cardsNumber SEQUENCE OF INTEGER,
                        issuingMemberState SEQUENCE OF NationAlpha,
                        cardsGeneration SEQUENCE OF INTEGER,
                        numberOfSimilarEvent INTEGER
                }

                SecurityBreachAttempt ::= SEQUENCE{
                        beginDate GeneralizedTime,
                        endDate GeneralizedTime OPTIONAL,
                        carsdType SEQUENCE OF UTF8String,
                        cardsNumber SEQUENCE OF INTEGER,
                        issuingMemberState SEQUENCE OF NationAlpha,
                        numberOfSimilarEvent INTEGER,
                        typeOfEvent SecurityBreachEvent
                }


                TimeConflict ::= SEQUENCE{
                        beginDate GeneralizedTime,
                        endDate GeneralizedTime,
                        carsdType SEQUENCE OF UTF8String,
                        cardsNumber SEQUENCE OF INTEGER,
                        issuingMemberState SEQUENCE OF NationAlpha,
                        cardsGeneration SEQUENCE OF INTEGER,
                        numberOfSimilarEvent INTEGER
                }

                ---------------
                --FAULTS LIST--
                ---------------

                CardFault ::= SEQUENCE{
```

```
596                     beginDate GeneralizedTime,
597                     endDate GeneralizedTime,
598                     carsdType SEQUENCE OF UTF8String,
599                     cardsNumber SEQUENCE OF INTEGER,
600                     issuingMemberState SEQUENCE OF NationAlpha,
601                     cardsGeneration SEQUENCE OF INTEGER,
602             }
603
604             RecordingEquipmentFault ::= SEQUENCE{
605                     beginDate GeneralizedTime,
606                     endDate GeneralizedTime,
607                     faultType RecordingEquipmentFaultType,
608                     carsdType SEQUENCE OF UTF8String,
609                     cardsNumber SEQUENCE OF INTEGER,
610                     issuingMemberState SEQUENCE OF NationAlpha,
611                     cardsGeneration SEQUENCE OF INTEGER,
612             }
613 END
```

Dodatak 14.

FUNKCIJA KOMUNIKACIJE NA DALJINU

SADRŽAJ

1 UVOD

U ovom se Dodatku utvrđuju izrada i postupci koje treba slijediti kako bi se provela funkcija komunikacije na daljinu (komunikacije) kako se zahtijeva u članu 9. Uredbe (EU) br. 165/2014 (Uredba).

DSC_1 U Uredbi (EU) br. 165/2014 utvrđuje se da tahograf mora biti opremljen funkcijom za komunikaciju na daljinu kojom se djelatnicima nadležnih nadzornih tijela omogućava da očitaju tahografske informacije iz vozila u prolazu upotrebom opreme za ispitivanje na daljinu (čitača komunikacije ranog otkrivanja na daljinu (eng. *Remote early detection communication reader*, REDCR), konkretno, opreme za ispitivanje koja se bežično spaja putem sučelja namjenskog komunikacijskog sistema kratkog dometa (eng. *Dedicated Short Range Communication*, DSRC) na frekvenciji od 5,8 GHz u skladu s normom CEN.

Važno je znati da je ta funkcija namijenjena isključivo kao predfiltar kako bi se odabrala vozila za detaljniji pregled te ne zamjenjuje službeni postupak pregleda kako je utvrđeno u odredbama Uredbe (EU) br. 165/2014. Vidjeti uvodnu izjavu 9. u preambuli te Uredbe u kojoj se navodi da komunikacija na daljinu između tahografa i nadzornih tijela u svrhu nadzora na putu olakšava provedbu ciljanih provjera na putu.

DSC_2 Podaci se razmjenjuju komunikacijom koja se odvija bežično upotrebom bežične namjenske komunikacije kratkog dometa na frekvenciji od 5,8 GHz koja je u skladu s ovim Dodatkom i ispitana u odnosu na odgovarajuće parametre norme EN 300 674-1 (*Electromagnetic compatibility and Radio spectrum Matters*

(ERM); Road Transport and Traffic Telematics (RTTT); Dedicated Short Range Communication (DSRC) transmission equipment (500 kbit/s / 250 kbit/s) operating in the 5,8 GHz Industrial, Scientific and Medical (ISM) band; Part 1: General characteristics and test methods for Road Side Units (RSU) and On-Board Units (OBU)).

DSC_3 Komunikacija se uspostavlja s pomoću komunikacijske opreme samo kada to zahtijeva oprema nadležnog nadzornog tijela upotrebom usklađenih radiokomunikacijskih sredstava (REDCR-a).

DSC_4 Podaci su zaštićeni kako bi se osigurao integritet.

DSC_5 Pristup prenesenim podacima ograničen je na nadležna nadzorna tijela koja imaju ovlasti za provjeru kršenja Uredbe (EZ) br. 561/2006 i Uredbe (EU) br. 165/2014 te na radionice ako treba provjeriti radi li tahograf ispravno.

DSC_6 Podaci razmijenjeni tokom komunikacije ograničuju se na podatke potrebne u svrhu ciljanih provjera vozila na putu čijim se tahografom možda neovlašteno rukovalo ili koji se pogrešno upotrebljavao.

DSC_7 Integritet i sigurnost podataka postižu se zaštitom podataka jedinice u vozilu (VU) i prenosom isključivo zaštićenih podataka te sigurnosnih podataka (vidjeti odjeljak 5.4.4) putem bežičnog komunikacijskog sredstva DSRC na frekvenciji od 5,8 GHz, što znači da samo ovlaštene osobe nadležnih nadzornih tijela mogu razumjeti podatke prenesene komunikacijom i provjeriti njihovu vjerodostojnost. Vidjeti Dodatak 11., Zajednički sigurnosni mehanizmi.

DSC_8 Podaci sadrže vremensku oznaku koja označava vrijeme njihova posljednjeg ažuriranja.

DSC_9 Sadržaj sigurnosnih podataka poznat je isključivo nadležnim nadzornim tijelima i stranama s kojima ona dijele te informacije u skladu s odredbama komunikacije koja je predmet ovog Dodatka, osim što se komunikacijom omogućava prenos sigurnosnih podataka sa svakim paketom prenesenih podataka.

DSC_10 Ista struktura i oprema prikladne su za upotrebu kako bi se dobili ostali koncepti podataka (kao što je vaganje u vozilu) upotrebom strukture navedene u nastavu.

DSC_11 Radi objašnjenja, u skladu s odredbama Uredbe (EU) br. 165/2014 (člana 7.), podaci o identitetu vozača ne smiju se prenositi komunikacijom.

2 PODRUČJE PRIMJENE

Područje primjene ovog Dodatka utvrđivanje je načina na koji djelatnici nadležnih nadzornih tijela upotrebljavaju navedenu bežičnu komunikaciju DSRC-a na frekvenciji od 5,8 GHz kako bi na daljinu od ciljanog vozila dobili podatke s pomoću kojih se utvrđuje krši li ciljano vozilo Uredbu (EU) br. 165/2014 i treba li ga se ciljano zaustavljati radi daljnje istrage.

U Uredbi (EU) br. 165/2014 zahtijeva se da se prikupljeni podaci ograniče na podatke ili pripadaju podacima kojima se utvrđuje moguće kršenje kako je navedeno u članu 9. Uredbe (EU) br. 165/2014.

U takvom je slučaju raspoloživo vrijeme za *komunikaciju* ograničeno jer je *komunikacija* ciljana i kratkog dometa. Nadalje, ista komunikacijska sredstva za praćenje tahografa na daljinu (remote tachograph monitoring, RTM) nadležna nadzorna tijela mogu upotrebljavati i u druge svrhe (kao što su praćenje najveće mase i dimenzija za teška teretna vozila kako je utvrđeno u Direktivi (EU) 2015/719), a takve radnje mogu biti zasebne ili uzastopne, o čemu odluku donose nadležna nadzorna tijela.

U ovom se Dodatku navodi sljedeće:

— komunikacijska oprema, postupci i protokoli koji će se upotrebljavati za komunikaciju;

— norme i uredbe s kojima je usklađena radijska oprema;

— iznošenje podataka komunikacijskoj opremi;

— postupci za ispitivanje i preuzimanje te slijed radnji;

— podaci koje je potrebno prenijeti;

— moguće tumačenje podataka prenesenih komunikacijom;

— odredbe za sigurnosne podatke koje se odnose na komunikaciju;

— dostupnost podataka nadležnim nadzornim tijelima;

— način na koji čitač komunikacije ranog otkrivanja na daljinu može zatražiti različite koncepte podataka o teretu i voznom parku (eng. *Freight&Fleet*).

Radi objašnjenja, u ovom se Dodatku ne navodi sljedeće:

— prikupljanje podataka i upravljanje podacima u jedinici u vozilu (što je funkcija izvedbe proizvoda osim ako nije drugačije navedeno u Uredbi (EU) br. 165/2014);

— način iznošenja prikupljenih podataka djelatniku nadležnog nadzornog tijela, kao ni kriteriji koje nadležna nadzorna tijela upotrebljavaju za donošenje odluke o tome koja će vozila zaustaviti (što je funkcija izvedbe proizvoda osim ako nije drugačije navedeno u Uredbi (EU) br. 165/2014 ili odluci u okviru politike nadležnih nadzornih tijela). Radi objašnjenja: komunikacijom se podaci stavljaju na raspolaganje nadležnim nadzornim tijelima isključivo kako bi ona mogla donositi informirane odluke;

— odredbe o sigurnosti podataka (kao što je šifriranje) koje se odnose na sadržaj podataka (koje se navode u Dodatku 11., Zajednički sigurnosni mehanizmi);

— pojedinosti o svim konceptima podataka osim RTM-a koji se mogu dobiti upotrebom iste strukture i opreme;

— pojedinosti o ponašanju i upravljanju između VU-a i DSRC-VU-a, kao ni ponašanje u DSRC-VU-u (osim u svrhu slanja podataka kada to zatraži REDCR).

3 KRATICE, DEFINICIJE I BILJEŠKE

U ovom Dodatku upotrebljavaju se sljedeće skraćenice i definicije specifične za ovaj Dodatak:

antena električni uređaj koji pretvara električnu energiju u radiovalove i obratno, a upotrebljava se u kombinaciji s radio-odašiljačem ili radio-prijamnikom. Pri radu, radio-odašiljač dovodi električnu struju koja oscilira na radijskoj frekvenciji na priključku antene, a antena zrači energiju iz struje u obliku elektromagnetskih valova (radiovalova). Pri prijamu, antena presreće dio energije elektromagnetskog vala kako bi proizvela minimalni napon na svojim priključcima koji se primjenjuje na prijamnik kako bi se pojačao;

komunikacija razmjena informacija/podataka između DSRC-REDCR-a i DSRC-VU-a u skladu s odjeljkom 5. prema načelu odnosa „nadređen–podređen” kako bi se dobili podaci.
podaci zaštićeni podaci utvrđena formata (vidjeti odjeljak 5.4.4.) koje zahtijeva DSRC-REDCR, a DSRC-REDCR-u ih šalje DSRC-VU putem veze DSRC-a na frekvenciji od 5,8 GHz kako je utvrđeno u odjeljku 5. u nastavu;
Uredba (EU) br. 165/2014 Evropskog parlamenta i Vijeća od 4. februar 2014. o tahografima u drumskom prometu, stavljanju izvan snage Uredbe Vijeća (EEZ) br. 3821/85 o tahografu u drumskom prometu i izmjeni Uredbe (EZ) br. 561/2006 Evropskog parlamenta i Vijeća o usklađivanju određenog socijalnog zakonodavstva koje se odnosi na drumski promet;
AID identifikator aplikacije (eng. Application Identifier)
BLE sistem Bluetooth niske razine energije (eng. Bluetooth Low Energy)
BST tablica usluga radiofara (eng. Beacon Service Table)
CIWD umetanje kartice tokom vožnje (eng. Card insertion while driving)
CRC kružna provjera zalihosti u prenosu podataka (eng. cyclic redundancy check)
DSC (n) identifikator zahtjeva za određeni dodatak DSRC-u (eng. identifier of a requirement for a specific DSRC appendix)
DSRC namjenski komunikacijski sistem kratkog dometa (eng. Dedicated Short Range Communication)
DSRC-REDCR DSRC – čitač komunikacije ranog otkrivanja na daljinu (eng. DSRC – Remote Early Detection Communication Reader)
DSRC-VU DSRC – jedinica u vozilu. (eng. DSRC – Vehicle Unit) Riječ je o „uređaju za rano otkrivanje na daljinu” koji je definisan u Prilogu I.C.
DWVC vožnja bez važeće kartice (eng. Driving without valid card)
EID identifikator elemenata (eng. Element Identifier)
LLC kontrola logičke veze (eng. Logical Link Control)
LPDU podatkovna jedinica protokola LLC (eng. LLC Protocol Data Unit)
OWS sistem za vaganje u vozilu (eng. Onboard Weighing System)
PDU podatkovna jedinica protokola (eng. Protocol Data Unit)
REDCR čitač komunikacije ranog otkrivanja na daljinu (eng. Remote early detection communication reader). Riječ je o „opremi čitača komunikacije ranog otkrivanja na daljinu” koja je definisana u Prilogu I.C.
RTM praćenje tahografa na daljinu (eng. Remote Tachograph Monitoring)
SM-REDCR sigurnosni modul čitača komunikacije ranog otkrivanja na daljinu (eng. Security Module-Remote early detection communication reader)
TARV telematske aplikacije za regulirana vozila (serija normi ISO 15638) (eng. Telematics Applications for Regulated Vehicles)
VU jedinica u vozilu (eng. Vehicle Unit)
VUPM prenosna memorija jedinice u vozilu (eng. Vehicle Unit Payload Memory)
VUSM sigurnosni modul jedinice u vozilu (eng. Vehicle Unit Security Module)
VST tablica usluga vozila (eng. Vehicle Service Table)
WIM vaganje u pokretu (eng. Weigh in motion)
WOB vaganje u vozilu (eng. Weigh on board)
Specifikacija utvrđena u ovom Dodatku odnosi se na i ovisi o svim sljedećim uredbama i normama ili o njihovim dijelovima. U okviru odredbi ovog Dodatka utvrđuju se mjerodavne norme ili mjerodavne odredbe normi. U slučaju protivrječnosti, odredbe ovog Dodatka imaju prednost. U slučaju bilo kakve protivrječnosti, pri čemu se u ovom Dodatku jasno ne utvrđuje nikakva specifikacija, postepene u skladu s preporukom ERC 70-03 (i ispitano u odnosu na odgovarajuće parametre norme EN 300 674-1) ima prednost, a slijede ih, počevši s najpoželjnijom, norme EN 12795, EN 12253, EN 12834 i EN 13372, točke 6.2., 6.3., 6.4. i 7.1.
Uredbe i norme na koje se upućuje u ovom Dodatku su:
[1] Uredba (EU) br. 165/2014 Evropskog parlamenta i Vijeća od 4. februar 2014. o tahografima u drumskom prometu, stavljanju izvan snage Uredbe Vijeća (EEZ) br. 3821/85 o tahografu u drumskom prometu i izmjeni Uredbe (EZ) br. 561/2006 Evropskog parlamenta i Vijeća o usklađivanju određenog socijalnog zakonodavstva koje se odnosi na drumski promet;
[2] Uredba (EZ) br. 561/2006 Evropskog parlamenta i Vijeća od 15. ožujka 2006. o usklađivanju određenog socijalnog zakonodavstva koje se odnosi na drumski promet i o izmjeni uredbi Vijeća (EEZ) br. 3821/85 i (EZ) br. 2135/98 te o stavljanju izvan snage Uredbe Vijeća (EEZ) br. 3820/85 (Tekst značajan za EGP);
[3] ERC 70-03 CEPT: *ECC Recommendation 70-03: Relating to the Use of Short Range Devices (SRD)*;
[4] norma ISO 15638, *Intelligent transport systems – Framework for cooperative telematics applications for regulated commercial freight vehicles (TARV)*;
[5] norma EN 300 674-1, *Electromagnetic compatibility and Radio spectrum Matters (ERM); Road Transport and Traffic Telematics (RTTT); Dedicated Short Range Communication (DSRC) transmission equipment (500 kbit/s / 250 kbit/s) operating in the 5,8 GHz Industrial, Scientific and Medical (ISM) band; Part 1: General characteristics and test methods for Road Side Units (RSU) and On-Board Units (OBU)*;
[6] norma EN 12253, *Road transport and traffic telematics – Dedicated short-range communication – Physical layer using microwave at 5.8 GHz*;
[7] norma EN 12795, R*oad transport and traffic telematics – Dedicated short-range communication – Data link layer: medium access and logical link control*;
[8] norma EN 12834, *Road transport and traffic telematics – Dedicated short-range communication – Application layer*;

[9] norma EN 13372, *Road transport and traffic telematics – Dedicated short-range communication – Profiles for RTTT applications*;
[10] norma ISO 14906, *Electronic fee collection – Application interface definition for dedicated short- range communication*.

4 OPERATIVNI SCENARIJI

4.1 Pregled

U Uredbi (EU) br. 165/2014 navode se specifični i kontrolirani scenariji u kojima se komunikacija treba upotrebljavati.
Podržani su scenariji sljedeći:
„Komunikacijski profil 1.: Provjera na putu upotrebom čitača komunikacije ranog otkrivanja na daljinu u okviru bežičnog komunikacijskog sistema kratkog dometa čime se pokreće fizički pregled na putu (načelo ‚nadređen-podređen').
Profil čitača 1.a: putem ručnog usmjerenog ili privremeno postavljenog uz cestu i usmjerenog čitača komunikacije ranog otkrivanja na daljinu
Profil čitača 1.b: putem ugrađenog u vozilu i usmjerenog čitača komunikacije ranog otkrivanja na daljinu".

4.1.1 *Preduslovi za prenos podataka putem sučelja DSRC-a na frekvenciji od 5,8 GHz*

NAPOMENA: Za razumijevanje konteksta ovih preduvjeta čitatelja se upućuje na sliku 14.3. u nastavu.

4.1.1.1 Podaci sadržani u jedinici u vozilu (VU)

DSC_12 VU je zadužen za ažuriranje svakih 60 sekundi i za održavanje podataka koji se arhiviraju u VU-u, bez uključivanja funkcije komunikacije DSRC-a. Način na koji se to postiže unutarnji je u odnosu na VU i naveden je u Uredbi (EU) br. 165/2014 Prilogu I.C odjeljku 3.19., „Komunikacija na daljinu za ciljane provjere na putu", no nije naveden u ovom Dodatku.

4.1.1.2 Podaci koji se šalju uređaju DSRC-VU

DSC_13 VU je zadužen za ažuriranje tahografskih podataka DSRC-a (podataka) svaki put kad se podaci arhivirani u VU-u ažuriraju u intervalu određenom u odjeljku 4.1.1.1. (DSC_12), bez uključivanja funkcije komunikacije DSRC-a.
DSC_14 Podaci VU-a upotrebljavaju se kao osnova za popunjavanje i ažuriranje podataka, a način na koji se to postiže naveden je u Prilogu I.C odjeljku 3.19., „Komunikacija na daljinu za ciljane provjere na putu" ili, ako takva specifikacija ne postoji, čini funkciju izvedbe proizvoda i nije navedena u ovom Dodatku. Izrada priključka između uređaja DSRC-VU i VU-a opisana je u odjeljku 5.6.

4.1.1.3 Sadržaj podataka

DSC_15 Sadržaj i format podataka takvi su da se nakon dešifriranja strukturiraju i čine dostupnima u obliku i formatu navedenima u odjeljku 5.4.4. ovog Dodatka (Strukture podataka).

4.1.1.4 Iznošenje podataka

DSC_16 Podaci, koji se redovito ažuriraju u skladu s postupcima utvrđenima u odjeljku 4.1.1.1., zaštićuju se prije iznošenja u DSRC-VU te se iznose kao zaštićena vrijednost koncepata podataka za privremenu arhiviranje u DSRC-VU-u kao trenutna verzija podataka. Ti se podaci prenose iz VUSM-a u funkciju DSRC-a VUPM. VUSM i VUPM su funkcije i nisu nužno fizički subjekti. Oblik fizičke instance za izvršenje tih funkcija pitanje je izvedbe proizvoda osim ako nije drugačije navedeno u Uredbi (EU) br. 165/2014.

4.1.1.5 Sigurnosni podaci

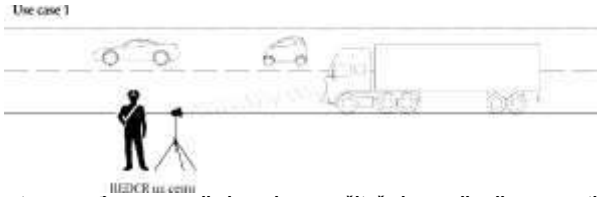
DSC_17 Sigurnosni podaci (*securityData*), koji obuhvaćaju podatke koje zahtijeva REDCR kako bi dovršio svoju mogućnost dešifriranja podataka, dostavljaju se kako je navedeno u Dodatku 11., Zajednički sigurnosni mehanizmi, te iznose kao vrijednost koncepata podataka za privremenu arhiviranje u DSRC-VU-u kao trenutna verzija sigurnosnih podataka *securityData*, u obliku utvrđenom u odjeljku 5.4.4. ovog Dodatka.

4.1.1.6 Podaci VUPM-a dostupni za prenos sučeljem DSRC-a

DSC_18 Koncept podataka koji mora uvijek biti dostupan u okviru funkcije VUPM-a za DSRC za neposredan prenos na zahtjev putem REDCR-a utvrđuje se u odjeljku 5.4.4. za potpune specifikacije modula ASN.1.
Opći pregled komunikacijskog profila 1.
Ovaj profil obuhvaća slučajeve upotrebe u kojima djelatnik nadležnog nadzornog tijela upotrebljava čitač komunikacije ranog otkrivanja na daljinu komunikacijskog sistema kratkog dometa (uz sučelja DSRC-a na frekvenciji od 5,8 GHz koja rade u skladu s preporukom ERC 70-03, a ispitana su u odnosu na odgovarajuće parametre norme EN 300 674-1 kako je opisano u odjeljku 5.) (REDCR) za daljinsko utvrđivanje vozila koje bi moglo kršiti odredbe Uredbe (EU) br. 165/2014. Nakon njegova utvrđivanja, djelatnik nadležnog nadzornog tijela koji nadzire ispitivanje donosi odluku o tome treba li vozilo zaustaviti.

4.1.2 *Profil 1.a: putem ručnog usmjerenog ili privremeno postavljenog uz cestu i usmjerenog čitača komunikacije ranog otkrivanja na daljinu*

U ovom slučaju upotrebe djelatnik nadležnog nadzornog tijela nalazi se uz cestu i usmjeruje ručni uređaj, uređaj na postolju ili sličan prenosni REDCR prema središtu vjetrobranskog stakla ciljanog vozila. Ispitivanja se vrše upotrebom sučelja DSRC-a na frekvenciji od 5,8 GHz koja rade u skladu s preporukom ERC 70-03, a ispitana su u odnosu na odgovarajuće parametre norme EN 300 674-1, kako je opisano u odjeljku 5. Vidjeti sliku 14.1. (slučaj upotrebe 1.).
Slika 14.1.
Ispitivanje uz cestu upotrebom DSRC-a na frekvenciji od 5,8 GHz



4.1.3 ***Profil 1.b: putem ugrađenog u vozilu i usmjerenog čitača komunikacije ranog otkrivanja na daljinu (REDCR)***

U ovom slučaju upotrebe djelatnik nadležnog nadzornog tijela nalazi se u vozilu koje se kreće te usmjeruje ručni prenosni REDCR iz vozila prema središtu vjetrobranskog stakla ciljanog vozila, ili je REDCR ugrađen u ili na vozilo kako bi bio usmjeren prema središtu vjetrobranskog stakla ciljanog vozila kada se vozilo s čitačem komunikacije ranog otkrivanja na daljinu nalazi u određenom položaju bitnom za ciljano vozilo (primjerice, direktno ispred kolone vozila u prometu). Ispitivanja se vrše upotrebom sučelja DSRC-a na frekvenciji od 5,8 GHz koja rade u skladu s preporukom ERC 70-03, a ispitana su u odnosu na odgovarajuće parametre norme EN 300 674-1, kako je opisano u odjeljku 5. Vidjeti sliku 14.2. (slučaj upotrebe 2.).

Slika 14.2.

Ispitivanje s pomoću vozila upotrebom DSRC-a na frekvenciji od 5,8 GHz

4.2 Sigurnost/integritet

Kako bi se omogućila provjera vjerodostojnosti i integriteta preuzetih podataka putem komunikacije na daljinu, zaštićeni podaci provjeravaju se i dešifriraju u skladu s Dodatkom 11., Zajednički sigurnosni mehanizmi.

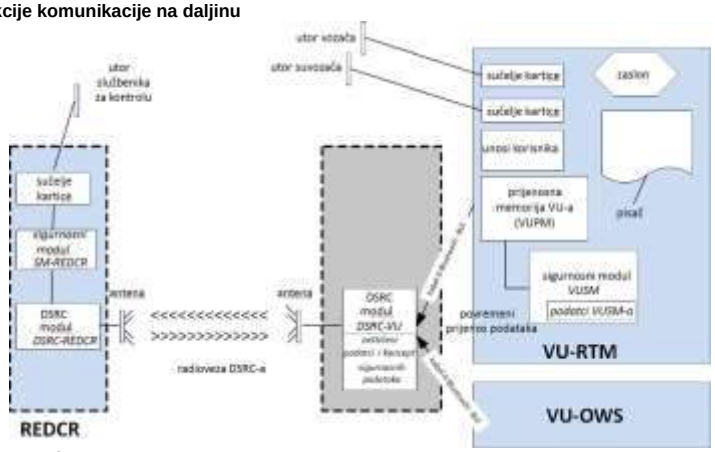
5 IZRADA I PROTOKOLI KOMUNIKACIJE NA DALJINU

5.1 Izrada

Izrada funkcije komunikacije na daljinu u pametnom tahografu prikazana je kako je opisano na slici 14.3.

Slika 14.3.

Izrada funkcije komunikacije na daljinu



DSC_19 Sljedeće funkcije nalaze se u VU-u:

— Sigurnosni modul (*VUSM*). Ova je funkcija prisutna u VU-u zadužena za zaštitu podataka koji će se prenijeti iz DSRC-VU-a djelatniku nadležnog nadzornog tijela putem komunikacije na daljinu.

— Zaštićeni podaci arhiviraju se u memoriju VUSM-a. U intervalima utvrđenima u odjeljku 4.1.1.1. (DSC_12) VU šifrira i nadopunjuje koncept RTMdata (koji obuhvaća vrijednosti koncepata prenesenih podataka i sigurnosnih podataka utvrđenih u ovom Dodatku) sadržan u memoriji DSRC-VU-a. Rad sigurnosnih modula utvrđen je u Dodatku 11., Zajednički sigurnosni mehanizmi, i nalazi se izvan područja primjene ovog Dodatka, osim ako je to potrebno kako bi se osigurala ažuriranja komunikacijskog uređaja VU-a svaki put kada se podaci iz VUSM-a promijene.

— Komunikacija između VU-a i DSRC-VU-a može biti žična komunikacija ili komunikacija putem sistema Bluetooth niske razine energije (BLE), a DSRC-VU fizički može biti spojen s antenom na vjetrobranskom staklu vozila, u unutrašnjosti VU-a ili negdje između.
— DSRC-VU mora u svakom trenutku imati pouzdan izvor napajanja. Način na koji se DSRC-VU napaja ovisi o njegovoj izvedbi.
— Memorija DSRC-VU-a neizbrisiva je kako bi se podaci zadržali u DSRC-VU-u čak i kada je kontakt vozila isključen.
— Ako se komunikacija između VU-a i DSRC-VU-a ostvaruje putem BLE-a, a izvor napajanja je baterija koja se ne puni ponovno, izvor napajanja DSRC-VU-a zamjenjuje se pri svakom periodičnom pregledu, a odgovornost je proizvođača opreme za DSRC-VU da osigura prikladno napajanje kako bi trajalo od jednog periodičnog pregleda do sljedećeg periodičnog pregleda te da se pritom održava uobičajen pristup podacima putem REDCR-a tokom čitava perioda bez pogrešaka ili prekida u radu.
— Uređaj VU RTM za „prenosnu memoriju" (*VUPM*). Ova je funkcija prisutna u VU-u zadužena za slanje i ažuriranje podataka. Sadržaj podataka („TachographPayload") utvrđuje se u odjeljcima 5.4.4. i 5.4.5. u nastavu i ažurira u intervalu određenom u odjeljku 4.1.1.1. (DSC_12).
— DSRC-VU. Riječ je o funkciji antene ili s antenom povezanoj funkciji koja je u komunikaciji s VU-om putem žičnog ili bežičnog (BLE) priključka i koja zadržava trenutne podatke (VUPM-podatke) i upravlja odgovorom na ispitivanje putem medija DSRC-a na frekvenciji od 5,8 GHz. Isključenje uređaja DSRC ili ometanje rada uređaja DSRC tokom uobičajenog rada vozila smatra se kršenjem Uredbe (EU) br. 165/2014.
— Sigurnosni modul (REDCR) (SM-REDCR) funkcija je koja se upotrebljava za dešifriranje i provjeru integriteta podataka koji potječu iz VU-a. Način na koji se to postiže utvrđen je u Dodatku 11., Zajednički sigurnosni mehanizmi, te nije definisan u ovom Dodatku.
— Funkcija uređaja DSRC-a (REDCR) (*DSRC-REDCR*) obuhvaća primopredajnik koji radi na frekvenciji od 5,8 GHz i povezani ugrađeni program te softver koji upravlja komunikacijom s DSRC-VU-om u skladu s ovim Dodatkom.
— DSRC-REDCR ispituje DSRC-VU ciljanog vozila i dobiva podatke (trenutne VUPM-podatke o ciljanom vozilu) putem veze i postupaka u okviru DSRC-a te arhivira primljene podatke u svoj SM-REDCR.
— Antena DSRC-VU ugrađuje se na mjesto koje omogućava komunikaciju DSRC-a između vozila i antene čitača uz cestu, kad je čitač postavljen na 15 metara udaljenosti ispred vozila i na dva metra visine, ciljajući vodoravno i okomito središte vjetrobranskog stakla. U slučaju lakih vozila prikladna je ugradnja na gornji dio vjetrobranskog stakla. U slučaju svih drugih vozila antena DSRC-a ugrađuje se ili blizu donjeg ili blizu gornjeg dijela vjetrobranskog stakla.
DSC_20 Antena i komunikacija rade u skladu s preporukom ERC 70-03, a ispitane su u odnosu na odgovarajuće parametre norme EN 300 674-1 kako je opisano u odjeljku 5. Antena i komunikacija mogu primijeniti tehnike ublažavanja rizika od interferencija u bežičnoj vezi kako je opisano u izvješću ECC-a 228, npr. primjenom filtara u komunikaciji CEN DSRC na frekvenciji od 5,8 Ghz.
DSC_21 Antena DSRC-a spaja se s uređajem DSRC-VU direktno unutar modula postavljenog na ili blizu vjetrobranskog stakla, ili putem namjenskog kabela izrađenog tako da otežava nezakonito isključenje. Isključenje ili ometanje rada antene smatraju se kršenjem Uredbe (EU) br. 165/2014. Namjerno prekrivanje ili drugačije štetno utjecanje na radnu učinkovitost antene smatra se kršenjem Uredbe (EU) br. 165/2014.
DSC_22 Faktor oblika antene nije utvrđen i ovisi o komercijalnoj odluci pod uslovom da ugrađeni DSRC-VU ispunjava zahtjeve u pogledu shodnosti utvrđene u odjeljku 5. u nastavu. Antena se postavlja kako je utvrđeno u DSC_19 i učinkovito podržava slučajeve upotrebe opisane u 4.1.2 i 4.1.3.
Slika 14.4.
Primjer postavljanja antene DSRC-a s frekvencijom od 5,8 GHz na vjetrobransko staklo regulisanih vozila

Faktor oblika REDCR-a i njegove antene može se razlikovati u skladu s okolnostima čitača (na postolju, ručni, ugrađen u vozilo itd.) i načinom rada koji primjenjuje djelatnik nadležnog nadzornog tijela.
Funkcija prikaza i/ili obavještenjei upotrebljava se za iznošenje rezultata funkcije komunikacije na daljinu djelatniku nadležnog nadzornog tijela. Prikaz se može osigurati na zaslonu, u obliku ispisa na papiru, zvučnog signala ili kombinacije takvih obavještenjei. Oblik takvog prikaza i/ili obavještenjei pitanje je zahtjeva djelatnika nadležnog nadzornog tijela i izvedbe opreme te nije naveden u ovom Dodatku.
DSC_23 Izrada i faktor oblika REDCR-a ovise o komercijalnoj izvedbi, koja je u skladu s preporukom ERC 70-03, te specifikacijama za izvedbu i učinkovitost utvrđenima u ovom Dodatku (odjeljku 5.3.2.) čime se tržištu omogućava maksimalna nivo fleksibilnosti za izradu i osiguravanje opreme kako bi se ispunile određene potrebe u pogledu specifičnih scenarija ispitivanja svakog pojedinog nadležnog nadzornog tijela.
DSC_24 Izrada i faktor oblika DSRC-VU-a te njegovo postavljanje unutar ili izvan VU-a ovise o komercijalnoj izvedbi koja je u skladu s preporukom ERC 70-03 i specifikacijama u pogledu izvedbe i učinkovitosti utvrđenima u ovom Dodatku (odjeljku 5.3.2.) te u ovoj tački (5.1.).

DSC_25 Međutim, DSRC-VU mora biti sposoban u razumnoj mjeri prihvaćati vrijednosti koncepata podataka iz ostale pametne opreme vozila s pomoću veza i protokola u skladu s otvorenim industrijskim normama. To treba biti moguće, primjerice, iz opreme za vaganje u vozilu, pod uslovom da se takvi koncepti podataka utvrde s pomoću jedinstvenih i prepoznatljivih identifikatora aplikacija ili naziva datoteka, a upute za rukovanje tim protokolima stavljaju se na raspolaganje Evropskoj komisiji i proizvođačima odgovarajuće opreme bez naknade.

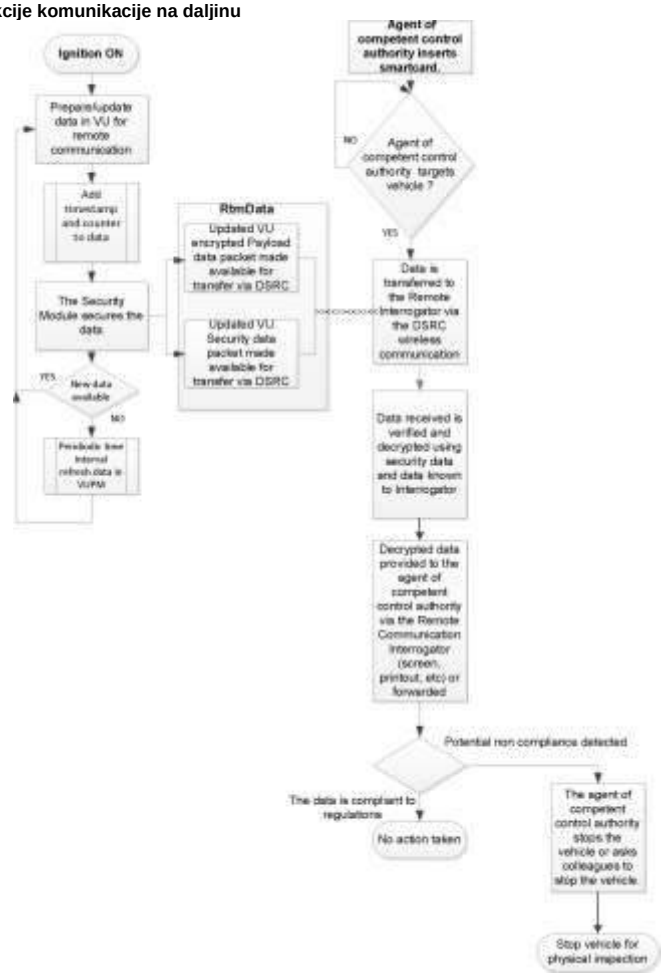
5.2 Tok rada

5.2.1 *Radnje*

Tok rada za radnje prikazan je na slici 14.5.

Slika 14.5.

Tok rada funkcije komunikacije na daljinu



Koraci su opisani u nastavu:

a. Kad god vozilo radi (kontakt UKLJUČEN), tahograf šalje podatke funkciji VU-a. Funkcija VU-a priprema podatke za funkciju komunikacije na daljinu (šifrirane) i ažurira VUPM sadržan u memoriji DSRC-VU-a (kako je utvrđeno u odjeljcima 4.1.1.1. i 4.1.1.2.). Prikupljeni podaci formatiraju se kako je utvrđeno u odjeljcima 5.4.4. i 5.4.5. u nastavu.

b. Svaki put kada se podaci ažuriraju, ažurira se i vremenska oznaka utvrđena u konceptu sigurnosnih podataka.

c. Funkcija VUSM-a zaštićuje podatke u skladu s postupcima utvrđenima u Dodatku 11.

d. Svaki put kada se podaci ažuriraju (vidjeti odjeljke 4.1.1.1. i 4.1.1.2.), prenose se u DSRC-VU gdje zamjenjuju sve prethodne podatke kako bi ažurirani trenutni podaci uvijek bili dostupni za slanje u slučaju ispitivanja s pomoću *REDCR-a*. Kada ih VU dostavi DSRC-VU-u, podaci se prepoznaju prema nazivu datoteke RTMData ili prema identifikatorima ApplicationID i Attribute.

e. Ako djelatnik nadležnog nadzornog tijela želi ciljati vozilo i prikupiti podatke iz ciljanog vozila, djelatnik nadležnog nadzornog tijela prvo umeće svoju pametnu karticu u REDCR kako bi se omogućila komunikacija i kako bi SM-REDCR mogao provjeriti njezinu vjerodostojnost i dešifrirati podatke.
f. Djelatnik nadležnog nadzornog tijela zatim cilja vozilo i zahtijeva podatke putem komunikacije na daljinu. REDCR otvara razmjenu podataka između sučelja DSRC-a na frekvenciji od 5,8 GHz i DSRC-VU-a ciljanog vozila te zahtijeva podatke. Podaci se prenose REDCR-u putem bežičnog komunikacijskog sistema kao atribut DSRC-a primjenom usluge aplikacije GET kako je utvrđeno u odjeljku 5.4. Atribut sadrži šifrirane vrijednosti prenesenih podataka i sigurnosne podatke DSRC-a.
g. Podatke analizira oprema REDCR-a te se šalju djelatniku nadležnog nadzornog tijela.
h. Djelatnik nadležnog nadzornog tijela upotrebljava podatke kao pomoć u donošenju odluke o tome hoće li zaustaviti vozilo radi detaljnog pregleda ili zatražiti od drugog djelatnika nadležnog nadzornog tijela da zaustavi vozilo.

5.2.2 ***Tumačenje podataka primljenih putem komunikacije DSRC-a***

DSC_26 Podaci primljeni putem sučelja na frekvenciji od 5,8 GHz nose samo i isključivo značenje i format utvrđene u odjeljcima 5.4.4. i 5.4.5. u nastavu i tumače se u okviru ondje utvrđenih ciljeva. U skladu s odredbama Uredbe (EU) br. 165/2014, podaci se upotrebljavaju isključivo za pružanje bitnih informacija nadležnom nadzornom tijelu i služe im kao pomoć u donošenju odluke o tome koje vozilo treba zaustaviti radi fizičkog pregleda, a potom se uništavaju u skladu s člankom 9. Uredbe (EU) br. 165/2014.

5.3 Parametri fizičkog sučelja DSRC-a za komunikaciju na daljinu

5.3.1 ***Ograničenja u pogledu lokacije***

DSC_27 Ispitivanje vozila na daljinu primjenom sučelja DSRC-a na frekvenciji od 5,8 GHz ne bi se trebalo sprovoditi unutar 200 metara od operativnog pokretnog postolja DSRC-a na frekvenciji od 5,8 GHz.

5.3.2 ***Parametri silazne i uzlazne veze***

DSC_28 Oprema koja se upotrebljava za praćenje tahografa na daljinu mora biti usklađena i raditi u skladu s preporukom ERC 70-03 i parametrima utvrđenima u tablicama 14.1. i 14.2. u nastavu.
DSC_29 Nadalje, kako bi se osigurala shodnost s operativnim parametrima ostalih normiranih sistema DSRC-a na frekvenciji od 5,8 GHz, oprema koja se upotrebljava za praćenje tahografa na daljinu mora biti usklađena s parametrima normi EN 12253 i EN 13372.
To su:

Tablica 14.1.
Parametri silazne veze

Tačka br.	**Parametar**	**Vrijednost(i)**	**Napomena**
D1	Frekvencije nosača silazne veze	Postoje četiri mogućnosti koje može upotrebljavati REDCR: 5,7975 GHz 5,8025 GHz 5,8075 GHz 5,8125 GHz	U skladu s preporukom ERC 70-03. Frekvencije nosača može odabrati sprovoditelj sistema uz cestu i ne moraju biti poznate u DSRC-VU-u. (U skladu s normama EN 12253, EN 13372)
D1a (*1)	Dopušteno odstepene nosača Frekvencije	unutar ± 5 ppm	(U skladu s normom EN 12253)
D2 (*1)	Spektralna maska prenosnika RSU-a (REDCR-a)	U skladu s preporukom ERC 70-03. REDCR je u skladu s razredima B i C, kako je utvrđeno u normi EN 12253. Nema drugih specifičnih zahtjeva u okviru ovog Priloga.	Parametar koji se upotrebljava za nadzor interferencije između REDCR-ova u blizini (kako je utvrđeno u normama EN 12253 i EN 13372).
D3	Najmanji raspon frekvencije OBU-a (DSRC-VU-a)	5,795 – 5,815 GHz	(U skladu s normom EN 12253)
D4 (*1)	Najveći EIRP	U skladu s preporukom ERC 70-03 (nelicenciran) i u skladu s nacionalnim propisima Najviše +33 dBm	(U skladu s normom EN 12253)
D4a	Kutna maska za EIRP	U skladu s objavljenom specifikacijom proizvođača REDCR-a	(U skladu s normom EN 12253)
D5	Polarizacija	Lijeva kružna	(U skladu s normom EN 12253)
D5a	Križna polarizacija	XPD: U smjeru maksimalnog zračenja: (REDCR) RSU t ≥ 15 dB (DSRC-VU) OBU r ≥ 10 dB Na području od –3 dB: (REDCR) RSU t ≥ 10 dB (DSRC-VU) OBU r ≥ 6 dB	(U skladu s normom EN 12253)
D6 (*1)	Modulacija	Dvorazinska amplitudna modulacija	(U skladu s normom EN 12253)
D6a (*1)	Indeks modulacije	0,5 ... 0,9	(U skladu s normom EN 12253)
D6b	Otvor oka	≥ 90 % (vrijeme) / ≥ 85 % (amplituda)	
D7 (*1)	Kodiranje podataka	FM0 Bit „1” ima prelaze samo na početku i kraju intervala bita. Bit „0” ima dodatne prelaze u sredini intervala bita u usporedbi s bitom „1”.	(U skladu s normom EN 12253)
D8 (*1)	Brzina bita	500 kBit/s	(U skladu s normom EN 12253)

D8a	Dopušteno odstepene brojača bitova	više od ± 100 ppm	(U skladu s normom EN 12253)
D9	Brzina pogreške bita (BER) za komunikaciju	≤ 10^{-6} kada je ulazno napajanje u OBU-u (DSRC-VU-u) u rasponu navedenom [od D11a do D11b].	(U skladu s normom EN 12253)
D10	Okidač za ponovno pokretanje OBU-a (DSRC-VU-a)	OBU (DSRC-VU) ponovno se pokreće nakon primanja okvira s 11 ili više okteta (uključujući preambulu).	Nije potreban nikakav poseban uzorak ponovnog pokretanja. DSRC-VU se može ponovno pokrenuti nakon primanja okvira s manje od 11 okteta. (U skladu s normom EN 12253)
D10a	Najveće vrijeme početka	≤ 5 ms	(U skladu s normom EN 12253)
D11	Komunikacijska zona	Područje unutar kojeg se postiže BER u skladu s D9.	(U skladu s normom EN 12253)
D11a (*1)	Ograničenje napajanja za komunikaciju (gornje)	– 24 dBm	(U skladu s normom EN 12253)
D11b (*1)	Ograničenje napajanja za komunikaciju (donje)	Ulazno napajanje: – 43 dBm (smjer maksimalnog zračenja) – 41 dBm (unutar – 45° do + 45°, što odgovara ravnini paralelnoj s površinom ceste kada se DSRC-VU naknadno ugrađuje u vozilo (azimut))	(U skladu s normom EN 12253) Prošireni zahtjev za vodoravne kutove do ± 45° zbog slučajeva upotrebe utvrđenih u ovom Prilogu.
D12 (*1)	Nivo prekida napajanja DSRC-VU-a	– 60 dBm	(U skladu s normom EN 12253)
D13	Preambula	Preambula je obavezna.	(U skladu s normom EN 12253)
D13a	Dužina i uzorak preambule	16 bitova ± 1 bit bitova „1" kodiranih putem FM0	(U skladu s normom EN 12253)
D13b	Valni oblik preambule	Naizmjenični slijed niske razine i visoke razine uz trajanje impulsa od 2 µs. Dopušteno odstepene navedeno je u D8a.	(U skladu s normom EN 12253)
D13c	Prateći bitovi	RSU (REDCR) smije prenijeti najviše 8 bitova nakon oznake završetka. OBU (DSRC-VU) ne treba uzeti u obzir takve dodatne bitove.	(U skladu s normom EN 12253)
(*1) Parametri silazne veze podložni su ispitivanju shodnosti u skladu s mjerodavnim ispitivanjem parametara iz norme EN 300 674-1.			

Tablica 14.2.
Parametri uzlazne veze

Tačka br.	Parametar	Vrijednost(i)	Napomena
U1 (*1)	Frekvencije podnosača	OBU (DSRC-VU) podržava 1,5 MHz i 2,0 MHz. RSU (REDCR) podržava 1,5 MHz ili 2,0 MHz ili oboje. U1-0: 1,5 MHz U1-1: 2,0 MHz	Odabir frekvencije podnosača (1,5 MHz ili 2,0 MHz) ovisi o odabranom profilu iz norme EN 13372.
U1a (*1)	Dopušteno odstepene frekvencija podnosača	unutar ± 0,1 %	(U skladu s normom EN 12253)
U1b	Upotreba bočnih pojaseva	Isti podaci na obje strane	(U skladu s normom EN 12253)
U2 (*1)	Spektralna maska prenosnika OBU-a (DSRC-VU-a)	U skladu s normom EN12253 1. ulazno napajanje: vidjeti normu ETSI EN 300674-1; 2. izlazno napajanje: [U4a] dBm u 500 kHz; 3. emisija u bilo koji drugi uzlazni kanal: U2(3)-1 = – 35 dBm u 500 kHz	(U skladu s normom EN 12253)
U4a (*1)	Najveći jedinstveni bočni pojas EIRP-a (smjer maksimalnog zračenja)	Dvije mogućnosti: U4a-0: – 14 dBm U4a-1: – 21 dBm	U skladu s objavljenom specifikacijom proizvođača opreme
U4b (*1)	Najveći jedinstveni bočni pojas EIRP-a (35°)	Dvije mogućnosti: — nije primjenjivo — – 17 dBm	U skladu s objavljenom specifikacijom proizvođača opreme
U5	Polarizacija	Lijeva kružna	(U skladu s normom EN 12253)
U5a	Križna polarizacija	XPD: U smjeru maksimalnog zračenja: (REDCR) RSU r ≥ 15 dB (DSRC-VU) OBU t ≥ 10 dB Na – 3 dB: (REDCR) RSU r ≥ 10 dB (DSRC-VU) OBU t ≥ 6 dB	(U skladu s normom EN 12253)
U6	Modulacija podnosača	2-PSK Kodirani podaci sinkronizirani s podnosačem: prelazi kodiranih podataka podudaraju se s prelazima podnosača.	(U skladu s normom EN 12253)

U6b	Radni ciklus	Radni ciklus: 50 % ± α, α ≤ 5 %	(U skladu s normom EN 12253)
U6c	Modulacija na nosaču	Multiplikacija moduliranog podnosača s nosačem	(U skladu s normom EN 12253)
U7 (*1)	Kodiranje podataka	NRZI (nema prelaza na početku bita „1”, prelazi na početku bita „0”, nema prelaza unutar bita)	(U skladu s normom EN 12253)
U8 (*1)	Brzina bita	250 kbit/s	(U skladu s normom EN 12253)
U8a	Dopušteno odstepene brojača bitova	Unutar ± 1 000 ppm	(U skladu s normom EN 12253)
U9	Brzina pogreške bita (eng. *Bit Error Rate*, BER) za komunikaciju	≤ 10^{-6}	(U skladu s normom EN 12253)
U11	Komunikacijska zona	Područje unutar kojeg se nalazi DSRC-VU tako da njegove prenose prima REDCR s BER-om manjim od navedenog u U9a.	(U skladu s normom EN 12253)
U12a (*1)	Dobitak pretvorbe (donja granica)	1 dB za svaki bočni pojas Raspon kuta: kružno simetričan između smjera maksimalnog zračenja i ± 35°	
		i unutar – 45° do + 45°, što odgovara ravnini paralelnoj s površinom ceste kada se DSRC-VU naknadno ugrađuje u vozilo (azimut).	Veći od navedene vrijednosti raspona za vodoravne kutove do ± 45° zbog slučajeva upotrebe utvrđenih u ovom Prilogu.
U12b (*1)	Dobitak pretvorbe (gornja granica)	10 dB za svaki bočni pojas	Manji od određenog raspona vrijednosti za svaki bočni pojas unutar kružnog stošca oko smjera maksimalnog zračenja kuta otvaranja od ± 45°.
U13	Preambula	Preambula je obavezna.	(U skladu s normom EN 12253)
U13a	Preambula Dužina i uzorak	32 do 36 µs isključivo uz modulaciju podnosača, zatim 8 bitova „0” kodiranih putem NRZI-a	(U skladu s normom EN 12253)
U13b	Prateći bitovi	DSRC-VU smije prenijeti najviše 8 bitova nakon oznake završetka. RSU (REDCR) ne treba uzeti u obzir takve dodatne bitove.	(U skladu s normom EN 12253)
(*1) Parametri uzlazne veze podložni ispitivanju shodnosti u skladu s mjerodavnim ispitivanjem parametara iz norme EN 300 674-1.			

5.3.3 *Izrada antene*

5.3.3.1 Antena REDCR-a

DSC_30 Izrada antene REDCR-a ovisi o komercijalnoj izvedbi koja je u skladu s ograničenjima utvrđenima u odjeljku 5.3.2., prilagođenoj radi optimizacije učinkovitosti očitavanja DSRC-REDCR-a za određenu svrhu i okolnosti očitavanja za koje je REDCR izrađen i u kojima mora raditi.

5.3.3.2 Antena VU-a

DSC_31 Izrada antene DSRC-VU-a ovisi o komercijalnoj izvedbi koja je u skladu s ograničenjima utvrđenima u odjeljku 5.3.2., prilagođenoj radi optimizacije učinkovitosti očitavanja DSRC-REDCR-a za određenu svrhu i okolnosti očitavanja za koje je *REDCR* izrađen i u kojima mora raditi.

DSC_32 Antena VU-a pričvršćuje se ili postavlja na prednje vjetrobransko staklo vozila ili blizu njega, kako je navedeno u odjeljku 5.1.

DSC_33 U ispitnom okruženju radionice (vidjeti odjeljak 6.3.) antena DSRC-VU-a, pričvršćena u skladu s odjeljkom 5.1., učinkovito se povezuje s normiranom ispitnom komunikacijom te učinkovito osigurava transakcije RTM-a kako je utvrđeno u ovom Dodatku, na udaljenosti između 2 i 10 metara, tokom najmanje 99 % vremena, izračunano kao prosjek na temelju 1 000 ispitivanja s pomoću čitača.

5.4 Zahtjevi u pogledu protokola DSRC-a za RTM

5.4.1 *Pregled*

DSC_34 Protokol transakcije za preuzimanje podataka putem veze sučelja DSRC-a na frekvenciji od 5,8 GHz mora biti u skladu sa sljedećim koracima. U ovom je odjeljku opisan tok transakcije u idealnim uslovima bez ponovnih prenosa ili prekida komunikacije.

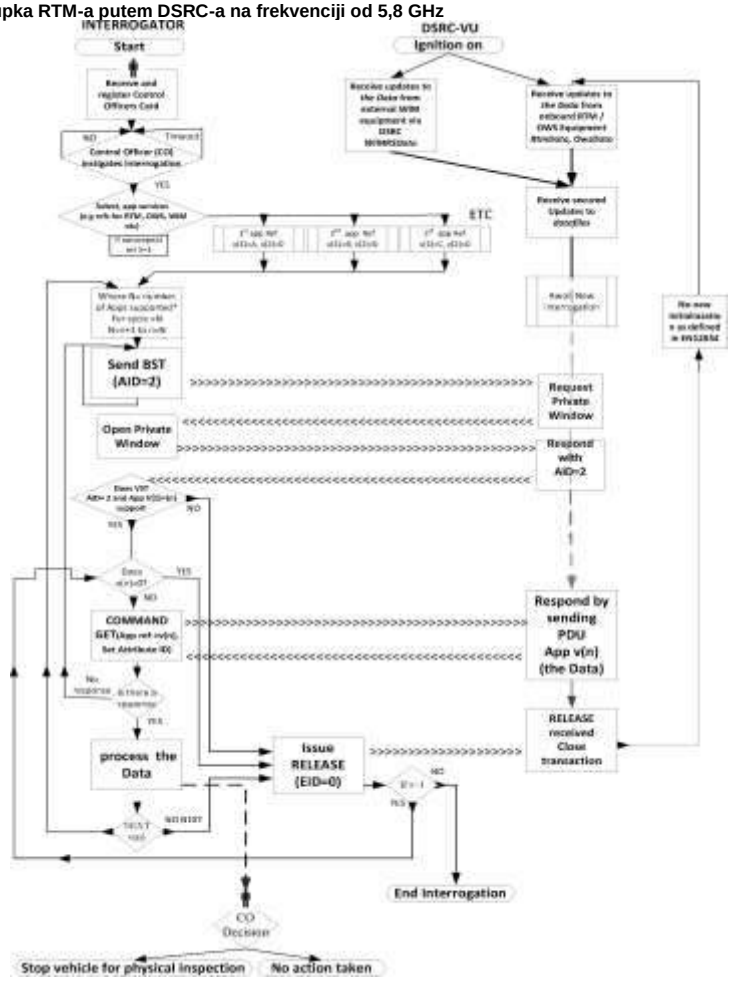
NAPOMENA Svrha faze inicijalizacije (1. korak) uspostavljanje je komunikacije između REDCR-a i DSRC-VU-ova koji su ušli u transakcijsko područje DSRC-a na frekvenciji od 5,8 GHz (u skladu s načelom odnosa „nadređen – podređen”), ali još nisu uspostavili komunikaciju s REDCR-om, te slanje obavještenjei o procesima uređaja.

—1. korakInicijalizacija. REDCR šalje okvir koji sadrži „tablicu s uslugama radiofara” (BST) koja uključuje identifikatore aplikacije (AID-ove) na popisu usluga koji podržava. U aplikaciji RTM-a to će jednostavno biti usluga s vrijednošću AID = 2 (Freight&Fleet). DSRC-VU ocjenjuje primljeni BST i odgovara (vidjeti u nastavu) popisom podržanih aplikacija unutar domene Freight&Fleet, ili ne odgovara ako nijedna aplikacija nije podržana. Ako REDCR ne ponudi vrijednost AID = 2, DSRC-VU ne odgovara REDCR-u.

—2. korakDSRC-VU šalje okvir koji sadrži zahtjev za dodjelu privatnog prozora.

—3. korakREDCR šalje okvir koji sadrži dodjelu privatnog prozora.

—4. korakDSRC-VU upotrebljava dodijeljeni privatni prozor za slanje okvira koji sadrži tablicu usluga vozila (VST). VST uključuje popis različitih instanci aplikacija koje DSRC-VU podržava u okviru vrijednosti AID = 2. Različite instance utvrđuju se s pomoću EID-ova generiranih na jedinstven način, a svaka je povezana s vrijednošću parametra kontekstualne oznake aplikacije koja označava podržanu aplikaciju i normu.
—5. korakZatim REDCR analizira ponuđeni VST i prekida vezu (RELEASE) jer mu nije potrebno ništa od onoga što nudi VST (odnosno prima VST iz DSRC-VU-a koji ne podržava transakciju RTM-a) ili, u slučaju da prima odgovarajući VST, pokreće instancu uređaja.
—6. korakKako bi se to provelo, REDCR šalje okvir koji sadrži naredbu za dohvat podataka RTM-a i koji utvrđuje instancu aplikacije RTM-a određivanjem identifikatora koji odgovara instanci aplikacije RTM-a (kako je navedeno u okviru DSRC-VU-a u VST-u) te dodjeljuje privatni prozor.
—7. korakDSRC-VU upotrebljava novi dodijeljeni privatni prozor za slanje okvira koji sadrži navedeni identifikator koji odgovara instanci aplikacije RTM-a kako je navedeno u VST-u, a slijedi ga atribut RtmData (prenosni element + sigurnosni element).
—8. korakAko se zatraži veći broj usluga, vrijednost „n” mijenja se na sljedeći referentni broj usluge, a postupak se ponavlja.
—9. korakREDCR potvrđuje primitak podataka slanjem okvira koji sadrži naredbu RELEASE DSRC-VU-u za prekid razmjene podataka ili se, u slučaju da potvrđivanje uspješnog primitka LDPU-a nije uspjelo, vraća na 6. korak.
Slikovni opis protokola transakcije prikazan je na slici 14.6.
Slika 14.6.
Tok postupka RTM-a putem DSRC-a na frekvenciji od 5,8 GHz



5.4.2 *Naredbe*

DSC_35 Sljedeće naredbe jedine su funkcije koje se upotrebljavaju u transakcijskoj fazi RTM-a.

—INITIALISATION.request : Naredba koju izdaje REDCR u obliku slanja s definicijom aplikacija koje podržava REDCR.

—INITIALISATION.response : Odgovor iz DSRC-VU-a kojim se potvrđuje veza i koji sadrži popis podržanih instanci aplikacija sa značajkama i informacijama o tome kako ih riješiti (EID).

—GET.request : Naredba, koju REDCR izdaje DSRC-VU-u, u kojoj se navode instance aplikacija koje treba riješiti putem utvrđenog EID-a, kako je primljeno u VST-u, i kojom se DSRC-VU-u nalaže da pošalje jedan ili više odabranih atributa s podacima. Cilj je naredbe GET da REDCR dobije podatke iz DSRC-VU-a.

—GET.response : Odgovor iz DSRC-VU-a koji sadrži zatražene podatke.

—ACTION.request ECHO : Naredba kojom se DSRC-VU-u nalaže da vrati podatke iz DSRC-VU-a REDCR-u. Cilj je naredbe ECHO omogućiti radionicama ili uređajima za homologacijska ispitivanja da ispitaju radi li DSRC veza bez potrebe za pristupom sigurnosnim podacima.

—ACTION.response ECHO : Odgovor iz DSRC-VU-a na naredbu ECHO.

—EVENT_REPORT.request RELEASE : Naredba kojom se DSRC-VU-u nalaže prekid transakcije. Cilj naredbe RELEASE prekid je razmjene podataka s DSRC-VU-om. Nakon primitka naredbe RELEASE, DSRC-VU ne smije odgovoriti na daljnja ispitivanja u sklopu trenutne veze. Imajte na umu da se, u skladu s normom EN 12834, DSRC-VU neće dvaput povezati s istim REDCR-om osim u slučaju da se nalazio izvan komunikacijskog područja tokom perioda od 255 sekundi ili u slučaju da je identifikator radiofara REDCR-a promijenjen.

5.4.3 *Slijed naredbi za ispitivanje*

DSC_36 S gledišta slijeda naredbi i odgovora, transakcija je opisana kako slijedi:

Slijed	Pošiljatelj		Primatelj	Opis	Radnja
1	REDCR	>	DSRC-VU	Inicijalizacija komunikacijske veze – zahtjev	REDCR šalje BST
2	*DSRC-VU*	>	*REDCR*	*Inicijalizacija komunikacijske veze – odgovor*	*Ako BST podržava vrijednost AID = 2, DSRC-VU šalje zahtjev za privatni prozor.*
3	REDCR	>	DSRC-VU	Dodjeljuje privatni prozor.	Šalje okvir koji sadrži dodjelu privatnog prozora.
4	*DSRC-VU*	>	*REDCR*	*Šalje VST.*	*Šalje okvir koji sadrži VST.*
5	REDCR	>	DSRC-VU	Šalje GET.request za podatke u atributu za određeni EID.	
6	*DSRC-VU*	>	*REDCR*	*Šalje GET.response sa zatraženim atributom za određeni EID.*	*Šalje atribut (RTMData, OWSData...) s podacima za određeni EID.*
7	REDCR	>	DSRC-VU	Šalje GET.request za podatke drugog atributa (prema potrebi).	
8	*DSRC-VU*	>	*REDCR*	*Šalje GET.response sa zatraženim atributom.*	*Šalje atribut s podacima za određeni EID.*
9	REDCR	>	DSRC-VU	Potvrđuje uspješan primitak podataka.	Šalje naredbu RELEASE koja zatvara transakciju.
10	*DSRC-VU*			*Zatvara transakciju.*	

Primjer slijeda transakcije i sadržaja razmijenjenih okvira utvrđen je u odjeljcima 5.4.7. i 5.4.8.

5.4.4 *Strukture podataka*

DSC_37 Semantička struktura podataka pri prolazu sučeljem DSRC-a na frekvenciji od 5,8 GHz u skladu je s opisom u ovom Dodatku. Način na koji su ti podaci strukturirani naveden je u ovoj tački.

DSC_38 Prenos (podaci RTM-a) sastoji se od ulančavanja

1. podataka EncryptedTachographPayload, što čini šifru TachographPayload kako je utvrđeno u modulu ASN.1 u odjeljku 5.4.5. Način šifriranja opisan je u Dodatku 11.

2. DSRCSecurityData naveden je u Dodatku 11.

DSC_39 Podaci RTM-a rješavaju se kao atribut RTM-a = 1 i prenose se u spremnik RTM-a = 10.

DSC_40 Kontekstualna oznaka RTM-a utvrđuje podržani dio norme u seriji normi TARV (RTM odgovara Dijelu 9.).

Definicija modula ASN.1 za podatke DSRC-a u okviru aplikacije RTM-a utvrđuje se kako slijedi:

```
TarvRtm {iso(1) standard(0) 15638 part8(8) version1(1)}
DEFINITIONS AUTOMATIC TAGS
::= BEGIN
IMPORTS
-- Imports data attributes and elements from EFC which are used for RTM
LPN
FROM EfcTarvApplication {iso(1) standard(0) 14906 application(0) version5(5)}

-- Imports function parameters from the EFC Application Interface Definition
SetRTMReq
FROM EfcTarvApplication {iso(1) standard(0) 14906 application(0) version5(5)}

-- Imports the IT DSRCData module data from the EFC Application Interface Definition
Action-Request, Action-Response, ActionType, ApplicationList, AttributeIdList, AttributeList,
Attributes,
BeaconID, EID, Dsrc-EID, DSRCApplicationEntityID, Event-Report-Request, Event-Report- Response,
EventType, Get-Request, Get-Response, Initialization-Request, Initialization-Response,
OBEConfiguration, Profile, ReturnStatus, Time, T-APDUs, VST
FROM EfcTarvGeneric {iso(1) standard(0) 14906 generic(1) version5(5)};


-- Definitions of the RTM functions:
RTM-InitialiseComm-Request ::= BST
RTM-InitialiseComm-Response::= VST
RTM-DataRetrieval-Request::= Get-Request (WITH COMPONENTS {fill (SIZE(1)), eid, accessCredentials ABSENT, lid
ABSENT, attrIdList})
RTM-DataRetrieval-Response::= Get-Response {RtmContainer} (WITH COMPONENTS {..., eid, lid ABSENT})
RTM-TerminateComm::= Event-Report-Request {RtmContainer}(WITH COMPONENTS {mode (FALSE), eid (0),
eventType (0)})

RTM-TestComm-Request::= Action-Request {RtmContainer} (WITH COMPONENTS {..., eid (0), actionType
(15), accessCredentials ABSENT, lid ABSENT})

RTM-TestComm-Response::= Action-Response {RtmContainer} (WITH COMPONENTS {..., fill (SIZE(1)), eid
(0), lid ABSENT})

-- Definitions of the RTM attributes:
RtmData ::= SEQUENCE {
     encryptedTachographPayload OCTET STRING (SIZE(47)) (CONSTRAINED BY { -- calculated encrypting
TachographPayload as per Appendix 12 --}),
     DSRCSecurityData OCTET STRING
     }
TachographPayload ::= SEQUENCE {
          tp1563fVehicleRegistrationPlate LPN - Vehicle Registration Plate as per EN 15509,
          tp1563fSpeedingEvent            BOOLEAN,  -- 1= Irregularities in speed (see Annex 1C)
          tp1563fDrivingWithoutValidCard  BOOLEAN,    -- 1= Invalid card usage (see Annex 1C)
          tp1563fDriverCard               BOOLEAN,-- 0= Indicates a valid driver card (see Annex 1C)
          tp1563fCardInsertion            BOOLEAN, -- 1= Card insertion while driving (see Annex 1C)
          tp1563fMotionDataError          BOOLEAN, -- 1= Motion data error (see Annex 1C)
          tp1563fVehicleMotionConflict    BOOLEAN, -- 1= Motion conflict (see Annex 1C)
          tp1563f2ndDriverCard            BOOLEAN, -- 1= Second driver card inserted (see Annex 1C)
          tp1563fCurrentActivityDriving   BOOLEAN, -- 1= other activity selected;
                                                   -- 0= driving selected
          tp1563fLastSessionClosed        BOOLEAN, -- 1= improperly, 0= properly, closed
          tp1563fPowerSupplyInterruption  INTEGER (0..127), -- Supply interrupts in the last 10 days
          tp1563fSensorFault              INTEGER (0..255),-- eventFaultType as per data dictionary
     -- All subsequent time related types as defined in Annex 1C:
          tp1563fTimeAdjustment           INTEGER(0..4294967295), -- Time of the last time adjustment
          tp1563fLatestBreachAttempt      INTEGER(0..4294967295), -- Time of last breach attempt
          tp1563fLastCalibrationData      INTEGER(0..4294967295), -- Time of last calibration data
          tp1563fPrevCalibrationData      INTEGER(0..4294967295), -- Time of previous calibration data
          tp1563fDateTechnoConnected      INTEGER(0..4294967295), -- Date technograph connected
          tp1563fCurrentSpeed             INTEGER (0..255), -- Last current recorded speed
          tp1563fTimestamp                INTEGER(0..4294967295) -- Timestamp of current record
          }
RtmContextMark ::= SEQUENCE {
  standardIdentifier    StandardIdentifier, --- identifier of the TARV part and its version

  RtmCommProfile          INTEGER {
                               C1 (1),
                               C2 (2)
                               } (0..255) DEFAULT 1

  }
RtmTransferAck ::= INTEGER {
                  OK (1),
                  NoM (2)
                  }(1..255)


---

(5) Ako LPN sadrži AlphabetIndicator.LatinAlphabetNo2 ili latinCyrillicAlphabet, posebni znakovi ponovno se mapiraju u jedinici za ispitivanje cesta za primjenu posebnih pravila u skladu s Prilogom E normi ISO/CEN 14 906,2.

StandardIdentifier ::= OBJECT IDENTIFIER
RtmContainer ::= CHOICE {
        integer                         [0]   INTEGER,
        bitstring                       [1]   BIT STRING,
        octetstring                     [2]   OCTET STRING (SIZE (0..127, ...)),
        universalString                 [3]   UniversalString,
        BeaconId                        [4]   BeaconID,
        t-apdu                          [5]   T-APDUs,
        dsrcApplicationEntityId         [6]   DSRCApplicationEntityID,
        dsrc-Ase-Id                     [7]   Dsrc-EID,
        attrIdList                      [8]   AttributeIdList,
        attrList                        [9]   AttributeList{RtmContainer},
        rtmData                         [10]  RtmData,
        rtmContextmark                  [11]  Rtm-ContextMark,
        reserved12                      [12]  NULL,
        reserved13                      [13]  NULL,
        reserved14                      [14]  NULL,
        time                            [15]  Time,
-- values from 16 to 255 reserved for ISO/CEN usage
        }

END
```

5.4.5 ***Elementi RtmData, provedene radnje i definicije***

DSC_41 Vrijednosti podataka koje treba izračunati VU i koje se upotrebljavaju za ažuriranje zaštićenih podataka u DSRC-VU-u izračunavaju se u skladu s pravilima utvrđenima u tablici 14.3.:

Tablica 14.3.

Elementi RtmData, provedene radnje i definicije

(1) Element podataka RTM-a	**(2) Radnja koju sprovodi VU**		**(3) Definicija podataka u skladu s modulom ASN.1**
RTM1 Registarska pločica vozila	VU postavlja vrijednost *tp15638VehicleRegistrationPlate* podatkovnog elementa RTM1 iz zabilježene vrijednosti vrste podatka VehicleRegistrationIdentification kako je utvrđeno u Dodatku 1. *VehicleRegistrationIdentification*	Registarska pločica vozila u obliku skupine znakova	tp15638VehicleRegistrati onPlate IA5, --Registarska pločica vozila uvezena iz ZAO 14906 s ograničenjem iz EN 15509, koja je SLIJEDI koji sadržava oznaka države nakon koje slijede abecedna oznaka i broj registarske pločice, koji je uvijek u obliku 14 okteta (nadopunjenih nulama) tako da je duljina tipa EN 15509 IA5 uvijek 17 okteta, od kojih 14 predstavlja "pravu" broj registarske pločice.
RTM2 Događaj prekoračenja brzine	VU generiše Booleovu vrijednost za varijablu podatkovnog elementa RTM2 tp15638SpeedingEvent. Vrijednost tp15638SpeedingEvent izračunava se s pomoću VU-a iz broja varijabli speedingEvents zabilježenih u VU-u u zadnjih 10 dana pojave kako je utvrđeno u Prilogu I.C. Ako postoji najmanje jedna varijabla tp15638SpeedingEvent zadnjih 10 dana pojave, vrijednost varijable tp15638SpeedingEvent postavlja se na TAČNO (TRUE). ILI ako nije bilo nikakvih događaja u zadnjih 10 dana pojave, vrijednost varijable tp15638SpeedingEvent postavlja se na NETAČNO (FALSE).	1 (TAČNO) – označava nepravilnosti u brzini u zadnjih 10 dana pojave	tp15638SpeedingEvent BOOLEAN,
RTM3 Vožnja bez važeće kartice	VU generiše Booleovu vrijednost za varijablu podatkovnog elementa RTM3 tp15638DrivingWithoutValidCard. VU dodjeljuje vrijednost TAČNO varijabli tp15638DrivingWithoutValidCard ako je u podacima VU-a zabilježen najmanje jedan događaj u zadnjih 10 dana pojave vrste događaja „vožnja bez odgovarajuće kartice" kako je utvrđeno u Prilogu I.C. ILI ako nije bilo nikakvih događaja u zadnjih 10 dana pojave, vrijednost varijable tp15638DrivingWithoutValidCard postavlja se na NETAČNO.	1 (TAČNO) = označava nevažeću upotrebu kartice	tp15638DrivingWithoutVa lidCard BOOLEAN,
RTM4 Važeća kartica vozača	VU generiše Booleovu vrijednost za varijablu podatkovnog elementa RTM4 tp15638DriverCard na temelju podataka arhivirani u VU-u i utvrđenih u Dodatku 1. Ako nije prisutna važeća kartica vozača, VU postavlja varijablu na TAČNO. ILI ako je važeća kartica vozača prisutna, VU postavlja varijablu na NETAČNO.	0 (NETAČNO) = označava važeću karticu vozača	tp15638DriverCard BOOLEAN,
RTM5 Umetanje kartice tokom vožnje	VU generiše Booleovu vrijednost za podatkovni element RTM5. VU dodjeljuje vrijednost TAČNO varijabli tp15638CardInsertion ako je u podacima VU-a u zadnjih 10 dana pojave zabilježena najmanje jedna vrsta događaja „umetanje kartice tokom vožnje" kako je utvrđeno u Prilogu I.C. ILI ako nije bilo nikakvih događaja u posljednjih 10 dana pojave, vrijednost varijable tp15638CardInsertion postavlja se na NETAČNO.	1 (TAČNO) = označava umetanje kartice tokom vožnje u zadnjih 10 dana pojave	tp15638CardInsertion BOOLEAN,
RTM6 Pogreška u podacima o	VU generiše Booleovu vrijednost za podatkovni element RTM6. VU dodjeljuje vrijednost TAČNO varijabli	1 (TAČNO) = označava pogrešku u podacima o	tp15638MotionDataError BOOLEAN,

kretanju	tp15638MotionDataError ako je u podacima VU-a u zadnjih 10 dana pojave zabilježena najmanje jedna vrsta događaja „pogreška u podacima o kretanju" kako je utvrđeno u Prilogu I.C. ILI ako nije bilo nikakvih događaja u posljednjih 10 dana pojave, vrijednost varijable tp15638MotionDataError postavlja se na NETAČNO.	kretanju u zadnjih 10 dana pojave.	
RTM7 Konflikt u kretanju vozila	VU generiše Booleovu vrijednost za podatkovni element RTM7. VU dodjeljuje vrijednost TAČNO varijabli tp15638vehicleMotionConflict ako je u podacima VU-a zabilježen najmanje jedan događaj u zadnjih 10 dana pojave vrste događaja „konflikt u kretanju vozila" (vrijednost '0A'H). ILI ako nije bilo nikakvih događaja u posljednjih 10 dana pojave, vrijednost varijable tp15638vehicleMotionConflict postavlja se na NETAČNO.	1 (TAČNO) = označava konflikt u kretanju u zadnjih 10 dana pojave.	tp15638VehicleMotionCon flict BOOLEAN,
RTM8 Druga kartica vozača	VU generiše Booleovu vrijednost za podatkovni element RTM8 na temelju Priloga I.C („podaci o aktivnosti vozača", POSADA i SUVOZAČ). Ako je druga važećia kartica vozača prisutna, VU postavlja varijablu na TAČNO. ILI ako druga važećia kartica vozača nije prisutna, VU postavlja varijablu na NETAČNO.	1 (TAČNO) = označava umetnutu drugu karticu vozača	tp15638SecondDriverCard BOOLEAN,
RTM9 Trenutna aktivnost	VU generiše Booleovu vrijednost za podatkovni element RTM9. Ako je trenutna aktivnost zabilježena u VU-u kao bilo koja aktivnost osim „VOŽNJE", kako je utvrđeno u Prilogu I.C, VU postavlja varijablu na TAČNO. ILI ako je trenutna aktivnost zabilježena u VU-u kao „VOŽNJA", VU postavlja varijablu na NETAČNO.	1 (TAČNO) = odabrana druga aktivnost; 0 (NETAČNO) = odabrana vožnja	tp15638currentActivityD riving BOOLEAN
RTM10 Posljednja razmjena podataka zatvorena	VU generiše Booleovu vrijednost za podatkovni element RTM10. Ako posljednja razmjena podataka kartice nije ispravno zatvorena, kako je utvrđeno u Prilogu I.C, VU postavlja varijablu na TAČNO. ILI ako je posljednja razmjena podataka kartice ispravno zatvorena, VU postavlja varijablu na NETAČNO.	1 (TAČNO) = neispravno zatvorena 0 (NETAČNO) = ispravno zatvorena	tp15638lastSessionClose d BOOLEAN
RTM11 Prekid napajanja	VU generiše vrijednost u obliku cijelog broja za podatkovni element RTM11. VU dodjeljuje vrijednost za varijablu tp15638PowerSupplyInterruption jednaku najdužem razdoblju prekida napajanja u skladu s člankom 9. Uredbe (EU) br. 165/2014 vrste događaja „prekid napajanja" kako je utvrđeno u Prilogu 1.C. ILI ako u posljednjih 10 dana pojave nije bilo nikakvih događaja prekida napajanja, vrijednost u obliku cijelog broja postavlja se na 0.	— broj prekida napajanja u zadnjih 10 dana pojave	tp15638powerSupplyInter ruption INTEGER (0..127),
RTM12 Kvar senzora	VU generiše vrijednost u obliku cijelog broja za podatkovni element RTM12. VU dodjeljuje varijabli sensorFault vrijednost: — 1 ako je događaj vrste '35H' „kvar senzora" zabilježen u zadnjih 10 dana; — 2 ako je događaj vrste „kvar prijamnika GNSS-a" (unutarnjeg ili vanjskog s rednim brojem '36'H ili '37'H) zabilježen u zadnjih 10 dana; — 3 ako je događaj vrste '0E'H „greška u komunikaciji s vanjskim uređajem GNSS-a" zabilježen u zadnjih 10 dana; — 4 ako su „kvar senzora" i „kvar prijemnika GNSS-a" zabilježeni u zadnjih 10 dana; — 5 ako su i „kvar senzora" i „greška u komunikaciji s vanjskim uređajem GNSS-a" zabilježeni u zadnjih 10 dana; — 6 ako su događaji „kvar prijemnika GNSS-a" i „greška u komunikaciji s vanjskim uređajem GNSS-a" zabilježeni u zadnjih 10 dana; — 7 ako su sva tri kvara senzora zabilježena u zadnjih 10 dana ILI dodjeljuje vrijednost 0 ako ni jedan od tih događaja nije zabilježen u zadnjih 10 dana.	– kvar senzora od jednog okteta u skladu s rječnikom s podacima	sensor[redacted] INTEGER (0..255),
RTM13 Prilagodba vremena	VU generiše vrijednost u obliku cijelog broja (timeReal iz Dodatka 1.) za podatkovni element RTM13 na temelju prisutnosti podataka o prilagodbi vremena kako je utvrđeno u Prilogu I.C.	Vrijeme posljednje prilagodbe	tp15638TimeAdjustment INTEGER(0..4294967295),

	VU dodjeljuje vrijednost vremena u kojem se odvio posljednji događaj prilagodbe vremena podataka. ILI ako u podacima VU-a nije prisutan nijedan događaj „prilagodbe vremena" kako je utvrđeno u Prilogu I.C, VU postavlja vrijednost 0.		
RTM14 Pokušaj povrede sigurnosti	VU generiše vrijednost u obliku cijelog broja (timeReal iz Dodatka 1.) za podatkovni element RTM14 na temelju prisutnosti događaja „pokušaj povrede sigurnosti" kako je utvrđeno u Prilogu I.C. VU postavlja vrijednost vremena posljednjeg događaja pokušaja povrede sigurnosti zabilježenog u VU-u. ILI ako u podacima VU-a nije prisutan nijedan događaj „pokušaj povrede sigurnosti" kako je utvrđeno u Prilogu I.C, VU postavlja vrijednost 0x00FF.	Vrijeme posljednjeg pokušaja povrede — Zadana vrijednost = 0x00FF	tp15638LatestBreachAtte mpt INTEGER(0..4294967295),
RTM15 Posljednja kalibracija	VU generiše vrijednost u obliku cijelog broja (timeReal iz Dodatka 1.) za podatkovni element RTM15 na temelju prisutnosti podataka o posljednjoj kalibraciji kako je utvrđeno u Prilogu I.C. VU postavlja vrijednost vremena posljednjih dviju kalibracija (RTM15 i RTM16) koje su postavljene u podacima VuCalibrationData utvrđenima u Dodatku 1. VU postavlja vrijednost za RTM15 na timeReal posljednjeg zapisa kalibracije.	Vrijeme podataka posljednje kalibracije	tp15638LastCalibrationD ata INTEGER(0..4294967295),
RTM16 Prethodna kalibracija	VU generiše vrijednost u obliku cijelog broja (timeReal iz Dodatka 1.) za podatkovni element RTM16 za zapis kalibracije koja je prethodila zapisu posljednje kalibracije. ILI ako nije bilo prethodne kalibracije, VU postavlja vrijednost RTM16 na 0.	Vrijeme podataka prethodne kalibracije	tp15638PrevCalibrationD ata INTEGER(0..4294967295),
RTM17 Datum povezivanja tahografa	Za podatkovni element RTM17 VU generiše vrijednost u obliku cijelog broja (timeReal iz Dodatka 1.). VU postavlja vrijednost vremena prve ugradnje VU-a. VU izdvaja ove podatke iz VuCalibrationData (Dodatak 1.) iz vuCalibrationRecords uz CalibrationPurpose koja je jednaka: '03'H	Vrijeme povezivanja tahografa	tp15638DateTachoConnect ed INTEGER(0..4294967295),
RTM18 Trenutna brzina	VU generiše vrijednost u obliku cijelog broja za podatkovni element RTM18. VU postavlja vrijednost za RTM16 na posljednju trenutačnu zabilježenu brzinu u trenutku posljednjeg ažuriranja RtmData.	Posljednja trenutna zabilježena brzina	tp15638CurrentSpeed INTEGER (0..255),
RTM19 Vremenska oznaka	Za podatkovni element RTM19 VU generiše vrijednost u obliku cijelog broja (timeReal iz Dodatka 1.). VU postavlja vrijednost za RTM19 na vrijeme posljednjeg ažuriranja RtmData.	Vremenska oznaka trenutačnog zapisa TachographPayload	tp15638Timestamp INTEGER(0..4294967295),

5.4.6 *Mehanizam prenosa podataka*

DSC_42 REDCR zahtijeva prethodno utvrđene prenesene podatke nakon faze inicijalizacije, a zatim ih prenosi putem DSRC-VU-a u dodijeljeni prozor. REDCR upotrebljava naredbu GET za dohvaćanje podataka.

DSC_43 Za sve razmjene u DSRC-u podaci se kodiraju primjenom PER-a (pravila paketnog šifriranja, eng. Packed Encoding Rules) UNALIGNED, osim podataka TachographPayload i CurrentSpeed, koji se kodiraju primjenom OER-a (pravila oktetnog šifriranja, eng. Octet Encoding Rules) utvrđenog normom ISO/IEC 8825-7, Preporukom ITU-T za X.696.

5.4.7 *Detaljni opis transakcija u okviru DSRC-a*

DSC_44 Inicijalizacija se sprovodi prema DSC_44 do DSC_48 i tablicama 14.4. do 14.9. U fazi inicijalizacije REDCR počinje slati okvir koji sadrži BST (tablicu usluga radiofara, eng. *Beacon Service Table*) u skladu s normama EN 12834 i EN 13372, tačkama 6.2., 6.3., 6.4. i 7.1., uz postavke kako su navedene u tablici 14.4.

Tablica 14.4

Inicijalizacija – postavke okvira BST-a

Polje	Postavke
Link Identifier	Adresa slanja
BeaconId	U skladu s normom EN 12834
Time	U skladu s normom EN 12834
Profile	Nema proširenja, upotrebljavati 0 ili 1
MandApplications	Nema proširenja, EID nije prisutan, parametar nije prisutan, AID = 2 Freight&Fleet
NonMandApplications	Nije prisutno
ProfileList	Nema proširenja, broj profila na popisu = 0
Fragmentation header	Nema fragmentiranja
Layer 2 settings	Naredba PDU-a, naredba UI-a

Praktični primjer postavki utvrđenih u tablici 14.4. uz oznaku kodiranja bitova naveden je u tablici 14.5. u nastavu.

Tablica 14.5.

Inicijalizacija – primjer sadržaja okvira BST-a

Oktet #	Atribut/polje	Bitovi u oktetima	Opis

1	FLAG		Oznaka početka
2	Broadcast ID		Adresa slanja
3	MAC Control Field		Naredba PDU-a
4	LLC Control field		Naredba UI-a
5	Fragmentation header		Nema fragmentiranja
6	BST		Zahtjev za inicijalizaciju
	SEQUENCE {		
	OPTION indicator BeaconID SEQUENCE { ManufacturerId INTEGER (0..65535)		aplikacije NonMand nisu prisutne
			Identifikator proizvođača
7			
8			
9	IndividualID INTEGER (0..134217727) }		27-bitni identifikator dostupan za proizvođača
10			
11			
12	Time INTEGER (0..4294967295)		Realno vrijeme 32-bitnog sistema UNIX
13			
14			
15			
16	Profile INTEGER (0..127,…)		Nema proširenja, primjer profila 0
17	MandApplications SEQUENCE (SIZE(0..127,…)) OF {		Nema proširenja, broj mandApplications = 1
18	SEQUENCE {		
	OPTION indicator		EID nije prisutan
	OPTION indicator		Parametar nije prisutan
	AID DSRCApplicationEntityID } }		Nema proširenja, AID = 2 Freight&Fleet
19	ProfileList SEQUENCE (0..127,…) OF Profile }		Nema proširenja, broj profila na popisu = 0
20	FCS		Slijed provjere okvira
21			
22	Flag		Oznaka završetka

DSC_45 DSRC-VU, nakon primanja BST-a, šalje zahtjev za dodjelu privatnog prozora kako je navedeno u normama EN 12795 i EN 13372 tački 7.1.1., bez posebnih postavki RTM-a. U tablici 14.6. nalazi se primjer kodiranja bitova.

Tablica 14.6.

Inicijalizacija – sadržaj okvira zahtjeva za dodjelu privatnog prozora

Oktet #	Atribut/polje	Bitovi u oktetima	Opis
1	FLAG		Oznaka početka
2	Private LID		Adresa veze određenog DSRC-VU-a
3			
4			
5			
6	MAC Control field		Zahtjev za privatni prozor
7	FCS		Slijed provjere okvira
8			
9	Flag		Oznaka završetka

DSC_46 REDCR zatim odgovara dodjeljivanjem privatnog prozora, kako je navedeno u normama EN 12795 i EN 13372, tački 7.1.1., bez posebnih postavki RTM-a.

U tablici 14.7. nalazi se primjer kodiranja bitova.

Tablica 14.7.

Inicijalizacija – sadržaj okvira dodjele privatnog prozora

Oktet #	Atribut/polje	Bitovi u oktetima	Opis
1	FLAG		Oznaka početka
2	Private LID		Adresa veze određenog DSRC-VU-a
3			
4			
5			
6	MAC Control field		Dodjela privatnog prozora
7	FCS		Slijed provjere okvira
8			
9	Flag		Oznaka završetka

DSC_47 DSRC-VU, nakon primanja dodjele privatnog prozora, šalje svoj VST (tablicu usluga vozila) kako je utvrđeno u normama EN 12834 i EN 13372, tačkama 6.2., 6.3., 6.4. i 7.1., uz postavke kako su navedene u tablici 14.8., upotrebom dodijeljenog prozora za prenos.

Tablica 14.8.
Inicijalizacija – postavke okvira VST-a

Polje	Postavke
Private LID	U skladu s normom EN 12834
VST parameters	Fill = 0, zatim za svaku podržanu aplikaciju: EID prisutan, parametar prisutan, AID = 2, EID kako ga je generisao OBU
Parameter	Nema proširenja, sadrži kontekstualnu oznaku RTM-a
ObeConfiguration	Opcionalno polje ObeStatus može biti prisutno, ali ga REDCR ne smije upotrebljavati.
Fragmentation header	Nema fragmentiranja
Layer 2 settings	Naredba PDU-a, naredba UI-a

DSC_48 DSRC-VU podržava aplikaciju za „Freight and Fleet" kako je utvrđena u okviru identifikatora aplikacije „2". Ostali identifikatori aplikacije mogu biti podržani, no ne smiju biti prisutni u ovom VST-u jer BST zahtijeva isključivo AID = 2. Polje „Aplikacije" sadrži popis podržanih instanci aplikacija u DSRC-VU-u. Za svaku podržanu instancu aplikacije navedeno je upućivanje na odgovarajuću normu, a čini je kontekstualna oznaka RTM-a koja se sastoji od IDENTIFIKATORA OBJEKATA (OBJECT IDENTIFIER) koji predstavlja povezanu normu, njezina dijela (Dijela 9. za RTM) i po mogućnosti njezine verzije te EID-a koji generiše DSRC-VU, a povezan je s tom instancom aplikacije.
Praktični primjer postavki utvrđenih u tablici 14.8. uz oznaku kodiranja bitova naveden je u tablici 14.9.

Tablica 14.9.
Inicijalizacija – primjer sadržaja okvira VST-a

Oktet #	Atribut/polje	Bitovi u oktetima	Opis
1	FLAG		Oznaka početka
2	Private LID		Adresa veze određenog DSRC-VU-a
3			
4			
5			
6	MAC Control field		Naredba PDU-a
7	LLC Control field		Naredba UI-a
8	Fragmentation header		Nema fragmentiranja
9	VST SEQUENCE {		Odgovor inicijalizacije
	Fill BIT STRING (SIZE(4))		Neupotrijebljeno i postavljeno na 0
10	Profile		Nema proširenja, primjer profila 0
11	INTEGER (0..127,...) Applications SEQUENCE OF {		Nema proširenja, 1 aplikacija
12	SEQUENCE {		
	OPTION indicator		EID prisutan
	OPTION indicator		Parametar prisutan
	AID DSRCApplicationEntityID		Nema proširenja, AID = 2 Freight&Fleet
13	EID Dsrc-EID		Utvrđen u okviru OBU-a i utvrđuje instancu aplikacije.
14	Parameter Container {		Nema proširenja, odabir spremnika = 02, niz okteta
15			Nema proširenja, dužina kontekstualne oznake RTM-a = 8
16	Rtm-ContextMark::=		Identifikator objekata podržane norme, dio i verzija. Primjer: ISO (1) norma (0) TARV (15638) Dio9. (9) verzija1. (1). Prvi je oktet 06H koji čini identifikator objekata. Drugi je oktet 06H koji čini njegovu dužinu. Sljedećih šest okteta kodira primjer identifikatora objekta.
17	SEQUENCE {		
18	StandardIdentifier		
19	standardIdentifier		
20			
21			
22			
23			
24	ObeConfiguration Sequence {		
	OPTION indicator		ObeStatus nije prisutan
	EquipmentClass		
25	INTEGER (0..32767)		
26	ManufacturerId		Identifikator proizvođača za DSRC-VU kako je opisano u registru normi ISO 14816
27	INTEGER (0..65535)		
28	FCS		Slijed provjere okvira
29			
30	Flag		Oznaka završetka

DCS_49 REDCR zatim očitava podatke izdavanjem naredbe GET, u skladu s naredbom GET utvrđenom u normi EN 13372, tačkama 6.2., 6.3., 6.4., i u normi EN 12834, uz postavke kako su navedene u tablici 14.10.

Tablica 14.10.
Iznošenje – postavke okvira za GET.request

Polje	Postavke
Invoker Identifier (IID)	Nije prisutno
Link Identifier (LID)	Adresa veze određenog DSRC-VU-a
Chaining	Nema
Element Identifier (EID)	Kako je navedeno u VST-u. Nema proširenja.
Access Credentials	Nema
AttributeIdList	Nema proširenja, 1 atribut, AttributeID = 1 (RtmData)
Fragmentation	Nema
Layer2 settings	Naredba PDU-a, provjerena naredba ACn

U tablici 14.11. prikazan je primjer očitavanja podataka RTM-a.

Tablica 14.11.

Iznošenje – primjer okvira za GET.request

Oktet #	Atribut/polje	Bitovi u oktetima	Opis
1	FLAG		Oznaka početka
2	Private LID		Adresa veze određenog DSRC-VU-a
3			
4			
5			
6	MAC Control field		Naredba PDU-a
7	LLC Control field		Provjerena naredba ACn, n bitova
8	Fragmentation header		Nema fragmentiranja
9	GET.request SEQUENCE {		GET.request
	OPTION indicator		Pristupni podaci nisu prisutni
	OPTION indicator		IID nije prisutan
	OPTION indicator		AttributeIdList prisutan
	Fill BIT STRING(SIZE(1))		Postavljeno na 0.
10	EID INTEGER(0..127,…)		EID instance aplikacije RTM-a kako je navedeno u VST-u. Nema proširenja.
11	AttributeIdList SEQUENCE		Nema proširenja, broj atributa = 1
12	OF { AttributeId }}		AttributeId=1, RtmData. Nema proširenja
13	FCS		Slijed provjere okvira
14			
15	Flag		Oznaka završetka

DSC_50 DSRC-VU, nakon primanja naredbe GET.request, šalje naredbu GET.response sa zatraženim podacima u skladu s naredbom GET.response utvrđenom u normi EN 13372 tačkama 6.2., 6.3., 6.4. i u normi EN 12834 uz postavke kako su navedene u tablici 14.12.

Tablica 14.12.

Iznošenje – postavke okvira za GET.response

Polje	Postavke
Invoker Identifier (IID)	Nije prisutno
Link Identifier (LID)	U skladu s normom EN 12834
Chaining	Nema
Element Identifier (EID)	Kako je navedeno u VST-u.
Access Credentials	Nema
Fragmentation	Nema
Layer2 settings	Odgovor PDU-a, odgovor dostupan i naredba prihvaćena, naredba ACn

U tablici 14.13. prikazan je primjer očitavanja podataka RTM-a.

Tablica 14.13.

Iznošenje – primjer sadržaja okvira odgovora

Oktet #	Atribut/polje	Bitovi u oktetima	Opis
1	FLAG		Oznaka početka
2	Private LID		Adresa veze određenog DSRC-VU-a
3			
4			
5			
6	MAC Control field		Odgovor PDU-a
7	LLC Control field		Odgovor dostupan, naredba ACn, n bitova
8	LLC Status field		Odgovor dostupan i naredba prihvaćena
9	Fragmentation header		Nema fragmentiranja
10	GET.response SEQUENCE {		GET.Response
	OPTION indicator		IID nije prisutan
	OPTION indicator		Popis atributa prisutan
	OPTION indicator		Uzvratni status nije prisutan

	Fill BIT STRING(SIZE(1))		Ne upotrebljava se
11	EID INTEGER(0..127,…)		Odgovor iz aplikacije RTM-a Instanca. Nema proširenja.
12	AttributeList SEQUENCE OF {		Nema proširenja, broj atributa = 1
13	Attributes SEQUENCE { AttributeId		Nema proširenja, AttributeID = 1 (RtmData)
14	AttributeValue CONTAINER {		Nema proširenja, odabir spremnika = 10_{10}.
15			RtmData
16			
17			
…		…	
n	}}}}		
n+1	FCS		Slijed provjere okvira
n+2			
n+3	Flag		Oznaka završetka

DSC_51 REDCR zatim zatvara vezu izdavanjem naredbe EVENT_REPORT, RELEASE u skladu s normom EN 13372, tačkama 6.2., 6.3., 6.4. i normom EN 12834, točkom 7.3.8., bez posebnih postavki RTM-a. U tablici 14.14. prikazan je primjer kodiranja bitova naredbe RELEASE:

Tablica 14.14.

Prekid. Sadržaj okvira naredbe EVENT_REPORT, RELEASE

Oktet #	Atribut/polje	Bitovi u oktetima	Opis
1	FLAG		Oznaka početka
2	Private LID		Adresa veze određenog DSRC-VU-a
3			
4			
5			
6	MAC Control field		Okvir sadrži naredbu LPDU.
7	LLC Control field		Naredba UI-a
8	Fragmentation header		Nema fragmentiranja.
9	EVENT_REPORT.request SEQUENCE {		EVENT_REPORT (Release)
	OPTION indicator		Pristupni podaci nisu prisutni.
	OPTION indicator		Parametar događaja nije prisutan.
	OPTION indicator		IID nije prisutan.
	Mode BOOLEAN		Ne očekuje se odgovor.
10	EID INTEGER (0..127,…)		Nema proširenja, EID = 0 (sistem)
11	EventType INTEGER (0..127,…) }		Vrsta događaja 0 = RELEASE
12	FCS		Slijed provjere okvira
13			
14	Flag		Oznaka završetka

DSC_52 Ne očekuje se odgovor DSRC-VU-a na naredbu RELEASE. Komunikacija se zatim zatvara.

5.4.8 *Opis ispitivanja transakcija u okviru DSRC-a*

DSC_53 Potpuna ispitivanja koja uključuju zaštitu podataka trebaju provesti, kako je utvrđeno u Dodatku 11., Zajednički sigurnosni mehanizmi, ovlaštene osobe s pristupom sigurnosnim postupcima upotrebom uobičajene naredbe GET kako je utvrđeno u prethodnom tekstu.

DSC_54 Puštanje u pogon i periodička ispitivanja koja zahtijevaju dešifriranje i razumijevanje dešifriranog sadržaja podataka provode se kako je navedeno u Dodatku 11., Zajednički sigurnosni mehanizmi, i Dodatku 9., Homologacija, Popis obveznih ispitivanja.

Međutim, temeljna komunikacija DSRC-a može se ispitati s pomoću naredbe ECHO. Takva ispitivanja mogu biti potrebna pri puštanju u pogon, pri periodičkom pregledu ili drugačije na zahtjev nadležnog nadzornog tijela ili u skladu s Uredbom (EU) br. 165/2014 (vidjeti odjeljak 6. u nastavu).

DSC_55 Kako bi se provelo ovo temeljno komunikacijsko ispitivanje, REDCR izdaje naredbu ECHO tokom razmjene podataka, odnosno nakon uspješnog dovršetka faze inicijalizacije. Slijed interakcija stoga je sličan slijedu ispitivanja:

—1. korakREDCR šalje „tablicu usluga radiofara" (BST) koja uključuje identifikatore aplikacije (AID-ove) na popis usluga koji podržava. U aplikacijama RTM-a to će jednostavno biti usluga s vrijednošću AID = 2.

DSRC-VU ocjenjuje primljeni BST i ako utvrdi da BST zahtijeva Freight&Fleet (AID = 2), DSRC-VU odgovara. Ako REDCR ne ponudi vrijednost AID = 2, DSRC-VU zaustavlja svoju transakciju s REDCR-om.

—2. korakDSRC-VU šalje zahtjev za dodjelu privatnog prozora.

—3. korakREDCR šalje dodjelu privatnog prozora.

—4. korakDSRC-VU upotrebljava dodijeljeni privatni prozor za slanje tablice usluga vozila (eng. Vehicle Service Table, VST). VST uključuje popis različitih instanci aplikacija koje DSRC-VU podržava u okviru vrijednosti AID =

2. Različite instance utvrđuju se s pomoću jedinstvenih EID-ova, a svaki je povezan s vrijednošću parametra koji označava instancu podržane aplikacije.
—5. korakZatim REDCR analizira ponuđeni VST i prekida vezu (RELEASE) jer mu nije potrebno ništa od onoga što nudi VST (odnosno prima VST iz DSRC-VU-a koji nije VU RTM-a, ili, u slučaju da primi odgovarajući VST, pokreće instancu uređaja.
—6. korakREDCR izdaje naredbu (ECHO) određenom DSRC-VU-u i dodjeljuje privatni prozor.
—7. korakDSRC-VU upotrebljava nedavno dodijeljeni privatni prozor za slanje okvira za odgovor ECHO.
U sljedećoj tablici nalazi se primjer razmjene podataka ECHO u praksi.
DSC_56 Inicijalizacija se sprovodi u skladu s odjeljkom 5.4.7. (DSC_44 do DSC_48) i tablicama 14.4. do 14.9.
DSC_57 REDCR zatim izdaje naredbu ACTION, ECHO u skladu s normom ISO 14906, koja sadrži 100 okteta podataka, ali ne sadrži posebne postavke za RTM. U tablici 14.15. prikazan je sadržaj okvira koji šalje REDCR.

Tablica 14.15.
Primjer okvira za ACTION, zahtjev ECHO

Oktet #	Atribut/polje	Bitovi u oktetima	Opis
1	FLAG		Oznaka početka
2	Private LID		Adresa veze određenog DSRC-VU-a
3			
4			
5			
6	MAC Control field		Naredba PDU-a
7	LLC Control field		Provjerena naredba ACn, n bitova
8	Fragmentation header		Nema fragmentiranja.
9	ACTION.request SEQUENCE {		Zahtjev za radnju (ECHO)
	OPTION indicator		Pristupni podaci nisu prisutni.
	OPTION indicator		Parametar radnje prisutan.
	OPTION indicator		IID nije prisutan.
	Mode BOOLEAN		Odgovor se očekuje.
10	EID INTEGER (0..127,...)		Nema proširenja, EID = 0 (sistem)
11	ActionType INTEGER (0..127,...)		Nema proširenja, zahtjev ECHO za vrstu radnje
12	ActionParameter CONTAINER {		Nema proširenja, odabir spremnika = 2
13			Nema proširenja, Dužina niza = 100 okteta
14			Podaci za koje se treba izvršiti naredba ECHO
…		…	
113	}}		
114	FCS		Slijed provjere okvira
115			
116	Flag		Oznaka završetka

DSC_58 DSRC-VU, nakon primanja zahtjeva ECHO, šalje odgovor ECHO od 100 okteta podataka odražavanjem primljene naredbe, u skladu s normom ISO 14906, bez posebnih postavki za RTM. U tablici 14.16. prikazan je primjer kodiranja na nivou bitova.

Tablica 14.16.
Primjer okvira za ACTION, odgovor ECHO

Oktet #	Atribut/polje	Bitovi u oktetima	Opis
1	FLAG		Oznaka početka
2	Private LID		Adresa veze određenog VU-a
3			
4			
5			
6	MAC Control field		Odgovor PDU-a
7	LLC Control field		Naredba ACn, n bitova
8	LLC status field		Odgovor dostupan.
9	Fragmentation header		Nema fragmentiranja.
10	ACTION.response SEQUENCE {		Odgovor RADNJE (ECHO)
	OPTION indicator		IID nije prisutan.
	OPTION indicator		Parametar odgovora prisutan.
	OPTION indicator		Uzvratni status nije prisutan.
	Fill BIT STRING (SIZE (1))		Ne upotrebljava se.
11	EID INTEGER (0..127,...)		Nema proširenja, EID = 0 (sistem)
12	ResponseParameter		Nema proširenja, odabir spremnika = 2
13	CONTAINER {		Nema proširenja, Dužina niza = 100 okteta

14		XXXX XXXX	Podaci za koje je izvršena naredba ECHO
…		…	
113	}}	XXXX XXXX	
114	FCS	XXXX XXXX	Slijed provjere okvira
115		XXXX XXXX	
116	Flag	[illegible]	Oznaka završetka

5.5 Potpora Direktivi (EU) 2015/719

5.5.1 ***Pregled***

DSC_59 Za potporu Direktivi (EU) 2015/719 o najvećim masama i dimenzijama za teška teretna vozila, protokol transakcije za preuzimanje podataka OWS-a putem veze sučelja DSRC-a na frekvenciji od 5,8 GHz bit će jednak protokolu koji se upotrebljava za podatke RTM-a (vidjeti 5.4.1), a jedina je razlika u tome što će identifikator objekta koji se odnosi na normu TARV upućivati na normu ISO 15638 (TARV) Dio 20. koji se odnosi na WOB/OWS.

5.5.2 ***Naredbe***

DSC_60 Naredbe koje se upotrebljavaju za transakciju OWS-a bit će jednake naredbama koje se upotrebljavaju za transakcije u okviru RTM-a.

5.5.3 ***Slijed naredbi za ispitivanje***

DSC_61 Slijed naredbi za ispitivanje za podatke OWS-a bit će jednak slijedu za podatke RTM-a.

5.5.4 ***Strukture podataka***

DSC_62 Korisni podaci (podaci OWS-a) sastoje se od ulančavanja

1. podataka EncryptedOwsPayload, što čini šifru OwsPayload kako je utvrđeno u modulu ASN-1 u odjeljku 5.5.5. Način šifriranja jednak je načinu donesenom za RtmData koji je naveden u Dodatku 11.,
2. podataka DSRCSecurityData, izračunano s pomoću jednakih algoritama kao i za RtmData, kako je navedeno u Dodatku 11.

5.5.5 ***Modul ASN.1 za transakcije OWS-a u okviru DSRC-a***

DSC_63. Definicija modula ASN.1 za podatke DSRC-a u okviru aplikacije RTM-a utvrđuje se kako slijedi:

5.5.6 ***Elementi OwsData, provedene radnje i definicije***

Elementi OwsData utvrđeni su radi potpore Direktivi (EU) 2015/719 o najvećim masama i dimenzijama za teška teretna vozila. Njihovo je značenje sljedeće:

— recordedWeight predstavlja ukupnu izmjerenu masu teškog teretnog vozila uz rezolucija od 10 kg kako je utvrđeno u normi EN ISO 14906. Primjerice, vrijednost od 2 500 predstavlja masu od 25 tona.

— axlesConfiguration predstavlja konfiguraciju teškog teretnog vozila u pogledu broja osovina. Konfigura cija se utvrđuje s pomoću maske bitova od 20 bitova (u skladu s normom EN ISO 14906).

— Maska bitova od 2 bita predstavlja konfiguraciju osovine sa sljedećim formatom:

— vrijednost 00B znači da je vrijednost „nedostupna” jer vozilo ne raspolaže opremom za preuzimanje mase na osovini;

— vrijednost 01B znači da osovina nije prisutna;

— vrijednost 10B znači da je osovina prisutna, a masa izračunata i preuzeta te navedena u polju axlesRecordedWeight;

— vrijednost 11B rezervisana je za buduće upotrebe.

— Posljednja su četiri bita rezervisana za buduće upotrebe.

Broj osovina										
Broj osovina na jedinici vozila			**Broj osovina na prikolici**							
00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	RFU (4 bita)

— axlesRecordedWeight predstavlja specifičnu masu za svaku osovinu uz rezolucija od 10 kg. Za svaku se osovinu upotrebljavaju dva okteta. Primjerice, vrijednost od 150 predstavlja masu od 1 500 Kg.
Ostale vrste podataka utvrđuju se u odjeljku 5.4.5.

5.5.7 *Mehanizmi prenosa podataka*

DSC_64 Mehanizam prenosa podataka za podatke OWS-a između REDCR-a i uređaja DSRC-a u vozilu jednak je mehanizmu za podatke RTM-a (vidjeti odjeljak 5.4.6).
DSC_65 Prenos podataka između platforme na kojoj se prikupljaju podaci o najvećim masama i uređaja DSRC-a u vozilu temelji se na fizičkoj vezi i sučeljima te protokolu utvrđenom u odjeljku 5.6.

5.6 Prenos podataka između DSRC-VU-a i VU-a

5.6.1 *Fizička veza i sučelja*

DSC_66 Veza između VU-a i DSRC-VU-a može se uspostaviti s pomoću fizičkog kabela ili putem bežične komunikacije kratkog dometa na temelju sistema Bluetooth v4.0 BLE.
DSC_67 Nezavisno o izboru fizičke veze i sučelja, potrebno je ispuniti sljedeće zahtjeve:
DSC_68
a) Kako bi se mogli angažirati različiti dobavljači za isporuku VU-a i DSRC-VU-a te različitih serija DSRC-VU-a, veza između VU-a i DSRC-VU-a koji nije unutar VU-a mora biti veza u okviru otvorene norme. VU se povezuje s DSRC-VU-om ◄
i) upotrebom fiksnog kabela od najmanje 2 metra, upotrebom ravnog priključka DIN 41612 H11, odobrenog 11-pinskog muškog priključka iz DSRC-VU-a koji odgovara ženskom priključku iz uređaja VU-a;
ii) upotrebom sistema Bluetooth niske razine energije (BLE);
iii) upotrebom priključka u skladu s normom ISO 11898 ili normom SAE J1939.
DSC_69
b) Definicija sučelja i veze između VU-a i DSRC-VU-a mora podržavati naredbe protokola aplikacije utvrđene u odjeljku 5.6.2. i
DSC_70
c) VU i DSRC-VU moraju podržavati rad prenosa podataka putem veze u pogledu učinkovitosti i napajanja.

5.6.2 *Protokol aplikacije*

DSC_71 Protokol aplikacije između uređaja jedinice u vozilu za komunikaciju na daljinu i DSRC-VU-a zadužen je za periodični prenos podataka komunikacijom na daljinu iz VU-a DSRC-u.
DSC_72 Utvrđuju se sljedeće glavne naredbe:
1. Inicijalizacija komunikacijske veze – zahtjev
2. Inicijalizacija komunikacijske veze – odgovor
3. Slanje podataka uz identifikator aplikacije RTM-a i prenos utvrđen u okviru podataka RTM-a
4. Potvrđivanje podataka
5. Prekid komunikacijske veze – zahtjev
6. Prekid komunikacijske veze – odgovor
DSC_73 U modulu ASN1.0, prethodne naredbe mogu se utvrditi kao:

DSC_74 Opis je naredbi i parametara sljedeći:
— RCDT-Communication Link Initialization - Request upotrebljava se za inicijalizaciju komunikacijske veze. VU šalje naredbu DSRC-VU-u. VU postavlja LinkIdentifier i prenosi ga DSRC-VU-u za pronalaženje određene komunikacijske veze.
(Napomena: to služi za potporu budućim vezama i ostalim aplikacijama/modulima kao što je vaganje u vozilu).
— RCDT-Communication Link Initialization - Response upotrebljava DSRC-VU za pružanje odgovora na zahtjev za inicijalizaciju komunikacijske veze. DSRC-VU šalje naredbu VU-u. Naredbom se pruža rezultat inicijalizacije kao odgovor = 1 (uspješno) ili = 0 (neuspješno).

DSC_75 Inicijalizacija komunikacijske veze sprovodi se isključivo nakon ugradnje, kalibracije i pokretanja motora / uključivanja VU-a.

— RCDT-Send Data upotrebljava VU za slanje potpisanih podataka RCDTData (odnosno podataka u okviru komunikacije na daljinu) DSRC-VU-u. Podaci će se slati svakih 60 sekundi. Parametar DataTransactionId utvrđuje određeni prenos podataka. Parametar LinkIdentifier također se upotrebljava kako bi se osiguralo da je odgovarajuća veza ispravna.

— RCDT-Data Acknowledgment šalje DSRC-VU kako bi pružio povraćajne informacije VU-u nakon primitka podataka s pomoću naredbe RCDT-Send Data koju utvrđuje parametar DataTransactionId. Parametar odgovora iznosi 1 (uspješno) ili 0 (neuspješno). Ako VU primi više od tri odgovora koji su jednaki 0 ili ako VU ne primi potvrdu podataka RCDT-a za određene prethodno poslane podatke RCDT s određenim parametrom DataTransactionId, VU će generišeti i zabilježiti događaj.

— RCDT-Communication Link Termination request request šalje VU DSRC-VU-u za prekid veze za određeni LinkIdentifier.

DSC_76 Pri ponovnom pokretanju DSRC-VU-a ili VU-a treba ukloniti sve postojeće komunikacijske veze jer bi moglo biti „zaostalih" veza zbog iznenadna isključenja VU-a.

— RCDT-Communication Link Termination - Response šalje DSRC-VU VU-u za potvrđivanje zahtjeva za prekid veze za određeni LinkIdentifier koji vrši VU.

5.7 Rješavanje pogrešaka

5.7.1 *Bilježenje i prenos podataka u okviru DSRC-VU-a*

DSC_77 Podaci se u već zaštićenom obliku pružaju *DSRC-VU-u* u okviru funkcije *VUSM-a. VUSM* provjerava jesu li podaci zabilježeni u *DSRC-VU-u* zabilježeni na ispravan način. Zapisi i izvješća o pogreškama prenosa podataka iz *VU-a* u memoriju *DSRC-VU-a* bilježe se vrstom EventFaultType i rednim brojem postavljenim na događaj '0C'H „greška u komunikaciji s uređajem za komunikaciju na daljinu" zajedno s oznakom vremena.

DSC_78 VU zadržava datoteku utvrđenu jedinstvenim nazivom koji se lako može utvrditi provjerom u svrhu bilježenja „grešaka unutarnje komunikacije VU-a".

DSC_79 Ako VUPM pokuša dobiti podatke VU-a iz sigurnosnog modula (kako bi ih poslao VU-DSRC-u), a u tome ne uspije, tu pogrešku bilježi tipom EventFaultType i rednim brojem postavljenim na pogrešku komunikacije '62'H Remote Communication Facility zajedno s oznakom vremena. Greška komunikacije otkriva se ako se za taj događaj ne primi poruka RCDT Data Acknowledgment (odnosno, uz iste poruke za DataTransactionId in the In the Send Data and Acknowledgment) [illegible] više od tri puta zaredom.

5.7.2 *Pogreške bežične komunikacije*

DSC_80 Rješavanje pogrešaka komunikacije u skladu je s povezanim normama za DSRC, odnosno EN 300 674-1, EN 12253, EN 12795, EN 12834 i odgovarajućim parametrima norme EN 13372.

5.7.2.1 *Pogreške šifriranja i potpisa*

DSC_81 Pogreške šifriranja i potpisa rješavaju se kako je utvrđeno u Dodatku 11., Zajednički sigurnosni mehanizmi, te nisu prisutne u bilo kojoj od poruka o pogreškama povezanima s prenosom podataka u okviru DSRC-a.

5.7.2.2 *Bilježenje pogrešaka*

Medij DSRC dinamična je bežična komunikacija u okruženju neizvjesnih atmosferskih uvjeta i uvjeta interferencija, osobito u kombinacijama „prenosnog REDCR-a" i „vozila u pokretu" uključenima u ovu aplikaciju. Stoga je potrebno utvrditi razliku između „greške očitavanja" i stanja „pogreške". U transakciji putem bežičnog sučelja greška očitavanja uobičajena je, a posljedica je obično ponovni pokušaj odnosno ponovno slanje BST-a ili ponovni pokušaj slijeda koji će u većini okolnosti dovesti do uspješnog uspostavljanja veze u komunikaciji i prenosa podataka, osim ako se ciljano vozilo kreće izvan dometa tokom vremena potrebnog za ponovni prenos. („Uspješna" instanca „očitavanja" može uključivati nekoliko ponovnih pokušaja.)

Do greške očitavanja može doći zbog neispravnog uparivanja antena (pogreška „ciljanja") jer je jedna antena zaštićena. To može biti namjerno, no može biti i uzrokovano fizičkom prisutnošću drugog vozila, interferencijama u radiokomunikaciji, osobito na frekvenciji bežične mreže od oko 5,8 GHz ili drugim bežičnim komunikacijama s javnim pristupom, ili može biti uzrokovano radarskim interferencijama ili teškim atmosferskim uslovima (npr. tokom oluje), ili pak jednostavno kretanjem izvan dometa komunikacije DSRC-a. Pojedinačne instance grešaka očitavanja zbog svoje se naravi ne mogu zabilježiti, jednostavno jer do komunikacije u opšte nije došlo.

Međutim, ako djelatnik nadležnog nadzornog tijela cilja vozilo i pokuša ispitati njegov DSRC-VU, ali ne uslijedi uspješan prenos podataka, do greške je moglo doći zbog namjernog neovlaštenog rukovanja i stoga su djelatniku nadležnog nadzornog tijela potrebna sredstva za bilježenje greške i upozoravanje suradnika o mogućem kršenju. Suradnici tada mogu zaustaviti vozilo i provesti fizički pregled. Međutim, s obzirom na to da nije uspostavljena uspješna komunikacija, DSRC-VU ne može poslati podatke o grešci. Takvo je je izvješćivanje stoga funkcija izvedbe opreme REDCR-a.

„Greška očitavanja" s tehničkog se gledišta razlikuje od „pogreške". U ovom kontekstu „pogrešku" čini dobivanje pogrešne vrijednosti.

Podaci preneseni u DSRC-VU dostavljaju se u već zaštićenom obliku, stoga ih mora provjeriti dostavljač podataka (vidjeti odjeljak 5.4).

Podaci koji se potom prenose putem zračnog sučelja provjeravaju se kružnim provjerama zalihosti na komunikacijskoj nivou. Ako ih CRC potvrdi, podaci su ispravni. Ako ih CRC ne potvrdi, podaci se ponovno prenose. Vjerojatnost da neispravni podaci mogu uspješno proći CRC-om statistički je toliko malena da se može zanemariti.

Ako CRC ne potvrdi podatke te nema dovoljno vremena za ponovni prenos i primitak ispravnih podataka, rezultat neće biti pogreška nego instanca određenog tipa pogreške očitavanja.
Jedina značajna „pogreška" podataka koja se može zabilježiti pogreška je broja uspješnih inicijalizacija transakcija koje se dogode i koje ne rezultiraju uspješnim prenosom podataka u REDCR.
DSC_82 REDCR stoga bilježi, uz vremensku oznaku, broj slučajeva u kojima je faza „inicijalizacije" ispitivanja funkcije DSRC-a uspješna, ali je transakcija prekinuta prije nego što je REDCR uspješno dohvatio podatke. Ti podaci dostupni su djelatniku nadležnog nadzornog tijela i arhiviraju se u memoriju opreme REDCR-a. Način na koji se to postiže pitanje je izvedbe proizvoda ili specifikacije nadležnog nadzornog tijela.
Jedina značajna „pogreška" podataka koja se može zabilježiti broj je slučajeva u kojima REDCR ne uspije dešifrirati primljene podatke. Međutim, treba napomenuti da će se to odnositi isključivo na učinkovitost softvera REDCR-a. Podatke je moguće dešifrirati s tehničkog gledišta, no sa semantičkog gledišta oni nisu smisleni.
DSC_83 REDCR stoga bilježi, uz vremensku oznaku, broj slučajeva u kojima je pokušao dešifrirati podatke primljene putem sučelja DSRC-a, ali u tome nije uspio.

6 PUŠTANJE U POGON I PERIODIČKA ISPITIVANJA PREGLEDA ZA FUNKCIJU KOMUNIKACIJE NA DALJINU

6.1 Opšte karakteristike

DSC_84 Predviđene su dvije vrste ispitivanja za funkciju komunikacije na daljinu:
1) ispitivanje ECHO za potvrđivanje komunikacijskog kanala DSRC-REDCR >>-:-<bežični DSRC-VU;
2) cjelovito sigurnosno ispitivanje kojim se osigurava da se s pomoću kartice radionice može pristupiti šifriranom i potpisanom sadržaju podataka koje je stvorio VU i koji su preneseni bežičnim komunikacijskim kanalom.

6.2 ECHO

U ovoj se tački nalaze odredbe posebno namijenjene ispitivanju funkcionalne aktivnosti za DSRC-REDCR >>-:-<DSRC-VU.
Cilj je naredbe ECHO omogućiti radionicama ili uređajima za homologacijsko ispitivanje da ispitaju radi li DSRC veza bez potrebe za pristupom sigurnosnim podacima. Oprema ispitivača stoga mora biti sposobna pokrenuti komunikaciju DSRC-a (slanjem BST-a uz vrijednost AID = 2), a zatim poslati naredbu ECHO te će, ako DSRC ispravno radi, primiti odgovor ECHO. Više pojedinosti možete pronaći u odjeljku 5.4.8. Ako veza DSRC-a odgovor primi na ispravan način, može se potvrditi njezin ispravan rad (DSRC-REDCR >>-:-<DSRC-VU).

6.3 Ispitivanja za potvrđivanje sigurnog sadržaja podataka

DSC_85 Ovo se ispitivanje sprovodi za potvrđivanje cjelovitog sigurnosnog protoka podataka. Za takvo je ispitivanje potreban čitač za ispitivanje u okviru DSRC-a. Čitač za ispitivanje u okviru DSRC-a ima istu funkciju i ugrađuje se s jednakim specifikacijama kao i čitač koji upotrebljavaju nadležna tijela, uz tu razliku da se kartica radionice upotrebljava za autentifikaciju korisnika čitača za ispitivanje DSRC-a umjesto kontrolne kartice. Ispitivanje se može provesti nakon početne aktivacije pametnog tahografa ili na kraju postupka kalibracije. Nakon aktivacije jedinica u vozilu generiše i prenosi DSRC-VU-u zaštićene podatke za rano otkrivanje.
DSC_86 Osoblje radionice mora postaviti čitač za ispitivanje DSRC-a na udaljenost između 2 i 10 metara ispred vozila.
DSC_87 Zatim će osoblje radionice umetnuti karticu radionice u čitač za ispitivanje u okviru DSRC-a kako bi zatražilo ispitivanje ranog otkrivanja podataka u jedinici u vozilu. Nakon uspješnog ispitivanja osoblje radionice pristupit će primljenim podacima kako bi osigurali da je njihov integritet uspješno potvrđen i da su uspješno dešifrirani.

Dodatak 15.

MIGRACIJA: UPRAVLJANJE ISTOVREMENIM POSTOJANJEM VIŠE GENERACIJA OPREME

SADRŽAJ

1. DEFINICIJE

Za potrebe ovog Dodatka upotrebljavaju se sljedeće definicije:

sistem pametnog tahografa : prema definiciji u ovom Prilogu (poglavlje 1., definicija bbb));

tahografski sistem prve generacije : prema definiciji u ovoj Uredbi (članak 2., definicija 1.);

tahografski sistem druge generacije : prema definiciji u ovoj Uredbi (članak 2., definicija 7.);

datum uvođenja : prema definiciji u ovom Prilogu (poglavlje 1., definicija ccc));

inteligentna namjenska oprema (eng. *Intelligent Dedicated Equipment*, IDE): oprema koja se upotrebljava za preuzimanje podataka, prema definiciji u Dodatku 7. ovog Priloga.

2. OPŠTE ODREDBE

2.1. Pregled prelaza

U uvodu ovog Priloga naveden je pregled prelaza između sistema tahografa prve i druge generacije.

Uz odredbe ovog uvoda navodi se i sljedeće:

— prva generacija senzora kretanja neće biti interoperabilna s drugom generacijom jedinica u vozilu;

— druga generacija senzora kretanja početa će se ugrađivati u vozila u isto vrijeme kada i druga generacija jedinica u vozilu;

— opremu za preuzimanje podataka i kalibraciju trebat će unaprijediti kako bi se podržale obje generacije uređaja za bilježenje podataka i tahografskih kartica.

2.2. Interoperabilnost između jedinice u vozilu i kartica

Podrazumijeva se da su tahografske kartice prve generacije interoperabilne s jedinicama u vozilu prve generacije u skladu s Prilogom I.B Uredbi (EEZ) 3821/85, dok su tahografske kartice druge generacije interoperabilne s jedinicama u vozilu druge generacije u skladu s Prilogom I.C ovoj Uredbi. Osim toga, primjenjuju se i sljedeći zahtjevi:

MIG_001 Osim kako je predviđeno u zahtjevima MIG_004 i MIG_005, tahografske kartice prve generacije mogu se i dalje upotrebljavati u jedinicama u vozilu druge generacije do isteka važnosti. Međutim, nositelji kartica mogu zatražiti njihovu zamjenu tahografskim karticama druge generacije čim budu dostupne.

MIG_002 Jedinice u vozilu druge generacije moraju moći upotrebljavati bilo koju umetnutu važećiu karticu vozača, kontrolnu karticu i karticu preduzeće prve generacije.

MIG_003 Tu mogućnost radionice mogu zauvijek onemogućiti u takvim jedinicama u vozilu, tako da se tahografske kartice prve generacije ne mogu više primati. To se može učiniti tek nakon što Evropski komisija započne postupak kojim se od radionica zatraži da to učine, primjerice, tokom svakog periodičnog pregleda tahografa.

MIG_004 Jedinice u vozilu druge generacije mogu upotrebljavati samo kartice radionice druge generacije.

MIG_005 Za određivanje načina rada jedinice u vozilu druge generacije u obzir uzimaju samo vrstu umetnutih važećiih kartica, bez obzira na generaciju.

MIG_006 Bilo koja važećia tahografska kartica druge generacije mora se moći upotrebljavati u jedinicama u vozilu druge generacije na potpuno isti način kao i tahografske kartice prve generacije iste vrste.

2.3. Interoperabilnost između jedinice u vozilu i senzora kretanja

Podrazumijeva se da su senzori kretanja prve generacije interoperabilni s jedinicama u vozilu prve generacije, dok su senzori kretanja druge generacije interoperabilni s jedinicama u vozilu druge generacije. Osim toga, primjenjuju se i sljedeći zahtjevi:

MIG_007 Jedinice u vozilu druge generacije neće se moći upariti i upotrebljavati sa senzorima kretanja prve generacije.

MIG_008 Senzori kretanja druge generacije mogu se upariti i upotrebljavati samo s jedinicama u vozilu druge generacije ili s jedinicama u vozilu obiju generacija.

2.4. Interoperabilnost između jedinica u vozilu, tahografskih kartica i opreme za preuzimanje podataka

MIG_009 Oprema za preuzimanje podataka može se upotrebljavati samo s jednom generacijom jedinica u vozilu i tahografskih kartica ili s objema.

2.4.1 *Direktno preuzimanje putem IDE-a*

MIG_010 Podaci se preuzimaju putem IDE-a s tahografskih kartica jedne generacije umetnutih u njihove čitače, koristeći se sigurnosnim mehanizmima i protokolom za preuzimanje podataka te generacije. Preuzeti podaci moraju biti u formatu koji je definisan za tu generaciju.

MIG_011 Kako bi se omogućilo da nadzor nad vozačima provode nadzorna tijela koja nisu iz EU-a, mora biti moguće i preuzeti podatke s kartica vozača (i radionice) druge generacije na potpuno isti način kao i s kartica vozača (i radionice) prve generacije. Takvo preuzimanje uključuje:
— nepotpisane EF-ove ic i icc (neobvezno);
— nepotpisane EF-ove (prve generacije) Card_Certificate i [illegible];
— druge EF-ove aplikacijskih podataka (unutar podatkovne datoteke (DF-a) tahografa) koje zatraži protokol preuzimanja podataka s kartice prve generacije. Te informacije zaštićuju se digitalnim potpisom u skladu sa sigurnosnim mehanizmima prve generacije.
Takvo preuzimanje ne uključuje EF-ove aplikacijskih podataka koji se nalaze samo na karticama vozača (i radionice) druge generacije (EF-ovi aplikacijskih podataka unutar DF-a Tachograph_G2).

2.4.2 ***Preuzimanje podataka s kartice putem jedinice u vozilu***

MIG_012 Podaci se preuzimaju s kartice druge generacije umetnute u jedinicu u vozilu prve generacije koristeći se protokolom za preuzimanje podataka prve generacije. Kartica odgovara na naredbe jedinice u vozilu na potpuno isti način kao i kartica prve generacije. Preuzeti podaci moraju biti istog formata kao i podaci preuzeti s kartice prve generacije.
MIG_013 Podaci se preuzimaju s kartice prve generacije umetnute u jedinicu u vozilu druge generacije koristeći se protokolom za preuzimanje podataka definisanim u Dodatku 7. ovog Priloga. Jedinica u vozilu šalje naredbe kartici na potpuno isti način kao i jedinica u vozilu prve generacije, a preuzeti podaci slijede format definisan za kartice prve generacije.

2.4.3 ***Preuzimanje podataka iz jedinice u vozilu***

MIG_014 Izvan okvira nadzora nad vozačima koji provode nadležna tijela za kontrolu izvan EU-a, podaci iz jedinica u vozilu druge generacije preuzimaju se koristeći se sigurnosnim mehanizmima druge generacije te protokolom za preuzimanje podataka određenim u Dodatku 7. ovog Priloga.
MIG_015 Kako bi se omogućilo da nadzor nad vozačima provode nadležna tijela za kontrolu izvan EU-a, može postojati mogućnost da se podaci iz jedinica u vozilu druge generacije preuzmu koristeći se sigurnosnim mehanizmima prve generacije. Preuzeti podaci u tom slučaju moraju biti istog formata kao i podaci preuzeti iz jedinica u vozilu prve generacije. Ta se mogućnost može odabrati putem naredbi u izborniku.

2.5. Interoperabilnost između jedinice u vozilu i opreme za kalibraciju

MIG_016 Oprema za kalibraciju mora moći izvršiti kalibraciju tahografa svih generacija koristeći se protokolom za kalibraciju te generacije. Oprema za kalibraciju može se koristiti samo s jednom generacijom tahografa ili s objema.

3. GLAVNI KORACI TOKOM PERIODA KOJE PRETHODI DATUMU UVOĐENJA

MIG_017 Ispitni ključevi i certifikati moraju biti dostupni proizvođačima najkasnije **30 mjeseci** prije datuma uvođenja.
MIG_018 Ispitivanja interoperabilnosti mogu započeti ako to proizvođači zatraže najkasnije **15 mjeseci** prije datuma uvođenja.
MIG_019 Službeni ključevi i certifikati moraju biti dostupni proizvođačima najkasnije **12 mjeseci** prije datuma uvođenja.
MIG_020 Države članice moraju biti u mogućnosti izdati kartice radionice druge generacije najkasnije **tri mjeseca** prije datuma uvođenja.
MIG_021 Države članice moraju biti u mogućnosti izdati sve vrste tahografskih kartica druge generacije najkasnije **mjesec dana prije datuma uvođenja**.

4. ODREDBE ZA PERIOD NAKON DATUMA UVOĐENJA

MIG_022 Nakon datuma uvođenja države članice izdaju isključivo tahografske kartice druge generacije.
MIG_023 Proizvođači jedinica u vozilu / senzora kretanja smiju proizvoditi jedinice u vozilu / senzore kretanja prve generacije sve dok se upotrebljavaju na terenu kako bi se neispravni sastavni dijelovi mogli zamijeniti.
MIG_024 Proizvođači jedinica u vozilu / senzora kretanja smiju zatražiti i dobiti zadržavanje homologacije za one vrste jedinica u vozilu / senzora kretanja prve generacije koji su već homologirani.

Dodatak 16.

ADAPTER ZA VOZILA KATEGORIJE M1 I N1

KAZALO

1. SKRAĆENICE I REFERENTNI DOKUMENTI

1.1. Skraćenice

TBD bit će definisano (eng. To Be Defined)

VU jedinica u vozilu (eng. Vehicle Unit)

1.2. Referentne norme

ISO 16844-3 *Road vehicles – Tachograph systems – Part 3*: *Motion sensor interface*

2. OPĆA OBILJEŽJA I FUNKCIJE ADAPTERA

2.1. Opći opis adaptera

ADA_001 Adapter šalje spojenoj jedinici u vozilu zaštićene podatke o kretanju, koji trajno predstavljaju brzinu vozila i prijeđenu udaljenost.

Adapter je namijenjen samo za ona vozila koja u skladu s ovom Uredbom moraju biti opremljena uređajem za bilježenje podataka.

Ugrađuje se i upotrebljava samo u onim vrstama vozila definisanima u definiciji yy) „adapter" iz priloga I.C kada nije mehanički moguće ugraditi bilo koju drugu vrstu postojećeg senzora kretanja, koji je inače usklađen s odredbama ovog Priloga i njegovih dodataka od 1. do 16.

Adapter nije mehanički spojen s pomičnim dijelom vozila, već je povezan s impulsima brzine/udaljenosti koje proizvode integrirani senzori ili alternativna sučelja.

ADA_002 Homologirani senzor kretanja (u skladu s odredbama iz odjeljka 8. Priloga I.C, Homologacija uređaja za bilježenje podataka i tahografskih kartica) ugrađuje se u kućište adaptera, u kojem se nalazi i uređaj za pretvaranje impulsa koji dolazne impulse vodi do ugrađenog senzora kretanja. Ugrađeni senzor kretanja spojen je na jedinicu u vozilu, čime je sučelje između jedinice u vozilu i adaptera u skladu sa zahtjevima navedenima u normi ISO 16844-3.

2.2. Funkcije

ADA_003 Adapter ima sljedeće funkcije:

— spajanje i prilagođavanje dolaznih impulsa brzine;

— dovođenje dolaznih impulsa do ugrađenog senzora kretanja;

— sve funkcije ugrađenog senzora kretanja, slanje zaštićenih podataka o kretanju jedinici u vozilu.

2.3. Sigurnost

ADA_004 Adapter se sigurnosno ne certificira u skladu s generičkom sigurnosnom ciljnom vrijednosti za senzore kretanja definisanom u Dodatku 10. ovog Priloga. Umjesto toga primjenjuju se sigurnosni zahtjevi navedeni u odjeljku 4.4. ovog Dodatka.

3. ZAHTJEVI ZA UREĐAJ ZA BILJEŽENJE PODATAKA KADA JE ADAPTER UGRAĐEN

Zahtjevi navedeni u sljedećim poglavljima upućuju na to kako se tumače zahtjevi iz ovog Priloga prilikom upotrebe adaptera. Brojevi povezanih zahtjeva navedenih u Prilogu I.C navedeni su u zagradama.

ADA_005 Uređaj za bilježenje podataka bilo kojeg vozila opremljenog adapterom mora biti u skladu s odredbama navedenima u ovom Prilogu, osim ako u Dodatku nije drugačije navedeno.

ADA_006 Kada je adapter ugrađen, uređaj za bilježenje podataka sastoji se od kabela, adaptera (uključujući senzor kretanja) i jedinice u vozilu [01].

ADA_007 Funkcija za otkrivanje događaja i/ili kvarova uređaja za bilježenje podataka izmijenjena je kako slijedi:

— događaj „prekid napajanja” aktivira jedinica u vozilu, dok nije u načinu rada za kalibraciju, pri svakom prekidu napajanja ugrađenog senzora kretanja dužem od 200 milisekundi [79];
— događaj „pogreška u podacima o kretanju” aktivira jedinica u vozilu u slučaju prekida uobičajenog protoka podataka između ugrađenog senzora kretanja i jedinice u vozilu i/ili u slučaju greške u integritetu podataka ili greške u autentifikaciji podataka tokom razmjene podataka između ugrađenog senzora kretanja i jedinice u vozilu [83];
— događaj „pokušaj probijanja zaštite” aktivira jedinica u vozilu u slučaju bilo kojeg drugog događaja koji utječe na sigurnost ugrađenog senzora kretanja dok nije u načinu rada za kalibraciju [85];
— grešku „uređaj za bilježenje podataka” aktivira jedinica u vozilu, dok nije u načinu rada za kalibraciju, u slučaju bilo kakvog kvara ugrađenog senzora kretanja [88].
ADA_008 Kvarovi adaptera koje uređaj za bilježenje podataka može otkriti kvarovi su povezani s ugrađenim senzorom kretanja [88].
ADA_009 Funkcija za kalibraciju jedinice u vozilu omogućava automatsko uparivanje ugrađenog senzora kretanja s jedinicom u vozilu [202, 204].

4. ZAHTJEVI U POGLEDU IZRADE I FUNKCIONALNOSTI ADAPTERA

4.1. Povezivanje i prilagođavanje dolaznih impulsa brzine

ADA_011 Ulazno sučelje adaptera prihvaća impulse frekvencije koji predstavljaju brzinu vozila i prijeđenu udaljenost. Električne karakteristike dolaznih impulsa su sljedeće: *definirat će ih proizvođač*. Prilagodbe dostupne isključivo proizvođaču adaptera te ovlaštenoj radionici koja sprovodi ugradnju adaptera moraju omogućiti ispravno povezivanje ulaznog sučelja adaptera s vozilom, ako je primjenjivo.
ADA_012 Ulazno sučelje adaptera mora imati mogućnost, ako je primjenjivo, pomnožiti ili podijeliti impulse frekvencije dolaznih impulsa brzine s fiksnim faktorom kako bi se signal prilagodio rasponu k faktora određenom u ovom Prilogu (4 000 do 25 000 impulsa/km). Fiksni faktor mogu programirati samo proizvođač adaptera i ovlaštena radionica koja obavlja ugradnju adaptera.

4.2. Dovođenje dolaznih impulsa do ugrađenog senzora kretanja

ADA_013 Dolazni impulsi, koji su eventualno prilagođeni kako je prethodno navedeno, dovode se do ugrađenog senzora kretanja tako da senzor kretanja otkrije svaki dolazni impuls.

4.3. Ugrađeni senzor kretanja

ADA_014 Dolazni impulsi stimuliraju ugrađeni senzor kretanja te mu time omogućavaju da generiše podatke o kretanju koji tačno predstavljaju kretanje vozila, kao da je mehanički spojen s pomičnim dijelom vozila.
ADA_015 Jedinica u vozilu identificira adapter s pomoću identifikacijskih podataka ugrađenog senzora kretanja [95].
ADA_016 Smatra se da instalacijski podaci spremljeni u ugrađenom senzoru kretanja predstavljaju instalacijske podatke adaptera [122].

4.4. Sigurnosni zahtjevi

ADA_017 Kućište adaptera mora biti oblikovano tako da se ne može otvoriti i plombirano tako da se pokušaji fizičkog neovlaštenog rukovanja mogu jednostavno otkriti (npr. vizualnim pregledom; vidjeti ADA_035). Za plombe vrijede isti zahtjevi kao i za plombe senzora kretanja [398 do 406].
ADA_018 Ne smije biti moguće ukloniti ugrađeni senzor kretanja iz adaptera bez uništavanja plombe (plombi) kućišta adaptera ili uništavanja plombe između senzora i kućišta adaptera (vidjeti ADA_034).
ADA_019 Adapterom se mora osigurati da se podaci o kretanju mogu obrađivati i dobiti samo putem ulaznog sučelja adaptera.

4.5. Karakteristike izvedivosti

ADA_020 Adapter mora biti u potpunosti operativan pri rasponu temperatura koji je definirao proizvođač.
ADA_021 Adapter mora biti u potpunosti operativan pri rasponu vlažnosti od 10 % do 90 % [214].
ADA_022 Adapter mora biti zaštićen od prenapona, zamjene polariteta napajanja i kratkih spojeva [216].
ADA_023 Adapter mora:
— reagovati na magnetsko polje koje ometa detekciju kretanja vozila. U takvim okolnostima jedinica u vozilu bilježi i arhivira kvar senzora [88] ili
— imati senzorski element koji je zaštićen od magnetskih polja ili je na njih neosjetljiv [217].
ADA_024 Adapter mora biti u skladu s međunarodnim pravilnikom UN ECE R10 koji se odnosi na elektromagnetsku kompatibilnost te mora biti zaštićen od elektrostatičkih pražnjenja i prelaznih pojava [218].

4.6. Materijali

ADA_025 Adapter mora zadovoljavati stepen zaštite (*definirat će ga proizvođač zavisno o položaju ugradnje*) [220, 221].
ADA_026 Kućište adaptera žute je boje.

4.7. Oznake

ADA_027 Opisna pločica pričvršćuje se na adapter te su na njoj navedene sljedeće pojedinosti:
— naziv i adresa proizvođača adaptera;
— kataloški broj proizvođača i godina proizvodnje adaptera;
— homologacijska oznaka tipa adaptera ili tipa uređaja za bilježenje podataka koji sadrži adapter;
— datum ugradnje adaptera;
— identifikacijski broj vozila na koje je ugrađen.
ADA_028 Na opisnoj pločici navode se i sljedeće pojedinosti (ako ih se ne može direktno pročitati s vanjske strane ugrađenog senzora kretanja):
— naziv proizvođača ugrađenog senzora kretanja;
— kataloški broj proizvođača i godina proizvodnje ugrađenog senzora kretanja;

— homologacijska oznaka ugrađenog senzora kretanja.

5. UGRADNJA UREĐAJA ZA BILJEŽENJE PODATAKA KADA SE UPOTREBLJAVA ADAPTER

5.1. Ugradnja

ADA_029 Adaptere koji se ugrađuju u vozila ugrađuju isključivo proizvođači vozila ili radionice ovlaštene za ugradnju, aktivaciju i kalibraciju digitalnih i pametnih tahografa.

ADA_030 Ovlaštene radionice koje ugrađuju adaptere izvršavaju prilagodbu ulaznog sučelja i odabiru omjer dijeljenja ulaznog signala (ako je primjenjivo).

ADA_031 Ovlaštene radionice koje ugrađuju adapter plombiraju kućište adaptera.

ADA_032 Adapter se postavlja što je bliže moguće onom dijelu vozila iz kojeg se šalju dolazni impulsi.

ADA_033 Kablovi kojima se napaja adapter crvene su (pozitivan pol) odnosno crne boje (uzemljenje).

5.2. Plombiranje

ADA_034 U pogledu plombiranja primjenjuju se sljedeći zahtjevi:

— kućište adaptera plombirano je (vidjeti ADA_017);

— kućište ugrađenog senzora pričvršćeno je plombom na kućište adaptera, osim ako nije moguće ukloniti senzor iz kućišta adaptera bez uništavanja plombe (plombi) kućišta adaptera (vidjeti ADA_018);

— kućište adaptera plombom je pričvršćeno na vozilo;

— veza između adaptera i uređaja koji šalje ulazne impulse mora biti plombirana na oba kraja (u mjeri u kojoj je to moguće).

6. PROVJERE, PREGLEDI I POPRAVCI

6.1. Periodični pregledi

ADA_035 Kada se upotrebljava adapter, svaki periodični pregled (periodični pregledi u skladu sa zahtjevima [409] do [413] Priloga I.C) uređaja za bilježenje podataka uključuje sljedeće provjere:

— nalazi li se na adapteru odgovarajuća homologacijska oznaka;

— jesu li plombe na adapteru i priključcima netaknute;

— je li adapter ugrađen na način naveden na tipskoj pločici;

— je li adapter ugrađen na način koji je naveo proizvođač adaptera i/ili vozila;

— je li postavljanje adaptera odobreno za vozilo koje se pregledava.

ADA_036 Ove provjere uključuju kalibraciju te zamjenu svih plombi, bez obzira na njihovo stanje.

7. HOMOLOGACIJA UREĐAJA ZA BILJEŽENJE PODATAKA KADA SE UPOTREBLJAVA ADAPTER

7.1. Opći zahtjevi

ADA_037 Uređaj za bilježenje podataka mora se predati na homologaciju u cjelovitom stanju zajedno s adapterom [425].

ADA_038 Svaki adapter može se predati na zasebnu homologaciju ili na homologaciju kao sastavni dio uređaja za bilježenje podataka.

ADA_039 Takva homologacija uključuje provjere funkcionalnosti u vezi s adapterom. Pozitivni rezultati svih tih provjera navode se u odgovarajućem certifikatu [426].

7.2. Certifikat o ispravnosti

ADA_040 Certifikat o ispravnosti adaptera ili uređaja za bilježenje podataka koji sadrži adapter dostavlja se proizvođaču adaptera tek nakon uspješne provedbe svih sljedećih minimalnih ispitivanja funkcionalnosti.

Br.	Ispitivanje	Opis	Povezani zahtjevi
1.	**Administrativna provjera**		
1.1.	Dokumentacija	Je li dokumentacija adaptera tačna?	
2.	**Vizualni pregled**		
2.1.	Je li adapter u skladu s dokumentacijom?		
2.2.	Identifikacija / oznake adaptera		ADA_027, ADA_028
2.3.	Materijali adaptera		[219] do [223] ADA_026
2.4.	Plombiranje		ADA_017, ADA_018, ADA_034
3.	**Ispitivanje funkcionalnosti**		
3.1.	Dovođenje impulsa brzine do ugrađenog senzora kretanja		ADA_013
3.2.	Povezivanje i prilagođavanje dolaznih impulsa brzine		ADA_011, ADA_012
3.3.	Preciznost mjerenja kretanja		[30] do [35], [217]
4.	**Ispitivanja u vezi s okolišem**		
4.1.	Rezultati ispitivanja proizvođača	Rezultati ispitivanja proizvođača u vezi s okolišem	ADA_020, ADA_021, ADA_022, ADA_024
5.	**EMC**		
5.1.	Emisije zračenja i osjetljivost	Provjeriti usklađenost s Uredbom 2006/28/EZ	ADA_024
5.2.	Rezultati ispitivanja proizvođača	Rezultati ispitivanja proizvođača u vezi s okolišem	ADA_024

PRILOG II

Commented [DD1]: obartiti pažnju na prilog 5 našeg novog pravilnika), jer se u prilogu Uredbe 164/2014 sve ovo niže dolje ponavlja osim setifikata za pametne tahografe. Osnovna verzija Implementacione Uredbu 799/2016 nema ovaj prilog a u izmjenjeni uredbe 2018/502 se poziva na prilog.

HOMOLOGACIJSKA OZNAKA I CERTIFIKAT O HOMOLOGACIJI

I. HOMOLOGACIJSKA OZNAKA

1. Homologacijsku oznaku čini:

(a) pravougaonik, unutar kojeg se upisuje slovo „e”, iza kojeg slijedi poznati broj ili slovo države koja je izdala homologaciju, u skladu sa sljedećim dogovorenim znakovima:

Belgija	6,
Bugarska	34,
Češka	8,
Danska	18,
Njemačka	1,
Estonija	29,
Irska	24,
Grčka	23,
Španjolska	9,
Francuska	2,
Hrvatska	25,
Italija	3,
Cipar	CY,
Latvija	32,
Litva	36,
Luksemburg	13,
Mađarska	7,
Malta	MT,
Holandija	4,
Austrija	12,
Poljska	20,
Portugal	21,
Rumunija	19,
Slovenija	26,
Slovačka	27,
Finska	17,
Švedska	5,
Ujedinjena Kraljevina	11,

i

(b) homologacijski broj koji odgovara broju certifikata o homologaciji sastavljenog za prototip uređaja za bilježenje podataka ili tahografskog listića ili tahografske kartice, zapisan bilo gdje u neposrednoj blizini tog pravougaonika.

2. Homologacijska oznaka navodi se na opisnoj pločici svakog uređaja te na svakom tahografskom listiću i na svakoj tahografskoj kartici. Oznaka mora biti neizbrisiva i mora biti trajno čitljiva.

3. Dimenzije homologacijske oznake prikazane na crtežu u nastavu ([20]) izražene su u milimetrima, a te su dimenzije minimalne. Potrebno je zadržati odnose veličina između dimenzija.

II. CERTIFIKAT O HOMOLOGACIJI ZA ANALOGNE TAHOGRAFE

Država članica koja je odobrila homologaciju podnositelju zahtjeva izdaje certifikat o homologaciji prema modelu u nastavu. Za obavješćivanje ostalih država članica o izdatim ili, ako je potrebno, povučenim homologacijama, država članica upotrebljava preslike tog certifikata.

CERTIFIKAT O HOMOLOGACIJI

Naziv nadležnog tijela …

Obavještenje o ([21]):

— homologaciji uređaja za bilježenje podataka

— povlačenju homologacije uređaja za bilježenje podataka

— homologaciji uzorka tahografskog listića

— povlačenju homologacije uzorka tahografskog listića

Homologacijski br.:

…

1. Zaštitni znak ili naziv …

2. Naziv tipa ili modela …

3. Naziv proizvođača …
4. Adresa proizvođača …
5. Podneseno za homologaciju dana …
6. Ispitano u …
7. Datum i broj ispitivanja …
8. Datum homologacije …
9. Datum povlačenja homologacije …
10. Tip ili tipovi uređaja za bilježenje podataka namijenjenih za rad s tahografskim listićima
11. Mjesto …
12. Datum …
13. Priloženi opisni dokumenti …
14. Napomene (uključujući mjesto plombe, prema potrebi)
(Potpis)

III. CERTIFIKAT O HOMOLOGACIJI ZA DIGITALNE TAHOGRAFE

Država članica koja je odobrila homologaciju podnositelju zahtjeva izdaje certifikat o homologaciji prema modelu u nastavu. Za obavješćivanje ostalih država članica o izdatim ili, ako je potrebno, povučenim homologacijama, država članica upotrebljava preslike tog certifikata.

CERTIFIKAT O HOMOLOGACIJI ZA DIGITALNE TAHOGRAFE

Naziv nadležnog tijela …
Obavještenje o ([22]):
□ homologaciji za:
□ povlačenju homologacije za:
□ model uređaja za bilježenje podataka
□ sastavni dio uređaja za bilježenje podataka ([23])
□ karticu vozača
□ karticu radionice
□ karticu preduzeće
□ karticu nadzornika
Homologacijski br.:
….
1. Robna marka ili zaštitni znak proizvođača …
2. Naziv modela …
3. Naziv proizvođača …
4. Adresa proizvođača …
5. Predano na homologaciju dana …
6. Laboratorij(i) …
7. Datum i broj izvješća o ispitivanju …
8. Datum homologacije …
9. Datum povlačenja homologacije …
10. Model uređaja za bilježenje podataka s kojim treba upotrebljavati sastavni dio
11. Mjesto …
12. Datum …
13. Priloženi opisni dokumenti …
14. Napomene (uključujući mjesto plombe, prema potrebi)
(Potpis)

IV. CERTIFIKAT O HOMOLOGACIJI ZA PAMETNE TAHOGRAFE

Država članica koja je odobrila homologaciju podnositelju zahtjeva izdaje certifikat o homologaciji prema modelu u nastavu. Za obavješćivanje ostalih država članica o izdatim ili, ako je potrebno, povučenim homologacijama, država članica upotrebljava preslike tog certifikata.

CERTIFIKAT O HOMOLOGACIJI ZA PAMETNE TAHOGRAFE

Naziv nadležnog tijela …
Obavještenje o ([24]):
□ homologaciji za:
□ povlačenju homologacije za:
□ model uređaja za bilježenje podataka
□ sastavni dio uređaja za bilježenje podataka ([25])
□ karticu vozača
□ karticu radionice
□ karticu preduzeće
□ karticu nadzornika
Homologacijski br.:
….
1. Robna marka ili zaštitni znak proizvođača …
2. Naziv modela …
3. Naziv proizvođača …
4. Adresa proizvođača …
5. Predano na homologaciju dana …

6.
(a) ispitni laboratorij za certifikaciju ispravnosti …
(b) ispitni laboratorij za sigurnosnu certifikaciju …
(c) ispitni laboratorij za certifikaciju interoperabilnosti …
7.
(a) datum i broj certifikata o ispravnosti …
(b) datum i broj certifikata o sigurnosti …
(c) datum i broj certifikata o interoperabilnosti …
8. Datum homologacije …
9. Datum povlačenja homologacije …
10. Model uređaja za bilježenje podataka s kojim treba upotrebljavati sastavni dio
11. Mjesto …
12. Datum …
13. Priloženi opisni dokumenti …
14. Napomene (uključujući mjesto plombe, prema potrebi)

(Potpis)

([1]) Uredba Vijeća (EEZ) br. 3821/85 od 20. decembra 1985. o tahografu u drumskom prometu (SL L 370, 31.12.1985., str. 8.).
([2]) Direktiva 2014/53/EU Evropskog parlamenta i Vijeća od 16. travnja 2014. o usklađivanju zakonodavstava država članica o stavljanju na raspolaganje radijske opreme na tržištu i stavljanju izvan snage Direktive 1999/5/EZ (SL L 153, 22.5.2014., str. 62.).
([3]) Ovaj način izračuna neprekidnog vremena vožnje i kumulativnog vremena pauze služi uređaju za bilježenje podataka za izračun upozorenja o neprekidnom vremenu vožnje. Time se ne dovodi u pitanje pravno tumačenje navedenih vremena. Alternativni načini izračuna neprekidnog vremena vožnje i kumulativnog vremena pauze mogu se upotrijebiti za zamjenu tih definicija ako su postale zastarjele ažuriranjem u drugim odgovarajućim zakonima.
([4]) Perioda NEPOZNATO odnose se na perioda kada kartica vozača nije bila umetnuta u uređaj za bilježenje podataka i za koja nisu ručno upisivani podaci o aktivnostima vozača.
([5]) Uredba (EZ) br. 561/2006 Evropskog parlamenta i Vijeća od 15. ožujka 2006. o usklađivanju određenog socijalnog zakonodavstva koje se odnosi na drumski promet i o izmjeni uredbi Vijeća (EEZ) br. 3821/85 i (EZ) br. 2135/98 te o stavljanju izvan snage Uredbe Vijeća (EEZ) br. 3820/85 (SL L 102, 11.4.2006., str. 1.).
([6]) Uredba Komisije (EU) br. 1230/2012 od 12. decembra 2012. o sprovođenju Uredbe (EZ) br. 661/2009 Evropskog parlamenta i Vijeća o zahtjevima za homologaciju tipa za mase i dimenzije vozila i njihovih prikolica te o izmjeni Direktive 2007/46/EZ Evropskog parlamenta i Vijeća (SL L 353, 21.12.2012.,str. 31.), kako je zadnji put izmijenjena.
([7]) Direktiva Vijeća 92/6/EEZ od 10. februar 1992. o ugradnji i upotrebi uređaja za ograničenje brzine za određene kategorije motornih vozila u Zajednici (SL L 57, 2.3.1992., str. 27.).
([8]) Direktiva Vijeća 92/23/EEZ od 31. ožujka 1992. o gumama za motorna vozila i njihove prikolice i o njihovoj ugradbi (SL L 129, 14.5.1992., str. 95.).
([9]) Direktiva Vijeća 76/114/EEZ od 18. decembra 1975. o usklađivanju zakonodavstava država članica u odnosu na propisane pločice i natpise za motorna vozila i njihove prikolice te na njihov položaj i način pričvršćivanja (SL L 24, 30.1.1976., str. 1.).
([10]) Direktiva 2007/46/EZ Evropskog parlamenta i Vijeća od 5. rujna 2007. o uspostavi okvira za homologaciju motornih vozila i njihovih prikolica te sistema, sastavnih dijelova i zasebnih tehničkih jedinica namijenjenih za takva vozila (Okvirna direktiva) (SL L 263, 9.10.2007., str. 1.).
([11]) Direktiva 95/46/EZ Evropskog parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom ličnih podataka i o slobodnom protoku takvih podataka (SL L 281, 23.11.1995., str. 31.).
([12]) Direktiva 2002/58/EZ Evropskog parlamenta i Vijeća od 12. srpnja 2002. o obradi ličnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (SL L 201, 31.7.2002., str. 37.).
([13]) Uredba (EU) br. 165/2014 Evropskog parlamenta i Vijeća od 4. februar 2014. o tahografima u drumskom prometu, stavljanju izvan snage Uredbe Vijeća (EEZ) br. 3821/85 o tahografu u drumskom prometu i izmjeni Uredbe (EZ) br. 561/2006 Evropskog parlamenta i Vijeća o usklađivanju određenog socijalnog zakonodavstva koje se odnosi na drumski promet (SL L 60, 28.2.2014., str. 1.).
([14]) SL L 281, 23.11.1995., str. 31.
([15]) SL L 201, 31.7.2002., str. 37.
([16]) SL L 102, 11.4.2006., str. 1.
([17]) Uredba Komisije (EZ) br. 68/2009 od 23. siječnja 2009. o devetoj prilagodbi tehničkom napretku Uredbe Vijeća (EEZ) br. 3821/85 o tahografu u drumskom prometu (SL L 21, 24.1.2009., str. 3.).
([*1]) Umetnuta će kartica aktivirati odgovarajuća prava pristupa funkciji preuzimanja podataka i samim podacima. Međutim, mora biti moguće preuzeti podatke s kartice vozača umetnute u jedan od otvora jedinice u vozilu ako nijedna druga kartica nije umetnuta u drugi otvor.
([18]) Treba napomenuti da ključevi uparivanja prve, druge i treće generacije mogu zapravo biti isti ključ ili mogu biti tri različita ključa različite dužine, kako je objašnjeno u CSM_117.
([19]) Uredba (EU) br. 1285/2013 Evropskog parlamenta i Vijeća od 11. decembra 2013. o sprovođenju i upotrebi evropskih sistema za satelitsku navigaciju i stavljanju izvan snage Uredbe Vijeća (EZ) br. 876/2002 i Uredbe (EZ) br. 683/2008 Evropskog parlamenta i Vijeća (SL L 347, 20.12.2013., str. 1.).
([20]) Te su brojke prikazane samo kao ilustracija.
([21]) Prekrižiti nepotrebno.
([22]) Označiti odgovarajuća polja.
([23]) Navesti sastavni dio koji je predmet obavještenjei.
([24]) Označiti odgovarajuća polja.
([25]) Navesti sastavni dio koji je predmet obavještenjei.