**PRILOG II**

**ZAHTJEVI U POGLEDU IZRADE, PREGLEDA, UGRADNJE I NADZORA ZA DIGITALNE TAHOGRAFE (PRILOG I. B)**

**SADRŽAJ**

|  |  |
| --- | --- |
| I. | DEFINICIJE … |
| II. | OPŠTA OBELJEŽJA I FUNKCIJE TAHOGRAFA … |
| 1. | Opšta obelježja … |
| 2. | Funkcije: … |
| 3. | Načini rada … |
| 4. | Sigurnost … |
| III. | III. ZAHTJEVI U POGLEDU IZRADE I FUNKCIONALNI ZAHTJEVI ZA TAHOGRAFE … |
| 1.1 | Praćenje ubacivanja i vađenja kartica … |
| 2. | Mjerenje brzine i udaljenosti … |
| 2.1 | Mjerenje pređene udaljenosti … |
| 2.2. | Mjerenje brzine … |
| 3. | Mjerenje vremena … |
| 4. | Praćenje aktivnosti vozača … |
| 5. | Praćenje stanja vožnje … |
| 6. | Ručni unos od strane vozača … |
| 6.1. | Unos mjesta početka i/ili kraja dnevnog perioda rada … |
| 6.2. | Ručni unos aktivnosti vozača … |
| 6.3. | Unos posebnih stanja … |
| 7. | Upravljanje blokadom preduzeća … |
| 8. | Praćenje nadzornih aktivnosti … |
| 9. | Prepoznavanje događaja i/ili grešaka … |
| 9.1. | Događaj ‚ubacivanje nevažeće kartice’ … |
| 9.2. | Događaj ‚sukob kartica’ … |
| 9.3. | Događaj ‚vremensko preklapanje’ … |
| 9.4. | Događaj ‚vožnja bez odgovarajuće kartice’ … |
| 9.5. | Događaj ‚ubacivanje kartice tokom vožnje’ … |
| 9.6. | Događaj ‚neispravno zatvaranje posljednje razmjene podataka s karticom’ … |
| 9.7. | Događaj ‚prekoračenje brzine’ … |
| 9.8. | Događaj ‚prekid napajanja’ … |
| 9.9. | Događaj ‚greška podataka kretanja’ … |
| 9.10. | Događaj ‚pokušaj probijanja zaštite’ … |
| 9.11. | Greška ‚kartica’ … |
| 9.12. | Greška ‚tahograf’ … |
| 10. | Postupak provjere i samoprovjere … |
| 11. | Očitavanje podataka iz memorije … |
| 12. | Zapis i čuvanje u podakovnoj memoriji … |
| 12.1. | Identifikacijski podaci o uređaju … |
| 12.1.1 | .Identifikacijski podaci jedinice u vozilu … |
| 12.1.2. | Identifikacijski podaci senzora kretanja … |
| 12.2. | Sigurnosni elementi … |
| 12.3. | Podaci o ubacivanju i vađenju kartice vozača … |
| 12.4. | Podaci o aktivnosti vozača … |
| 12.5. | Mjesta početka i/ili završetka dnevnog perioda rada … |
| 12.6. | Stanje brojača pređenih kilometara … |
| 12.7. | Detaljni podaci o brzini … |
| 12.8. | Podaci o događanjima … |
| 12.9. | Podaci o greškama … |
| 12.10. | Podaci o kalibraciji … |
| 12.11. | Podaci o podešavanju vremena … |
| 12.12. | Podaci o nadzornim aktivnostima … |
| 12.13. | Podaci o zaključavanju podataka preduzeća … |
| 12.14. | Podaci o aktivnostima preuzimanja podataka … |
| 12.15. | Podaci o posebnim uslovima … |
| 13. | Očitavanje kartica tahografa … |
| 14. | Zapisivanje i čuvanje podataka na tahografske kartice … |
| 15. | Prikaz … |
| 15.1. | Standardni prikaz … |
| 15.2. | Prikaz upozorenja … |
| 15.3. | Pristub meniju … |
| 15.4. | Ostali prikazi … |
| 16. | Ispis … |
| 17. | Upozorenja … |
| 18. | Preuzimanje podataka na vanjske medije … |
| 19. | Izlazni podaci za dodatne vanjske uređaje … |
| 20. | Kalibracija … |
| 21. | Podešavanje vremena … |
| 22. | Radna obelježja … |
| 23. | Materijali … |
| 24. | Oznake … |
| IV. | ZAHTJEVI U POGLEDU IZRADE I FUNKCIONALNI ZAHTJEVI ZA KARTICE TAHOGRAFA ... |
| 1. | Vidljivi podaci … |
| 2. | Sigurnost … |
| 3. | Norme … |
| 4. | Okolina i električne karakteristike … |
| 5. | Čuvanje podataka … |
| 5.1. | Identifikacija kartice i sigurnosni podaci … |
| 5.1.1. | Identifikacija programa … |
| 5.1.2. | Identifikacija čipa … |
| 5.1.3. | IC identifikacija kartice … |
| 5.1.4. | Sigurnosni elementi … |
| 5.2. | Kartica vozača … |
| 5.2.1. | Identifikacija kartice … |
| 5.2.2. | Identifikacija nosioca kartice … |
| 5.2.3. | Podaci o vozačkoj dozvoli … |
| 5.2.4. | Podaci o korišćenim vozilima … |
| 5.2.5. | Podaci o aktivnostima vozača … |
| 5.2.6. | Mjesta početka i/ili završetka dnevnih aktivnosti … |
| 5.2.7. | Podaci o događajima … |
| 5.2.8. | Podaci o greškama … |
| 5.2.9. | Podaci o nadzornim aktivnostima … |
| 5.2.10. | Podaci o upotrebi kartice … |
| 5.2.11. | Podaci o posebnim stanjima … |
| 5.3. | Kartica radionice … |
| 5.3.1. | Sigurnosni elementi … |
| 5.3.2. | Identifikacija kartice … |
| 5.3.3. | Identifikacija nosioca kartice … |
| 5.3.4. | Podaci o korišćenim vozilima … |
| 5.3.5. | Podaci o aktivnosti vozača … |
| 5.3.6. | Podaci o početku i/ili završetku dnevnog perioda rada … |
| 5.3.7. | Podaci o događajima i greškama … |
| 5.3.8. | Podaci o nadzornim aktivnostima … |
| 5.3.9. | Podaci o kalibraciji i podešavanju vremena … |
| 5.3.10. | Podaci o posebnim uslovima … |
| 5.4. | Kontrolna kartica … |
| 5.4.1. | Identifikacija kartice … |
| 5.4.2. | Identifikacija nosioca kartice … |
| 5.4.3. | Podaci o nadzornim aktivnostima … |
| 5.5. | Kartica prevoznika … |
| 5.5.1. | Identifikacija kartice … |
| 5.5.2. | Identifikacija nosioca kartice … |
| 5.5.3. | Podaci o aktivnostima prevoznika … |
| V. | UGRADNJA TAHOGRAFA … |
| 1. | Ugradnja … |
| 2. | Ugradna pločica … |
| 3. | Postavljanje žigova … |
| VI. | ISPITIVANJE, PREGLEDI I POPRAVKE … |
| 1. | Ovlaštenje ugraditelja ili radionica … |
| 2. | Ispitivanje novih ili popravljenih uređaja … |
| 3. | Nadzor pri ugradnji … |
| 4. | Periodični pregledi … |
| 5. | Mjerenje grešaka … |
| 6. | Popravke … |
| VII. | IZDAVANJE KARTICA … |
| VIII. | TIPSKO ODOBRENJE TAHOGRAFA I KARTICA TAHOGRAFA … |
| 1. | Uopšteno … |
| 2. | Sigurnosna potvrda … |
| 3. | Potvrda o funkcionalnosti … |
| 4. | Potvrda o interoperabilnosti … |
| 5. | Potvrda o tipskom odobrenju … |
| 6. | Vanredni postupak: prva provjera interoperabilnosti … |

Dodatak 1. Rečnik podataka

Dodatak 2. Opis kartica tahografa

Dodatak 3. Piktogrami

Dodatak 4. Ispisi

Dodatak 5. Prikaz

Dodatak 6. Spoljna sučelja

Dodatak 7. Protokoli preuzimanja podataka

Dodatak 8. Protokol kalibracije

Dodatak 9. TIPSKO ODOBRENJE – POPIS NAJMANJEG OBIMA OBVEZNIH ISPITIVANJA

Dodatak 10. GENERIČKI SIGURNOSNI CILJEVI

Dodatak 11. ZAJEDNIČKI SIGURNOSNI MEHANIZMI

Dodatak 12. ADAPTER ZA VOZILA KATEGORIJE M1 I N1

**I. DEFINICIJE**

|  |  |
| --- | --- |
| (a) | **‚aktivacija’** znači: faza u kojoj tahograf dostiže punu radnu sposobnost i izvršava sve funkcije, uključujući i sigurnosne funkcije; Za aktiviranje tahografa potrebna je kartica radionice i unos njenog PIN-a; |
| (b) | **‚autentifikacija’** znači: funkcija namijenjena utvrđivanju i provjeri identiteta osobe; |
| (c) | **‚autentičnost’** znači: obilježje da informacija dolazi od osobe čiji je identitet moguće provjeriti; |
| (d) | **‚ugrađeni test’** (BIT) znači: provjera koja se sprovodi na zahtjev i koju aktivira operater ili spoljna oprema; |
| (e) | **‚kalendarski dan’** znači: dan koji traje od 00:00 sati do 24:00 sata. Svi kalendarski dani se odnose na UTC vrijeme (univerzalno usklađeno vrijeme); |
| (f) | **‚kalibracija’** znači: ažuriranje ili potvrđivanje parametara vozila koji se čuvaju u memoriji podataka. Parametri vozila uključuju identifikaciju vozila (VIN, VRN i država registracije) i karakteristike vozila (w, k, l, veličina guma, podešenje ograničivača brzine (prema potrebi), trenutno UTC vrijeme, trenutno stanje na brojaču kilometara);  Svako ažuriranje ili potvrđivanje samo UTC vremena, smatra se podešavanjem vremena, a ne kalibracijom, pod uslovom da ne protivrječi zahtjevu 256.  Za kalibraciju tahografa potrebna je kartica radionice. |
|  |
|  |
| (g) | **‚broj kartice’** znači: broj od 16 alfanumeričkih znakova kojime se na jedinstven način identifikuje kartica tahografa unutar neke države članice. Broj kartice obuhvaća indeks rednog broja (prema potrebi), indeks zamjene i indeks obnavljanja; kartica se tako na jedinstven način identifikuje oznakom države članice izdavaoca i brojem kartice; |
| (h) | **‚indeks rednog broja kartice’** znači: 14. alfanumerički znak broja kartice koji se koristi za razlikovanje kartica izdanih tvrtki ili tijelu koje ima pravo na više kartica tahografa. Preduzeće ili tijelo se na jedinstven način identifikuje pomoću prvih 13 znakova broja kartice; |
|  |
| (i) | **‚indeks obnavljanja kartice’** znači: 16. alfanumerički znak broja kartice koji se uvećava prilikom svakog obnavljanja kartice tahografa; |
| (j) | **‚indeks zamjene kartice’** znači: 15. alfanumerički znak broja kartice koji se uvećava prilikom svake zamjene kartice tahografa; |
| (k) | **‚karakteristični koeficijent vozila’** znači: numerička vrijednost koja označava karakteristiku izlaznog signala koja nastaje na priključnom mjestu vozila s tahografom (izlazno vratilo mjenjača ili pogonska osovina vozila) dok vozilo prelazi udaljenost od jednog kilometra pod standardnim ispitnim uslovima (v. poglavlje VI. tački (5)). Karakteristični koeficijent izražava se u impulsima po kilometru (w = … imp/km); |
|  |
| (l) | **‚kartica prevoznika’** znači: kartica tahografa koju nadležna tijela države članice izdaju vlasniku ili držalac vozila opremljenih tahografom;  kartica preduzeća identifikuje preduzeće i omogućava prikaz, preuzimanje podataka i ispis podataka arhiviranih u tahografu, koje je blokiralo to preduzeće ili koje nije blokiralo nijedno preduzeće. |
|  |
|  |
| (m) | **‚konstanta tahografa’** znači: numerička vrijednost koja označava karakteristiku ulaznog signala potrebnog za prikaz i zapis pređene udaljenosti od jednog kilometra; konstanta se izražava u impulsima po kilometru (k = … imp/km); |
|  |
| (n) | **‚neprekidno vrijeme vožnje’** proračunava se u tahografu kao: kao trenutno akumulirano vrijeme vožnje određenog vozača od završetka posljednjeg periodi PRIPRAVNOSTI ili PAUZE/ODMORA ili NEPOZNATO u trajanju od najmanje 45 minuta (navedeni period može biti podijeljeno na nekoliko periodi od najmanje 15 minuta). Navedeni proračun se prema potrebi uzimaju u obzir i prethodne aktivnosti sačuvane na kartici vozača. Ako vozač nije ubacio svoju karticu, proračun se temelji na zapisima iz podakovne memorije koji se odnose na tekuće period u kojemu kartica nije bila umetnuta u odgovarajući otvor za kartice (slot); |
|  |
| (o) | ‚kontrolna kartica’ znači: kartica tahografa koju tijela države članice izdaju domaćem nadležnom nadzornom tijelu; kontrolna kartica identifikuje kontrolno tijelo i po mogućnosti službenika za kontrolu i omogućava pristub podacima sačuvanim u memoriji ili karticama vozača radi očitavanja, ispisa i/ili preuzimanja; |
|  |
|  |
| (p) | **‚ukupno vrijeme pauze’** proračunava se pomoću tahografa kao: kao tekuće akumulirano vrijeme PRIPRAVNOSTI ili PAUZE/ODMORA ili NEPOZNATO u trajanju od najmanje 15 minuta za pojedinog vozača, od završetka posljednjeg periodi njegove PRIPRAVNOSTI ili PAUZE/ODMORA ili NEPOZNATO u trajanju od najmanje 45 minuta (taj period može biti podijeljeno na nekoliko periodi od najmanje 15 minuta). Navedeni proračun prema potrebi uzima u obzir prethodne aktivnosti sačuvane na vozačkoj kartici. Nepoznata periodi negativnog vremenskog proračuna (početak nepoznatog periodi je vremenski kasniji od završetka nepoznatog periodi) zbog vremenskih preklapanja između dva različita tahografa se ne uzimaju u obzir za proračun. Ako vozač nije ubacio svoju karticu, proračun se temelji na zapisima iz podakovne memorije vezanim za tekuće period u kojemu kartica nije bila umetnuta u odgovarajući otvor za kartice (slot); |
|  |
|  |
|  |
| (q) | **‚podaci memorija’** znači: elektronsko sredstvo za čuvanje podataka ugrađeno u tahografu; |
| (r) | **‚digitalni potpis’** znači: podaci stavljeni na blok podataka ili kriptografsku pretvaranje bloka podataka koja omogućava primatelju bloka podataka dokazivanje autentičnosti i potpunosti bloka podataka; |
|  |
| (rr) | **‘adapter’** znači: dio tahografa koji stalno daje signal brzine vozila i/ili pređenu udaljenost, te koji se:   * ugrađuje i upotrebljava samo u vozilima tipa M1 i N1 (kako je utvrđeno u Prilogu II. Direktivi Vijeća 70/156/EEZ) koja su prvi put stavljena u upotrebu između 1. maj 2006. i 31. decembra 2013., * ugrađuje kada nije mehanički moguće ugraditi bilo kakvu drugu vrstu postojećeg senzora kretanja, koji je inače usklađen s odredbama ovog Priloga i njegovih dodataka 1. do 11., * ugrađuje između jedinice u vozilu i tamo gdje otprije ugrađeni senzori ili alternativna sučelja proizvode impulse brzine/udaljenosti.   Gledano iz jedinice u vozilu, ponašanje adaptera jednako je kao da je senzor kretanja, usklađen odredbama ovog Priloga i njegovih dodataka 1. do 11., spojen na jedinicu u vozilu.  Upotreba takvog adaptera u gore opisanim vozilima omogućava ugradnju i ispravnu upotrebu jedinice u vozilu koja je u skladu sa svim zahtjevima ovog Priloga.  Za ta vozila, tahograf je sastavljen od kablova, adaptera i jedinice vozila. |
| (s) | **‚preuzimanje podataka’** znači: kopiranje, zajedno s digitalnim potpisom, dijela ili čitave grupa datoteka arhiviranih u memoriji podataka vozila ili u memoriji kartice tahografa, za koje su ti podaci potrebni, kako bi se ustanovila usklađenost s odredbama Uredbe (EZ) br. 561/2006.  Proizvođači jedinica vozila digitalnih tahografa i proizvođači opreme, oblikovane i namijenjene za preuzimanje datoteka, poduzimaju sve razumne mjere kojima osiguravaju, da se takvi podaci mogu preuzeti s minimalnim gubitkom vremena za prevoznička preduzeća ili vozače.  Pri preuzimanju podataka arhivirani se podaci ne smiju mijenjati niti brisati. Preuzimanje datoteke s detaljnim podacima o brzini ne mora biti potrebno za ustanovljenje usklađenosti s Uredbom (EZ) br. 561/2006, no može se upotrijebiti za druge potrebe, kao što je istraživanje nesreća. |
| (t) | **‚kartica vozača’** znači: kartica tahografa koju su izdala tijela države članice određenom vozaču; kartica vozača identifikuje vozača i omogućava čuvanje podataka o aktivnosti vozača; |
| (u) | **‚aktivni opseg pogonskih točkova’** znači: prosjek udaljenosti koju prijeđe svaki od točkova koji pokreću vozilo (pogonski kotači) tokom jednog potpunog okretaja. Mjerenje tih udaljenosti obavlja se pod standardnim ispitnim uslovima (poglavlje VI. tačka 5.) i izražava se u obliku ‚l = … mm’. Proizvođači vozila mogu nadomjestiti mjerenje takvih udaljenosti teoretskim proračunom koji uzima u obzir raspored opterećenja po osovinama za prazno vozilo i uobičajeno radno stanje. Metode takvog teoretskog proračuna odobrava nadležno tijelo države članice; |
|  |
| (v) | **‚događaj’** znači: nepravilan rad tahografa koji može biti posljedica pokušaja prevare; |
| (w) | **‚greška’** znači: nepravilan rad ustanovljen od tahografa koji može biti posljedica nepravilnog rada ili kvara; |
| (x) | **‚ugradnja’** znači: postavljanje tahografa u vozilo; |
| (y) | **‚senzor kretanja’** znači: dio tahografa koji daje signal koji predstavlja brzinu kretanja vozila i/ili pređenu udaljenost; |
| (z) | **‚nevažeća kartica’** znači: kartica za koju je ustanovljeno da je neispravna ili čija početna autentifikacija nije uspjela ili čiji datum početka važenja još nije nastubio ili čiji je datum važenja istekao; |
| (aa) | **‚van nadležnosti**’ znači: kad tahograf nije potrebno koristiti u skladu sa propisanim odredbama; |
| (bb) | **‚prekoračenje brzine’** znači: prekoračenje dopuštene brzine vozila koja se utvrđuje u bilo kojem razdoblju dužem od 60 sekundi, tokom kojega izmjerena brzina vozila prelazi graničnu brzinu podešenu ograničavačem brzine, a utvrđenu Direktivom Vijeća 92/6/EEZ od 10. veljače 1992. o ugradnji i uporabi uređaja za ograničenje brzine za određene kategorije motornih vozila u Zajednici; |
| (cc) | **‚periodični pregled’** znači: niz postupaka koji se provode radi provjere ispravnosti rada tahografa i usklađenosti podešenih vrijednosti s parametrima vozila; |
| (dd) | **‚pisač’** znači: sastavni dio tahografa koji daje ispis arhiviranih podataka; |
| (ee) | **‚tahograf’** znači: svu opremu namijenjenu ugradnji u drumska vozila radi prikaza, evidentirajunja i automatskog ili poluautomatskog pohranjivanja podataka o kretanju takvih vozila i o određenim razdobljima aktivnosti njihovih vozača; |
| (ff) | **‚obnavljanje’** znači: izdavanje nove kartice tahografa kada postojećoj kartici istekne valjanost ili kada postane neispravna pa je vraćena tijelu koje ju je izdalo. Obnavljanje uvijek podrazumijeva nedvosmislenost da postoje dvije važeće kartice; |
| (gg) | **‚popravak’** znači: svaki popravak senzora kretanja ili jedinice u vozilu koji zahtijeva isključivanje njegovog napajanja ili isključivanje s drugih sastavnih dijelova tahografa ili njegovo otvaranje; |
| (hh) | **‚zamjena’** znači: izdavanje kartice tahografa kao zamjene za postojeću karticu čiji je gubitak, krađa ili neispravnost prijavljen, a nije vraćena tijelu koje ju je izdalo. Zamjena uvijek podrazumijeva rizik da mogu istovremeno postojati dvije važeće kartice. |
| (ii) | **‚sigurnosna potvrda’** znači: postupak koji je potvrdilo certifikacijsko tijelo ITSEC da tahograf (ili njegov dio) ili kartica tahografa koja se ispituje zadovoljava sigurnosne zahtjeve utvrđene u Dodatku 10.: Generički sigurnosni ciljevi; |
| (jj) | **‚samoprovjera’** znači: ispitivanje koje tahograf sprovodi ciklički i automatski radi otkrivanja grešaka; |
| (kk) | **‚kartica tahografa’** znači: pametna kartica namijenjena korištenju uz tahograf. Kartica tahografa omogućava tahografu prepoznavanje identiteta (ili grupa identiteta) nosioca kartice, te omogućava prenos i čuvanje podataka. Kartica tahografa može biti sljedećeg tipa:   * kartica vozača, * kontrolna kartica, * kartica radionice, * kartica prevoznika; |
|  |
| (ll) | **‚tipsko odobrenje’** znači: postupak u kojem država članica potvrđuje da tahograf (ili njegov sastavni dio) ili kartica tahografa koja se ispituje zadovoljava zahtjeve ove Uredbe; |
| (mm) | **‚dimenzije guma’** znači: oznaka dimenzije guma (spoljnih pogonskih točkova) |
| (nn) | **‚identifikacija vozila’** znači: brojevi kojima se identifikuje vozilo: registracijski broj vozila (VRN) s oznakom države članice registracije i identifikacijski broj vozila (VIN); |
| (oo) | **‚jedinica u vozilu’ (VU)** znači: tahograf bez senzora kretanja i vodiča priključenih na senzor kretanja. Jedinica u vozilu može biti bilo jedna jedinica ili više jedinica raspoređenih u vozilu, ako udovoljava sigurnosnim zahtjevima iz ove Uredbe; |
| (pp) | za potrebe proračunavanja u tahografu **‚nedelja’** znači: period između 00:00 sati UTC vremena u ponedjeljak i 24:00 sata UTC u nedjelju; |
| (qq) | **‚kartica radionice’** znači: kartica tahografa koju su izdala tijela države članice proizvođaču tahografa, ugraditelju, proizvođaču vozila ili servisu koji je ovlastila takva država članica. Servisna kartica identifikuje nosioca kartice i omogućava provjeru, kalibraciju i/ili preuzimanje podataka s tahografa. |
|  |
|  |

**II. OPŠTA OBELJEŽJA I FUNKCIJE TAHOGRAFA**

000  
Svako vozilo opremljeno tahografom u skladu s odredbama ovog Priloga mora imati pokazivač brzine i brojač kilometara. Ove funkcije mogu biti ugrađene u tahograf.

**1.   Opšta obelježja**

Svrha tahografa je belježenje, čuvanje, prikazivanje, ispis i davanje podataka o aktivnosti vozača.

001  
Tahograf se sastoji od vodiča, senzora kretanja i jedinice u vozilu.

001a Sučelje između senzora kretanja i jedinice vozila u skladu je s normom ISO 16844-3:2004, Cor 1:2006.

002  
Jedinica u vozilu sastoji se od jedinice za obradu podataka, podakovne memorije, sata za prikaz realnog vremena, sučelja za dvije pametne kartice (za vozača i suvozača), pisača, displeja, vizualnog upozorenja, priključka za kalibraciju/preuzimanje podataka i uređaja za unos korisničkih ulaznih podataka.

Tahograf se može priključiti na druge uređaje pomoću dodatnih priključaka.

003  
Svako odobreno ili bilo koje drugo priključivanje ili spajanje na tahograf, neke funkcije, jednog ili više uređaja, ne smije ometati ili imati mogućnost ometanja pravilnog i sigurnog rada tahografa i odredbi ove Uredbe.

Korisnici tahografa identifikujeju se uz pomoć kartice tahografa.

004  
Tahograf daje pravo selektivnog pristupa podacima i funkcijama u skladu s vrstom i/ili identitetom korisnika.

Tahograf evidentira i arhivira podatke u memoriju podataka i na kartice tahografa.

To se odvija u skladu s Direktivom 95/46/EZ od 24. oktobar 1995. o zaštiti pojedinaca u vezi s obradom ličnih podataka i o slobodnom prenosu takvih podataka.

**2.   Funkcije:**

005  
Tahograf osigurava sljedeće funkcije:

005

Tahograf osigurava sljedeće funkcije:

* praćenje ubacivanja i vađenja kartice,
* mjerenje brzine i udaljenosti,
* mjerenje vremena,
* praćenje aktivnosti vozača,
* praćenje stanja vožnje,
* ručne unose vozača,
* unos mjesta početka i/ili završetka dnevnog perioda rada
* ručni unos aktivnosti vozača,
* unos posebnih uslova,
* upravljanje zaključavanjem podataka o tvrtki,
* praćenje aktivnosti nadzora,
* otkrivanje događaja i/ili grešaka,
* ugrađene provjere i samoprovjere,
* očitavanje iz podakovne memorije,
* zapis i čuvanje u podakovnoj memoriji,
* očitavanje iz kartica tahografa,
* zapis i čuvanje na karticama tahografa,
* prikaz,
* ispis,
* upozorenja,
* preuzimanje podataka na vanjske medije,
* izlaz podataka na dodatne vanjske uređaje,
* kalibracija,
* podešavanje vremena.

**3.   Načini rada**

006  
Tahograf mora ima četiri načina rada:

radni način,

* nadzorni način,
* kalibracijski način,
* prevoznički način.

007  
Tahograf se prebacuje na sljedeći način rada u skladu s umetnutim valjanim karticama tahografa u kartično sučelje (otvore):

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Način rada** | | **Otvor vozača** | | | | |
| **Bez kartice** | **Kartica vozača** | **Kontrolna kartica** | **Kartica radionice** | **Kartica prevoznika** |
| Otvor suvozača | Bez kartice | Radni | Radni | Nadzorni | Kalibracijski | Prevoznički |
| Kartica vozača | Radni | Radni | Nadzorni | Kalibracijski | Prevoznički |
| Kontrolna kartica | Nadzorni | Nadzorni | Nadzorni[(9)](https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex:32002R1360#ntr9-L_2002207HR.01000402-E0009) | Radni | Radni |
| Kartica radionice | Kalibracijski | Kalibracijski | Radni | Kalibracijski[(9)](https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex:32002R1360#ntr9-L_2002207HR.01000402-E0009) | Radni |
| Kartica prevoznika | Prevoznički | Prevoznički | Radni | Radni | Prevoznički[(9)](https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex:32002R1360#ntr9-L_2002207HR.01000402-E0009) |

009  
Tahograf zanemaruje umetnutu nevažeću karticu, osim prikaza, ispisa ili preuzimanja podataka s istekle kartice, što mora biti omogućeno.

010  
Sve funkcije navedene pod II.2 moraju raditi u svim načinima rada, uz sljedeće iznimke:

* funkcija kalibracije je dostupna samo u kalibracijskom načinu rada,
* funkcija podešavanja vremena je ograničena kada nije u kalibracijskom načinu rada,
* upravljanje zaključavanjem podataka preduzeća je dostubno samo u prevozničkom načinu rada,
* funkcija praćenje nadzornih aktivnosti radi samo u nadzornom načinu rada,
* Funkcija preuzimanja podataka nije dostupna u radnom režimu (osim kako je predviđeno u zahtjevu 150) osim preuzimanja podataka s kartice vozača kad nijedna druga kartica nije umetnuta u jedinicu vozila.

011  
Tahograf može prenijeti sve podatke na displej, pisač ili spoljna sučelja uz sljedeće iznimke:

* u radnom načinu, sve osobne identifikacije (prezime i ime(na)) koji ne odgovaraju umetnutoj kartici tahografa ostaju nevidljivi, a svaki broj kartice koji ne odgovara umetnutoj kartici tahografa ostaju djelomično nevidljivi (nevidljiva je svaka neparna znamenka slijeva nadesno),
* u režimu preduzeća, podaci o vozaču (zahtjevi 081, 084 i 087) mogu se prenijeti samo za periode u kojima nema blokade ili za periode koja nije blokiralo neko drugo poduzeće (koje je identificirano s prvih 13 znamenki broja kartice preduzeća).
* kad u tahograf nije umetnuta kartica, podaci o vozaču se mogu prenijeti samo za tekući i prethodnih osam kalendarskih dana.

**4.   Sigurnost**

Sigurnost sistema ima za cilj zaštitu podakovne memorije tako da spriječi neovlašten pristub i manipuliranje podacima i otkrivanje svakog takvog pokušaja, zaštitu potpunosti i autentičnosti podataka koji se razmjenjuju između senzora kretanja i jedinice u vozilu, zaštitu potpunosti i autentičnosti podataka koji se razmjenjuju između tahografa i kartica tahografa, te provjeru potpunosti i autentičnosti preuzetih podataka.

012  
Kako bi se postigla sigurnost sistema, tahograf mora udovoljiti sigurnosnim zahtjevima navedenim u generičkim sigurnosnim ciljevima za senzor kretanja i jedinicu u vozilu (Dodatak 10.).

**III.   ZAHTJEVI U POGLEDU IZRADE I FUNKCIONALNI ZAHTJEVI ZA TAHOGRAFE**

**1.   Praćenje ubacivanja i vađenja kartica**

013  
Tahograf mora nadgledati kartične otvore tako da registrira ubacivanje i vađenje kartice.

014  
Po ubacivanju kartice tahograf mora ustanoviti je li umetnuta kartica važeća kartica tahografa i u tom slučaju identifikujeti vrstu kartice.

015  
Tahograf mora biti tako projektovan da se kartice tahografa zaključaju pri pravilnom ubacivanju u kartične otvore.

016  
Oslobađanje kartice tahografa može funkcionisati samo kada je vozilo zaustavljeno i nakon što su odgovarajući podaci sačuvani na kartice. Oslobađanje kartice zahtijeva aktivnost korisnika.

**2.   Mjerenje brzine i udaljenosti**

017  
Ova funkcija mora neprekidno mjeriti i biti u stanju dati stanje brojača kilometara koje odgovara ukupnoj udaljenosti koju je vozilo prešlo.

018  
Ova funkcija mora neprekidno mjeriti i biti u stanju dati brzinu vozila.

019  
Funkcija mjerenja brzine takođe daje informaciju kreće li se vozilo ili stoji. Smatra se da se vozilo kreće čim funkcija utvrdi više od 1 imp/sek u trajanju od najmanje pet sekundi na senzoru kretanja, u protivnom se smatra da vozilo stoji.

Uređaji za prikaz brzine (brzinomjer) i ukupno pređene udaljenosti (brojač kilometara) ugrađeni na svako vozilo opremljeno tahografom koji je usklađen odredbama ove Uredbe moraju zadovoljiti zahtjevima u pogledu maksimalnih odstupanja utvrđenih u ovom Prilogu (poglavlje III. dio 2. tačka 1. i poglavlje III. dio 2. tačka 2.).

019a

Za otkrivanje manipulacije podacima o kretanju vozila, podaci iz senzora kretanja potvrđuju se podacima o kretanju vozila iz jednog ili više izvora, koji su nezavisni od senzora kretanja.

**2.1.    Mjerenje pređene udaljenosti**

020  
Pređena udaljenost se može mjeriti:

* tako da se zbraja kretanje prema naprijed i prema natrag, ili
* tako da se računaju samo kretanja prema naprijed.

021  
Tahograf mora mjeriti udaljenost od 0 do 9 999 999,9 km.

022  
Izmjerena udaljenost mora biti u granicama sljedećih odstupanja (na najmanjoj udaljenosti od 1,000 m):

* ± 1 % prije ugradnje,
* ± 2 % pri ugradnji i periodičnom pregledu,
* ± 4 % pri korištenju.

023  
Izmjerena udaljenost mora imati razlučivost jednaku ili veću od 0,1 km.

**2.2.    Mjerenje brzine**

024  
Tahograf mora mjeriti brzinu od 0 do 220 km/h.

025  
Kako bi se osigurala najveća tolerancija prikazane brzine od ± 6 km/h pri korištenju, a s obzirom na:

* toleranciju od ± 2 km/h za ulazna odstupanja (trošenje guma, …),
* toleranciju od ± 1 km/h za mjerenja izvršena tokom ugradnje ili periodičnih pregleda,

tahograf mora, kod brzina između 20 i 180 km/h i za karakteristične koeficijente vozila između 4,000 i 25,000 imp/km mjeriti brzinu uz toleranciju od ± 1 km/h (pri konstantnoj brzini).

Napomena: Razlučivost spremanja podataka ima dodatnu toleranciju od ± 0,5 km/h za brzinu koju sprema tahograf.

025a  
Brzina se mora mjeriti ispravno unutar uobičajenih tolerancija u roku od 2 sekunde od kraja promjene brzine kada se brzina mijenjala više od 2 m/s2.

026  
Mjerenje brzine mora imati razlučivost jednaku ili bolju od 1 km/h.

**3.   Mjerenje vremena**

027  
Funkcija mjerenja vremena mora trajno mjeriti i digitalno iskazivati UTC datum i vrijeme.

028  
Pri datiranju podataka u tahografu (zapisi, razmjena podataka) i za sve ispise navedene u Dodatku 4. ‚Ispisi’, upotrebljavaju se UTC vrijeme i datum.

029  
Za prikaz lokalnog vremena mora biti moguće mijenjati prikaz razlike vremena u polusatnim koracima. Drugi pomaci, osim negativnih ili pozitivnih višekratnih pola sata, nisu dozvoljeni.

030  
Odstepene vremena može biti unutar vrijednosti od ± 2 sekunde po danu za uslove tipskog odobrenja.

031  
Vrijeme koje se mjeri mora imati razlučivost bolju od 1 sekunde ili jednaku.

032  
Na mjerenje vremena ne smije uticat prekid vanjskog napajanja kraći od 12 mjeseci u uslovima tipskog odobrenja.

**4.   Praćenje aktivnosti vozača**

033  
Ova funkcija mora neprekidno i odvojeno pratiti aktivnosti jednog vozača i jednog suvozača.

034  
Aktivnosti vozača su VOŽNJA, RAD, PRIPRAVNOST ili PAUZA/ODMOR.

035  
Vozač i/ili suvozač moraju imati mogućnost ručnog biranja između RADA, PRIPRAVNOSTI ili PAUZE/ODMORA.

036  
Kada se vozilo kreće, za vozača se automatski odabire VOŽNJA, a za suvozača se automatski odabire PRIPRAVNOST.

037  
Kad se vozilo zaustavi, za vozača se automatski odabire RAD.

038  
Prva promjena aktivnosti u aktivnost ODMOR ili PRIPRAVNOST nastaje u roku 120 sekundi od automatske promjene aktivnosti u aktivnost RAD nakon zaustavljanja vozila. Pretpostavlja se da je promjena aktivnosti nastubila u trenutku kad se vozilo zaustavilo (čime se moguće poništava promjena aktivnosti u RAD).

039  
Ova funkcija mora evidentirati podatke o promjenama aktivnosti u razlučivost od jedne minute.

041  
Ako je u minuti neposredno prije određene kalendarske minute i u minuti neposredno nakon nje registrirana aktivnost VOŽNJA, i ta minuta se u cijelosti smatra kao minuta VOŽNJE.”

042  
Određena kalendarska minuta, koja se po gornjem zahtjevu 041 ne smatra minutom VOŽNJE, u cijelosti se smatra kao minuta one vrste aktivnosti koja je najduže neprekidno trajala u toj minuti (ili posljednja aktivnost od jednako dugih aktivnosti).

043  
Ova funkcija takođe mora trajno pratiti neprekidno vrijeme vožnje i ukupno vrijeme pauze vozača.

**5.   Praćenje stanja vožnje**

044  
Ova funkcija mora neprekidno i automatski pratiti stanje vožnje.

045  
Stanje vožnje POSADA se odabire kada se dvije valjane vozačke kartice umetnu u tahograf, a u svim drugim slučajevima se odabire stanje vožnje JEDAN VOZAČ.

**6.   Ručni unos od strane vozača**

**6.1.    Unos mjesta početka i/ili kraja dnevnog perioda rada**

046  
Ova funkcija omogućava unos mjesta početka i/ili završetka dnevnog perioda rada vozača i/ili suvozača.

047  
Mjesta se definiraju kao država, te dodatno prema potrebi, kao regija.

048  
U vrijeme vađenja kartice vozača (ili kartice radionice) tahograf mora potaknuti (su)vozača da unese‚ mjesto završetka dnevnog perioda rada’.

049  
Tahograf mora omogućiti zanemarivanje ovog zahtjeva.

050  
Putem naredbi u menijima mora biti moguće unijeti mjesta početka i/ili završetka dnevnog periode rada. 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.

**6.2.    Ručni unos aktivnosti vozača**

050a  
Nakon umetanja kartice vozača (ili radionice), i samo tada, tahograf mora dopustiti ručne unose aktivnosti. Prema potrebi su ručni unosi mogući pri prvom umetanju prethodno neupotrebljavane kartice vozača (ili radionice).

Ručni unosi aktivnosti izvode se upotrebom vremenske zone lokalnog vremena i datuma (odstupanja UTC) koja je trenutno namještena u jedinicu u vozilu.

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

* datum i vrijeme njegovog posljednjeg vađenja kartice,
* po izboru: odstupanja lokalnog vremena, koji je trenutno namješten u jedinici vozila.

Mora biti moguć unos aktivnosti sa sljedećim ograničenjima:

* vrste aktivnosti su RAD, PRIPRAVNOST ili PAUZA/ODMOR,
* vremena početka i završetka za svaku aktivnost mogu biti samo u okviru periode od posljednjeg vađenja do trenutnog umetanja kartice.

Ne smije biti dopušteno da se aktivnosti uzajamno vremenski preklapaju.

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

Za vrijeme ručnih unosa povezanih uz umetanje kartice i ako je primjenljivo, vlasnik kartice ima mogućnost unijeti:

* mjesto gdje je završilo prethodni period dnevnog rada, povezano s odgovarajućim vremenom (ako nije već uneseno pri posljednjem vađenju kartice),
* mjesto gdje je trenutno period dnevnog rada započelo, povezano s odgovarajućim vremenom.
* Ako se unese lokacija, ista se bilježi na odgovarajuću tahografsku karticu.
* Ručni se unosi prekidaju, ako:
* se kartica izvadi, ili
* se vozilo kreće i kartica je u vozačkom prorezu.

Dozvoljeni su dodatni prekidi, npr. kratki odmor nakon određenog periode korisnikove neaktivnosti. Ako su ručni unosi prekinuti, tahograf potvrđuje sva potpuno unesena mjesta i aktivnosti (koja 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 ručnih unosa za drugu umetnutu karticu mora se omogućiti da se završe ručni unosi za prvu umetnutu karticu.

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

Ručni unos aktivnosti, hronološkim redom, za period od posljednjeg vađenja kartice do trenutnog umetanja kartice.

Vrijeme početka prve aktivnosti namješta se na vrijeme vađenja kartice. Za svaki sljedeći unos, vrijeme početka se unaprijed 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. Tahograf 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.

**6.3.    Unos posebnih stanja**

050b

Tahograf mora vozaču dopustiti unos sljedeća dva posebna stanja, u realnom vremenu:

‚IZVAN PODRUČJA PRIMJENE’ (početak, završetak)

‚VOŽNJA TRAJEKTOM/VOZOM

Stanje ‚VOŽNJA TRAJEKTOM/VOZOM ne može se pojaviti ako je otvoreno stanje ‚IZVAN PODRUČJA PRIMJENE’.

Otvoreno stanje ‚IZVAN PODRUČJA PRIMJENE’ tahograf automatski zatvara ako se kartica vozača umeće ili vadi.

Otvoreno stanje ‚IZVAN PODRUČJA PRIMJENE’ sprečava sljedeće događaje i upozorenja:

—vožnja bez odgovarajuće kartice,

—upozorenja povezana s neprekidnim periodm vožnje.”

**7.   Upravljanje blokadom preduzeća**

051  
Ova funkcija omogućava upravljanje blokadama koje postavi preduzeće kako bi ograničila pristub podacima preduzeća za sebe.

052  
Blokade preduzeća se sastoje od datuma/vremena početka (postavljanje blokade) i datuma/vremena završetka (skidanje blokade) pridruženih identifikaciji preduzeća naznačenoj u broju kartice preduzeća (pri postavljanju blokade).

053  
Blokade se mogu postaviti odnosno skinuti samo u realnom vremenu.

054  
Skidanje blokade može izvršiti samo preduzeće čija je blokada postavljena (što određuje prvih 13 karakteristika broja kartice preduzeća) ili,

055  
Skidanje blokade je automatsko kada druga preduzeće izvrši postavljanje blokade.

055a  
U slučaju postavljanja blokade od strane preduzeća kada je prethodna blokada bila za istu firmu, pretpostavlja se da prethodna blokada nije bila skinuta, te da je i dalje postavljena.

**8.   Praćenje nadzornih aktivnosti**

056  
Ova funkcija prati aktivnosti PRIKAZA, ISPISA i PREUZIMANJA podataka iz tahografa i kartice dok je u načinu nadzora.

057  
Ova funkcija takođe prati aktivnosti KONTROLE PREKORAČENJA BRZINE dok je u načinu nadzora. Smatra se da je kontrola prekoračenja brzine nastala ako je u načinu nadzora ispis ‚prekoračenja brzine’ poslan na pisač ili na displej ili ako su podaci o ‚događajima i greškama’ preuzeti iz podakovne memorije tahografa.

**9.   Prepoznavanje događaja i/ili grešaka**

058  
Ova funkcija otkriva sljedeće događaje i/ili greške:

**9.1.    Događaj ‚ubacivanje nevažeće kartice’**

059  
Ovaj događaj se aktivira ubacivanjem bilo koje nevažeće kartice i/ili ako istekne valjanost umetnute važeće kartice.

**9.2.    Događaj ‚sukob kartica’**

060  
Ovaj događaj se aktivira ako se javi bilo koja kombinacija s valjanim karticama označena u tablici s X:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sukob kartica** | | **Otvor vozača** | | | | |
| **Bez kartice** | **Kartica vozača** | **Kontrolna kartica** | **Kartica radionice** | **Kartica prevoznika** |
| Otvor suvozača | Bez kartice |  |  |  |  |  |
| Kartica vozača |  |  |  | X |  |
| Kontrolna kartica |  |  | X | X | X |
| Kartica radionice |  | X | X | X | X |
| Kartica prevoznika |  |  | X | X | X |

**9.3.    Događaj ‚vremensko preklapanje’**

061  
Ovaj slučaj se aktivira kada su datum/vrijeme posljednjeg vađenja vozačke kartice, očitani s kartice, kasniji nego tekući datum/vrijeme tahografa u koji je umetnuta kartica.

**9.4    Događaj ‚vožnja bez odgovarajuće kartice’**

062  
Ovaj događaj se aktivira za bilo koju kombinaciju kartica tahografa označenu s 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 kartice (ili nevažeća kartica)** | **Kartica vozača** | **Kontrolna kartica** | **Kartica radionice** | **Kartica prevoznika** |
| Otvor suvozača | Bez kartice (ili nevažeća kartica) | X |  | X |  | X |
| Kartica vozača | X |  | X | X | X |
| Kontrolna kartica | X | X | X | X | X |
| Kartica radionice | X | X | X |  | X |
| Kartica prevoznika | X | X | X | X | X |

**9.5.    Događaj ‚ubacivanje kartice tokom vožnje’**

063  
Ovaj događaj se aktivira ako se kartica tahografa umetne u bilo koji otvor u vrijeme dok je aktivnost vozača VOŽNJA.

**9.6.    Događaj ‚neispravno zatvaranje posljednje razmjene podataka s karticom’**

064  
Ovaj događaj se aktivira kada pri ubacivanju kartice tahograf utvrdi da unatoč odredbama utvrđenim u stavu III. tački 1. prethodna razmjena podataka s karticom nije pravilno završena (kartica je izvađena prije nego su svi potrebni podaci sačuvani na karticu). Ovaj događaj se aktivira samo s karticom vozača i karticom radionice.

**9.7.    Događaj ‚prekoračenje brzine’**

065  
Ovaj se događaj aktivira pri svakom prekoračenju brzine. Ovaj se zahtjev primjenjuje samo na vozila kategorije M2, M3, N2 ili N3, kako je definisano u Prilogu II. Direktivi 2007/46/EZ, o uspostavi okvira za homologaciju motornih vozila i njihovih prikolica.

**9.8.    Događaj ‚prekid napajanja’**

066  
Ovaj događaj se aktivira van kalibracije pri svakom prekidu napajanja senzora kretanja i/ili jedinice u vozilu dužeg od 200 milisekundi. Prag prekida utvrđuje proizvođač. Pad napajanja zbog pokretanja motora vozila ne aktivira ovaj događaj.

**9.9.    Događaj ‚greška podataka kretanja’**

067  
Ovaj događaj se aktivira u slučaju prekida redovnog protoka podataka između senzora kretanja i jedinice u vozilu i/ili u slučaju greške potpunosti podataka ili greške autentifikacije podataka tokom razmjene podataka između senzora kretanja i jedinice u vozilu.

**9.9.a Događaj   ‚Protivrječnost u kretanju vozila’**

067a Ovaj se događaj takođe aktivira kad je mjerenje nulte brzine u suprotnosti s podacima o kretanju iz najmanje još jednog nezavisnog izvora kretanja duže od jedne neprekinute minute.

067b Ovaj se događaj takođe može aktivirati u slučajevima kad jedinica vozila dobiva ili preračunava vrijednost brzine iz vanjskog nezavisnog izvora podataka o kretanju, ali su takve vrijednosti brzine znatno u suprotnostima s vrijednostima preračunatim na temelju signala brzine senzora kretanja i traju duže od jedne minute.

**9.10.    Događaj ‚pokušaj probijanja zaštite’**

068  
Ovaj događaj se aktivira za sve ostale događaje koji utiču na sigurnost senzora kretanja i/ili jedinice u vozilu kako je navedeno u generičkim sigurnosnim ciljevima za takve sastavne dijelove dok nisu u načinu kalibracije.

**9.11.    Greška ‚kartica’**

069  
Ova greška se aktivira ako se tokom rada javi greška na kartici tahografa.

**9.12.    Greška ‚tahograf’**

070  
Ova greška se aktivira za neku od sljedećih grešaka, dok nije u načinu kalibracije:

* interna greška jedinice u vozilu,
* greška pisača,
* greška displeja,
* greška pri preuzimanju podataka,
* greška senzora.

**10.   Postupak provjere i samoprovjere**

071  
Tahograf sam otkriva greške samoprovjerom i provjerama prema sljedećoj tablici:

|  |  |  |
| --- | --- | --- |
| **Podsistem koji se provjerava** | **Samoprovjera** | **Provjera** |
| Program |  | Potpunost |
| Memorija podataka | Pristub | Pristub, potpunost podataka |
| Uređaji kartičnog sučelja | Pristub | Pristub |
| Tipkovnica |  | Ručna provjera |
| Pisač | (zavisi o proizvođaču) | Ispis |
| Displej |  | Vizualna provjera |
| Preuzimanje podataka (vrši se samo tokom preuzimanja podataka) | Pravilan rad |  |
| Senzor | Pravilan rad | Pravilan rad |

**11.   Očitavanje podataka iz memorije**

072  
Tahograf mora biti u stanju očitati sve podatke sačuvane u njegovoj podakovnoj memoriji.

**12.   Zapis i čuvanje u podakovnoj memoriji**

Za potrebe ovog stava:

* ‚365 dana’ se definira kao 365 kalendarskih dana prosječne aktivnosti vozača u vozilu. Prosječna dnevna aktivnost u vozilu definira se kao najmanje šest vozača ili suvozača, šest ciklusa ubacivanja i vađenja kartice i 256 promjena aktivnosti. Tako ‚365 dana’ uključuje najmanje 2,190 (su)vozača, 2,190 ciklusa ubacivanja i vađenja kartice i 93,440 promjene aktivnosti,
* vremena se evidentiraju s razlučivošću od jedne minute, osim ako nije drugačije propisano,
* stanje brojača kilometara se evidentira s razlučivošću od jednog kilometra,
* brzine se evidentiraju s razlučivošću od 1 km/h.

073  
Na podatke sačuvane u podakovnoj memoriji ne smije uticat nikakav spoljni prekid napajanja kraći od dvanaest mjeseci u tipsko odobrenim uslovima.

074  
Tahograf mora moći zapisivati i spremati direktno ili indirektno sljedeće podatke u svojoj memoriji podataka:

**12.1.    Identifikacijski podaci o uređaju**

**12.1.1.   Identifikacijski podaci jedinice u vozilu**

075  
Tahograf mora moći sačuvati sljedeće identifikacijske podatke jedinice u vozilu u svojoj memoriji podataka:

* naziv proizvođača,
* adresa proizvođača,
* broj dijela,
* serijski broj,
* broj verzije programa,
* datum ugradnje verzije programa,
* godina proizvodnje uređaja,
* broj tipskog odobrenja.

076  
Identifikacijske podatke jedinice u vozilu evidentira i arhivira jednom zauvijek proizvođač jedinice u vozilu, osim podataka vezanih uz program i broja tipskog odobrenja koji se mogu mijenjati kod ažuriranja programa.

**12.1.2.   Identifikacijski podaci senzora kretanja**

077  
Senzor kretanja mora biti u stanju čuvati u svojoj memoriji sljedeće identifikacijske podatke:

* naziv proizvođača,
* broj dijela,
* serijski broj,
* broj tipskog odobrenja,
* identifikator ugrađene sigurnosne komponente (npr. interni broj ugrađenog čipa/procesora),
* identifikator operativnog sistema (npr. broj verzije programa).

078  
Identifikacijske podatke senzora kretanja evidentira i arhivira jednom zauvijek u senzoru kretanja proizvođač senzora kretanja.

079  
Jedinica u vozilu mora biti u stanju čuvati u svojoj podakovnoj memoriji sljedeće identifikacijske podatke senzora kretanja s kojim je trenutno uparena:

* serijski broj,
* broj tipskog odobrenja,
* datum prvog uparivanja.

**12.2.    Sigurnosni elementi**

080  
Tahograf mora biti u stanju sačuvati sljedeće sigurnosne elemente:

* evropski javni ključ,
* certifikat države članice,
* certifikat tahografa,
* privatni ključ tahografa.

Proizvođač jedinice u vozilu ugrađuje u tahograf sigurnosne elemente.

**12.3.    Podaci o ubacivanju i vađenju kartice vozača**

081  
Za svaki ciklus ubacivanja i vađenja kartice vozača ili kartice radionice u/iz uređaja, tahograf mora zaevidentirati i sačuvati u svoju memoriju podataka:

* prezime(na) i ime(na) nosioca kartice sačuvana na kartici,
* broj kartice, državu članicu izdavanja i datum isteka sačuvane na kartici,
* datum i vrijeme ubacivanja,
* stanje brojača kilometara vozila pri ubacivanju kartice,
* otvor u koji je kartica umetnuta,
* datum i vrijeme vađenja,
* stanje brojača kilometara vozila pri vađenju kartice,
* sljedeće informacije sačuvane na kartici o prethodnom vozilu koje je vozač koristio:
* registracijski broj vozila i državu članicu u kojoj je vozilo registrovano,
* datum i vrijeme vađenja kartice,
* oznaku koja pokazuje je li prilikom ubacivanju kartice vlasnik kartice ručno unio aktivnosti.

082  
Podaci memorija mora biti u stanju čuvati te podatke najmanje 365 dana.

083  
Kad se iscrpi kapacitet memorije za čuvanje, novi podaci zamjenjuju najstarije podatke.

**12.4.    Podaci o aktivnosti vozača**

084  
Tahograf zapisuje i sprema u svoju memoriju podataka svaku promjenu aktivnosti vozača i/ili suvozača i/ili svaku promjenu stanja vožnje i/ili svako ubacivanje ili vađenje kartice vozača ili kartice radionice:

* stanje vožnje (POSADA, JEDAN VOZAČ),
* otvor (VOZAČ, SUVOZAČ),
* status kartice u odgovarajućem otvoru (UMETNUTA, NIJE UMETNUTA) (vidjeti napomenu),
* aktivnost (VOŽNJA, PRIPRAVNOST, RAD, PAUZA/ODMOR),
* datum i vrijeme promjene.

Napomena: 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 prevoznika ili nije umetnuta nikakva kartica).

Napomena: podaci o aktivnosti koje ručno unosi vozač se ne evidentiraju u podakovnoj memoriji.

085  
Podaci memorija mora biti u stanju čuvati podatke o aktivnosti vozača najmanje 365 dana.

086  
Kada se iscrpi kapacitet memorije za pohranu, novi podaci zamjenjuju najstarije podatke.

**12.5.    Mjesta početka i/ili završetka dnevnog perioda rada**

087  
Tahograf evidentira i arhivira u svoju memoriju podataka svaki unos mjesta početka i/ili završetka dnevnog perioda rada od strane (su)vozača:

* prema potrebi, broj kartice (su)vozača i državu članicu izdavaoca kartice,
* datum i vrijeme unosa (ili datum/vrijeme koji se odnosi na ručni unos),
* vrsta unosa (početak ili završetak, stanje unosa),
* državu i regiju u koju se ulazi,
* stanje brojača kilometara vozila.

088  
Podaci memorija mora biti u stanju čuvati podatke o početku i/ili završetku dnevnog perioda rada najmanje 365 dana (uz pretpostavu da jedan vozač izvrši dva unosa dnevno).

089  
Kada se iscrpi kapacitet memorije za čuvanje, novi podaci zamjenjuju najstarije podatke.

**12.6.    Stanje brojača pređenih kilometara**

090  
Tahograf zapisuje i sprema u svoju memoriju podataka stanje brojača pređenih kilometara i pripadajući datum u ponoć svakog kalendarskog dana.

091  
Podaci memorija može biti u stanju pohranjivati ponoćna stanja brojača kilometara najmanje 365 kalendarskih dana.

092  
Kada se iscrpi kapacitet memorije za čuvanje, novi podaci zamjenjuju najstarije podatke.

**12.7.    Detaljni podaci o brzini**

093  
Tahograf zapisuje i sprema u memoriju podataka trenutnu brzinu vozila i pripadajući datum i vrijeme u svakoj sekundi tokom najmanje posljednja 24 sata kretanja vozila.

**12.8.    Podaci o događanjima**

Za potrebe ovog podstava, vrijeme se evidentira s razlučivošću od jedne sekunde.

094  
Za svaki otkriveni događaj, tahograf zapisuje i sprema u svoju memoriju podataka sljedeće podatke prema sljedećim pravilima spremanja:

|  |  |  |
| --- | --- | --- |
| **Događaj** | **Pravila spremanja** | **Podaci koji se zapisuju za svaki događaj** |
| Sukob kartica | |  |  | | --- | --- | | — | 10 posljednjih događaja | | |  |  | | --- | --- | | — | datum i vrijeme početka događaja, |  |  |  | | --- | --- | | — | datum i vrijeme kraja događaja, |  |  |  | | --- | --- | | — | vrsta kartica, broj i država članica izdavaoc dviju sukobljenih kartica. | |
| Vožnja bez odgovarajuće kartice | |  |  | | --- | --- | | — | najduži događaj od svih događaja u posljednjih 10 dana napauza, |  |  |  | | --- | --- | | — | pet najdužih događaja tokom posljednjih 365 dana. | | |  |  | | --- | --- | | — | datum i vrijeme početka događaja, |  |  |  | | --- | --- | | — | datum i vrijeme kraja događaja, |  |  |  | | --- | --- | | — | vrsta kartice, broj i država članica izdavaoc bilo koje kartice umetnute na početku i/ili kraju događaja, |  |  |  | | --- | --- | | — | broj sličnih događaja tog dana. | |
| Ubacivanje kartice tokom vožnje | |  |  | | --- | --- | | — | posljednji događaj od svih događaja u posljednjih 10 dana napauza. | | |  |  | | --- | --- | | — | datum i vrijeme događaja, |  |  |  | | --- | --- | | — | vrsta kartice, broj i država članica izdavanja, |  |  |  | | --- | --- | | — | broj sličnih događaja tog dana. | |
| Posljednje period razmjene podataka s karticom nije pravilno završeno | |  |  | | --- | --- | | — | 10 posljednjih događaja | | |  |  | | --- | --- | | — | datum i vrijeme ubacivanja kartice, |  |  |  | | --- | --- | | — | vrsta kartice, broj i država članica izdavaoc, |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | — | podaci o posljednjem razdoblju razmjene podataka očitani s kartice:   |  |  | | --- | --- | | — | datum i vrijeme ubacivanja kartice, |  |  |  | | --- | --- | | — | registracijski broj vozila i država članica registracije. | | |
| Prekoračenje brzine[(10)](https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex:32002R1360#ntr10-L_2002207HR.01000402-E0010) | |  |  | | --- | --- | | — | najteži događaj od svih događaja u posljednjih 10 dana napauza (tj. onaj s najvećom prosječnom brzinom), |  |  |  | | --- | --- | | — | pet najtežih događaja tokom posljednjih 365 dana, |  |  |  | | --- | --- | | — | prvi slučaj koji se desio nakon posljednje kalibracije. | | |  |  | | --- | --- | | — | datum i vrijeme početka događaja, |  |  |  | | --- | --- | | — | datum i vrijeme kraja događaja, |  |  |  | | --- | --- | | — | maksimalna brzina izmjerena tokom događaja, |  |  |  | | --- | --- | | — | aritmetička prosječna brzina izmjerena tokom događaja, |  |  |  | | --- | --- | | — | vrsta kartice, broj i država članica izdavaoc kartice vozača (prema potrebi), |  |  |  | | --- | --- | | — | broj sličnih događaja tog dana. | |
| Prekid napajanja[(11)](https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex:32002R1360#ntr11-L_2002207HR.01000402-E0011) | |  |  | | --- | --- | | — | najduži događaj od svih događaja u posljednjih 10 dana napauza, |  |  |  | | --- | --- | | — | pet najdužih događaja tokom posljednjih 365 dana. | | |  |  | | --- | --- | | — | datum i vrijeme početka događaja, |  |  |  | | --- | --- | | — | datum i vrijeme kraja događaja, |  |  |  | | --- | --- | | — | vrsta kartica, broj i država članica izdavaoc bilo koje kartice umetnute na početku i/ili kraju događaja, |  |  |  | | --- | --- | | — | broj sličnih događaja tog dana. | |
| Greška u podacima o kretanju | |  |  | | --- | --- | | — | najduži događaj od svih događaja u posljednjih 10 dana napauza, |  |  |  | | --- | --- | | — | pet najdužih događaja tokom posljednjih 365 dana. | | |  |  | | --- | --- | | — | datum i vrijeme početka događaja, |  |  |  | | --- | --- | | — | datum i vrijeme kraja događaja, |  |  |  | | --- | --- | | — | vrsta kartica, broj i država članica izdavaoc bilo koje kartice umetnute na početku i/ili kraju događaja, |  |  |  | | --- | --- | | — | broj sličnih događaja tog dana. | |
| Protivrječnost u kretanju vozila | |  |  | | --- | --- | | — | najduži događaj za svaki od 10 zadnjih dana pojave, | | — | 5 najdužih događaja u zadnjih 365 dana | | |  |  | | --- | --- | | — | datum i vrijeme početka događaja, | | — | datum i vrijeme završetka događaja, | |  | vrsta, broj i država članica izdavanja bilo koje kartice umetnute na početku i/ili završetku događaja, | | — | broj sličnih događaja tog dana. | |
| Pokušaj probijanja zaštite | |  |  | | --- | --- | | — | 10 posljednjih događaja po vrsti događaja | | |  |  | | --- | --- | | — | datum i vrijeme početka događaja, |  |  |  | | --- | --- | | — | datum i vrijeme kraja događaja (ako je bitno), |  |  |  | | --- | --- | | — | vrsta kartica, broj i država članica izdavaoc bilo koje kartice umetnute na početku i/ili kraju događaja, |  |  |  | | --- | --- | | — | broj sličnih događaja tog dana. | |

**12.9.    Podaci o greškama**

U smislu ovog podstava, vrijeme se evidentira s razlučivošću od jedne sekunde.

096  
Za svaku otkrivenu grešku tahograf mora pokušati zapisati i sačuvati u svoju memoriju podataka sljedeće podatke prema sljedećim pravilima spremanja:

|  |  |  |
| --- | --- | --- |
| **Događaj** | **Pravila spremanja** | **Podaci koji se zapisuju za događaj** |
| Greška kartice | |  |  | | --- | --- | | — | 10 posljednjih grešaka kartice vozača | | |  |  | | --- | --- | | — | datum i vrijeme početka greške, |  |  |  | | --- | --- | | — | datum i vrijeme završetka greške, |  |  |  | | --- | --- | | — | vrsta kartice, broj i država članica izdavaoc. | |
| Greška tahografa | |  |  | | --- | --- | | — | 10 posljednjih grešaka za svaku vrstu greške, |  |  |  | | --- | --- | | — | prva greška nakon posljednje kalibracije. | | |  |  | | --- | --- | | — | datum i vrijeme početka greške, |  |  |  | | --- | --- | | — | datum i vrijeme završetka greške, |  |  |  | | --- | --- | | — | vrsta greške, |  |  |  | | --- | --- | | — | vrsta kartice, broj i država članica izdavaoc bilo koje kartice koja je umetnuta na početku i/ili kraju greške. | |

**12.10.    Podaci o kalibraciji**

097  
Tahograf zapisuje i sprema u svojoj podakovnoj memoriji podatke od važnosti za:

* poznate parametre kalibracije u trenutku aktivacije,
* njegovu prvu kalibraciju nakon aktivacije,
* njegovu prvu kalibraciju u trenutnom vozilu (koje se identifikuje VIN brojem),
* pet posljednjih kalibracija (ako je tokom jednog kalendarskog dana izvršeno više kalibracija, sprema se samo posljednja izvršena tog dana).

098  
Za svaku od spomenutih kalibracija se evidentiraju sljedeći podaci:

* svrha kalibracije (aktivacija, prva ugradnja, ugradnja, periodični pregled),
* naziv i adresa radionice,
* broj kartice radionice, država članica izdavanja kartice i datum isteka važnosti kartice,
* identifikacija vozila,
* ažurirani ili potvrđeni parametri: w, k, l, dimenzije guma, podešenost ograničavača brzine, brojač kilometara (stare i nove vrijednosti), datum i vrijeme (stare i nove vrijednosti).

099  
Senzor kretanja zapisuje i sprema u svoju memoriju sljedeće podatke o ugradnji senzora kretanja:

* prvo uparivanje s jedinicom u vozilu (datum, vrijeme, broj tipskog odobrenja jedinice u vozilu, serijski broj jedinice u vozilu),
* posljednje uparivanje s jedinicom u vozilu (datum, vrijeme, broj tipskog odobrenja jedince u vozilu, serijski broj jedince u vozilu).

**12.11.    Podaci o podešavanju vremena**

100  
Tahograf zapisuje i sprema u svojoj memoriji podatke od važnosti za:

* posljednje podešavanje vremena,
* pet podešavanja vremena najvećih razmjera nakon posljednje kalibracije,

obavljenih u načinu kalibracije van redovne kalibracije (definicija (f)).

101  
Za svako od tih podešavanja vremena evidentiraju se sljedeći podaci:

* datum i vrijeme, stara vrijednost,
* datum i vrijeme, nova vrijednost,
* naziv i adresa radionice,
* broj kartice radionice, država članica izdavanja kartice i datum isteka važnosti kartice.

**12.12.    Podaci o nadzornim aktivnostima**

102  
Tahograf zapisuje i sprema u svoju memoriju sljedeće podatke od važnosti za 20 posljednjih nadzornih aktivnosti:

* datum i vrijeme nadzora,
* broj kontrolne kartice i državu članicu izdavaoca kartice,
* vrsta nadzora (prikaz i/ili ispis i/ili preuzimanje podataka s jedinice vozila i/ili s kartice).

103  
U slučaju preuzimanja podataka, evidentiraju se takođe datumi prvog i posljednjeg dana za koje se preuzimaju podaci.

**12.13.    Podaci o zaključavanju podataka preduzeća**

104  
Tahograf bilježi i arhivira u svojoj podatkovnoj memoriji sljedeće podatke koji se odnose na 255 posljednjih blokadi od strane preduzeća:

* datum i vrijeme zaključavanja blokade,
* datum i vrijeme otključavanja blokade,
* broj kartice preduzeća i državu članicu izdavanja kartice,
* naziv i adresu preduzeća.

Podaci koji su bili prethodno zaključani blokadom, koja je radi gore navedene granice odstranjena iz memorije, tretiraju se kao da nisu zaključani.

**12.14.    Podaci o aktivnostima preuzimanja podataka**

105  
Tahograf zapisuje i sprema u svojoj podakovnoj memoriji sljedeće podatke od važnosti za posljednje preuzimanje podataka iz podakovne memorije na vanjske medije u načinu rada prevoznika ili kalibracije:

* datum i vrijeme preuzimanja podataka,
* broj kartice prevoznika ili kartice radionice i država članica izdavaoca kartice,
* naziv prevoznika ili radionice.

**12.15.    Podaci o posebnim uslovima**

105a  
Tahograf zapisuje u svoju memoriju podataka sljedeće podatke od važnosti za posebna stanja:

* datum i vrijeme unosa,
* vrsta posebnog stanja.

105b  
Podaci memorija mora biti u stanju čuvati podatke o posebnim uslovima najmanje 365 dana (uz pretpostavu da se dnevno u prosjeku otvara i zatvara jedno stanje). Kada se iscrpi kapacitet za čuvanje, novi podaci zamjenjuju najstarije podatke.

**13.   Očitavanje kartica tahografa**

106  
Tahograf mora biti u stanju očitavati s kartica tahografa, ako je primjereno, sljedeće potrebne podatke:

* identifikujeti vrstu kartice, nosioca kartice, prethodno korišteno vozilo, datum i vrijeme posljednjeg vađenja kartice i aktivnost odabranu u to vrijeme,
* provjeriti je li posljednje period rada s karticom pravilno završeno,
* proračunati neprekidno vrijeme vožnje vozača, ukupno vrijeme pauze i ukupno vrijeme vožnje za prethodni i tekuću nedelju,
* izraditi ispise prema podacima zapisanim na kartici vozača,
* preuzeti podatke s kartice vozača na vanjske medije.

107  
U slučaju greške pri očitavanju, tahograf mora ponovo pokušati, najviše tri puta, istu naredbu očitavanja, te će tada, ako je očitavanje ponovno bilo neuspješno, karticu proglasiti neispravnom i nevažećom.

**14.   Zapisivanje i čuvanje podataka na tahografske kartice**

108  
Tahograf postavlja ‚podatke o razmjeni podataka s karticom’ u karticu vozača ili karticu radionice odmah nakon ubacivanja kartice.

109  
Tahograf ažurira podatke sačuvane na valjanoj kartici vozača, radionice i/ili nadzornoj kartici sa svim podacima koji su bitni za period u kojem je kartica umetnuta i koji se odnose na nosioca kartice. Podaci arhivirani na tim karticama navedeni su u poglavlju IV.

109a  
Tahograf ažurira podatke o aktivnosti vozača i lokaciji (kako je navedeno u poglavlju IV, stavcima 5.2.5. i 5.2.6.) sačuvane na valjanim karticama vozača i/ili karticama radionice s podacima o aktivnosti i lokaciji koje je vlasnik kartice unio ručno.

109b

događaj ‚Protivrječnost u kretanju vozila’ ne arhivira se na karticama vozača i radionice.

110  
Ažuriranje kartica tahografa mora biti takvo da, prema potrebi i uzimajući u obzir stvarni kapacitet za čuvanje, najnoviji podaci zamjenjuju najstarije.

111  
U slučaju greške zapisa, tahograf mora pokušati ponovno, najviše tri puta, izvršiti istu naredbu zapisivanja, te će ako je i dalje neuspješna, proglasiti karticu neispravnom i nevažećom.

112  
Prije oslobađanja vozačke kartice, a nakon što su svi potrebni podaci sačuvani na karticu, tahograf će poništiti podatke iz perioda rada s tom karticom.

**15.   Prikaz**

113  
Displej mora imati najmanje 20 znakova.

114  
Minimalna veličina znaka je 5 mm u visinu i 3,5 mm u širinu.

114a  
Prikaz podržava znakove navedene u Dodatku 1. poglavlja 4. ‚Grupa znakova’. Prikaz može koristiti pojednostavnjene znakove (npr. znakovi s naglaskom mogu se prikazivati bez naglaska ili se mala slova mogu prikazivati kao velika slova).

115  
Displej mora imati odgovarajuće neblješteće osvjetljenje.

116  
Oznake moraju biti vidljive s vanjske strane tahografa.

117  
Tahograf mora biti u stanju prikazati:

* standardne podatke,
* podatke upozorenja,
* podatke o pristubu meniju,
* ostale podatke koje korisnik zatraži.

Tahograf može prikazati dodatne informacije ako ih je moguće jasno razlikovati od gore navedenih podataka.

118  
Displej tahografa koristi piktograme ili kombinacije piktograma navedene u Dodatku 3. Na displeju se mogu takođe prikazati dodatni piktogrami ili kombinacije piktograma, ako ih je moguće jasno razlikovati od ranije spomenutih piktograma ili kombinacija piktograma.

119  
Displej mora biti uključen uvijek kada se vozilo kreće.

120  
Tahograf može imati ručnu ili automatsku mogućnost isključivanja displeja kada se vozilo ne kreće.

Oblik prikaza naveden je u Dodatku 5.

**15.1.    Standardni prikaz**

121  
Kada nije potreban prikaz nikakvih drugih podataka, tahograf mora standardno prikazivati sljedeće informacije:

* lokalno vrijeme (kao rezultat UTC vremena i odstupanja kojeg namješta vozač),
* režim rada,
* trenutnu aktivnost vozača i trenutnu aktivnost suvozača.

Informacije koje se odnose na vozača:

* ako je njegova trenutna aktivnost VOŽNJA, njegovo trenutno neprekidno period vožnje i njegovo trenutno ukupno vrijeme pauze,
* ako njegova trenutna aktivnost nije VOŽNJA, trenutno trajanje ove aktivnosti (od kada je odabrana) i njegovo trenutno ukupno vrijeme pauze.

122  
Prikaz podataka vezanih uz svakog vozača mora biti jasan, jednostavan i nedvosmislen. U slučaju kada se informacije o vozaču i suvozaču ne mogu prikazati istovremeno, tahograf mora standardno prikazivati informacije u vezi vozača, a korisniku mora omogućiti da prikaže i informacije u vezi suvozača.

123  
U slučaju kad širina displeja ne omogućava standardno prikazivanje načina rada, tahograf mora nakrako prikazati novi način rada kad se on izmijeni.

124  
Tahograf nakrako prikazuje ime nosioca kartice pri ubacivanju kartice.

124a  
Kad je započelo stanje ‚VAN NADLEŽNOSTI standardni displej mora, koristeći odgovarajući piktogram, prikazati da je takvo stanje započelo (prihvatljivo je da se tekuća aktivnost vozača ne mora prikazati istovremeno).

**15.2.    Prikaz upozorenja**

125  
Tahograf prikazuje informaciju upozorenja koristeći prvenstveno piktograme iz Dodatka 3., dopunjene prema potrebi dodatnim numerički šifriranim informacijama. Može se takođe dodati tekstualni opis upozorenja na jeziku po odabiru vozača.

**15.3.    Pristub meniju**

126  
Tahograf mora osigurati potrebne naredbe putem odgovarajuće strukture izbornika.

**15.4.    Ostali prikazi**

127  
Na zahtjev se mora omogućiti odabir sljedećih prikaza:

* UTC datum i vrijeme, te odstupanja lokalnog vremena,
* sadržaj bilo kojeg od šest ispisa u istom obliku kao što su sami ispisi,
* neprekidno period vožnje i ukupno vrijeme pauze vozača,
* neprekidno period vožnje i ukupno vrijeme pauze suvozača,
* ukupno period vožnje vozača u prethodnom i tekućoj nedelji,
* ukupno period vožnje suvozača u prethodnom i tekućoj nedelji.

Neobavezno:

* sadašnje trajanje aktivnosti suvozača (otkad je odabrana),
* ukupno period vožnje vozača u tekućoj nedelji,
* ukupno period vožnje vozača za tekući period dnevnog rada,
* ukupno period vožnje suvozača za tekući period dnevnog rada.

128  
Prikaz sadržaja ispisa je u slijedu, redak po redak. Ako je širina displeja manja od 14 slovnih znakova, korisniku se pruža potpuna informacija na primjeren način (nekoliko redaka, klizni prikaz teksta, …). Reci ispisa koji se odnose na ručno unesene informacije mogu se izostaviti iz prikaza.

**16.   Ispis**

129  
Tahograf mora biti u stanju ispisati informacije iz svoje podakovne memorije i/ili kartica tahografa u obliku šest sljedećih ispisa:

* dnevni ispis aktivnosti vozača s kartice,
* dnevni ispis aktivnosti vozača iz jedinice u vozilu,
* ispis događaja i grešaka s kartice,
* ispis događaja i grešaka iz jedinice u vozilu,
* ispis tehničkih podataka,
* ispis prekoračenja brzine.

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

Na kraju ispisa mogu se dati dodatni podaci.

Tahograf može omogućiti i druge ispise, ako se oni jasno razlikuju od šest gore spomenutih ispisa.

130  
‚Dnevni ispis aktivnosti vozača s kartice’ i ‚ispis događaja i grešaka s kartice’ moraju biti dostubni samo kada je kartica vozača ili kartica radionice umetnuta u tahograf. Tahograf zapisuje do tada sačuvane podatke na odgovarajućoj kartici prije početka ispisa.

131  
Kako bi se izradio ‚dnevni ispis aktivnosti vozača s kartice’ i ‚ispis događaja i grešaka iz kartice’, tahograf 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 umetnute u tahograf.

132  
Pisač mora moći ispisati 24 slovna znaka po retku.

133  
Minimalna veličina slovnih znakova mora biti 2,1 mm u visinu i 1,5 mm u širinu.

133a  
Pisač podržava znakove navedene u Dodatku 1. poglavlju 4. ‚Grupa znakova’.

134  
Pisači moraju biti tako izrađeni da daju ispise s takvom oštrinom da se izbjegne svaka nejasnoća pri njihovom čitanju.

135  
Ispisi moraju zadržati svoje dimenzije i zapise pod uobičajenim uslovima vlažnosti (10 do 90 %) i temperature.

136  
Papir za tahograf mora imati odgovarajuću oznaku homologacije i naznaku vrste (vrsta) tahografa u kojima se može upotrebljavati.

136a

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

136b Papir za ispis mora biti najmanje u skladu sa specifikacijama ispitivanja, definisanim na internetskoj stranici laboratorija imenovanog za obavljanje ispitivanja interoperabilnosti, kako je utvrđeno u zahtjevu 278.

136c Specifikacije, opisane u gornjem stavku, mogu se izmijeniti, dopuniti ili ažurirati samo nakon što se imenovani laboratorij, skupa s tijelima za homologaciju, posavjetuje s proizvođačem homologovanih jedinica vozila digitalnog tahografa.

137  
Takođe mora postojati mogućnost da se u ove dokumente dodaju rukom pisane zabilješke, kao što je potpis vozača.

138  
Slučajeve nepauza papira pri ispisu tahograf mora riješiti tako da nakon ponovnog ubacivanja papira, ponovno počne ispis od početka ili se ispis nastavi uz jasno upućivanje na prethodno ispisan dio.

**17.   Upozorenja**

139  
Tahograf upozorava vozača pri otkrivanju svakog događaja ili greške.

140  
Upozorenje o prekidu napajanja može se odgoditi do ponovne uspostave napajanja.

141  
Tahograf mora upozoriti vozača 15 minuta prije i u trenutku prekoračenja najvećeg dozvoljenog neprekidnog perioda vožnje.

142  
Upozorenja moraju biti vizualna. Pored vizualnih upozorenja moguće je predvidjeti i davanje zvučnog signala.

143  
Vizualna upozorenja moraju biti korisniku jasno prepoznatljiva, moraju biti smještena u vidnom polju vozača i jasno čitljiva i danju i noću.

144  
Vizualna upozorenja mogu biti ugrađena u tahograf i/ili odvojena od tahografa.

145  
U poslednjem slučaju treba se označiti simbolom ‚T’.

146  
Upozorenja moraju trajati najmanje 30 sekundi, osim ako ih korisnik ne potvrdi pritiskom na bilo koju tipku tahografa: Prva potvrda ne smije izbrisati prikaz uzroka upozorenja iz sljedećeg stava.

147  
Uzrok upozorenja se mora prikazati na tahografu i ostati vidljiv dok ga korisnik ne potvrdi korištenjem posebne tipke ili naredbe u tahografu.

148  
Dodatna upozorenja se mogu predvidjeti dokle god ona ne zbunjuju vozače u vezi s prethodno danim upozorenjima.

**18.   Preuzimanje podataka na vanjske medije**

149  
Tahograf mora moći na zahtjev preuzeti podatke iz svoje podakovne memorije ili s kartice vozača na vanjske medije za čuvanje preko svog priključka za kalibraciju/preuzimanje podataka. Tahograf mora ažurirati podatke spremljene na predmetnu karticu prije početka preuzimanja podataka.

150  
Pored toga, kao neobavezna funkcija, tahograf može, u bilo kojem načinu rada preuzimati podatke preko drugog priključka za firmu koja se identifikujela preko tog kanala. U tom slučaju se na takvo preuzimanje podataka primjenjuju prava pristupa podacima u načinu rada preduzeća.

151  
Preuzimanje podataka ne izmijenjuje ili briše niti jedan arhivirani podatak.

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

Protokoli preuzimanja podataka su opisani u Dodatku 7.

**19.   Izlazni podaci za dodatne vanjske uređaje**

152  
Kad tahograf ne posjeduje funkcije prikaza brzine i/ili brojača kilometara, tahograf mora imati izlazni signal ili signale koji omogućavaju prikaz brzine vozila (brzinomjer) i/ili ukupne pređene udaljenosti vozila (brojač kilometara).

153  
Jedinica u vozilu mora takođe biti u stanju osigurati izlaz sljedećih podataka preko odgovarajuće serijske veze neovisne o neobveznoj CAN bus sabirnici (ISO 11898 Drumska vozila – Razmjena digitalnih informacija – Controller Area Network (CAN) za brzu komunikaciju), kako bi se omogućila njihova obrada pomoću drugih elektronskih jedinica ugrađenih u vozilu:

* tekući UTC datum i vrijeme,
* brzina vozila,
* ukupno pređena udaljenost vozila (brojač kilometara),
* trenutno odabrana aktivnost vozača i suvozača,
* informacija o tome je li bilo koja kartica tahografa trenutno umetnuta u otvor vozača odnosno suvozača i (prema potrebi) informacije o identifikaciji odgovarajućih kartica (broj kartice i država članica izdavaoc).

Pored ovog popisa minimalnih informacija mogu se prenijeti i drugi podaci.

Kad je vozilu dan kontakt, ovi se podaci neprekidno šalju. Kad vozilu nije dan kontakt, šalje se najmanje svaka izmjena aktivnosti vozača ili suvozača i/ili svako ubacivanje ili vađenje kartice iz tahografa. U slučaju da pojedini podaci nisu poslani zbog toga što nije dan kontakt u vozilu, podaci se moraju poslati pri ponovnom davanju kontakta vozila.

**20.   Kalibracija**

154  
Funkcija kalibracije mora omogućavati:

* automatsko uparivanje senzora kretanja s jedinicom u vozilu,
* digitalnu prilagodbu konstante tahografa (k) karakterističnom koeficijentu vozila (w) (vozila s dva ili više završnih osovinskih prenosnih omjera moraju biti opremljena sklopnim uređajem pomoću koje se ti različiti omjeri automatski usklađuju s omjerom za koji je tahograf prilagođen vozilu),
* podešavanje (bez ograničenja) trenutnog vremena,
* podešavanje trenutačne vrijednosti brojača kilometara,
* ažuriranje identifikacijskih podataka senzora kretanja sačuvanih u memoriji podataka,
* ažuriranje ili potvrđivanje ostalih parametara poznatih tahografu: identifikacija vozila, w, l, dimenzije guma i prema potrebi podešavanje ograničavača brzine.

155  
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 memoriju podataka jedinice u vozilu potrebnih identifikacijskih podataka senzora kretanja.

156  
Funkcija kalibrisanja mora biti u stanju unijeti potrebne podatke preko priključnice za kalibraciju/preuzimanje podataka u skladu s protokolom kalibracije utvrđenim u Dodatku 8. Funkcija kalibrisanja takođe može unositi potrebne podatke preko drugih priključnica.

**21.   Podešavanje vremena**

157  
Funkcija podešavanja vremena mora omogućavati podešavanje trenutnog vremena za najviše jednu minutu u razmacima od najmanje sedam dana.

158  
Funkcija podešavanja vremena mora u načinu kalibracije omogućavati podešavanje trenutnog vremena bez ograničenja.

**22.   Radna obelježja**

159  
Jedinica u vozilu mora biti u potpunosti spremna za pogon u temperaturnom rasponu od - 20 °C do 70 °C a senzor kretanja u temperaturnom rasponu od - 40 °C do 135 °C. Sadržaj podakovne memorije se mora očuvati pri temperaturi do – 40 °C.

160  
Tahograf mora biti u potpunosti spreman za pogon pri rasponu vlažnosti od 10 % do 90 %.

161  
Tahograf mora biti zaštićen od prenapona, zamjene polariteta napajanja i kratkih spojeva.

161a

Senzori kretanja:

* reaguju na magnetsko polje koje ometa detekciju kretanja vozila. U takvim okolnostima jedinica vozila bilježi i arhivira grešku senzora (zahtjev 070) ili,
* su tako izvedeni da je senzorski element zaštićen od magnetskih polja ili je na njih imun.

162  
Tahograf mora zadovoljiti tehnički napredak koji se odnosu na elektromagnetsku kompatibilnost, te mora biti zaštićen od elektrostatskih pražnjenja i prelaznih stanja.

**23.   Materijali**

163  
Svi sastavni dijelovi tahografa moraju biti izrađeni od materijala dostatne stabilnosti i mehaničke čvrstoće i stabilnih električnih i magnetskih osobina.

164  
U normalnim uslovima korištenja svi unutarnji dijelovi tahografa moraju biti zaštićeni od vlage i prašine.

165  
Jedinica u vozilu mora zadovoljavati stepen zaštite IP 40, a senzor kretanja mora zadovoljavati stepen zaštite IP 64 prema normi IEC 529.

166  
Tahograf mora odgovarati važećim tehničkim specifikacijama u odnosu na ergonomsku izvedbu.

167  
Tahograf mora biti zaštićen od slučajnog oštećenja.

**24.   Oznake**

168  
Ako tahograf 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’.

Tahograf se takođe može prebaciti na prikaz brzine u miljama na sat, u kojem slučaju se jedinica mjere za brzinu prikazuje kraticom ‚mph’.

169  
Identifikacijska pločica pričvršćuje se na svakom odvojenom sastavnom dijelu tahografa i prikazuje sljedeće podatke:

* naziv i adresu proizvođača uređaja,
* kataloški broj proizvođača i godinu proizvodnje uređaja,
* serijski broj uređaja,
* tipsko odobrenje uređaja.

170  
Kad fizički prostor nije dostatan za prikaz svih gore navedenih podataka, identifikacijska pločica mora prikazivati barem naziv i zaštitni znak proizvođača i kataloški broj tahografa.

**IV.   ZAHTJEVI U POGLEDU IZRADE I FUNKCIONALNI ZAHTJEVI ZA KARTICE TAHOGRAFA**

**1.   Vidljivi podaci**

Prednja strana mora sadržavati:

171

riječi ‚kartica vozača’ ili ‚kontrolna kartica’ ili ‚kartica radionice’ ili ‚kartica prevoznika’ štampane velikim slovima na službenom jeziku ili jezicima države članice koja izdaje karticu, prema vrsti kartice;

172

iste riječi na drugim službenim jezicima Zajednice, štampane u pozadini kartice:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ES | TARJETA DEL CONDUCTOR | TARJETA DE CONTROL | TARJETA DEL CENTRO DE ENSAYO | TARJETA DE LA EMPRESA |
| DK | FØRERKORT | KONTROLKORT | VÆRKSTEDSKORT | VIRKSOMHEDSKORT |
| DE | FAHRERKARTE | KONTROLLKARTE | WERKSTATTKARTE | UNTERNEHMENSKARTE |
| EL | ΚΑΡΤΑ ΟΔΗΓΟΥ | ΚΑΡΤΑ ΕΛΕΓΧΟΥ | ΚΑΡΤΑ KENTPOY ΔOKIMΩN | ΚΑΡΤΑ EΠIXEIPHΣΗΣ |
| EN | DRIVER CARD | CONTROL CARD | WORKSHOP CARD | COMPANY CARD |
| FR | CARTE DE CONDUCTEUR | CARTE DE CONTRÔLEUR | CARTE D'ATELIER | CARTE D'ENTREPRISE |
| GA | CÁRTA TIOMÁNAÍ | CÁRTA STIÚRTHA | CÁRTA CEARDLAINNE | CÁRTA COMHLACHTA |
| IT | CARTA DEL CONDUCENTE | CARTA DI CONTROLLO | CARTA DELL'OFFICINA | CARTA DELL'AZIENDA |
| NL | BESTUURDERS KAART | CONTROLEKAART | WERKPLAATSKAART | BEDRIJFSKAART |
| PT | CARTÃO DE CONDOTVOR | CARTÃO DE CONTROLO | CARTÃO DO ENSAIO | CARTÃO DE EMPRESA |
| FI | KULJETTAJA KORTTILLA | VALVONTAKORTTI | KORJAAMOKORTTI | YRITYSKORTILLA |
| SV | FÖRARKORT | KONTROLLKORT | VERKSTADSKORT | FÖRETAGSKORT |

173

naziv države članice koja je izdala karticu (nije obvezno);

174

oznaku raspoznavanja države članice koja je izdala karticu, štampanu u negativu u plavom pravougaoniku i okruženu s 12 žutih zvjezdica. Oznake za raspoznavanje su sljedeće:

|  |  |
| --- | --- |
| B | Belgija |
| DK | Danska |
| D | Njemačka |
| GR | Grčka |
| E | Španija |
| F | Francuska |
| IRL | Irska |
| I | Italija |
| L | Luksemburg |
| NL | Holandija |
| A | Austrija |
| P | Portugalija |
| FIN | Finska |
| S | Švedska |
| UK | Ujedinjeno Kraljevstvo; |

175

informacije karakteristične za izdanu karticu, označene kako slijedi:

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Kartica vozača** | **Kontrolna kartica** | **Kartica radionice ili kartica prevoznika** |
| 1. | Prezime vozača | Naziv nadzornog tijela | Naziv preduzeća ili radionice |
| 2. | Ime(na) vozača | Prezime nadzornika  (prema potrebi) | Prezime nosioca kartice  (prema potrebi) |
| 3. | Datum rođenja vozača | Ime(na) nadzornika  (prema potrebi) | Ime(na) nosioca kartice  (prema potrebi) |
| 4.(a) | Datum početka važnosti kartice | | |
| (b) | Datum isteka važnosti kartice (ako postoji) | | |
| (c) | Naziv tijela koja izdaje karticu (može biti tiskano na 2. stranici) | | |
| (d) | Broj različit od navedenoga pod točkom 5. za administrativne potrebe (nije obvezno) | | |
| 5.(a) | Broj vozačke dozvole  (na datum izdavanja kartice vozača) |  |  |
| 5.(b) | Broj kartice | | |
| 6. | Fotografija vozača | Fotografija nadzornika  (nije obvezna) | — |
| 7. | Potpis vozača | Potpis nosioca kartice (nije obvezno) | |
| 8. | Uobičajeno mjesto prebivališta ili poštanska adresa nosioca (nije obvezno | Poštanska adresa nadzornog tijela | Poštanska adresa prevoznika ili radionice |

176

datumi se pišu u obliku ‚dd/mm/gggg’ ili ‚dd.mm.gggg.’ (dan, mjesec, godina).

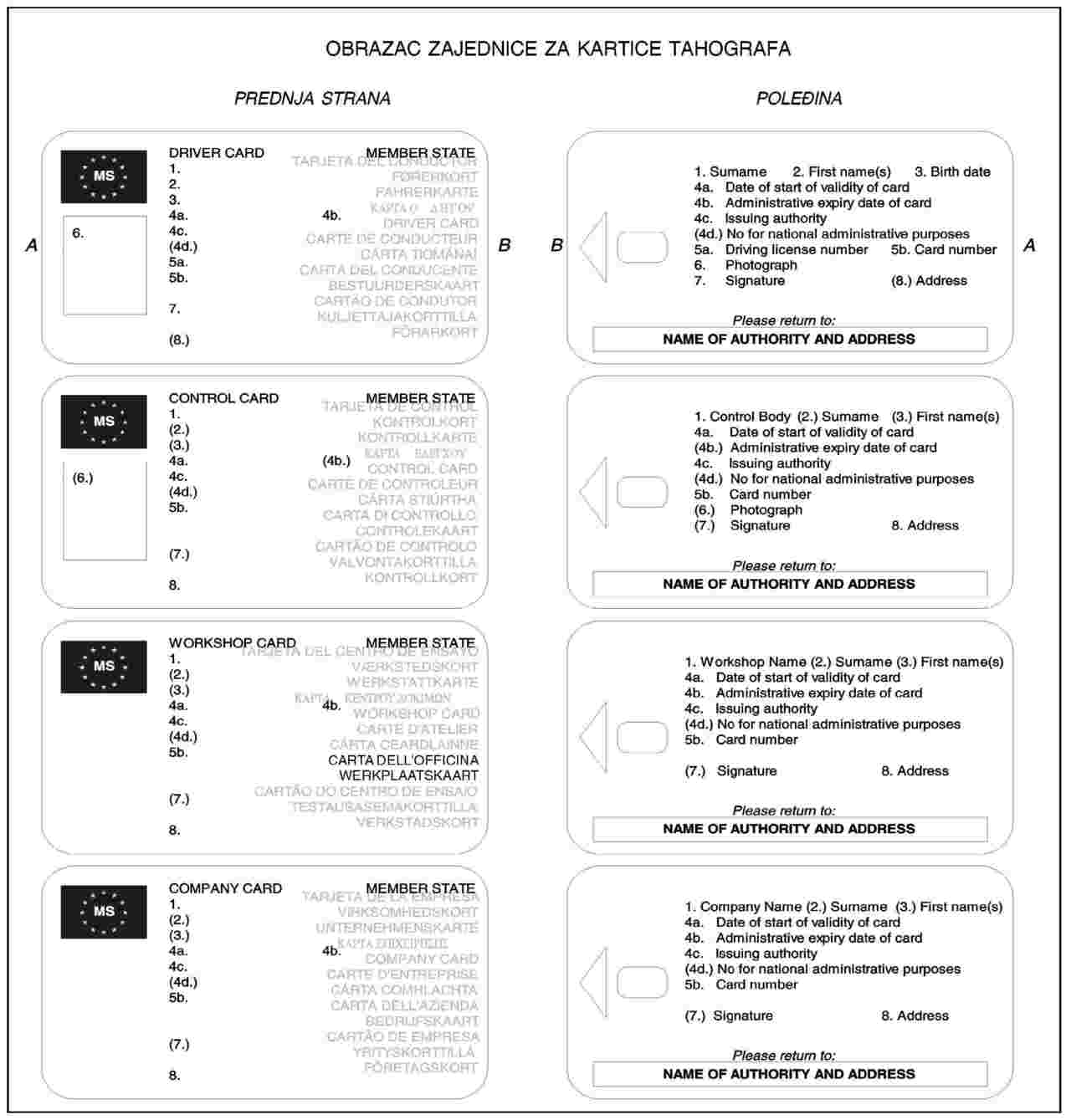
stražnja strana mora sadržavati:

177

pojašnjenja navedenih stavova na prednjoj strani kartice;

178

uz poseban pisani pristanak nosioca mogu se dodati i informacije koje se ne odnose na vođenje kartice, pri čemu njihovo dodavanje ni na koji način neće izmijeniti korištenje obrasca kao kartice tahografa.



179  
Kartice tahografa se moraju štampati sa sljedećim prevladavajućim bojama pozadine:

* kartica vozača: bijela,
* kontrolna kartica: plava,
* kartica radionice: crvena,
* kartica prevoznika: žuta.

180  
Kartice tahografa moraju imati barem sljedeća obelježja za zaštitu tijela kartice od krivotvorenja i neovlaštenog rukovanja:

* sigurnosno izvedenu pozadinu s finim guilloche uzorcima i nijansiranim tiskom,
* na prostoru za fotografiju, sigurnosno izvedena pozadina i fotografija se moraju preklapati,
* barem jedna dvobojna linija u mikrotisku.

181  
Nakon dogovora s Komisijom, države članice mogu dodavati boje i oznake kao što su nacionalni simboli i sigurnosna obelježja, ne dovodeći u pitanje druge odredbe ovog Priloga.

**2.   Sigurnost**

Sigurnost sistema ima za cilj zaštitu potpunosti i autentičnost podataka koji se razmjenjuju između kartica i tahografa, zaštitu potpunosti i autentičnosti podataka koji se preuzimaju s kartica, omogućavanje određenih aktivnosti upisivanja na kartice samo tahografu, isključivanje svake mogućnosti krivotvorenja podataka arhiviranih na karticama, sprečavanje neovlaštenog rukovanja i otkrivanje svih pokušaja te vrste.

182  
Kako bi se postigla sigurnost sistema, kartice tahografa moraju zadovoljavati sigurnosne zahtjeve utvrđene u generičkim sigurnosnim ciljevima za kartice tahografa (Dodatak 10.).

183  
Kartice tahografa moraju biti čitljive od strane druge opreme, kao što su osobna računala.

**3.   Norme**

184  
Kartice tahografa moraju zadovoljavati sljedeće norme:

* ISO/IEC 7810 Identifikacijske kartice – fizičke karakteristike,
* ISO/IEC 7816 Identifikacijske kartice – integirsani krugovi s kontaktima,
* 1. dio: Fizička obelježja,
* 2. dio: Dimenzije i smještaj kontakata,
* 3. dio: Elektronski signali i protokoli prenosa,
* 4. dio: Međugranske naredbe za razmjenu,
* 8. dio: Međugranske naredbe koje se odnose na sigurnost,
* ISO/IEC 10573 Identifikacijske kartice – metode provjere.

**4.   Okolina i električne karakteristike**

185  
Kartice tahografa moraju biti u stanju ispravno raditi u svim klimatskim uslovima uobičajenim 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.

186  
Kartice tahografa moraju biti u stanju ispravno raditi u rasponu vlažnosti između 10 % i 90 %.

187  
Kartice tahografa moraju biti u stanju ispravno raditi tokom perioda od pet godina ako se koriste u skladu sa specifikacijama okruženja i elektrotehničkim specifikacijama.

188  
Tokom korištenja kartice tahografa moraju biti u skladu sa elektromagnetskom kompatibilnošću, te moraju biti zaštićene od elektrostatskih pražnjenja.

**5.   Čuvanje podataka**

Za potrebe ovog stava,

* vremena se evidentiraju s razlučivošću od jedne minute, osim ako nije drugačije određeno,
* stanje brojača kilometara se evidentira s razlučivošću od 1 kilometra,
* brzine se evidentiraju s razlučivošću od 1 km/h.

Funkcije, naredbe i logičke strukture kartice tahografa koje ispunjavaju zahtjeve u pogledu spremanja podataka su navedene u Dodatku 2.

189  
Ovaj stavak navodi minimalan kapacitet spremanja podataka za različite podakovne datoteke. Kartice tahografa moraju biti u stanju prikazati tahografu stvarni kapacitet spremanja tih podakovnih datoteka.

Svi dodatni podaci koji se mogu sačuvati na karticama tahografa, a koji se odnose na druge podatke eventualno spremljene na kartici, moraju se čuvati u skladu sa propisima o zaštiti pojedinaca u vezi s obradom ličnih podataka i o slobodnom kretanju takvih podataka.

**5.1.    Identifikacija kartice i sigurnosni podaci**

**5.1.1.   Identifikacija programa**

190  
Kartice tahografa moraju biti u stanju sačuvati sljedeće programske identifikacijske podatke:

* identifikaciju tahografskog programa,
* identifikaciju vrste kartice tahografa.

**5.1.2.   Identifikacija čipa**

191  
Kartice tahografa moraju biti u stanju sačuvati sljedeće identifikacijske podatke o integriranom krugu (IC):

* serijski broj IC,
* proizvodne reference IC.

**5.1.3.   IC identifikacija kartice**

192  
Kartice tahografa moraju biti u stanju sačuvati sljedeće identifikacijske podatke pametnih kartica:

* serijski broj kartice (s proizvodnim referencama),
* broj tipskog odobrenja kartice,
* identifikaciju (ID) personalizatora kartice,
* identifikaciju ugraditelja (ID),
* identifikator IC.

**5.1.4.   Sigurnosni elementi**

193  
Kartice tahografa moraju biti u stanju sačuvati sljedeće podatke o sigurnosnim elementima:

* evropski javni ključ,
* certifikat države članice,
* certifikat kartice,
* privatni ključ kartice.

**5.2.    Kartica vozača**

**5.2.1.   Identifikacija kartice**

194  
Kartica vozača mora biti u stanju sačuvati sljedeće identifikacijske podatke kartice:

* broj kartice,
* država članica izdavaoc, naziv tijela izdavaoca, datum izdavanja,
* datum početka važnosti i isteka kartice.

**5.2.2.   Identifikacija nosioca kartice**

195  
Kartica vozača mora biti u stanju sačuvati sljedeće identifikacijske podatke nosioca kartice:

* prezime nosioca,
* ime(na) nosioca,
* datum rođenja,
* izabrani jezik.

**5.2.3.   Podaci o vozačkoj dozvoli**

196  
Kartica vozača mora biti u stanju sačuvati sljedeće podatke o vozačkoj dozvoli:

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

**5.2.4.   Podaci o korišćenim vozilima**

197  
Kartica vozača mora biti u stanju sačuvati sljedeće podatke za svaki kalendarski dan korištenja kartice i za svako period korištenja dotičnog vozila tog dana (period korištenja obuhvaća sve uzastopne cikluse ubacivanja i vađenja kartice u tom vozilu s gledišta kartice):

* datum i vrijeme prvog korištenja vozila (tj. prvog ubacivanja kartice u navedenom razdoblju korištenja vozila ili 00:00 ako je kartica korištena u to vrijeme),
* stanje brojača kilometara vozila u to vrijeme,
* datum i vrijeme posljednjeg korištenja vozila (tj. posljednjeg vađenja kartice u tom razdoblju korištenja vozila ili 23:59 ako je kartica korištena u to vrijeme)
* stanje brojača kilometara vozila u to vrijeme,
* registracijski broj vozila i država članica registracije vozila.

198  
Kartica vozača mora biti u stanju sačuvati najmanje 84 takva zapisa.

**5.2.5.   Podaci o aktivnostima vozača**

199  
Kartica vozača mora biti u stanju sačuvati, za svaki kalendarski dan korištenja kartice ili za koji je vozač ručno unio podatke, sljedeće podatke:

* datum,
* dnevni brojač prisustva (uvećan za 1 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 ubacio ili izvadio svoju karticu:
* status vožnje (POSADA, JEDAN VOZAČ),
* otvor (VOZAČ, SUVOZAČ),
* status kartice (UMETNUTA, NIJE UMETNUTA),
* aktivnost (VOŽNJA, PRIPRAVNOST, RAD, PAUZA/ODMOR),
* vrijeme promjene.

200  
Memorija vozačke kartice mora biti u stanju zadržati podatke o aktivnosti vozača najmanje 28 dana (pri čemu se prosječna aktivnost vozača utvrđuje na 93 promjene dnevno).

201  
Podaci navedeni u zahtjevima 197 i 199 spašavaju se na način koji omogućava učitavanje aktivnosti redoslijedom njihovog pojavljivanja, čak i u slučaju vremenskog preklapanja.

**5.2.6.   Mjesta početka i/ili završetka dnevnih aktivnosti**

202  
Kartica vozača mora biti u stanju sačuvati sljedeće podatke vezane uz mjesto početka i/ili završetka dnevnih aktivnosti koje unese vozač:

* datum i vrijeme unosa (ili datum/vrijeme vezane uz ručni unos),
* vrstu unosa (početak ili kraj, stanje unosa),
* državu i regiju ulaska,
* stanje brojača kilometara vozila.

203  
Memorija vozačke kartice mora biti u stanju sačuvati najmanje 42 parova takvih zapisa.

**5.2.7.   Podaci o događajima**

Za potrebe ovog podstava, vrijeme se arhivira s razlučivošću od jedne sekunde.

204  
Kartica vozača mora biti u stanju sačuvati podatke vezane uz sljedeće događaje koje je tahograf otkrio dok je bila umetnuta kartica:

* vremensko preklapanje (ako je navedena kartica uzrokovala događaj),
* ubacivanje kartice tokom vožnje (ako je navedena kartica predmet događaja),
* neispravan završetak posljednje razmjene podataka s karticom (kada je navedena kartica predmet događaja),
* prekid napajanja,
* greška u podacima o kretanju,
* pokušaji probijanja zaštite.

205  
Kartica vozača mora biti u stanju sačuvati sljedeće podatke za navedene događaje:

* šifru događaja,
* datum i vrijeme početka događaja (ili ubacivanja kartice ako je događaj u to vrijeme bio u tijeku),
* datum i vrijeme završetka događaja (ili vađenja kartice ako je događaj u to vrijeme bio u tijeku),
* registracijsku oznaku vozila i državu članicu registracije vozila u kojemu je nastao događaj.

Napomena: Kod događaja ‚vremenskog preklapanja’:

* datum i vrijeme početka događaja moraju odgovarati datumu i vremenu vađenja kartice iz prethodnog vozila,
* datum i vrijeme završetka događaja moraju odgovarati datumu i vremenu ubacivanja kartice u aktualnom vozilu,
* podaci o vozilu moraju se odnositi na aktualno vozilo, u kojemu je događaj nastubio.

Napomena: Kod događaja ‚neispravnog završetka posljednjeg korištenja kartice’:

* datum i vrijeme početka događaja moraju odgovarati datumu i vremenu ubacivanja kartice koji nije pravilno završen,
* datum i vrijeme završetka događaja moraju odgovarati datumu i vremenu ubacivanja kartice tokom kojeg je događaj otkriven (tekuća razmjena podataka),
* podaci o vozilu moraju se odnositi na vozilo u kojemu razmjena podataka nije pravilno završena.

206  
Kartica vozača mora biti u stanju sačuvati podatke za šest posljednjih događaja za svaku vrstu (tj. 36 događaja).

**5.2.8.   Podaci o greškama**

Za potrebe ovog podstava, vrijeme se evidentira s razlučivošću od jedne sekunde.

207  
Kartica vozača mora biti u stanju sačuvati podatke vezane uz sljedeće greške koje je tahograf otkrio dok je kartica bila umetnuta:

* greška kartice (kada je ta kartica predmet događaja),
* greška tahografa.

208  
Kartica vozača mora biti u stanju sačuvati sljedeće podatke za navedene greške:

* šifru greške,
* datum i vrijeme početka greške (ili ubacivanja kartice ako je u tom trenutku greška bila u tijeku),
* datum i vrijeme završetka greške (ili vađenja kartice ako je u tom trenutku greška bila u tijeku),
* registracijski broj vozila i državu članicu registracije vozila u kojemu je došlo do greške.

209  
Kartica vozača mora biti u stanju sačuvati podatke za dvanaest posljednjih grešaka za svaku vrstu (tj. 24 greške).

**5.2.9.   Podaci o nadzornim aktivnostima**

210  
Kartica vozača mora biti u stanju sačuvati sljedeće podatke vezane uz kontrolne aktivnosti:

* 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),
* registracijski broj vozila i državu članicu registracije vozila u kojoj je izvršen nadzor.

Napomena: sigurnosni zahtjevi podrazumijevaju da se preuzimanje podataka s kartice evidentira samo ako je izvršeno preko tahografa.

211  
Kartica vozača mora biti u stanju sačuvati jedan takav zapis.

**5.2.10.   Podaci o upotrebi kartice**

212  
Kartica vozača mora biti u stanju sačuvati podatke vezane o vozilu u kojem je započela upotreba kartice:

* datum i vrijeme početka upotrebe (tj. ubacivanje kartice) s razlučivošću od jedne sekunde,
* registracijski broj vozila i državu članicu registracije vozila.

**5.2.11.   Podaci o posebnim stanjima**

212a  
Kartica vozača mora biti u stanju sačuvati sljedeće podatke vezane uz posebna stanja koja su unesena dok je kartica bila umetnuta (bez obzira u koji otvor):

* datum i vrijeme unosa,
* vrsta posebnog stanja.

212b  
Kartica vozača mora biti u stanju sačuvati 56 takvih zapisa.

**5.3.    Kartica radionice**

**5.3.1.   Sigurnosni elementi**

213  
Kartica radionice mora biti u stanju sačuvati osobni identifikacijski broj (PIN oznaku).

214  
Kartica radionice mora biti u stanju sačuvati kriptografske ključeve potrebne za uparivanje senzora kretanja s jedinicama u vozilu.

**5.3.2.   Identifikacija kartice**

215  
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 važnosti kartice.

**5.3.3.   Identifikacija nosioca kartice**

216  
Kartica radionice mora biti u stanju sačuvati sljedeće identifikacijske podatke nosioca kartice:

* ime radionice,
* adresu radionice,
* prezime nosioca,
* ime(na) nosioca,
* izabrani jezik.

**5.3.4.   Podaci o korišćenim vozilima**

217  
Kartica radionice mora biti u stanju sačuvati podatke o korišćenim vozilima na isti način kao i kartica vozača.

218  
Kartica radionice mora biti u stanju čuvati najmanje 4 takva zapisa.

**5.3.5.   Podaci o aktivnosti vozača**

219  
Kartica radionice mora biti u stanju sačuvati podatke o aktivnostima vozača na isti način kao i kartica vozača.

220  
Kartica radionice mora biti u stanju čuvati podatke o aktivnostima vozača barem tokom jednog dana prosječne aktivnosti vozača.

**5.3.6.   Podaci o početku i/ili završetku dnevnog perioda rada**

221  
Kartica radionice mora biti u stanju sačuvati podatke o početku i/ili završetku dnevnog perioda rada na isti način kao i kartica vozača.

222  
Kartica radionice mora biti u stanju čuvati najmanje tri para takvih zapisa.

**5.3.7.   Podaci o događajima i greškama**

223  
Kartica radionice mora biti u stanju sačuvati podatke o događajima i greškama na isti način kao i kartica vozača.

224  
Kartica radionice mora biti u stanju čuvati podatke za tri posljednja događaja svake vrste (tj. 18 događaja) i šest posljednjih grešaka svake vrste (tj. 12 grešaka).

**5.3.8.   Podaci o nadzornim aktivnostima**

225  
Kartica radionice mora biti u stanju sačuvati podatke o aktivnostima nadzora na isti način kao i kartica vozača.

**5.3.9.   Podaci o kalibraciji i podešavanju vremena**

226  
Kartica radionice mora biti u stanju sačuvati zapise o kalibraciji i/ili vremenskim podešenjima izvršenim dok je kartica bila umetnuta u tahograf.

227  
Svaki zapis o kalibraciji mora sadržavati sljedeće podatke:

* svrha baždarenja (aktivacija, prvo postavljanje, postavljanje, periodična provjera),
* identifikaciju vozila,
* parametre koji se ažuriraju ili potvrđuju (w, k, l, dimenzije guma, postavke ograničavača brzine, stanje brojača kilometara (novu i staru vrijednost), datum i vrijeme (nove i stare vrijednosti),
* identifikaciju tahografa (kataloški broj jedinice vozila, serijski broj jedinice vozila, serijski broj senzora kretanja).

228  
Kartica radionica mora biti u stanju sačuvati barem 88 takvih zapisa.

229  
Kartica radionice mora sadržavati brojač za označivanje ukupnog broja kalibracija izvršenih s tom karticom.

230  
Kartica radionice mora sadržavati brojač za označivanje broja kalibracija izvršenih nakon posljednjeg preuzimanja podataka s kartice.

**5.3.10.   Podaci o posebnim uslovima**

230a  
Kartica radionice mora biti u stanju sačuvati podatke o posebnim uslovima na isti način kao i kartica vozača. Kartica radionice mora biti u stanju čuvati dva takva zapisa.

**5.4.    Kontrolna kartica**

**5.4.1.   Identifikacija kartice**

231  
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 važnosti kartice (ako postoji).

**5.4.2.   Identifikacija nosioca kartice**

232  
Kontrolna kartica mora moći sačuvati sljedeće identifikacijske podatke nosioca kartice:

* naziv nadzornog tijela,
* adresu nadzornog tijela,
* prezime nosioca,
* ime(na) nosioca,
* izabrani jezik.

**5.4.3.   Podaci o nadzornim aktivnostima**

233  
Kontrolna kartica mora moći sačuvati sljedeće podatke o nadzornim aktivnostima:

* datum i vrijeme nadzora,
* vrstu nadzora (prikaz i/ili ispis i/ili preuzimanje podataka s jedinice vozila i/ili s kartice),
* period preuzimanja podataka (ako postoji),
* registracijski broj vozila i država članica registracije kontroliranog vozila.
* broj kartice i država članica koja je izdala kontroliranu vozačku karticu.

234  
Kontrolna kartica mora moći sačuvati najmanje 230 takvih zapisa.

**5.5.    Kartica prevoznika**

**5.5.1.   Identifikacija kartice**

235  
Kartica prevoznika mora moći sačuvati sljedeće identifikacijske podatke kartice:

* broj kartice,
* država članica izdavanja, naziv tijela koje izdaje karticu, datum izdavanja,
* datum početka važenja i isteka kartice (ako postoji).

**5.5.2.   Identifikacija nosioca kartice**

236  
Kartica preduzeća mora moći sačuvati sljedeće identifikacijske podatke nosioca kartice:

* naziv preduzeća,
* adresu preduzeća.

**5.5.3.   Podaci o aktivnostima prevoznika**

237  
Kartica prevoznika mora moći sačuvati sljedeće podatke o aktivnostima prevoznika:

* datum i vrijeme aktivnosti,
* vrstu aktivnosti (zaključavanje ili otključavanje blokade jedinice vozila, preuzimanje podataka s jedinice vozila i/ili s kartice),
* period preuzimanja podataka (ako postoji),
* registracijski broj vozila i država registracije vozila,
* broj kartice i državu članicu izdavanja kartice (u slučaju preuzimanja podataka s kartice).

238  
Kartica prevoznika mora moći sačuvati barem 230 takvih zapisa.

**V.   UGRADNJA TAHOGRAFA**

**1.   Ugradnja**

239  
Novi tahograf se isporučuje neaktiviran ugradiocima ili proizvođačima vozila sa svim parametrima za kalibraciju navedenim u poglavlju III, dio 20., podešenim na odgovarajuće i osnovne vrijednosti. Ako neka određena vrijednost nije podešena, slovni parametri se zamjenjuju nizom znakova ’?’ a numerički parametri se postavljaju na ‚0’.

Dostava dijelova tahografa vezanih uz sigurnost može se ograničiti ako se tako zahtijeva za vrijeme sigurnosnog certifikovanja.

240  
Prije aktivacije, tahograf mora imati pristub funkciji kalibracije, čak i kada nije u režimu kalibracije.

241  
Prije aktivacije, tahograf ne smije zapisivati niti spremati podatke iz tačaka III.12.3 do III.12.9, te III.12.12 do i uključujući III.12.14.

242  
Tokom ugradnje proizvođači vozila moraju unaprijed podesiti sve poznate parametre.

243  
Proizvođači vozila ili instalateri aktiviraju ugrađene tahografe najkasnije prije upotrebe vozila u području primjene zakona i AETR Sporazuma.

244  
Stavljanje tahografa u pogon se vrši automatski prvim ubacivanjem kartice radionice u bilo koji uređaj kartičnog sučelja.

245  
Posebne operacije uparivanja senzora kretanja i jedinice u vozilu, ako ih ima, se vrše automatski prije ili tokom aktivacije.

246  
Nakon aktivacije, tahograf mora u potpunosti izvršavati funkcije i prava pristupa podacima.

247  
Funkcije zapisivanja i spremanja u tahografu postižu punu radnu sposobnost nakon njegove aktivacije.

248  
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 moguće je da vlasnik vozila samo jednom može unijeti VRN koristeći svoju karticu preduzeća prije upotrebe vozila u području primjene Uredbe (EZ) br. 561/2006 (npr. koristeći naredbe putem odgovarajuće strukture menija sučelja čovjek-mašina jedinice vozila.). Bilo koji naknadni unos ili ažuriranje postojećeg unosa moguće je samo karticom radionice.

248a  
Tahograf mora biti smješten u vozilu tako da omogući vozaču pristub potrebnim funkcijama iz svog sjedala.

**2.   Tipska naljepnica**

249  
Nakon provjere tahografa pri ugradnji, na njega se pričvršćuje jasno vidljiva i lako dostupna ugrađena naljepnica. Ako to nije moguće, naljepnica se pričvršćuje na stub ‚B’ vozila tako da je jasno vidljiva. Za vozila koja nemaju stub ‚B’, ugrađena se naljepnca pričvršćuje na okvir vrata na vozačevoj strani vozila i jasno je vidljiva u svim slučajevima.

Nakon svakog nadzora kod ovlaštenog instalatera ili radionice, na mjesto prethodne naljepnice pričvršćuje se nova naljepnica.

250.

Na naljepnici moraju biti navedeni najmanje sljedeći podaci:

* ime, adresa ili trgovački naziv ovlašćenog servisera ili radionice,
* stalnica vozila, u obliku ‚w = … imp/km’,
* konstanta tahografa, u obliku ‚k = … imp/km’,
* efektivni obim pogonskih točkova u obliku ‚l = … mm’,
* veličina guma,
* datum mjerenja karakterističnog koeficijenta vozila i djelatnog opsega pogonskih točkova,
* identifikacijska oznaka vozila (VIN),
* 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 koristi adapter,
* opis boje kabla između adaptera i onog dijela vozila koji daje njegove ulazne impulse,
* serijski broj ugrađenog senzora kretanja adaptera.

250.a.

250a Samo za vozila M1 i N1 koja su opremljena adapterom u skladu s Uredbom (EZ) br. 68/2009 (2), a kada nije moguće uključiti sve potrebne informacije opisane u zahtjevu 250, može se upotrijebiti druga, dodatna pločica. U takvim slučajevima, dodatna pločica sadrži najmanje zadnje četiri alineje opisane u zahtjevu 250.

Ako se upotrebljava druga, dodatna pločica, ista se pričvršćuje pored ili uz prvu primarnu pločicu, opisanu u zahtjevu 250, i ima istu razinu zaštite. Nadalje, na dodatnoj pločici je takođe navedeno ime, adresa ili trgovački naziv ovlaštenog instalatera ili radionice koja je izvršila ugradnju te datum ugradnje. **3.  Plombrianje:**

251  
Sljedeći dijelovi moraju se zaštiti plombom:

* svaki spoj čije bi razdvajanje uzrokovalo izmjene ili gubitak podataka koje ne bi bilo moguće otkriti,
* ugradna pločica, osim ako je pričvršćena na takav način da ju je nemoguće ukloniti bez uništavanja oznaka na istoj.

252  
Gore spomenuta plombe mogu se ukloniti:

* u vanrednom slučaju,
* pri ugradnji, podešavanju ili popravku ograničavača brzine ili nekog drugog uređaja koji doprinosi sigurnosti na cesti, pod uslovom da tahograf nastavi raditi pouzdano i ispravno, te da ovlašćeni ugraditelj ili radionica ponovno postavi žigove (u skladu s poglavljem VI.), odmah nakon postavljanja ograničavača brzine ili nekog drugog uređaja koji doprinosi sigurnosti na cestama ili u roku od sedam dana u drugim slučajevima.

253  
Svaki put kada se ti žigovi skidaju, sastavlja se pisana izjava u kojoj se navode razlozi zbog kojih je to učinjeno i koja mora biti dostupna nadležnom tijelu.

**VI.   ISPITIVANJE, PREGLEDI I POPRAVKE**

Zahtjevi u pogledu okolnosti u kojima se žigovi mogu skidati shodno poglavlju V. odjeljku 3. ovog Priloga.

**1.   Ovlaštenje ugraditelja ili radionica**

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

* ugradnju,
* ispitivanje,
* preglede,
* popravke.

Kartice radionice se izdaju samo u radiocima i/ili radionicama ovlašćenim za stavljanje u pogon i/ili kalibraciju tahografa u skladu sa ovim Prilogom i, osim ukoliko ne postoji valjano opravdanje:

* onima koji nemaju pravo na kartice prevoznika,
* i čija druga poslovna djelatnost ne dovodi u pitanje sveukupnu sigurnost sistema kako je utvrđeno u Dodatku 10 ovog priloga.

**2.   Ispitivanje novih ili popravljenih uređaja**

254  
Svaki pojedini uređaj, bilo da je nov ili popravljen, provjerava se u pogledu njegovog ispravnog rada i tačnosti očitavanja i zapisa, u granicama utvrđenim u poglavlju III.2.1. i III.2.2., putem stavljanja žigova u skladu s poglavljem V.3 i kalibracije.

**3.   Nadzor pri ugradnji**

255  
Pri postavljanju u vozilo, čitava instalacija (uključujući i tahograf) mora udovoljiti odredbama koje se tiču maksimalnih odstupanja utvrđenih u poglavlju III.2.1. i III.2.2.

**4.   Periodični pregled**

256  
Periodični pregledi tahografa u vozilu se obavlja nakon svakog popravka uređaja ili nakon svake izmjene karakterističnog koeficijenta vozila ili djelatnog opsega guma ili nakon greške UTC vremena veće od 20 minuta, ili pri promjeni registracijske oznake vozila, te bar jednom svake dvije godine (24 mjeseca) nakon posljednjeg pregleda.

257  
Ti pregledi obuhvaćaju sljedeće provjere:

* da tahograf radi ispravno, uključujući funkciju spremanja podataka na kartice tahografa,
* shodnost s odredbama poglavlja III.2.1. i III.2.2. o najvećem odstupanju,
* ima li tahograf oznaku tipskog odobrenja,
* da se pričvrsti ugrađena pločica, kao što je određeno zahtjevom 250, i opisna pločica, kao što je određeno zahtjevom 169
* da su svi žigovi na uređaju i na drugim dijelovima instalacije netaknuti,
* dimenziju i aktivni opseg guma točkova.
* da uređaju nije dodan uređaj za manipulaciju.

257a

Ako se ustanovi da se nakon posljednjeg nadzora dogodio jedan od događaja navedenih u poglavlju III. odjeljku 9. (Otkrivanje događaja i/ili pogrešaka) 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 registrovanog u jedinici vozila; (b) provjerava podudaraju li se informacije zabilježene na ugrađenoj pločici s informacijama koje sadrži zapis jedinice vozila; (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 vozila.

257b

Radionice u svojim izvješćima o nadzoru zapisuju sva saznanja o slomljenim pečatima ili uređajima za manipulaciju. Radionice te izvještaje čuvaju najmanje dvije godine i stavljaju ih na raspolaganje na zahtjev nadležnih tijela.

258  
Ovi pregledu moraju obuhvatiti i kalibraciju.

**5.   Mjerenje grešaka**

259  
Mjerenje grešaka pri ugradnji i tokom korištenja se sprovodi prema sljedećim uslovima, za koje se smatra da predstavljaju standardne ispitne uslove:

* vozilo prazno, u normalnom stanju rada,
* pritisak u gumama u skladu s uputama proizvođača,
* potrošenost gaznog sloja guma u granicama dopuštenim nacionalnim propisima,
* kretanje vozila:
* vozilo se kreće snagom vlastitog motora pravolinijski i na ravnom terenu, pri brzini od 50 ± 5 km/h. Mjerna udaljenost je najmanje 1,000 m,
* pod uslovom da im je tačnost usporedljiva, za provjeru se mogu koristiti i alternativne metode kao što je odgovarajuće ispitivanje na stolu.

**6.   Popravke**

260  
Radionice moraju biti u stanju preuzeti podatke s tahografa kako bi ih mogli dostaviti odgovarajućem prevozniku.

261  
Ovlaštene radionice izdaju prevoznicima potvrdu o nemogućnosti preuzimanja podataka kada neispravnost tahografa sprečava preuzimanje prethodno zaevidentirajunih podataka, čak i nakon popravka u radionici. Radionice čuvaju kopiju svake izdate potvrde u trajanju od najmanje godinu dana.

**VII.   IZDAVANJE KARTICA**

Postubci izdavanja kartica umašinaeni u državama članicama moraju biti u skladu sa sljedećim:

262

Broj kartice prvog izdavanja kartice tahografa tražitelju mora imati redni indeks (ako je primjereno) i indeks zamjene, te indeks ponovnog izdavanja postavljen na ‚0’.

263

Brojevi kartica svih nepersonaliziranih kartica tahografa koje se izdaju jednom nadzornom tijelu ili jednoj radionici ili jednom prevozniku moraju imati istih prvih 13 znamenaka, te različit redni indeks.

264

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

265

Kartica tahografa koja se izdaje kao zamjena za postojeću karticu tahografa mora imati isti datum isteka važnosti kartice kao i kartica koju zamjenjuje.

266

Kartica tahografa koja se izdaje zbog ponovnog izdavanja postojeće kartice tahografa mora imati isti broj kartice kao i kartica koja se obnavlja, osim indeksa ponovnog izdavanja koji se uvećava za 1 (redoslijedom 0, …, 9, A, …, Z).

267

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

268

Rubrika ‚prezime nosioca kartice’ za personalizirane kartice radionice ili kontrolne kartice se popunjavaju nazivom radionice ili nadzornog tijela.

268a

Države članice elektronski razmjenjuju podatke kako bi osigurale jedinstvenost tahografske kartice vozača koju izdaju.

Nadležna tijela država članica takođe mogu pri pregledima kartica vozača na cesti ili u prostorijama preduzeća elektronski razmjenjivati podatke, kako bi provjerili jedinstvenost i status kartica.

**VIII.   TIPSKO ODOBRENJE TAHOGRAFA I KARTICA TAHOGRAFA**

**1.   Uopšteno**

Za potrebe ovog poglavlja, riječ ‚tahograf’ znači ‚tahograf ili njegove sastavne dijelove’. Tipsko odobrenje nije potrebno za vodiče koji povezuju senzor kretanja s jedinom u vozilu. Papir koji se koristi u tahografu smatra se sastavnim dijelom tahografa.

Svaki proizvođač jedinice vozila može zahtijevati homologaciju njegovog sastavnog dijela s bilo kojom vrstom senzora kretanja, i obrnuto, pod uslovom da je svaki sastavni dio usklađen sa zahtjevom 001a.

269  
Tahograf se podnosi za tipsko odobrenje zajedno sa svim integirsanim dodatnim uređajima.

270  
Tipsko odobrenje tahografa i kartica tahografa mora uključivati sigurnosne provjere, provjere funkcionalnosti i interoperabilnosti. Pozitivni rezultati svih ovih provjera se utvrđuju u odgovarajućoj potvrdi.

271  
Tijelo vlasti država članica zaduženo za tipsko odobrenje neće izdati potvrdu o tipskom odobrenju u skladu s člankom 5. ove Uredbe ako nemaju:

* sigurnosnu potvrdu,
* potvrdu o funkcionalnosti,
* i potvrdu o interoperabilnosti

za tahograf ili karticu tahografa koja je predmet zahtjeva za tipsko odobrenje.

272  
Svaka izmjena softverske ili hardverske opreme tahografa, ili naravi materijala korištenih za njegovu izradu mora prije korištenja biti prijavljena tijelu koje je izvršilo tipsko odobrenje opreme. To nadležno tijelo mora potvrditi proizvođaču proširenje tipskog odobrenja ili može zatražiti ažuriranje ili odgovarajuće potvrde o funkcionalnosti, sigurnosti i/ili interoperabilnosti.

273  
Postupak softverske nadogradnje tahografa na licu mjesta, odobrava tijelo koje je izvršilo tipsko odobrenje tahografa. Nadogradnja softvera ne smije mijenjati ili brisati niti jedan podatak o aktivnosti vozača pohranjen u tahografu. Softver se može nadograđivati samo pod odgovornosti proizvođača uređaja.

**2.   Sigurnosna potvrda**

274  
Sigurnosna potvrda se izdaje u skladu s odredbama Dodatka 10. ovom Prilogu.

274a

U iznimnim okolnostima, kad tijela za sigurnosno certificiranje 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”.

274b

U takvim okolnostima, dotična država članica bez odgađanja obavještava Evropsku komisiju, koja u roku dvanaest kalendarskih mjeseci od dodjele homologacije, pokreće postupak kojim osigurava da se ponovno uspostavi prvobitni nivou sigurnosti.

**3.   Potvrda o funkcionalnosti**

275  
Svaki pristubnik za tipsko odobrenje mora dostaviti tijelu države članice odgovornom za tipsko odobrenje sve materijale i dokumente koje tijelo smatra potrebnima.

275a

Proizvođači u roku mjesec dana od datuma zahtjeva, osiguravaju odgovarajuće uzorke homologovanih proizvoda i s tim povezanu dokumentaciju, koju zahtijevaju laboratoriji imenovani za obavljanje funkcionalnih ispitivanja. Sve troškove koji nastanu radi tog zahtjeva snosi podvlasnik zahtjeva. Laboratoriji povjerljivo postupaju sa svim poslovno osjetljivim informacijama.

276  
Potvrda o funkcionalnosti se izdaje proizvođaču tek nakon uspješnog okončanja najmanje onih provjera funkcionalnosti koje su navedene u Dodatku 9.

277  
Tijelo za tipsko odobrenje izdaje potvrdu o funkcionalnosti. Osim naziva korisnika i identifikacije modela, ta potvrda detaljno opisuje izvršene provjere i postignute rezultate.

277a

U funkcionalnom certifikatu bilo kojeg dijela tahografa su takođe navedeni homologacijski brojevi svih drugih homologovanih kompatibilnih sastavnih dijelova tahografa.

**4.   Potvrda o interoperabilnosti**

278  
Provjera interoperabilnosti se sprovodi u jednom od laboratorija pod nadležnošću i odgovornosti Evropske komisije.

279  
Laboratorij mora upisati zahtjeve za provjeru interoperabilnosti koje podnose proizvođači hronološkim redom njihovog pristizanja.

280  
Zahtjevi se službeno upisuju samo kada laboratorij dođe u posjed:

* cjelokupnog niza materijala i dokumenata potrebnih za takvo ispitivanje interoperabilnosti,
* odgovarajuće potvrde o sigurnosti,
* odgovarajuće potvrde o funkcionalnosti.

Datum upisa zahtjeva se prijavljuje proizvođaču.

281  
Laboratorij ne obavlja nikakva ispitivanja interoperabilnosti za tahografe ili tahografske kartice, koji nisu dobili sigurnosni certifikat i funkcionalni certifikat, osim u iznimnim okolnostima opisanim u zahtjevu 274a. 282  
Svaki proizvođač koji traži provjeru interoperabilnosti mora se obvezati da će laboratoriju zaduženom za takve provjere ostaviti cjelokupan niz materijala i dokumenata koje je pribavio radi sprovođenje provjera.

283  
Provjere interoperabilnosti moraju se izvesti u skladu s odredbama tačke 5. Dodatka 9. ovom Prilogu, na svim vrstama tahografa odnosno kartica tahografa:

* za koje tipsko odobrenje još vrijedi, ili
* za koje je tipsko odobrenje u tijeku i koji imaju važeću potvrdu o interoperabilnosti.

284  
Potvrdu o interoperabilnosti laboratorij izdaje proizvođaču tek nakon uspješnog prolaska svih provjera interoperabilnosti.

285  
Ako provjere interoperabilnosti na jednom ili više tahografa ili kartice(a) tahografa nisu bila uspješne prema zahtjevu 283, potvrda o interoperabilnosti se ne smije izdati prije nego proizvođač koji je podnio zahtjev ne izvrši potrebne izmjene i prođe provjeru interoperabilnosti. Laboratorij uz pomoć proizvođača kojih se tiče ova greška interoperabilnosti utvrđuje uzrok problema te pokušava pomoći proizvođaču podnosiocu zahtjeva da iznađe tehničko rješenje. Ako je proizvođač izmijenio svoj proizvod, odgovornost je proizvođača da utvrdi kod nadležnih tijela vrijede li još uvijek potvrde o sigurnosti i uvjerenje o funkcionalnosti.

286  
Potvrda o interoperabilnosti vrijedi šest mjeseci. Na kraju tog perioda ona se opoziva ako proizvođač nije dobio odgovarajuću potvrdu o tipskom odobrenju. Proizvođač ga dostavlja tijelu države članice ovlaštenom za tipsko odobrenje koje je izdalo potvrdu o funkcionalnosti.

287  
Niti jedan element koji bi mogao biti ishodište neuspjeha provjere interoperabilnosti se ne smije koristiti za postizanje dobiti ili za preuzimanje vodećeg položaja.

**5.   Potvrda o tipskom odobrenju**

288  
Tijelo države članice ovlašteno za tipsko odobrenje može izdati potvrdu o tipskom odobrenju čim zaprimi tri potrebna uvjerenja.

289  
Tijelo ovlašteno za izdavanje tipskog odobrenja, potvrdu o tipskom odobrenju mora istovremeno dostaviti laboratoriju zaduženom za provjeru interoperabilnosti i proizvođaču.

290  
Laboratorij nadležan za provjeru interoperabilnosti mora imati javnu internet stranicu na kojoj će se ažurirati popis modela tahografa ili kartica tahografa:

* za koje je upisan zahtjev za provjeru interoperabilnosti,
* kojima je izdana potvrda o interoperabilnosti (čak i privremena),
* kojima je izdana potvrda o tipskom odobrenju.

**6.   Vanredni postupak: prva provjera interoperabilnosti**

291  
Do isteka četiri mjeseca od izdavanja potvrde o interoperabilnosti za prvi par tahografa i kartica tahografa (kartica vozača, kartica radionice, kontrolna kartica i kartica prevoznika), svaka izdana potvrda (uključujući i prvu) u vezi zahtjeva upisanih u tom razdoblju se smatra privremenom.

292  
Ako na kraju tog perioda svi predmetni proizvodi budu međusobno interoperabilni, sve odgovarajuće potvrde o interoperabilnosti postaju konačne.

293  
Ako se tokom tog perioda utvrde greške interoperabilnosti, laboratorij zadužen za provjeru interoperabilnosti mora utvrditi uz pomoć svih uključenih proizvođača uzroke problema, te ih mora pozvati da izvrše potrebne izmjene.

294  
Ako se po isteku tog perioda problemi interoperabilnosti nastave, laboratorij zadužen za provjeru interoperabilnosti, u suradnji sa svim zainteresiranim proizvođačima i tijelima ovlašćenim za tipsko odobrenje koja su izdala odgovarajuće potvrde o funkcionalnosti moraju iznaći uzrok grešaka interoperabilnosti i utvrditi koje izmjene svaki od dotičnih proizvođača treba izvršiti. Iznalaženje tehničkih rješenja može trajati najduže dva mjeseca, nakon čega će Komisija, ako se ne iznađe nikakvo zajedničko rješenje, nakon dogovora s laboratorijem zaduženim za provjeru interoperabilnosti, odlučiti koji će tahograf(i) i kartice dobiti konačnu potvrdu o interoperabilnosti i navesti razloge.

295  
Svaki zahtjev za provjeru interoperabilnosti upisan od strane laboratorija između kraja četveromjesečnog perioda nakon izdavanja prve privremene potvrde o interoperabilnosti i datuma odluke Komisije iz zahtjeva 294 se mora odgoditi dok se ne riješe prvi problemi interoperabilnosti. Takvi zahtjevi se potom obrađuju hronološkim redom njihovog upisivanja.

**Dodatak 1.**

**RJEČNIK PODATAKA**

SADRŽAJ

1. UVOD

1.1. Pristub definisanja vrsta podataka

1.2. Literatura

2. DEFINICIJE VRSTA PODATAKA

2.1. ActivityChangeInfo

2.2. Address

2.3. BCDString

2.4. CalibrationPurpose

2.5. CardActivityDailyRecord

2.6. CardActivityLengthRange

2.7. CardApprovalNumber

2.8. CardCertificate

2.9. CardChipIdentification

2.10. CardConsecutiveIndex

2.11. CardControlActivityDataRecord

2.12. CardCurrentUse

2.13. CardDriverActivity

2.14. CardDrivingLicenceInformation

2.15. CardEventData

2.16. CardEventRecord

2.17. CardFaultData

2.18. CardFaultRecord

2.19. CardIccIdentification

2.20. CardIdentification

2.21. CardNumber

2.22. CardPlaceDailyWorkPeriod

2.23. CardPrivateKey

2.24. CardPublicKey

2.25. CardRenewalIndex

2.26. CardReplacementlndex

2.27. CardSlotNumber

2.28. CardSlotsStatus

2.29. CardStructureVersion

2.30. CardVehicleRecord

2.31. CardVehiclesUsed

2.32. Certificate

2.33. CertificateContent

2.34. CertificateHolderAuthorisation

2.35. CertificateRequestID

2.36. CertificationAuthorityKID

2.37. CompanyActivityData

2.38. CompanyActivityType

2.39. CompanyCardApplicationIdentification

2.40. CompanyCardHolderIdentification

2.41. ControlCardApplicationIdentification

2.42. ControlCardControlActivityData

2.43. ControlCardHolderIdentification

2.44. ControlType

2.45. CurrentDateTime

2.46. DailyPresenceCounter

2.47. Datef

2.48. Distance

2.49. DriverCardApplicationldentification

2.50. DriverCardHolderIdentification

2.51. EntryTypeDailyWorkPeriod

2.52. EquipmentType

2.53. EuropeanPublicKey

2.54. EventFaultType

2.55. EventFaultRecordPurpose

2.56. ExtendedSerialNumber

2.57. FullCardNumber

2.58. HighResOdometer

2.59. HighResTripDistance

2.60. HolderName

2.61. K-ConstantOfRecordingEquipment

2.62. KeyIdentifier

2.63. L-TyreCircumference

2.64. Language

2.65. LastCardDownload

2.66. ManualInputFlag

2.67. ManufacturerCode

2.68. MemberStateCertificate

2.69. MemberStatePublicKey

2.70. Name

2.71. NationAlpha

2.72. NationNumeric

2.73. NoOfCalibrationRecords

2.74. NoOfCalibrationsSinceDownload

2.75. NoOfCardPlaceRecords

2.76. NoOfCardVehicleRecords

2.77. NoOfCompanyActivityRecords

2.78. NoOfControlActivityRecords

2.79. NoOfEventsPerType

2.80. NoOfFaultsPerType

2.81. OdometerValueMidnight

2.82. OdometerShort

2.83. OverspeedNumber

2.84. PlaceRecord

2.85. PreviousVehiclelnfo

2.86. PublicKey

2.87. RegionAlpha

2.88. RegionNumeric

2.89. RSAKeyModulus

2.90. RSAKeyPrivateExponent

2.91. RSAKeyPublicExponent

2.92. SensorApprovalNumber

2.93. SensorIdentification

2.94. SensorInstallation

2.95. SensorInstallationSecData

2.96. SensorOSIdentifier

2.97. SensorPaired

2.98. SensorPairingDate

2.99. SensorSerialNumber

2.100. SensorSCIdentifier

2.101. Signature

2.102. SimilarEventsNumber

2.103. SpecificConditionType

2.104. SpecificConditionRecord

2.105. Speed

2.106. SpeedAuthorised

2.107. SpeedAverage

2.108. SpeedMax

2.109. TDesSessionKey

2.110. TimeReal

2.111. TyreSize

2.112. VehicleldentificationNumber

2.113. VehicleRegistrationIdentification

2.114. VehicleRegistrationNumber

2.115. VuActivityDailyData

2.116. VuApprovalNumber

2.117. VuCalibrationData

2.118. VuCalibrationRecord

2.119. VuCardIWData

2.120. VuCardIWRecord

2.121. VuCertificate

2.122. VuCompanyLocksData

2.123. VuCompanyLocksRecord

2.124. VuControlActivityData

2.125. VuControlActivityRecord

2.126. VuDataBlockCounter

2.127. VuDetailedSpeedBlock

2.128. VuDetailedSpeedData

2.129. VuDownloadablePeriod

2.130. VuDownloadActivityData

2.131. VuEventData

2.132. VuEventRecord

2.133. VuFaultData

2.134. VuFaultRecord

2.135. VuIdentification

2.136. VuManufacturerAddress

2.137. VuManufacturerName

2.138. VuManufacturingDate

2.139. VuOverSpeedingControlData

2.140. VuOverSpeedingEventData

2.141. VuOverSpeedingEventRecord

2.142. VuPartNumber

2.143. VuPlaceDailyWorkPeriodData

2.144. VuPlaceDailyWorkPeriodRecord

2.145. VuPrivateKey

2.146. VuPublicKey

2.147. VuSerialNumber

2.148. VuSoftInstallationDate

2.149. VuSoftwareIdentification

2.150. VuSoftwareVersion

2.151. VuSpecificConditionData

2.152. VuTimeAdjustmentData

2.153. VuTimeAdjustmentRecord

2.154. W-VehicleCharacteristicConstant

2.155. WorkshopCardApplicationIdentification

2.156. WorkshopCardCalibrationData

2.157. WorkshopCardCalibrationRecord

2.158. WorkshopCardHolderIdentification

2.159. WorkshopCardPIN

3. DEFINICIJE RASPONA VRIJEDNOSTI I VELIČINA

3.1. Definicije za karticu vozača

3.2. Definicije za karticu radionice

3.3. Definicije za nadzornu karticu

3.4. Definicije za karticu prevoznika

4. NIZOVI ZNAKOVA

5. ŠIFRIRANJE

**1.   UVOD**

Ovaj Dodatak definira format podataka, elemente podataka i strukturu podataka za primjenu u tahografima i karticama tahografa.

**1.1.   Pristub definiranju vrsta podataka**

U ovom se dodatku za definiranje vrsta podataka koristi ASN.1 (Abstract Syntax Notation One). To omogućava definiranje jednostavnih i strukturiranih podataka, bez impliciranja posebne sintakse prenosa (pravila šifriranja) koja bi bila ovisna o aplikaciji i okruženju.

Dogovori o nazivlju tipa ASN.l su u skladu s normom ISO/IEC 8824-1. To znači da:

* gdje je moguće, značenje vrste podataka se naslućuje iz odabranih naziva,
* ako je vrsta podataka kombinacija različitih vrsta podataka, naziv vrste podataka i dalje je jedinstveni niz slovnih znakova koji počinje velikim slovom, međutim velika slova se u imenima koriste kako bi naglasilo odgovarajuće značenje,
* nazivi vrsta podataka uopšteno su vezani uz naziv vrste podataka iz kojih su izvedeni, uređaj u kojemu su podaci arhivirani, te funkciju vezanu uz podatke.

Ako je vrsta podataka po ASN.l već definirana u okviru neke druge norme, a važna je za korištenje u tahografu, ta ASN.1 vrsta podataka definirat će se u ovom Dodatku.

Kako bi se dopustilo više vrsta pravila šifriranja, neke ASN.1 vrste podataka, u ovom Dodatku su ograničene identifikatorima raspona vrijednosti. Identifikatori raspona vrijednosti su definirani u stavu 3.

**1.2.   Literatura**

U ovom Dodatku koriste se sljedeći izvori:

|  |  |
| --- | --- |
| ISO 639 | Kodeks o prikazivanju naziva jezika. Prvo izdanje: 1988 |
| EN 726-3 | Sistemi identifikacijskih kartica – Telekomunikacijske kartice i terminali s integirsanim krugovima – 3. dio: Zahtjevi za kartice, koje ne ovise o aplikaciji, prosinac 1994. |
| ISO 3779 | Drumska vozila – Identifikacijski broj vozila (VIN) – Sadržaj i struktura. 3. izdanje: 1983. |
| ISO/IEC 7816-5 | Informacijska tehnologija – Identifikacijske kartice – Kontaktna(e) kartica(e) s integirsanim krugovima – 5. dio: Sistem numeriranja i postupak registracije za identifikatore aplikacija. Prvo izdanje: 1994. + Dopuna 1: 1996. |
| ISO/IEC 8824-1 | Informacijska tehnologija – Sažeti sintaktički zapis 1 (ASN.l): Specifikacije osnovnog zapisa. 2. izdanje: 1998. |
| ISO/IEC 8825-2 | Informacijska tehnologija – Pravila šifriranja ASN.l: specifikacije pravila paketnog kodiranja (PER).2. izdanje: 1998. |
| ISO/IEC 8859-1 | Informacijska tehnologija – Grupa 8-bitnih jednobajtnih šifriranih grafičkih znakova – 1. dio: skupina latinica br. 1. Prvo izdanje: 1998. |
| ISO/IEC 8859-7 | Informacijska tehnologija – Grupa 8-bitnih jednobajtnih šifriranih grafičkih znakova – 7. dio: latinica/grčka abeceda. Prvo izdanje: 1987. |
| ISO 16844-3 | Drumska vozila – Tahografski sistemi – Sučelje senzora kretanja WD 3-20/05/99. |

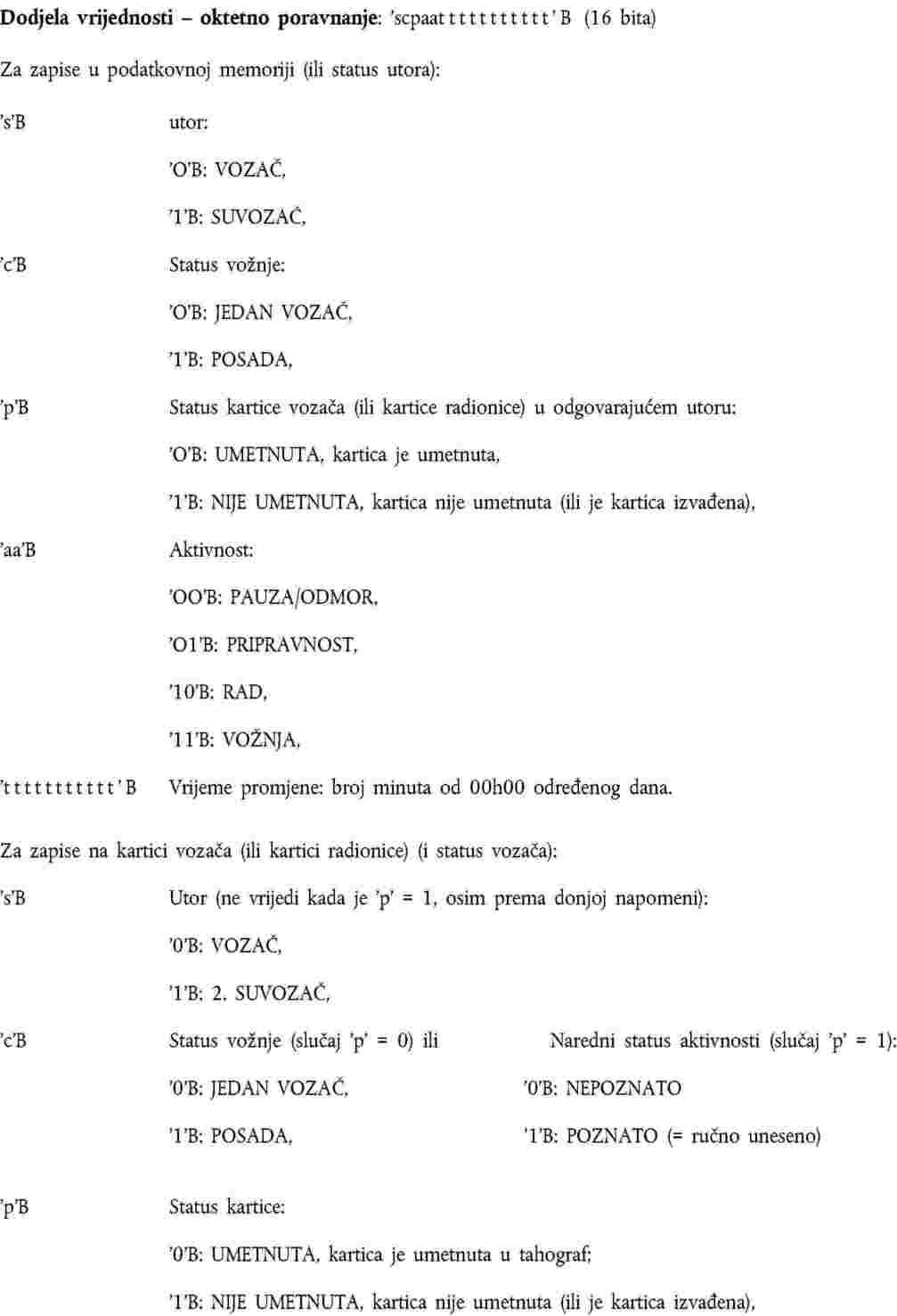
**2.   DEFINICIJE VRSTA PODATAKA**

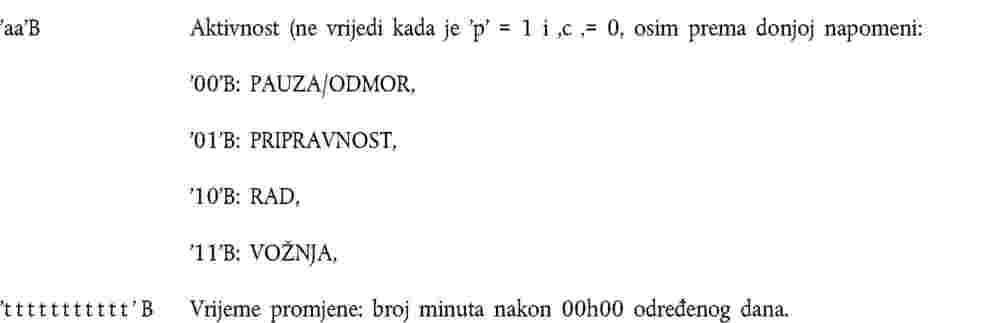
Za svaku od sljedećih vrsta podataka standardna vrijednost sadržaja ‚nepoznato’ ili ‚ne primjenjuje se’ se sastoji u popunjavanju elementa s ‚FF’ bajtima.

**2.1.   ActivityChangeInfo**

Ova vrsta podataka omogućava šifriranje, u okviru dvobajtne riječi, statusa otvora u 00:00 sati i/ili statusa vozača u 00:00 sati i/ili promjene aktivnosti i/ili promjene statusa vožnje i/ili promjene statusa kartice vozača ili kartice suvozača. Ova se vrsta podataka odnosi na zahtjeve 084, 109a, 199 i 219.

Image





**Napomena za slučaj ‚vađenja kartice’:**

Kad se kartica izvadi:

* ‚s’ vrijedi i označava otvor iz kojeg je kartica izvađena,
* ‚c’ se mora postaviti na 0,
* ‚p’ se mora postaviti na 1,
* ‚aa’ mora šifrirati tekuću aktivnost, izabranu u to vrijeme,

Kao rezultat ručnog unosa, bitovi riječi ‚c’ i ‚aa’ (arhivirani na kartici) mogu se kasnije prepisati preko postojećih zapisa.

**2.2.   Address**

Adresa.

Adress: = SEQUENCE {

codePage INTEGER (0..255),

address OCTET STRING (SIZE(35))

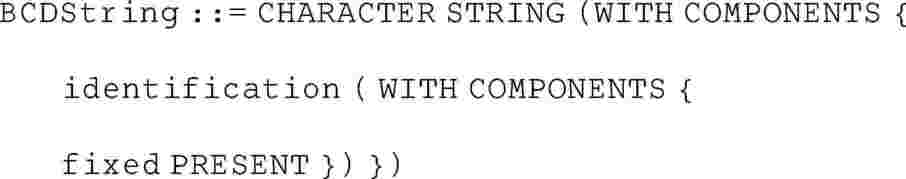
}

codePage utvrđuje niz znakova, definisanih u poglavlju 4.,

address je adresa, šifrirana određenim nizom znakova”.

**2.3.   BCDString**

BCDString se primjenjuje za prikaz binarno kodiranih decimalnih brojeva (BCD). Ova podaci vrsta se koristi za predstavljanje jednodecimalne znamenke u jednom poluoktetu (4 bita). BCDString se temelji na ISO/IEC 8824-1 ‚CharacterString Type’.



BCDString koristi zapis ‚hstring’. Krajnja lijeva heksadecimalna znamenka mora biti najznačajniji poluoktet prvog okteta. Višekratnik okteta tvori se tako da se prema potrebi umetne poluoktet sa završnim nulama od mjesta lijevog poluokteta u prvom oktetu.

Dopuštene znamenke su: 0, 1, … 9.

**2.4.   CalibrationPurpose**

Šifra pojašnjava zašto je zaevidentirajun niz parametara kalibrisanja. Ova podaci vrsta je vezana uz zahtjeve 097 i 098.

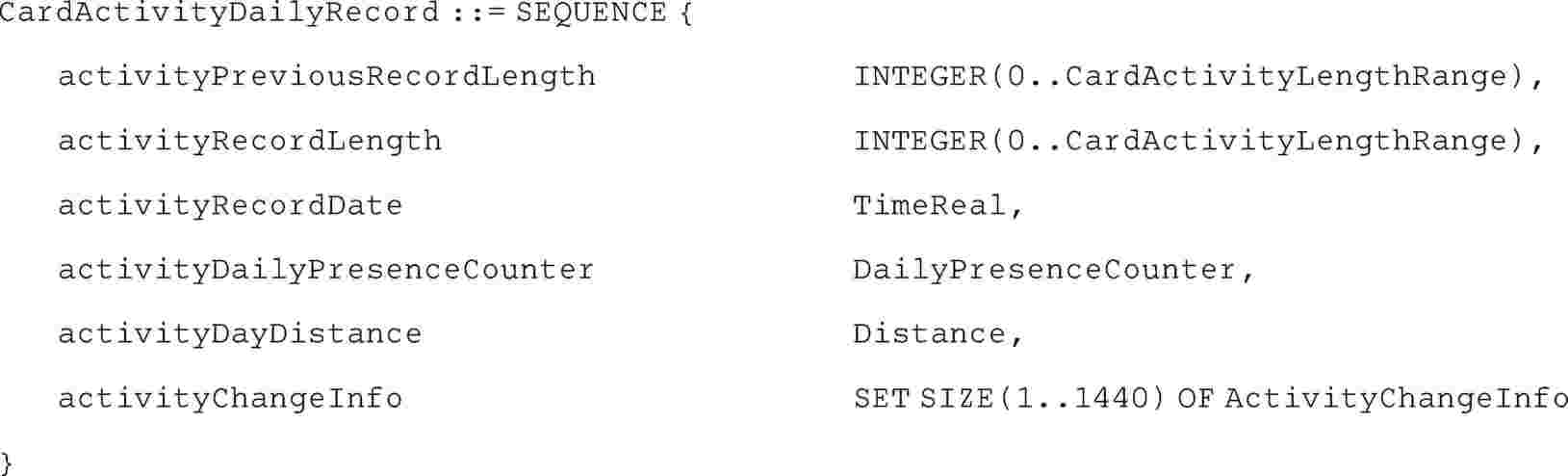
Image

**Dodjela vrijednosti:**

|  |  |
| --- | --- |
| ‚00’H | rezervirana vrijednost, |
| ‚01’H | aktivacija: belježenje poznatih parametara kalibracije u trenutku aktivacije jedinice vozila, |
| ‚02’H | prva ugradnja: prva kalibracija u jedinici vozila nakon aktivacije, |
| ‚03’H | ugradnja: prva kalibracija jedinice vozila u sadašnjem vozilu, |
| ‚04’H | periodični nadzor. |

**2.5   CardActivityDailyRecord**

Informacija sačuvana na kartici koja se odnosi na aktivnost vozača na određeni kalendarski dan. Ova vrsta podataka je povezana sa zahtjevima 199 i 219.



**activityPreviousRecordLength** je ukupna dužina prethodnog dnevnog zapisa u bajtima. Najveća vrijednost je iskazana u dužini OCTET STRING koja sadrži takve zapise (vidjeti CardActivityLengthRange, stavak 3). Kad je taj zapis najstariji dnevni zapis, vrijednost activityPreviousRecordLength mora biti postavljena na 0.

**activityRecordLength** je ukupna dužina tog zapisa u bajtima. Najveća vrijednost je dana dužinom OCTET STRING koja sadrži navedene zapise.

**activityRecordDate** je datum zapisa.

**activityDailyPresenceCounter** je dnevni brojač prisutnosti kartica za taj dan.

**activityDayDistance** je ukupna pređena udaljenost na taj dan.

**activityChangeInfo** je skupina podataka ActivityChangeInfo za vozača za taj dan. Može sadržavati najviše 1 440 vrijednosti (jedna promjena aktivnosti na minutu). Ta skupina uvijek uključuje i activityChangeInfo koja šifrira status vozača u 00:00.

**2.6   CardActivityLengthRange**

Broj bajta na kartici vozača ili kartici radionice raspoloživih za čuvanje zapisa o aktivnosti vozača.

Image

**Dodjela vrijednosti:** vidjeti stavak 3.

**2.7.   CardApprovalNumber**

Broj tipskog odobrenja kartice.

Image

**Dodjela vrijednosti:** Nije utvrđeno.

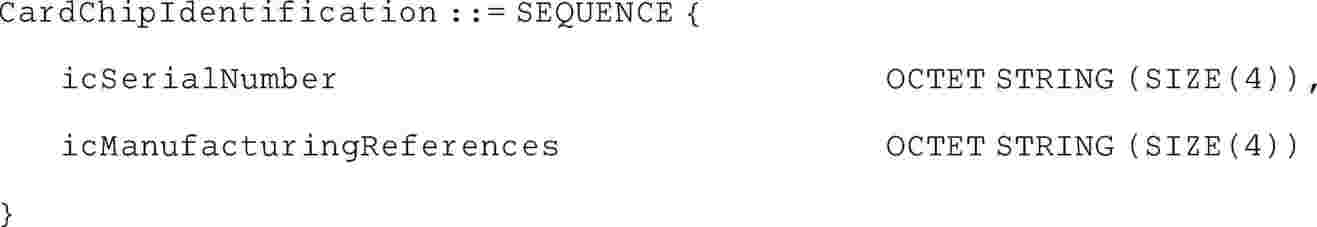
**2.8.   CardCertificate**

Certifikat javnog ključa kartice.

Image

**2.9   CardChipIdentification**

Informacija sačuvana na kartici koja se odnosi na identifikaciju integriranog kruga (IC) kartice (zahtjev 191).



**icSerialNumber** je serijski broj IC, kako je utvrđeno u EN 726-3.

**icManufacturingReferences** je identifikator proizvođača IC i ugradbenih elemenata, kako je utvrđeno u EN 726-3.

**2.10.   CardConsecutiveIndex**

Redni indeks kartice (definicija h).

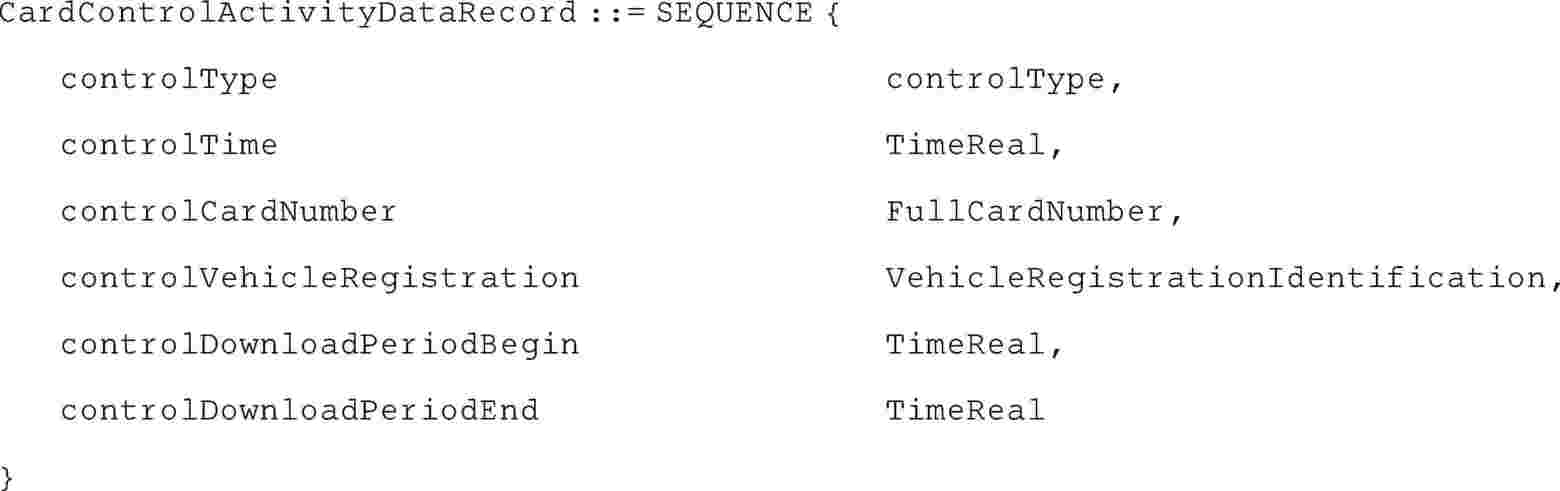
Image

**Dodjela vrijednosti:** (vidjeti poglavlje VII. ovog Priloga).

Redoslijed uvećavanja:: ‚0…9, A…Z, a…z’.

**2.11.   CardControlActivityDataRecord**

Informacija sačuvana na kartici vozačaj ili kartici radionice koja se odnosi na posljednju kontrolu kojoj je vozač bio podvrgnut (zahtjevi 210 i 225).



**controlType** je vrsta nadzora.

**controlTime** je datum i vrijeme nadzora.

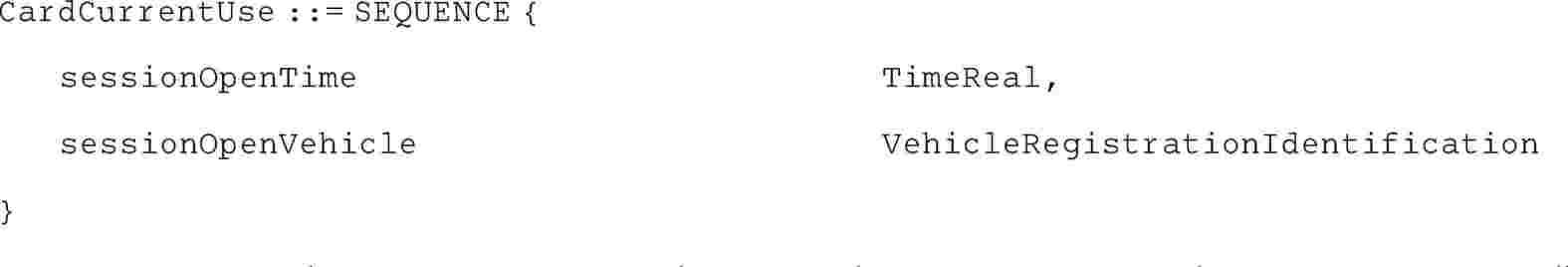
**controlCardNumber** je FullCardNumber službenika za nadzor koji je izvršio nadzor.

**controlVehicleRegistration** je registracijski broj vozila i država članica registracije vozila na kojemu je obavljen nadzor.

**controlDownloadPeriodBegin** i **controlDownloadPeriodEnd** je period za koje su preuzeti podaci, u slučaju preuzimanja podataka.

**2.12.   CardCurrentUse**

Informacija o trenutnom korištenju kartice (zahtjev 212).

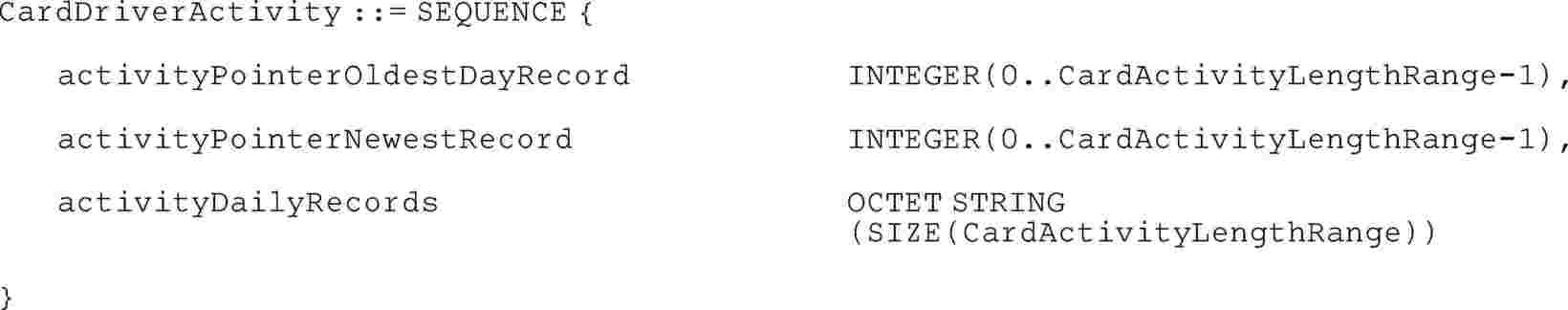


**sessionOpenTime** je vrijeme kada je kartica umetnuta radi trenutnog korištenja. Pri vađenju kartice ovaj se element postavlja na nulu.

**sessionOpenVehicle** je identifikacija trenutno korištenog vozila koja se postavlja ubacivanjem kartice. Pri vađenju kartice ovaj se element postavlja na nulu.

**2.13.   CardDriverActivity**

Informacija sačuvana na kartici vozača ili kartici radionice koja se odnosi na aktivnosti vozača (zahtjevi 199 i 219).



**activityPointerOldestDayRecord** je određivanje početka prostora za čuvanje (broj bajta od početka niza) najstarijeg punog dnevnog zapisa u nizu activityDailyRecords. Najveću vrijednost prikazuje dužina niza.

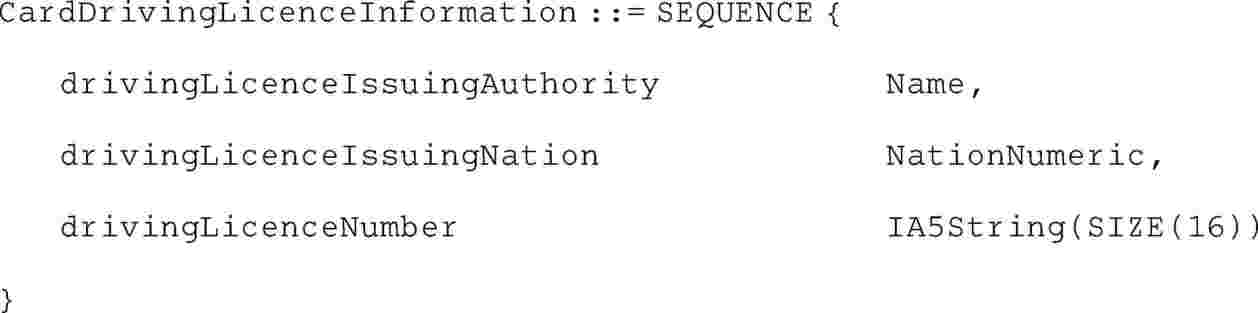
**activityPointerOldestDayRecord** je određivanje početka prostora za čuvanje (broj bajta od početka niza) najnovijeg dnevnog zapisa u nizu activityDailyRecords. Najveću vrijednost prikazuje dužina niza.

**activityDailyRecords** je prostor raspoloživ za čuvanje podataka o aktivnostima vozača (struktura podataka: CardActivityDailyRecord) za svaki kalendarski dan u kojemu je kartica korištena.

**Dodjela vrijednosti:** taj se oktetni niz ciklički popunjava zapisima CardActivityDailyRecord. Pri prvom korištenju čuvanje započinje s prvim bajtom niza. Svi novi zapisi se stavljaju na kraj prethodnog. Kad se niz popuni, čuvanje se nastavlja u prvi bajt niza bez obzira na prekid u podakovnom elementu. Prije stavljanja u niz novih podataka o aktivnostima (povećanje postojeće activityDailyRecord ili stavljanje nove activityDailyRecord), koji zamjenjuju stare podatke o aktivnostima, potrebno je ažurirati activityPointerOldestDayRecord tako da odražava novo mjesto najstarijeg punog dnevnog zapisa, a activityPreviousRecordLength takvog (novog) najstarijeg potpunog dnevnog zapisa ponovo postaviti na 0.

**2.14.   CardDrivingLicenceInformation**

Informacija sačuvana na kartici vozača, koja se odnosi na podatke o vozačkoj dozvoli nosioca kartice (zahtjev 196).



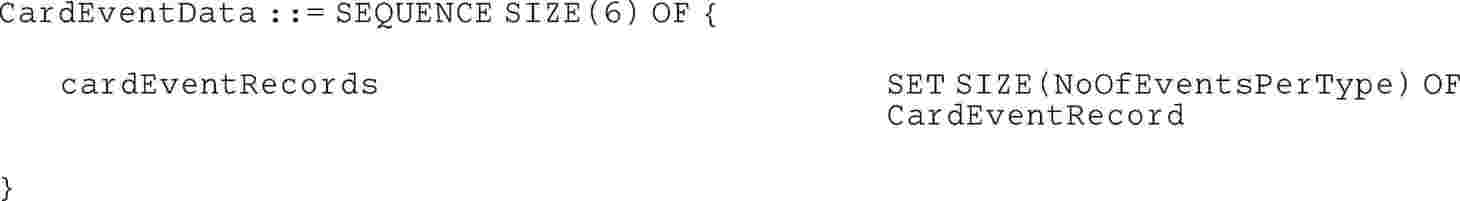
**drivingLicenceIssuingAuthority** je tijelo ovlašteno za izdavanje vozačke dozvole.

**drivingLicenceIssuingNation** je državna pripadnost tijela koje je izdalo vozačku dozvolu.

**drivingLicenceNumber** je broj vozačke dozvole.

**2.15.   CardEventData**

Informacija sačuvana na kartici vozača ili kartici radionice koja se odnosi na slučajeve vezane uz nosioca kartice (zahtjevi 204 i 223).

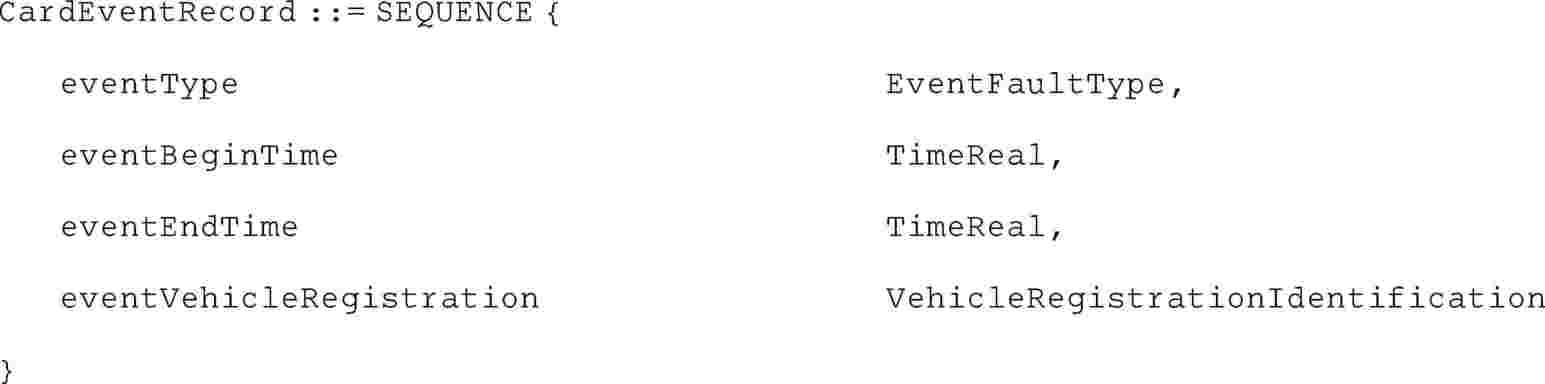


**CardEventData** je slijed, poredan prema rastućoj vrijednosti EventFaultType, zapisa cardEventRecords (osim o pokušajima probijanja zaštite koji su skupljeni u posljednjem nizu slijeda).

**cardEventRecords** je niz zapisa o događajima određene vrste (ili kategorija događaja pokušaja probijanja zaštite).

**2.16.   CardEventRecord**

Informacija sačuvana na kartici vozača ili kartici radionice koja se odnosi na slučaj vezan uz nosioca kartice (zahtjevi 205 i 223).



**eventType** je vrsta događaja.

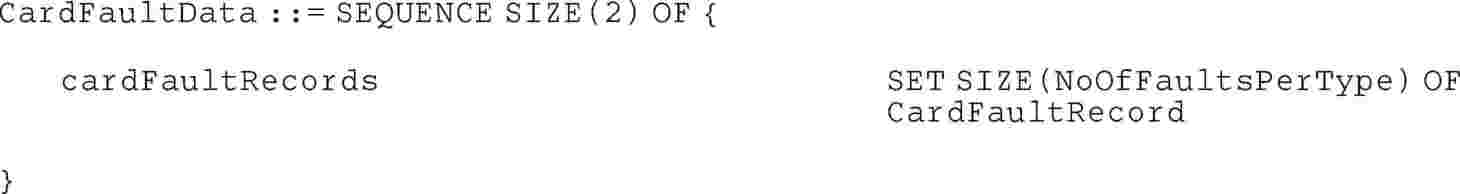
**eventBeginTime** je datum i vrijeme početka događaja.

**eventEndTime** je datum i vrijeme završetka događaja.

**eventVehicleRegistration** je registracijska oznaka vozila i država članica registracije vozila u kojem se događaj dogodio.

**2.17.   CardFaultData**

Informacija sačuvana na kartici vozača ili kartici radionice koja se odnosi na greške vezane uz nosioca kartice (zahtjevi 207 i 223).

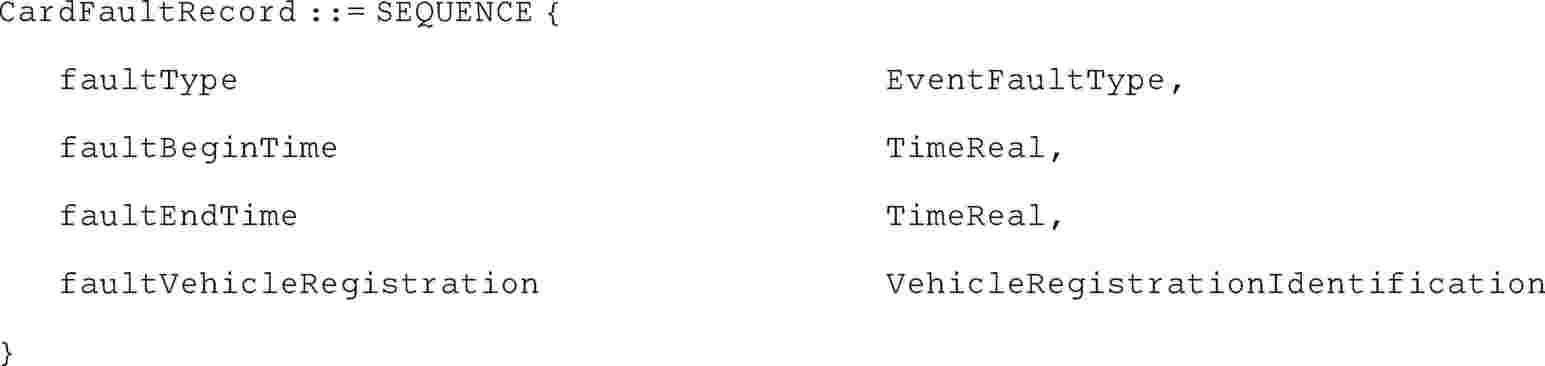


**cardFaultData** je slijed niza zapisa o greškama tahografa iza kojeg slijedi niz zapisa o greškama kartice.

**cardFaultRecords** je niz zapisa o greškama određene kategorije grešaka (tahografa ili kartica).

**2.18.   CardFaultRecord**

Informacija sačuvana na kartici vozača ili kartici radionice koja se odnosi na greške vezane uz nosioca kartice (zahtjevi 208 i 223).



**faultType** je vrsta greške.

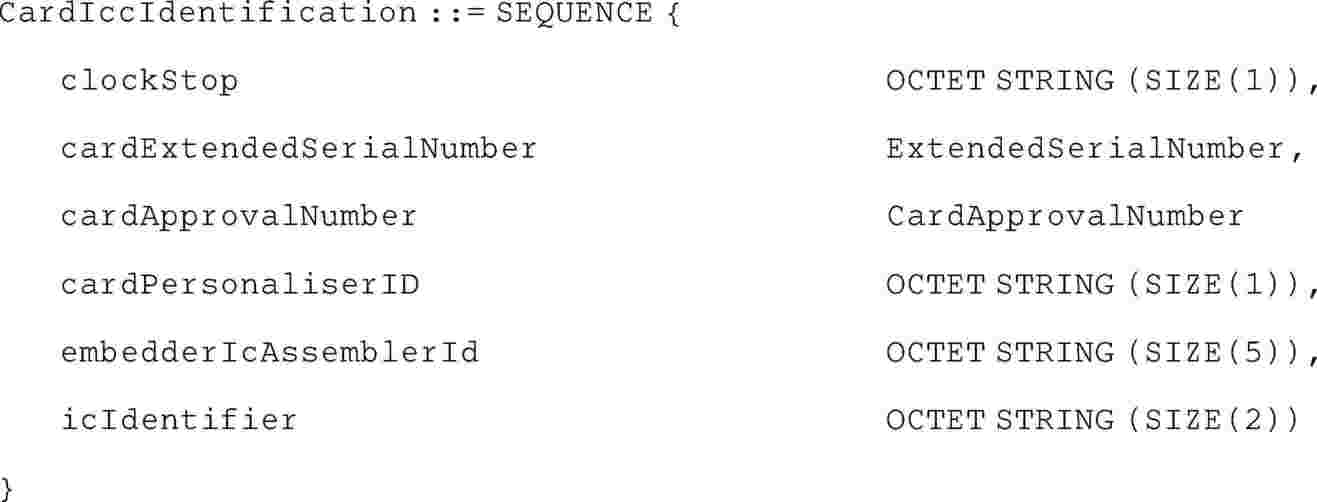
**faultBeginTime** je datum i vrijeme početka greške.

**faultEndTime** je datum i vrijeme završetka greške.

**faultVehicleRegistration** je registracijski broj vozila i država članica registracije vozila u kojemu je nastala greška.

**2.19.   CardIccIdentification**

Informacija sačuvana na kartici koja se odnosi na identifikaciju integriranog kruga (IC) kartice (zahtjev 192).



**clockStop** je režim Clockstop definiran u EN 726-3.

**cardExtendedSerialNumber** obuhvaća serijski broj IC i podatke o proizvodnji IC utvrđene u EN 726-3 i kako je podrobnije određeno vrstom podataka ExtendedSerialNumber.

**cardApprovalNumber** je broj tipskog odobrenja kartice.

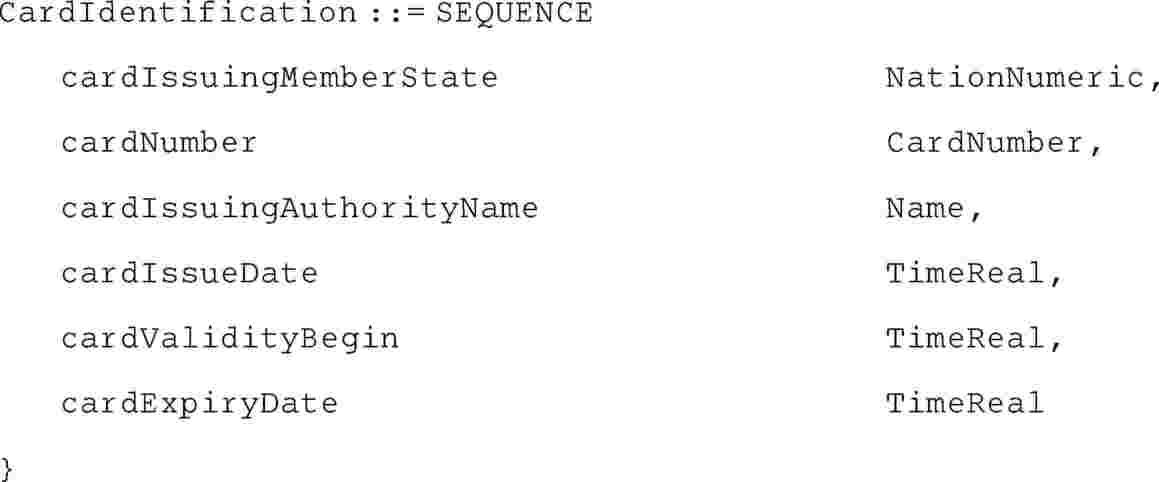
**cardPersonaliserlD** je ID personalizatora kartice, definiran u EN 726-3.

**embedderIcAssemblerId** je identifikator ugraditelja/instalatera IC, kako je definisano u EN 726-3.

**icIdentifier** je identifikator IC na kartici i proizvođača njenog IC, kako je definisano u EN 726-3.

**2.20.   CardIdentification**

Informacija sačuvana na kartici koja se odnosi na identifikaciju kartice (zahtjevi 194, 215, 231, 235).



**cardIssuingMemberState** je oznaka države članice koja je izdala karticu.

**cardNumber** je broj kartice.

**cardIssuingAuthorityName** je naziv tijela koje je izdalo karticu.

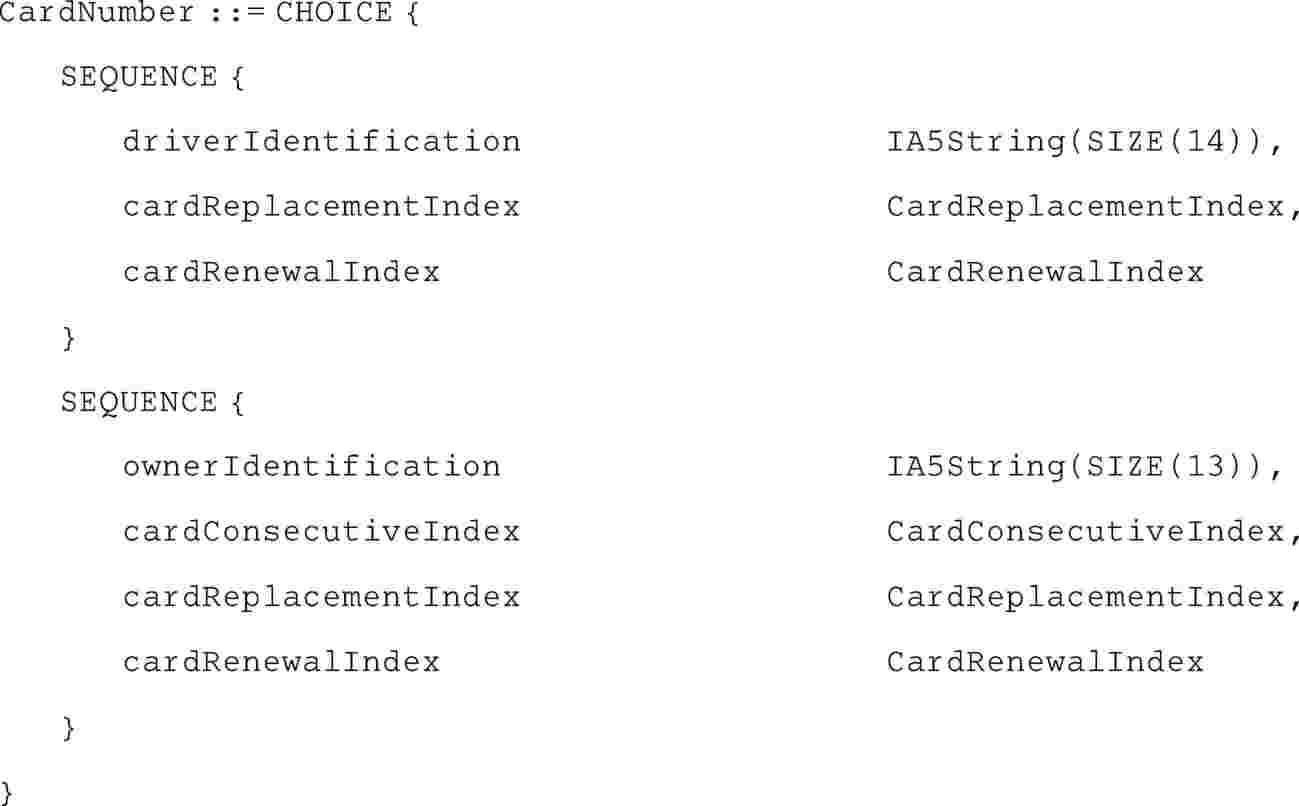
**cardIssueDate** je datum izdavanja kartice sadašnjem nosiocu.

**cardValidityBegin** je datum početka važnosti kartice.

**cardExpiryDate** je datum isteka važnosti kartice.

**2.21.   CardNumber**

Broj kartice prema definiciji g).



**driverIdentification** je jedinstvena identifikacija vozača u državi članici.

**ownerIdentification** je jedinstvena identifikacija prevoznika ili radionice ili nadzornog tijela u državi članici.

**cardConsecutiveIndex** je redni indeks kartice.

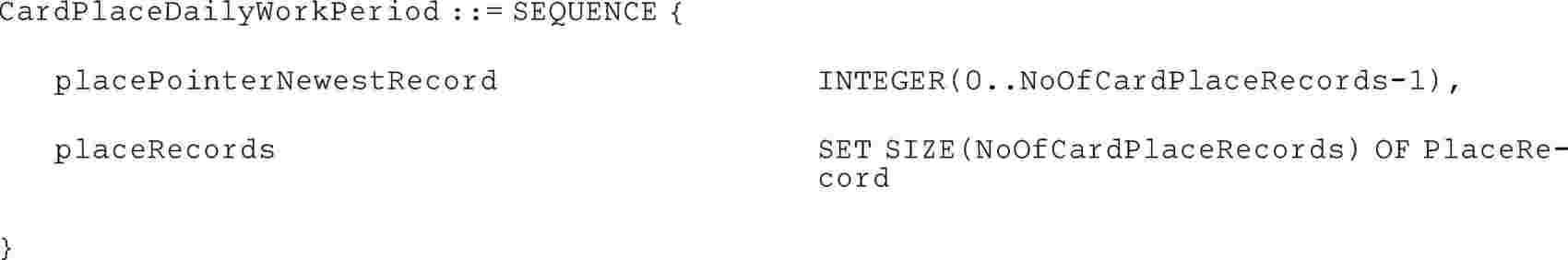
**cardConsecutiveIndex** je zamjenski indeks kartice.

**cardConsecutiveIndex** je indeks obnavljanja kartice.

Prvi slijed izbora je prikladan za šifriranje broja kartice vozača, drugi slijed izbora je prikladan za šifriranje brojeva kartice radionice, kontrolne kartice i kartice prevoznika.

**2.22.   CardPlaceDailyWorkPeriod**

Informacija sačuvana na kartici vozača ili kartici radionice koja se odnosi na mjesta početka i/ili završetka dnevnog perioda rada (zahtjevi 202 i 221).



**placePointerNewestRecord** je indeks posljednjeg ažuriranog zapisa mjesta.

**Pripisivanje vrijednosti:** Broj koji odgovara numeratoru zapisa mjesta, koji počinje s ‚0’ za prvu pojavu zapisa mjesta u strukturi.

**placeRecords** je niz zapisa koja sadrži informacije o upisanim mjestima.

**2.23.   CardPrivateKey**

Privatni ključ kartice.

Image

**2.24.   CardPublicKey**

Javni ključ kartice.

Image

**2.25.   CardRenewalIndex**

Indeks obnavljanja kartice (definicija i).

Image

**Dodjela vrijednosti:** (vidjeti poglavlje VII. ovog Priloga).

‚0’ prvo izdavanje.

Redoslijed uvećavanja: ‚0, …,9, A, …,Z’.

**2.26.   CardReplacementlndex**

Indeks zamjene kartice (definicija j).

Image

**Dodjela vrijednosti:** (vidjeti poglavlje VII. ovog Priloga).

‚0’ izvorna kartica.

Redoslijed uvećavanja: ‚0, …,9, A, …,Z’.

**2.27.   CardSlotNumber**

Razlikovna šifra za raspoznavanje između dvaju otvora jedinice u vozilu.

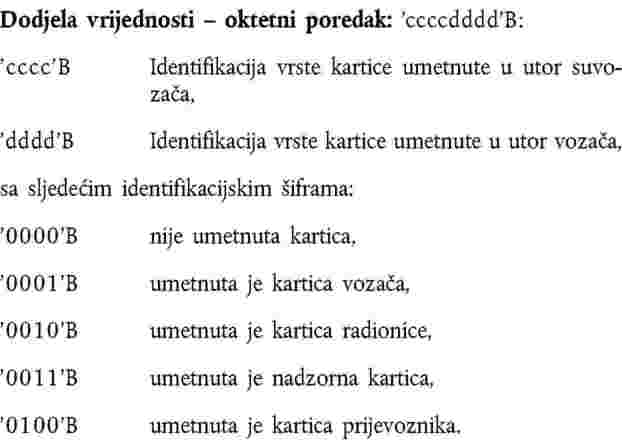


**Dodjela vrijednosti:** nije podrobnije određena.

**2.28.   CardSlotsStatus**

Šifra koja označava vrstu kartica umetnutih u dva otvora jedinice u vozilu.

Image



**2.29.   CardStructureVersion**

Oznaka koja prikazuje inačicu primijenjene strukture na kartici tahografa.

Image

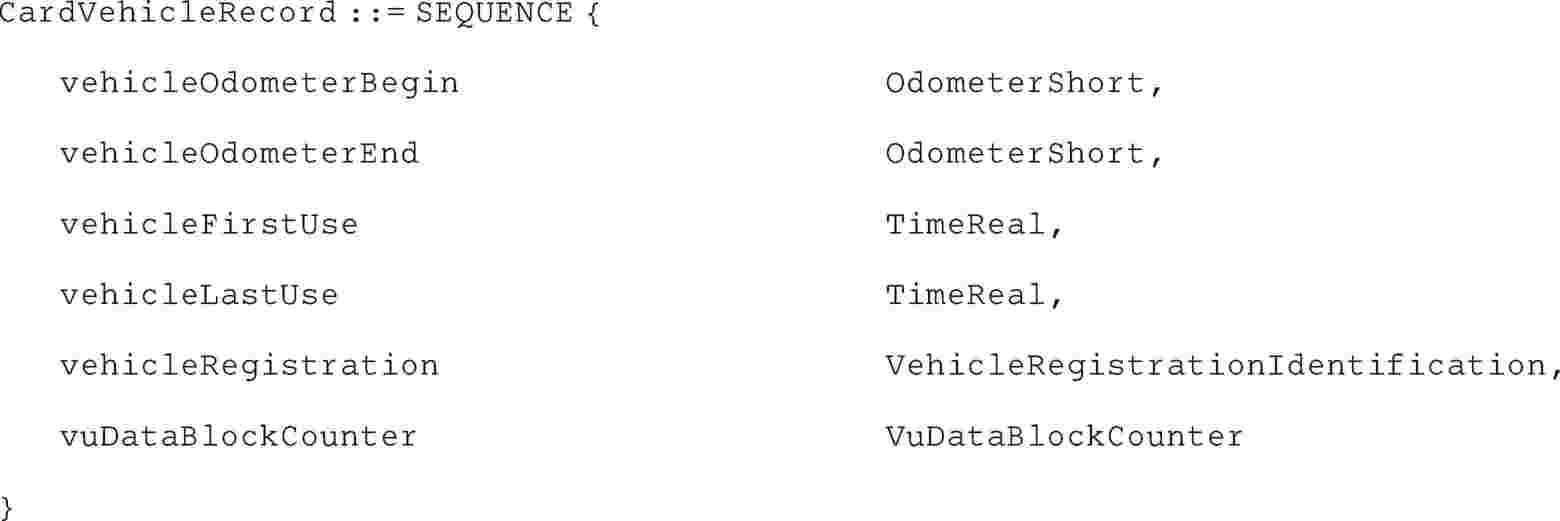
Dodjela vrijednosri: ‘aabb’H:

„aa”H Indeks za promjene strukture, „00h” za ovu inačicu

„bb”H Indeks za promjene vezane uz korištenje definisanih podatkovnih elemenata za strukturu višeg bajta, „00h” za ovu inačicu.;

**2.30.   CardVehicleRecord**

Informacija sačuvana na kartici vozača ili kartici radionice, koja se odnosi na period korištenja vozila tokom jednog kalendarskog dana (zahtjevi 197 i 217).



**vehicleOdometerBegin** je stanje brojača kilometara vozila na početku perioda korištenja vozila.

**vehicleOdometerEnd** je stanje brojača kilometara vozila na kraju perioda korištenja vozila.

**vehicleFirstUse** je datum i vrijeme početka perioda korištenja vozila.

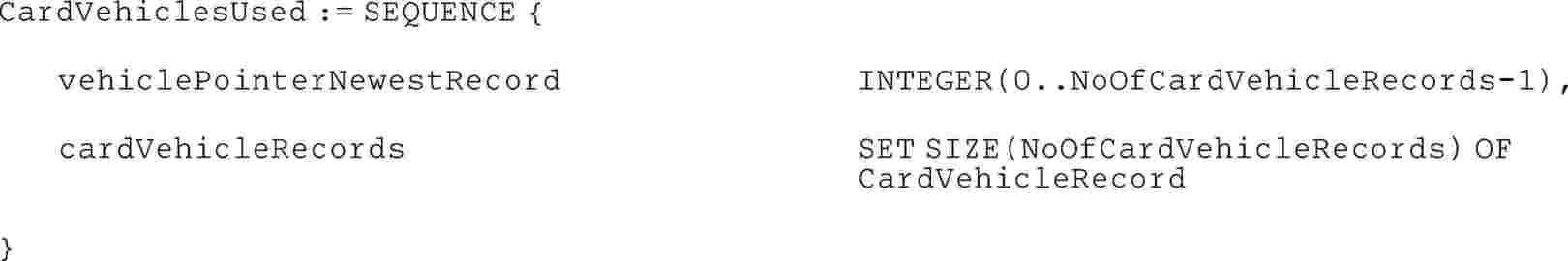
**vehicleLastUse** je datum i vrijeme završetka perioda korištenja vozila.

**vehicleRegistration** je registracijska oznaka vozila i država registracije vozila.

**vuDataBlockCounter** je vrijednost VuDataBlockCounter pri posljednjem razdoblju korištenja vozila.

**2.31.   CardVehiclesUsed**

Informacija sačuvana na kartici vozača ili kartici radionice, koja se odnosi na vozila koja je koristio vlasnik kartice (zahtjevi 197 i 217).



**vehiclePointerNewestRecord** je indeks posljednjeg ažuriranog zapisa o vozilu.

**Pripisivanje vrijednosti:** Broj koji odgovara numeratoru zapisa o vozilu koji počinje s ‚0’ za prvo pojavljivanje u strukturi zapisa o vozilu.

**cardVehicleRecords** je niz zapisa s podacima o korišćenim vozilima.

**2.32.   Certificate**

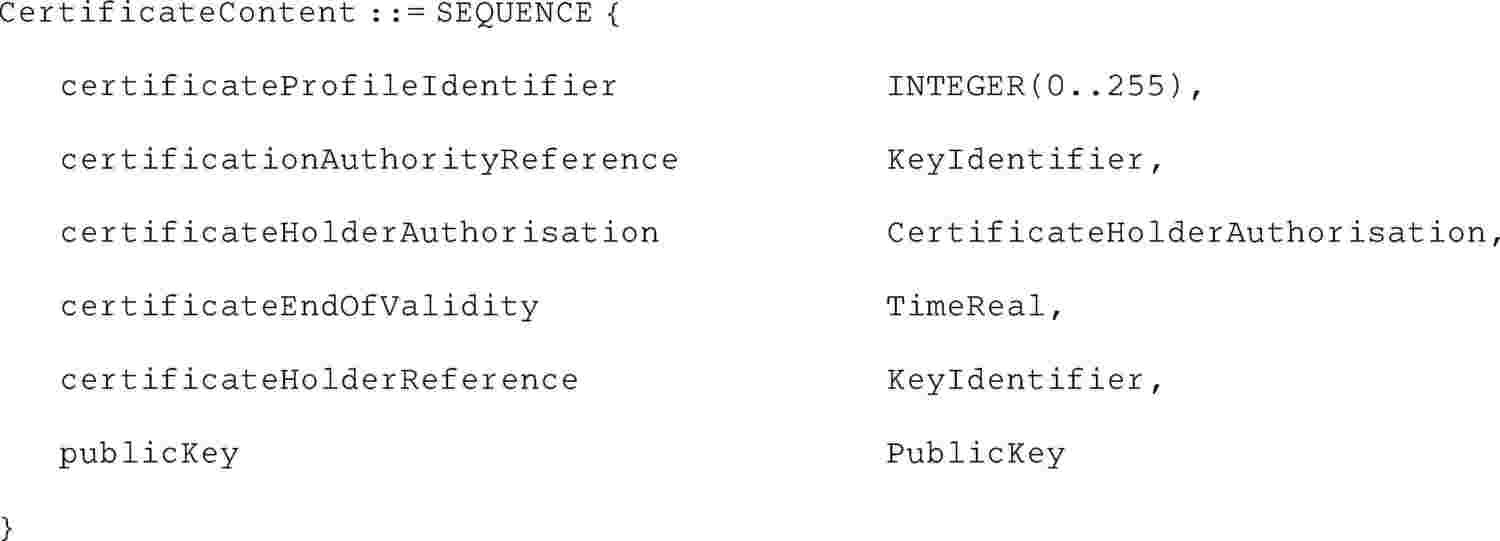
Certifikat javnog ključa, izdan od certifikacijske vlasti.

Image

**Dodjela vrijednosti:** digitalni potpis s djelomičnim obnavljanjem CertificateContent u skladu s Dodakom 11. ‚Zajednički sigurnosni mehanizmi’: Potpis (128 bajta) || Preostali dio javnog ključa (58 bajta) || Oznaka certifikacijske vlasti (8 bajta).

**2.33.   CertificateContent**

(Jasan) sadržaj certifikata javnog ključa u skladu s Dodakom 11. ‚Zajednički sigurnosni mehanizmi’.



**certificateProfileIdentifier** je inačica odgovarajućeg certifikata.

**Dodjela vrijednosti:**‚01h’ za takvu inačicu.

**certificationAuthorityReference** identifikuje certifikacijsku vlast koja je izdala certifikat. Takođe upućuje na javni ključ te certifikacijske vlasti.

**certificateHolderAuthorisation** identifikuje prava nosioca certifikata.

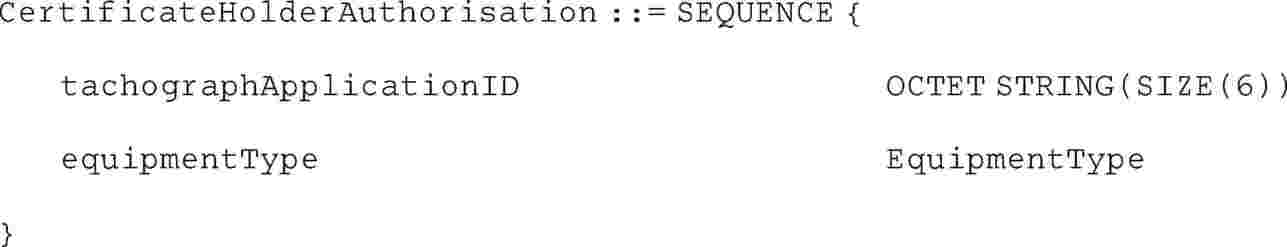
**certificateEndOfValidity** je datum administrativnog isteka važnosti certifikata.

**certificateHolderReference** identifikuje nosioca certifikata. Takođe upućuje na njegov javni ključ.

**publicKey** je javni ključ koji se potvrđuje tim certifikatom.

**2.34.   CertificateHolderAuthorisation**

Identifikacija prava nosioca certifikata.



**tachographApplicationID** je identifikator aplikacije za tahografsku aplikaciju.

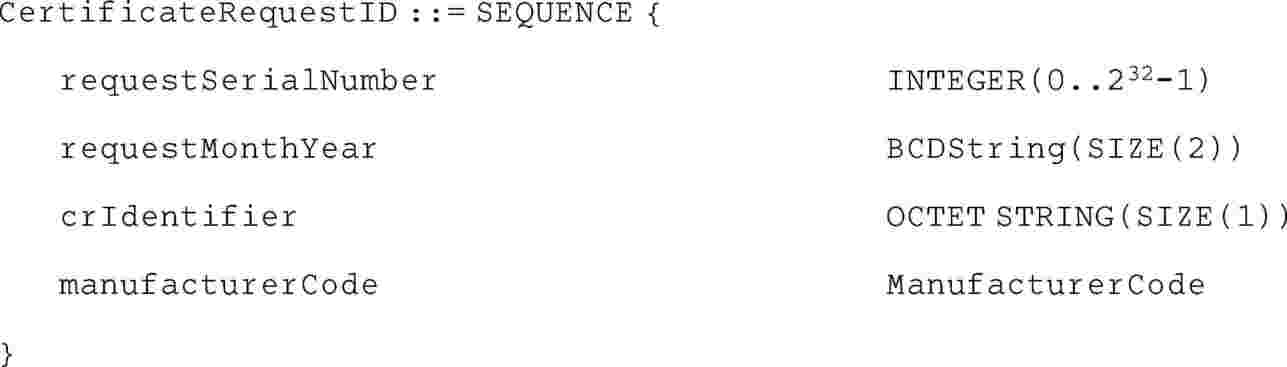
**Dodjela vrijednosti:**‚FFh’‚54h’‚41h’‚43h’‚48h’‚4Fh’. Taj AID je vlasnički neregistrirani identifikator aplikacije u skladu s ISO/IEC 7816-5.

**equipmentType** je identifikacija tipa uređaja za koji je certifikat namijenjen.

**dodjela vrijednosti:** u skladu s vrstom podatka EquipmentType. Vrijednost 0 ako je certifikat od jedne države članice.

**2.35.   CertificateRequestID**

Jedinstveni identifikator zahtjeva za certifikat. Može se takođe koristiti kao identifikator javnog ključa jedinice u vozilu ako u trenutku generisanja certifikata nije poznat serijski broj jedinice u vozilu za koju je ključ namijenjen.



**requestSerialNumber** je serijski broj zahtjeva za certifikat, jedinstven za proizvođača i niže navedeni mjesec.

**requestMonthYear** je identifikacija mjeseca i godine zahtjeva za certifikat.

**Dodjela vrijednosti:** šifra BCD za mjesec (dvije znamenke) i godinu (zadnje dvije znamenke).

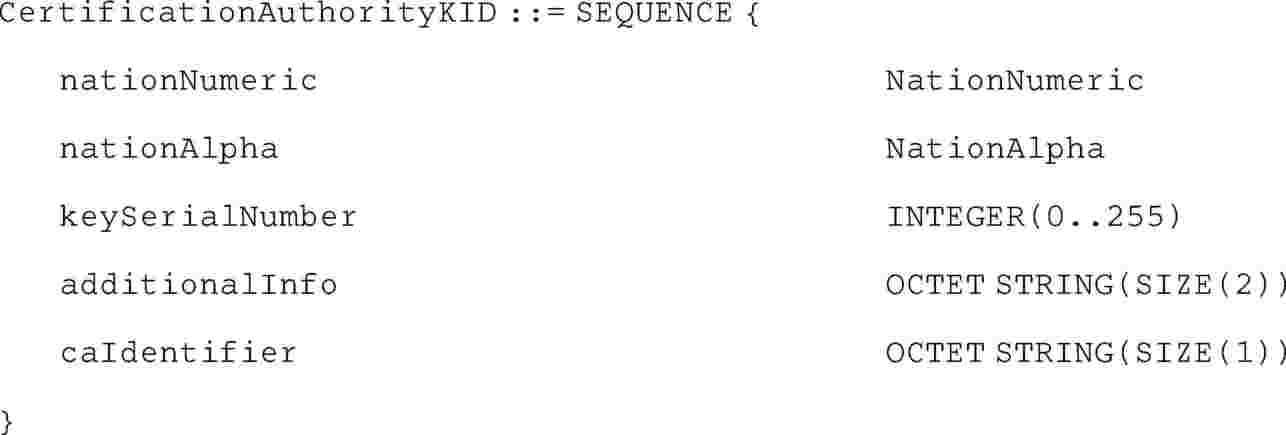
**crIdentifier:** je identifikator za raspoznavanje zahtjeva za certifikat od proširenog serijskog broja.

**Dodjela vrijednosti:**‚FFh’.

**manufacturerCode:** je brojčana šifra proizvođača koji traži certifikat.

**2.36.   CertificationAuthorityKID**

Identifikator javnog ključa certifikacijske vlasti (države članice ili evropske certifikacijske vlasti).



**nationNumeric** je brojčana nacionalna šifra certifikacijske vlasti.

**nationAlpha** je alfanumerička nacionalna šifra certifikacijske vlasti.

**keySerialNumber** je serijski broj za raspoznavanje različitih ključeva certifikacijske vlasti ako dođe do promjene ključeva.

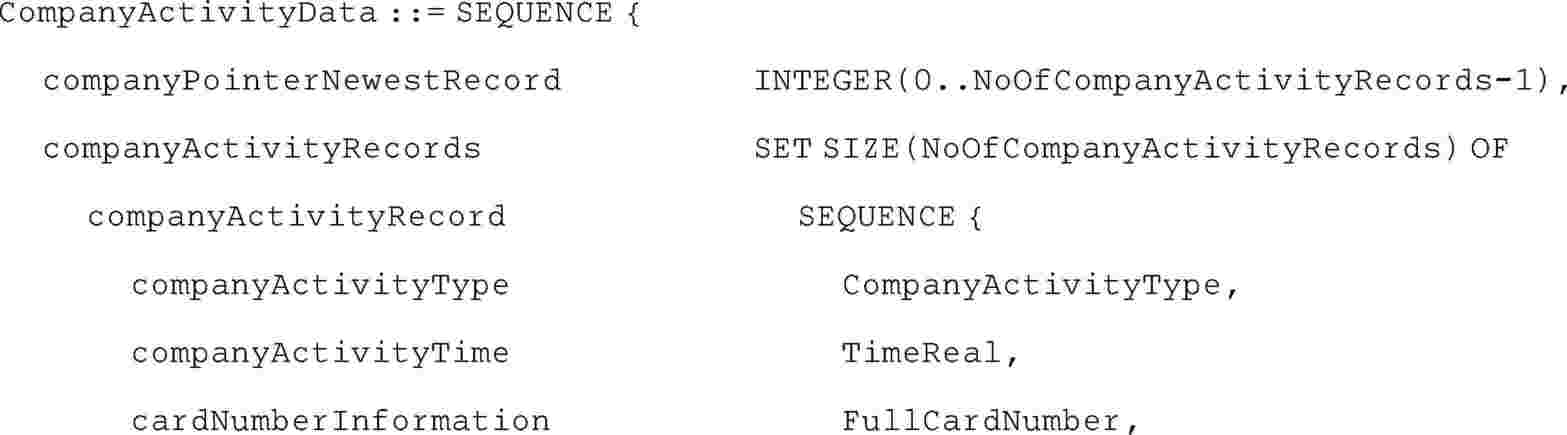
**additionalInfo** je dvobajtno polje za dodatno šifriranje (specifično za certifikacijsku vlast).

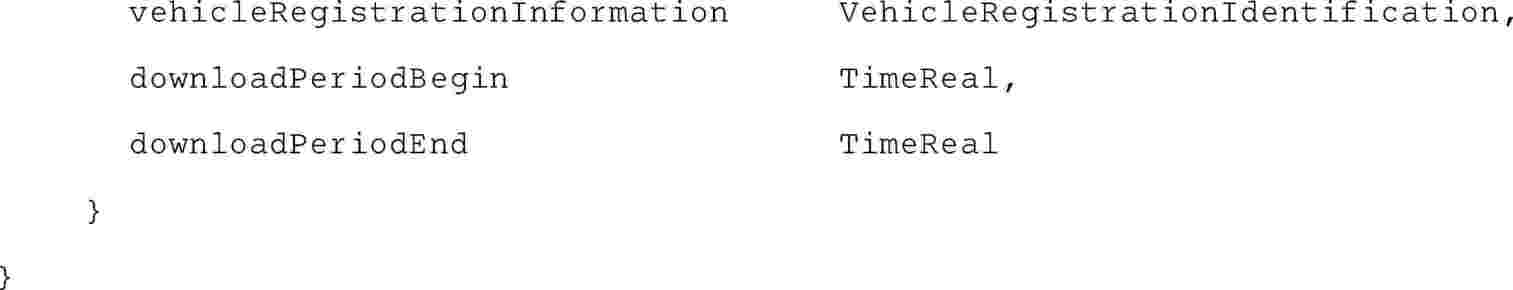
**caIdentifier** je identifikator za raspoznavanje identifikatora ključa certifikacijske vlasti od drugih identifikatora ključeva.

**Pripisivanje vrijednosti:**‚01h’.

**2.37.   CompanyActivityData**

Informacija sačuvana na kartici prevoznika koja se odnosi na aktivnosti izvršene s karticom (zahtjev 237).





**companyPointerNewestRecord** je indeks posljednjeg ažuriranja companyActivityRecord.

**Dodjela vrijednosti:** Broj koji odgovara brojaču zapisa o aktivnostima preduzeća, a koji započinje s ‚0’ za prvu pojavu zapisa o aktivnostima preduzeća u strukturi.

**companyActivityRecords** je niz svih zapisa o aktivnostima preduzeća.

**companyActivityRecord** je redoslijed informacija vezanih uz jednu aktivnost preduzeća.

**companyActivityType** je vrsta aktivnosti preduzeća.

**companyActivityTime** je datum i vrijeme aktivnosti preduzeća.

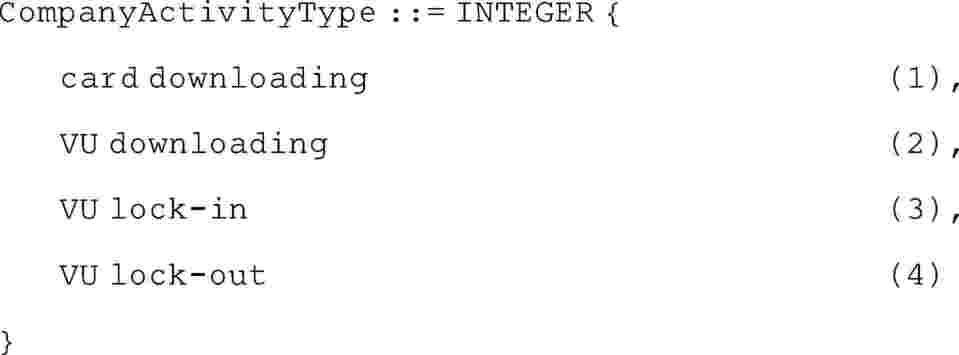
**cardNumberInformation** je broj kartice i država članica izdavanja kartice s koje se podaci preuzimaju, ako postoji.

**vehicleRegistrationInformation** je registracijska oznaka vozila i država članica registracije vozila u kojemu je izvršeno preuzimanje podataka odnosno zaključavanje ili otključavanje blokade.

**downloadPeriodBegin** i **downloadPeriodEnd** je period preuzimanja podataka iz jedinice vozila, ako postoji.

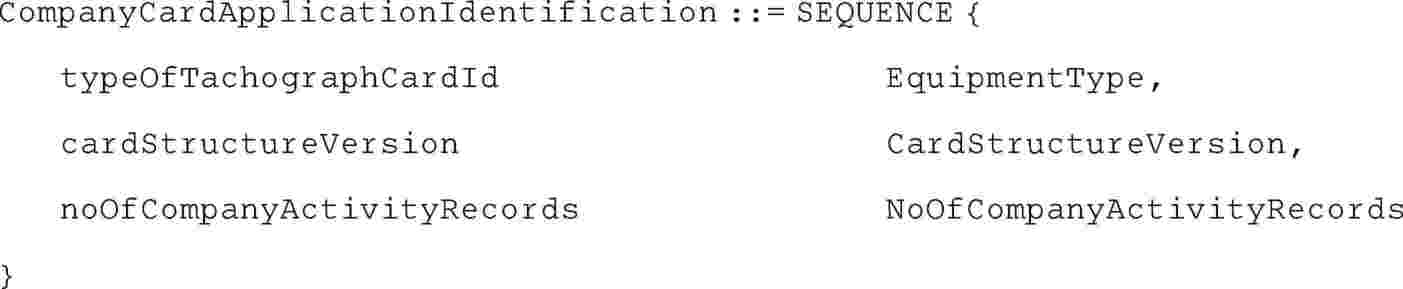
**2.38.   CompanyActivityType**

Šifra koja označava aktivnost koju obavlja preduzeće korištenjem svoje kartice prevoznika.



**2.39.   CompanyCardApplicationIdentification**

Informacija sačuvana na kartici prevoznika koja se odnosi na identifikaciju primjene kartice (zahtjev 190).



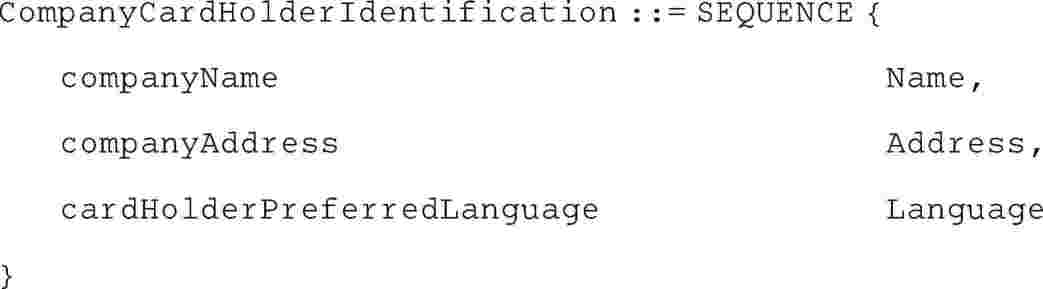
**typeOfTachographCardId** označava vrstu primijenjene kartice.

**cardStructureVersion** označava inačicu strukture primijenjene na kartici.

**noOfCompanyActivityRecords** je broj zapisa o aktivnostima preduzeća koje kartica može sačuvati.

**2.40.   CompanyCardHolderIdentification**

Informacija sačuvana na kartici prevoznika koja se odnosi na identifikaciju nosioca kartice (zahtjev 236).



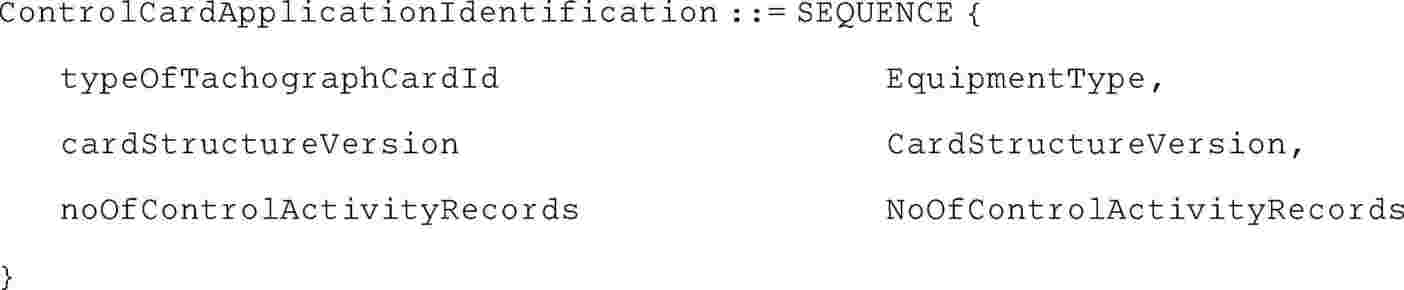
**companyName** je naziv preduzeća nosioca kartice.

**companyAddress** je adresa preduzeća nosioca.

**cardHolderPreferredLanguage** je odabrani jezik nosioca kartice.

**2.41.   ControlCardApplicationIdentification**

Informacija sačuvana na nadzornoj kartici koja se odnosi na identifikaciju primjene kartice (zahtjev 190).



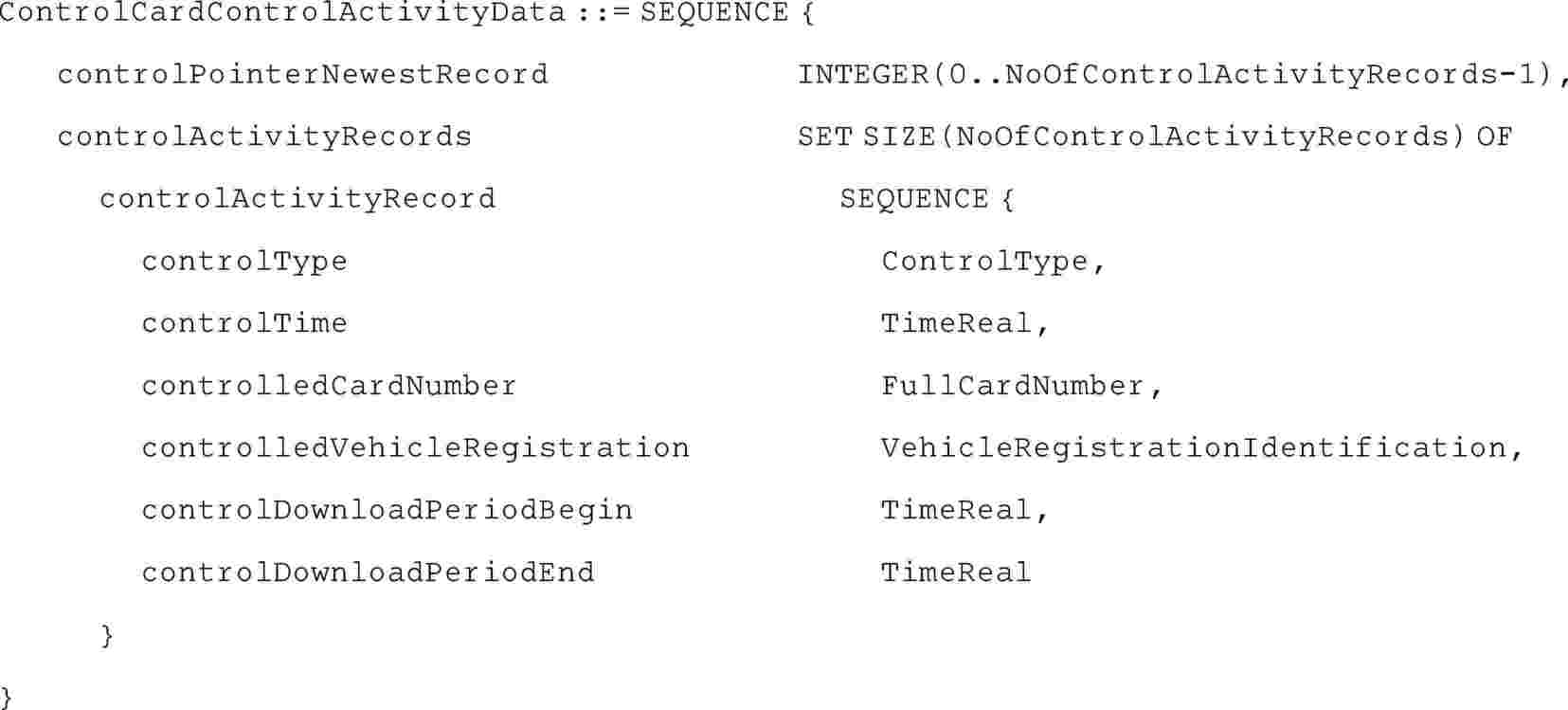
**typeOfTachographCardId** označava primijenjenu vrstu kartice.

**cardStructureVersion** označava inačicu strukture primijenjene na kartici.

**noOfControlActivityRecords** je broj zapisa o nadzornim aktivnostima koji se mogu sačuvati na kartici.

**2.42.   ControlCardControlActivityData**

Informacija sačuvana na nadzornoj kartici, koja se odnosi na aktivnosti nadzora izvršene s karticom (zahtjev 233).



**controlPointerNewestRecord** je indeks posljednjeg ažuriranog zapisa o aktivnostima nadzora.

**Dodjela vrijednosti:** broj koji odgovara brojaču zapisa o aktivnostima nadzora koji počinje s ‚0’ za prvu pojavu zapisa o aktivnosti nadzora u strukturi.

**controlActivityRecords** je niz svih zapisa o aktivnostima nadzora.

**controlActivityRecord** je redoslijed informacija vezanih uz jedan nadzor.

**controlType** je vrsta nadzora.

**controlTime** je datum i vrijeme nadzora.

**controlledCardNumber** je broj kartice i država članica izdavanja kartice koja je nadzorana.

**controlledVehicleRegistration** je VRN i država članica registracije vozila u kojemu je izvršen nadzor.

**controlDownloadPeriodBegin** i **controlDownloadPeriodEnd** je period za koje su moguće preuzeti podaci.

**2.43.   ControlCardHolderIdentification**

Informacija sačuvana na nadzornoj kartici koja se odnosi na identifikaciju nosioca kartice (zahtjev 232).



**controlBodyName** je naziv nadzornog tijela nosioca kartice.

**controlBodyAddress** je adresa nadzornog tijela nosioca kartice.

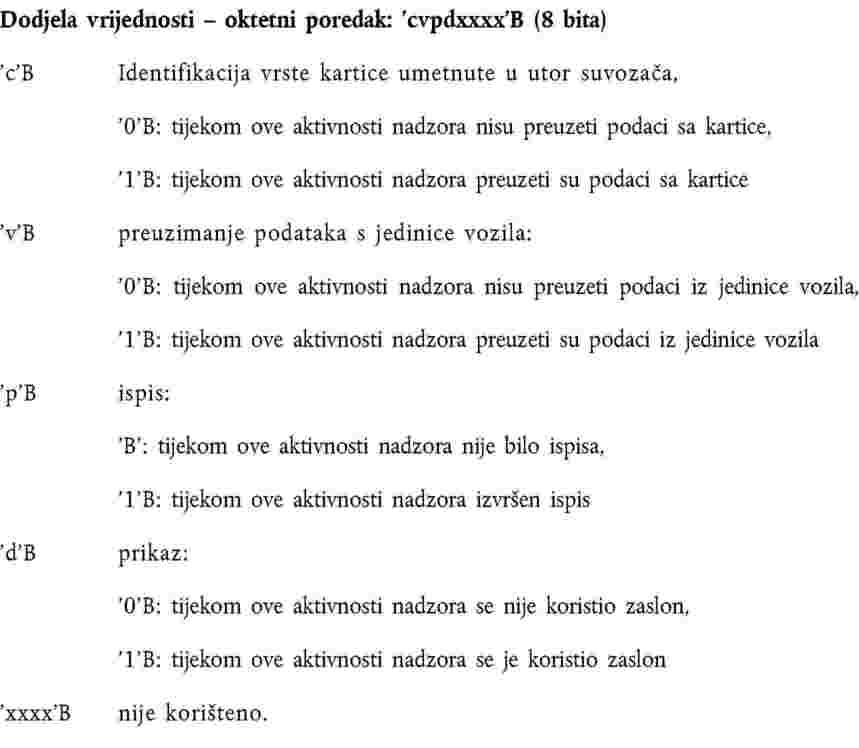
**cardHolderName** je prezime i ime(na) nosioca kontrolne kartice.

**cardHolderPreferredLanguage** je odabrani jezik nosioca kartice.

**2.44.   ControlType**

Šifra koja označava aktivnosti koje se vrše u sklopu nadzora. Ova vrsta podataka je vezana uz zahtjeve 102, 210 i 225.

Image



**2.45.   CurrentDateTime**

Tekući datum i vrijeme tahografa

Image

**Dodjela vrijednosti:** nije podrobnije određeno.

**2.46.   DailyPresenceCounter**

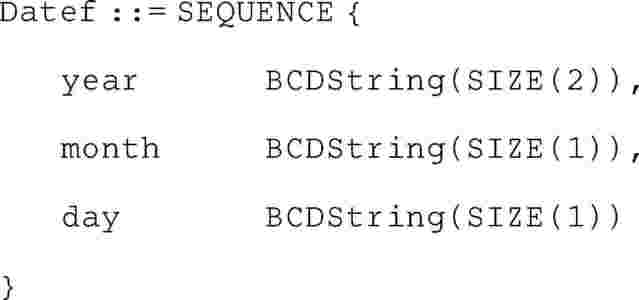
Brojač pohranjen na kartici vozača ili kartici radionice uvećan za 1 za svaki kalendarski dan kada je kartica bila umetnuta u jedinicu vozila. Ova vrsta podataka je vezana uz zahtjeve 199 i 219.

Image

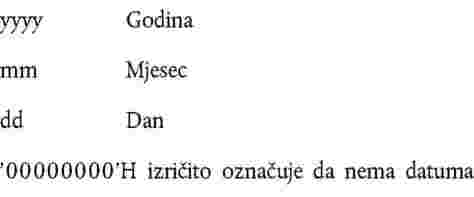
**Dodjela vrijednosti:** Redni broj s najvišom vrijednosti = 9 999; nakon čega ponovo počinje od 0. Pri prvom izdavanju kartice broj se postavlja na 0.

**2.47.   Datef**

Datum iskazan u brojčanom obliku spremnom za ispis.



**Dodjela vrijednosti**:



**2.48.   Distance**

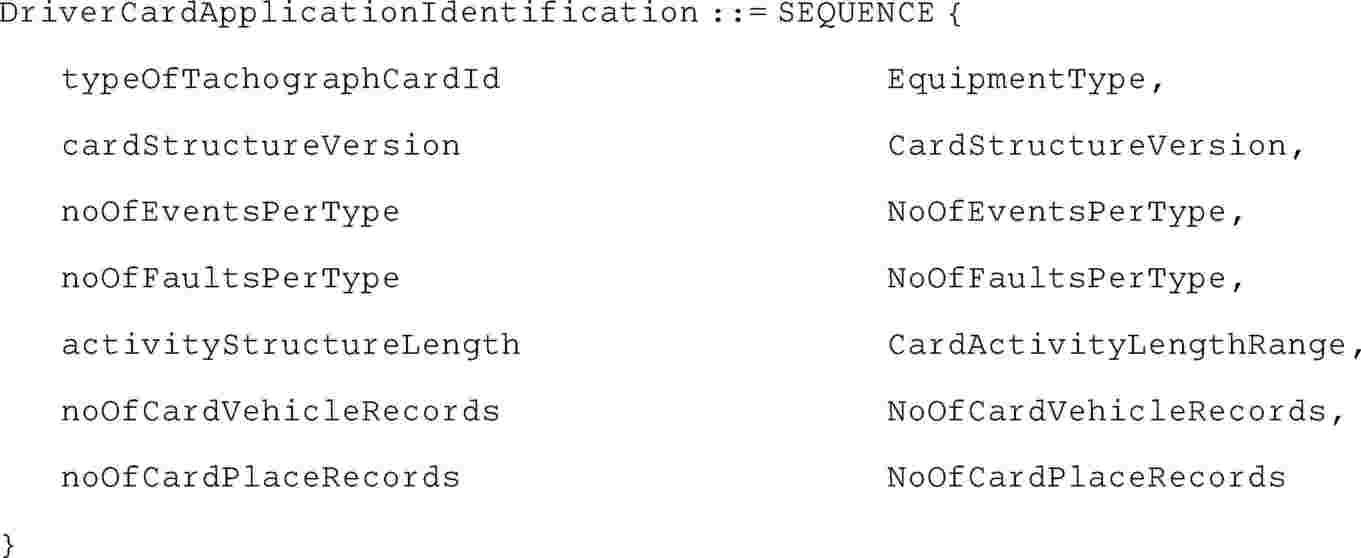
Pređena udaljenost (rezultat proračuna razlike između dvaju stanja brojača kilometara u kilometrima).

Image

**Dodjela vrijednosti:** nepotpisani binarni broj. Vrijednost u km u djelatnom rasponu od 0 do 9 999 km.

**2.49.   DriverCardApplicationldentification**

Informacija sačuvana na kartici vozača koja se odnosi na identifikaciju primjene kartice (zahtjev 190).



**typeOfTachographCardId** označava primijenjenu vrstu kartice.

**cardStructureVersion** označava inačicu primijenjene strukture na kartici.

**noOfEventsPerType** je broj događaja po vrsti događaja koji kartica može zaevidentirati.

**noOfFaultsPerType** je broj grešaka po vrsti greške koje kartica može zaevidentirati.

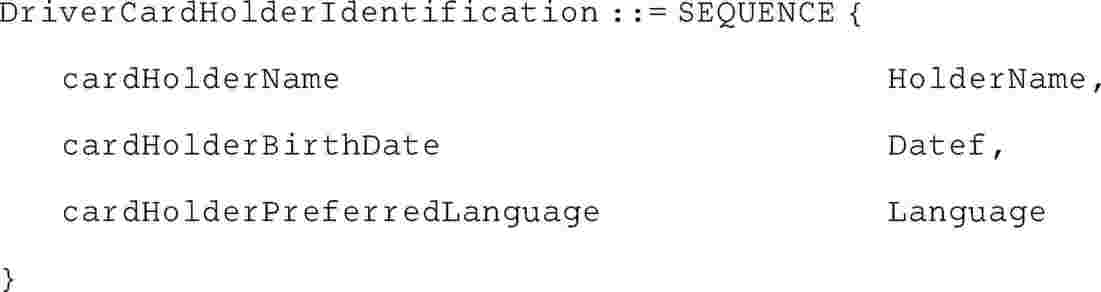
**activityStructureLength** označava broj rasposloživih bajtova za čuvanje zapisa o aktivnostima.

**noOfCardVehicleRecords** je broj zapisa o vozilu koje kartica može sadržavati.

**noOfCardPlaceRecords** je broj mjesta koje kartica može zaevidentirati.

**2.50.   DriverCardHolderIdentification**

Informacija sačuvana na kartici vozača koja se odnosi na identifikaciju nosioca kartice (zahtjev 195).



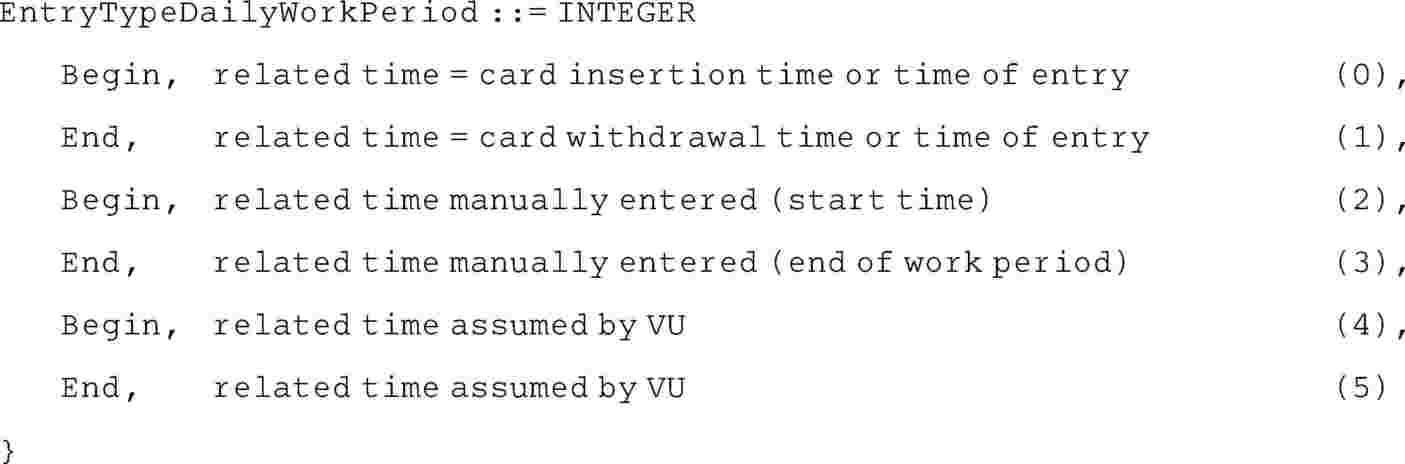
**cardHolderName** je prezime i ime(na) nosioca kartice vozača.

**cardHolderBirthDate** je datum rođenja nosioca kartice vozača.

**cardHolderPreferredLanguage** je izabrani jezik nosioca kartice.

**2.51.   EntryTypeDailyWorkPeriod**

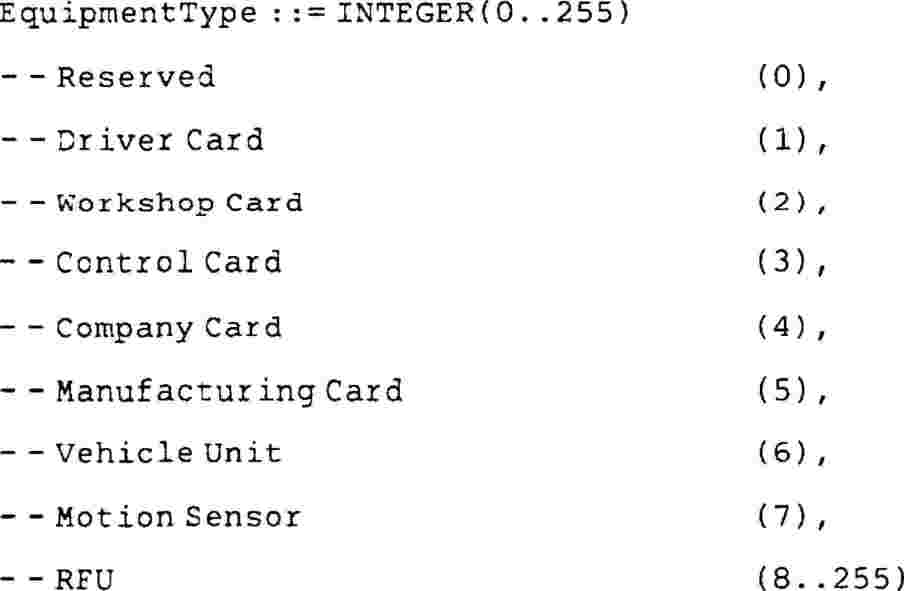
Oznaka za raspoznavanje između početka i kraja zapisa o dnevnom razdoblju rada i stanja unosa.



**Dodjela vrijednosti:** prema ISO/IEC8824-1.

**2.52.   EquipmentType**

Oznaka po kojoj se razlikuju vrste uređaja za tahografsku primjenu.



**Dodjela vrijednosti:** prema ISO/IEC8824-1.

Vrijednost 0 je rezervirana za označivanje države članice ili Europe u certifikacijskom polju CHA.

**2.53.   EuropeanPublicKey**

Evropski javni ključ.

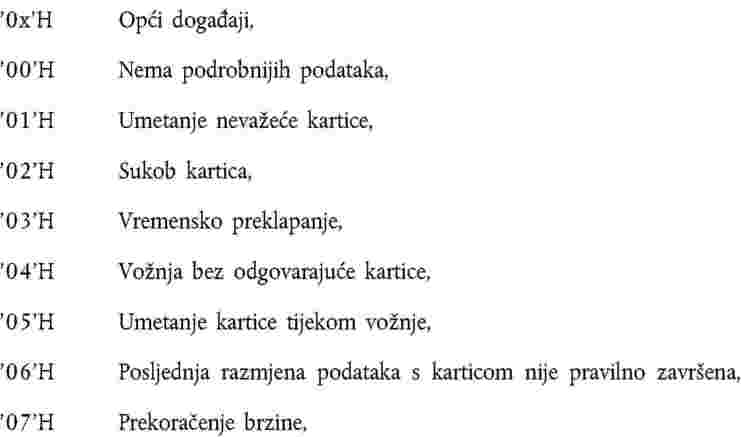
Image

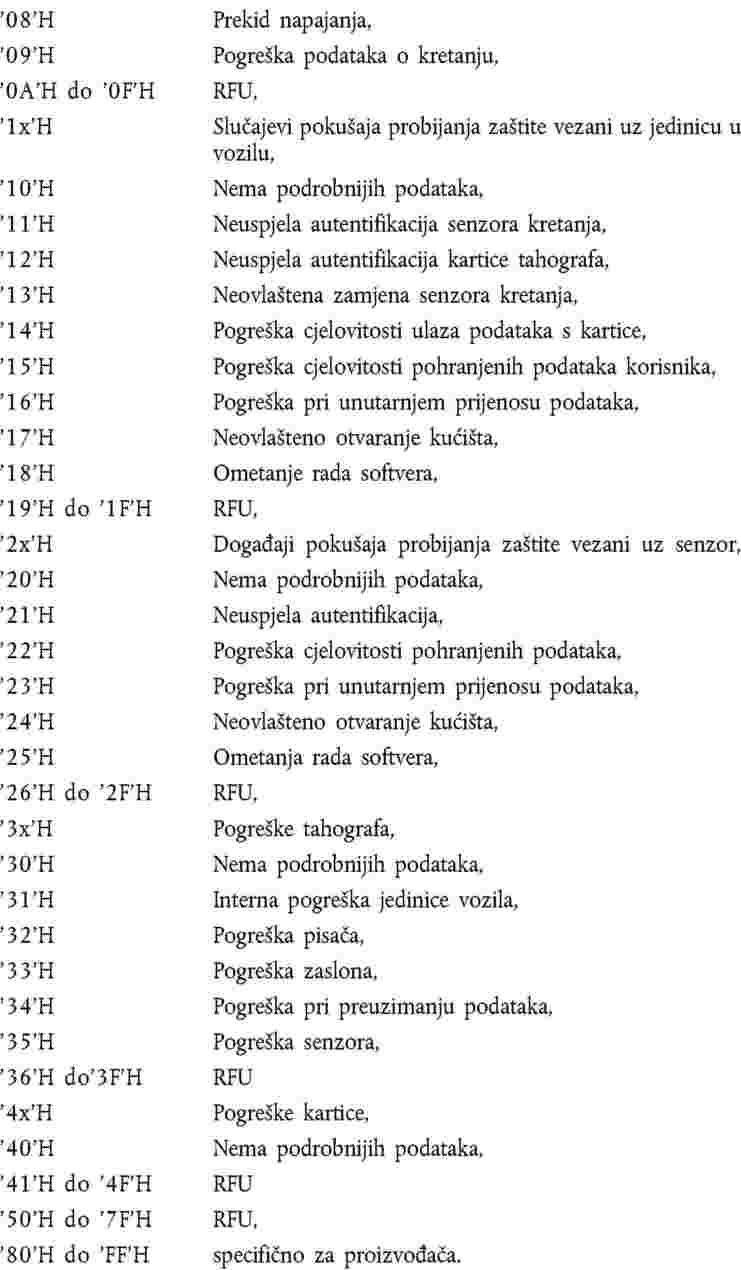
**2.54.   EventFaultType**

Šifra koja određuje događaj ili grešku.

Image

**Dodjela vrijednosti**:

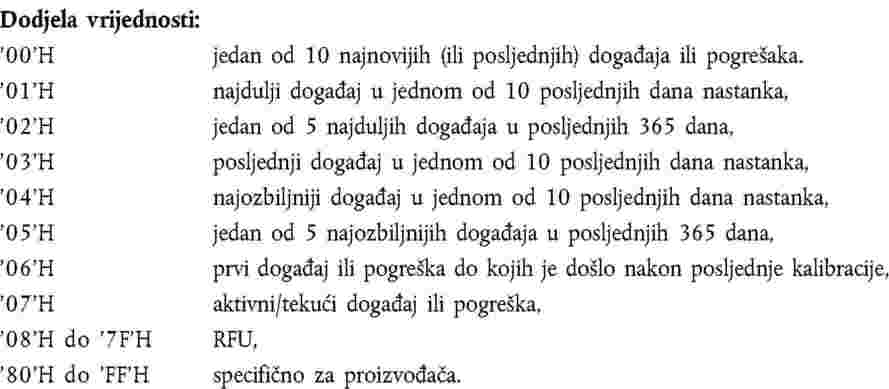




**2.55.   EventFaultRecordPurpose**

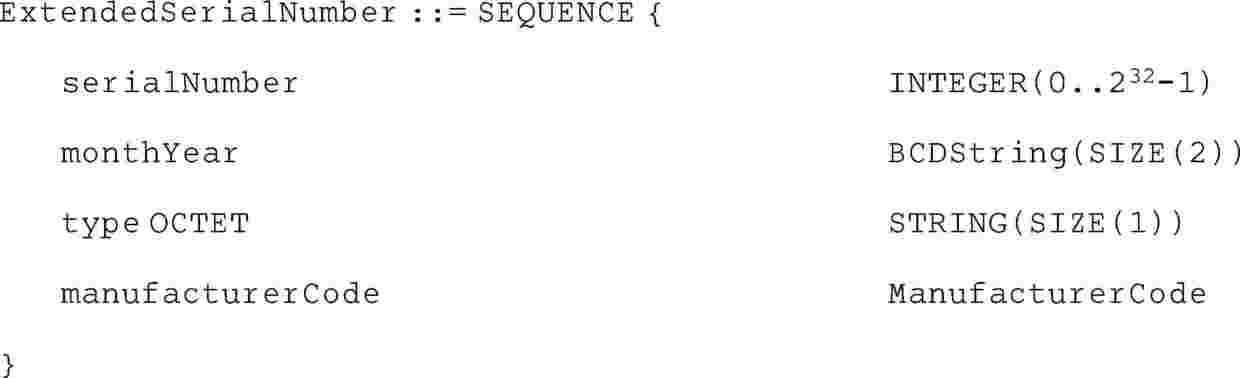
Šifra koja pojašnjava zašto su događaj ili greška zaevidentirajuni.

Image



**2.56.   ExtendedSerialNumber**

Jedinstvena identifikacija uređaja. Može se takođe koristiti i kao identifikator javnog ključa uređaja.



**serialNumber** je serijski broj uređaja, jedinstven za proizvođača, vrstu uređaja i mjesec proizvodnje.

**monthYear** je identifikacija mjeseca i godine proizvodnje (ili dodjele serijskog broja).

**Dodjela vrijednosti:** BCD šifra mjeseca (dvije znamenke) i godine (zadnje dvije znamenke).

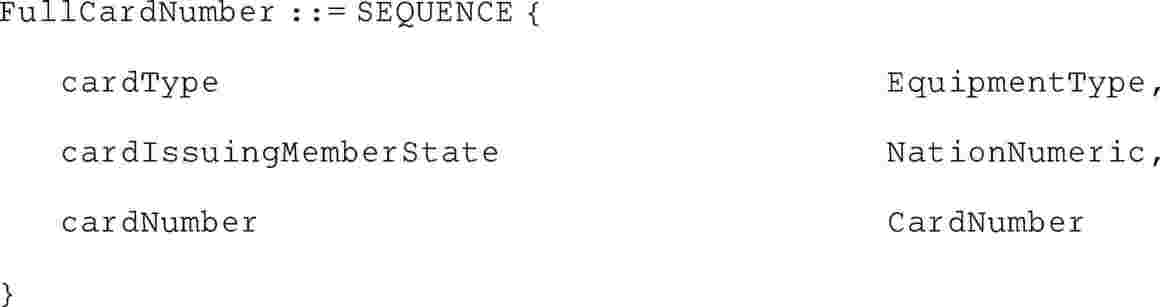
**type** je identifikator vrste uređaja.

**Dodjela vrijednosti:** odnosi se na proizvođača; vrijednost ‚FFh’ je rezervirana.

**manufacturerCode:** je brojčana šifra proizvođača uređaja.

**2.57.   FullCardNumber**

Šifra kojom se potpuno identifikuje kartica tahografa.



**cardType** je vrsta kartice tahografa.

**cardIssuingMemberState** je šifra države članice koja je izdala karticu.

**cardNumber** je broj kartice.

**2.58.   HighResOdometer**

Stanje brojača kilometara vozila: Ukupna udaljenost koju je vozilo prešlo tokom korištenja.

Image

**Dodjela vrijednosti:** nepotpisan binarni broj. Vrijednost u 1/200 km, u rasponu od 0 do 21 055 406 km.

**2.59.   HighResTripDistance**

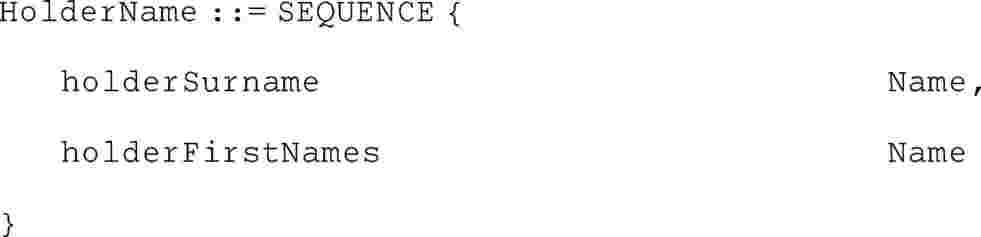
Udaljenost pređena tokom cjelokupne vožnje ili jednog njenog dijela.

Image

**Dodjela vrijednosti:** nepotpisan binarni broj. Vrijednost u 1/200 km, u rasponu od 0 do 21 055 406 km.

**2.60.   HolderName**

Prezime i ime(na) nosioca kartice.



**holderSurname** je prezime nosioca. Prezime ne uključuje titule.

**Dodjela vrijednosti:** Ako se ne radi o osobnoj kartici, holderSurname sadrži istu informaciju kao i companyName ili workshopName ili controlBodyName.

**holderFirstNames** su ime(na) i inicijali nosioca.

**2.61.   K-ConstantOfRecordingEquipment**

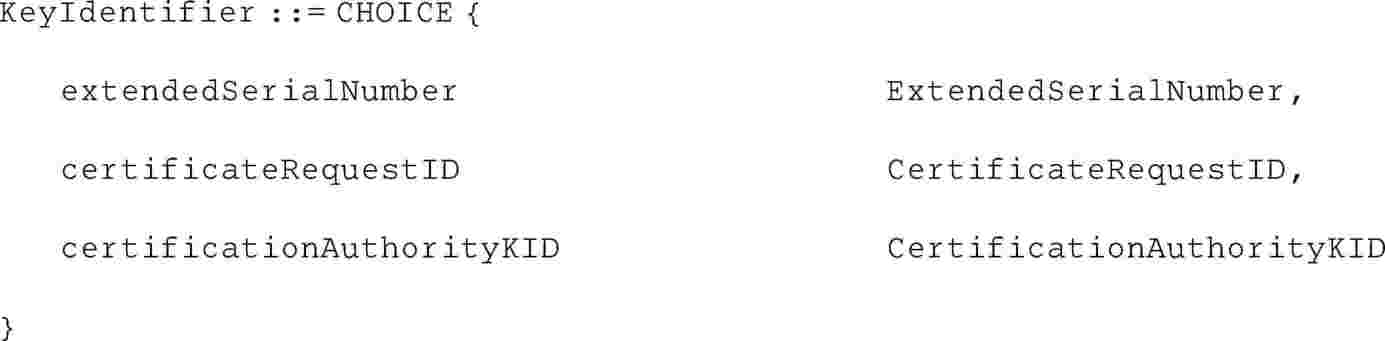
Konstanta tahografa (definicija m)).

Image

**Dodjela vrijednosti:** Broj impulsa po kilometru, u djelatnom rasponu od 0 do 64 255 impulsa/km.

**2.62.   KeyIdentifier**

Jedinstveni identifikator javnog ključa koji se koristi pri navođenju i izboru ključa. Takođe identifikuje i nosioca ključa.



Prvi odabir je prikladan za navođenje javnog ključa jedinice u vozilu ili kartice tahografa.

Drugi oblik je prikladan za navođenje javnog ključa jedinice u vozilu (u slučaju da u trenutku generisanja potvrde nije poznat serijski broj jedinice u vozilu).

Treći odabir je prikladan za navođenje javnog ključa države članice.

**2.63.   L-TyreCircumference**

Aktivni opseg guma točkova (definicija u)).

Image

**Dodjela vrijednosti:** nepotpisan binarni broj, vrijednost u 1/8 mm u djelatnom rasponu od 0 do 8 031 mm.

**2.64.   Language**

Šifra koja označava jezik.

Image

**Dodjela vrijednosti:** šifriranje s dva mala slova u skladu s ISO 639.

**2.65.   LastCardDownload**

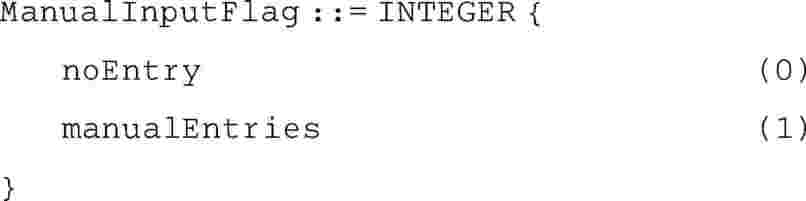
Datum i vrijeme arhivirani na vozačkoj kartici, o posljednjem preuzimanju podataka s kartice (za svrhe drugačije od nadzora). Taj datum može ažurirati jedinica vozila ili neki drugi čitač kartica.

Image

**Dodjela vrijednosti:** nije podrobnije određeno.

**2.66.   ManualInputFlag**

Šifra koja označava je li vlasnik kartice pri njenom ubacivanju ručno unio aktivnosti vozača ili nije (zahtjev 081).



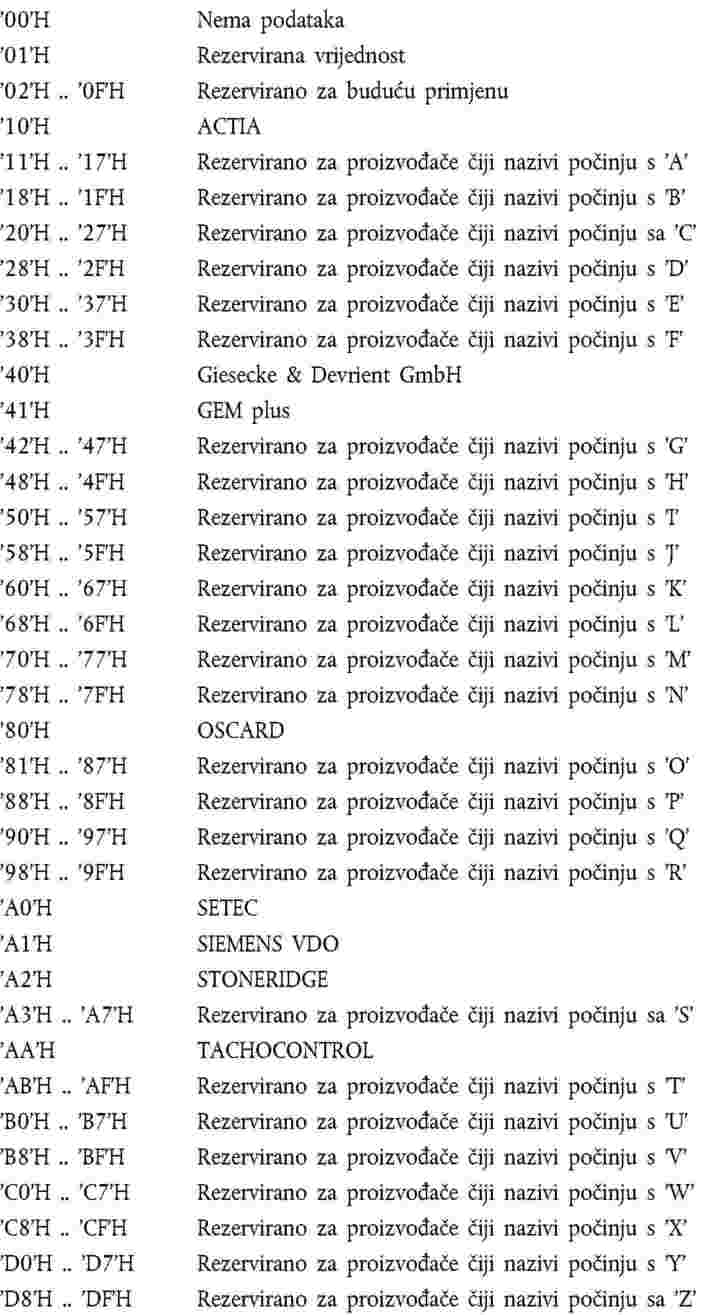
**Dodjela vrijednosti:** nije podrobnije određeno.

**2.67.   ManufacturerCode**

Šifra koja označava proizvođača.

Image

**Dodjela vrijednosti:**



Bilješka: Ažurirana lista šifri za identifikaciju proizvođača bit će dostupna na mrežnoj stranici Evropskog certifikacionog tijela.

**2.68.   MemberStateCertificate**

Certifikat javnog ključa države članice koji izdaje Europsko certifikacijsko tijelo.

Image

**2.69.   MemberStatePublicKey**

Javni ključ države članice.

Image

**2.70.   Name**

Naziv.

Name: = SEQUENCE {

codePage INTEGER (0..255),

name OCTET STRING (SIZE(35))

}

codePage utvrđuje niz znakova, definisanih u poglavlju 4.,

name je naziv, šifriran određenim nizom znakova”.

**2.71.   NationAlpha**

Abecedna oznaka države u skladu s dogovorenim šifriranjem država na naljepnicama branika vozila i/ili kako se koristi u međunarodno usklađenim ispravama o osiguranju vozila (zelena karta).

Image





**2.72.   NationNumeric**

Brojčana oznaka države.

Image





**2.73.   NoOfCalibrationRecords**

Broj zapisa o umjeravanju koje može sačuvati kartica radionice.

Image

**Dodjela vrijednosti:** vidjeti stavak 3.

**2.74.   NoOfCalibrationsSinceDownload**

Brojač koji pokazuje broj kalibracija izvršenih s karticom radionice od posljednjeg preuzimanja podataka (zahtjev 230).

Image

**dodjela vrijednosti:** nije podrobnije određeno.

**2.75.   NoOfCardPlaceRecords**

Broj zapisa o mjestima koji može sačuvati kartica vozača ili kartica radionice.

Image

**Dodjela vrijednosti:** vidjeti stavak 3.

**2.76.   NoOfCardVehicleRecords**

Broj zapisa o korišćenim vozilima koje može sačuvati kartica vozača ili kartica radionice.

Image

**Dodjela vrijednosti:** vidjeti stavak 3.

**2.77.   NoOfCompanyActivityRecords**

Broj zapisa o aktivnostima preduzeća koji može sačuvati kartica prevoznika.

Image

**Pripisivanje vrijednosti:** vidjeti stavak 3.

**2.78.   NoOfControlActivityRecords**

Broj zapisa o aktivnostima nadzora koje kontrolna kartica može sačuvati.

Image

**Dodjela vrijednosti:** vidjeti stavak 3.

**2.79.   NoOfEventsPerType**

Broj događanja po vrstama događaja koji kartica može sačuvati.

Image

**Dodjela vrijednosti:** vidjeti stavak 3.

**2.80.   NoOfFaultsPerType**

Broj događanja po vrsti događaja koje kartica može sačuvati.

Image

**Dodjela vrijednosti:** vidjeti stavak 3.

**2.81.   OdometerValueMidnight**

Stanje brojača kilometara u ponoć određenog dana (zahtjev 090).

Image

**Dodjela vrijednosti:** nije podrobnije određeno.

**2.82.   OdometerShort**

Stanje brojača kilometara u krakom obliku.

Image

**Dodjela vrijednosti:** neoznačen binarni broj. Vrijednost u km u djelatnom rasponu od 0 do 9 999 999 km.

**2.83.   OverspeedNumber**

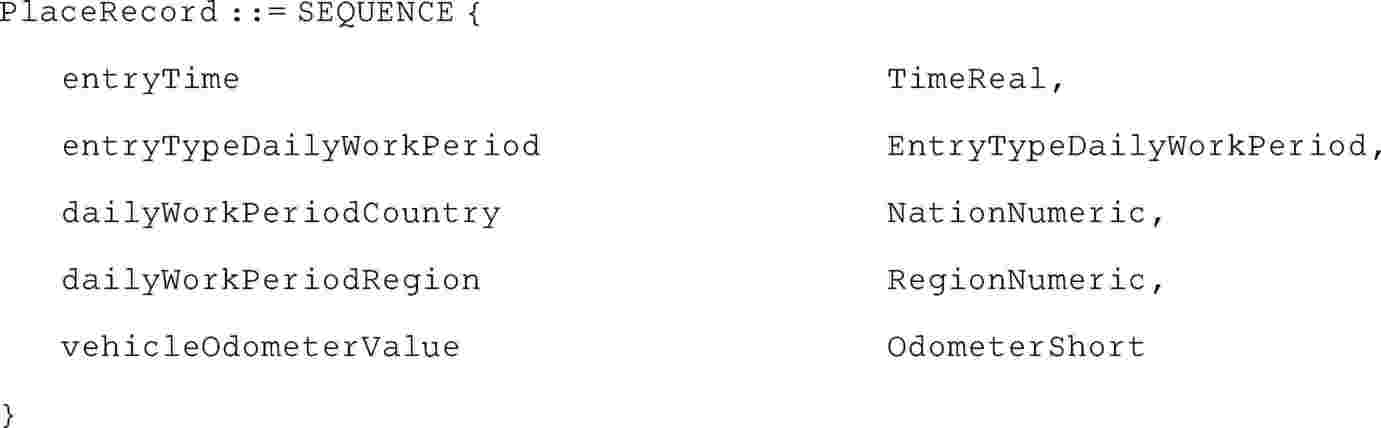
Broj događaja prekoračenja brzine od posljednje kontrole prekoračenja brzine.

Image

**Dodjela vrijednosti:** 0 označava da od posljednje kontrole prekoračenja brzine nije bilo prekoračenja brzine; 1 označava da se od posljednje kontrole prekoračenja brzine dogodio jedan događaj prekoračenja brzine, … 255 označava da se od posljednje kontrole prekoračenja brzine desilo 255 ili više događaja prekoračenja brzine.

**2.84.   PlaceRecord**

Informacija koja se odnosi na mjesto početka ili završetka dnevnog perioda rada (zahtjevi 087, 202, 221).



**entryTime** je datum i vrijeme unosa.

**entryTypeDailyWorkPeriod** je vrsta unosa.

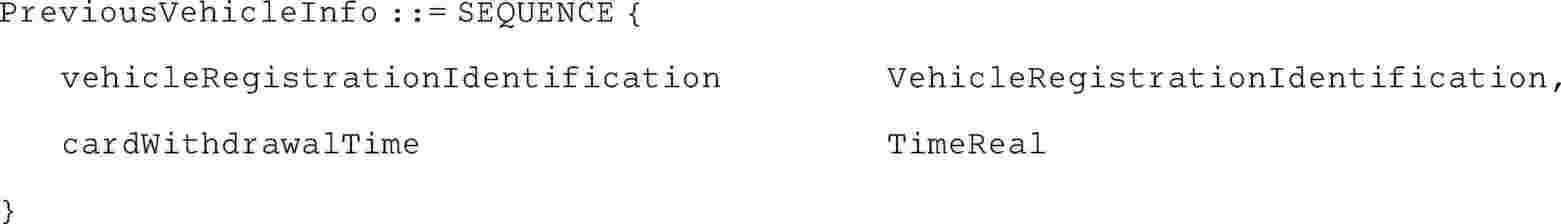
**dailyWorkPeriodCountry** je unesena država.

**dailyWorkPeriodRegion** je unesena regija.

**vehicleOdometerValue** je stanje brojača kilometara u trenutku unosa mjesta.

**2.85.   PreviousVehiclelnfo**

Informacija koja se odnosi na vozilo koje je vozač prethodno koristio pri ubacivanju kartice u jedinicu vozila (zahtjev 081).



**vehicleRegistrationIdentification** je registracijska oznaka vozila i država registracije vozila.

**cardWithdrawalTime** je datum i vrijeme vađenja kartice.

**2.86.   PublicKey**

Javni ključ RSA.



**rsaKeyModulus** je modul para ključeva.

**rsaKeyPublicExponent** je javni eksponent para ključeva.

**2.87.   RegionAlpha**

Slovna oznaka regije u određenoj državi.

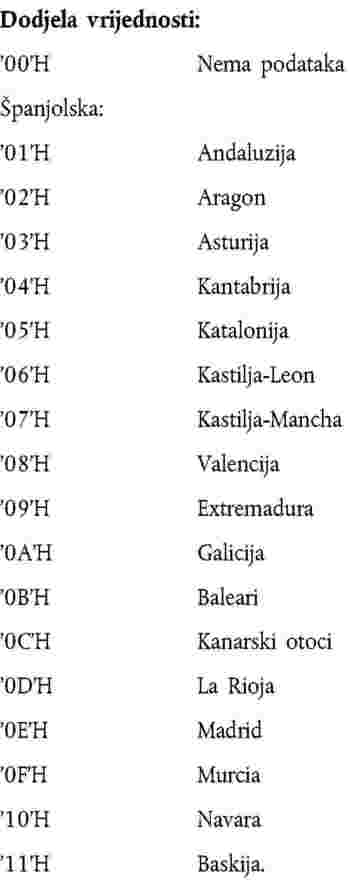
Image



**2.88.   RegionNumeric**

Brojčana oznaka regije u određenoj državi.

Image



**2.89.   RSAKeyModulus**

Modul para ključeva RSA.

Image

**Dodjela vrijednosti:** Nije određeno.

**2.90.   RSAKeyPrivateExponent**

Javni eksponent para ključeva RSA.

Image

**Dodjela vrijednosti:** Nije određeno.

**2.91.   RSAKeyPublicExponent**

Javni eksponent para ključeva RSA.

Image

**Dodjela vrijednosti:** Nije određeno.

**2.92.   SensorApprovalNumber**

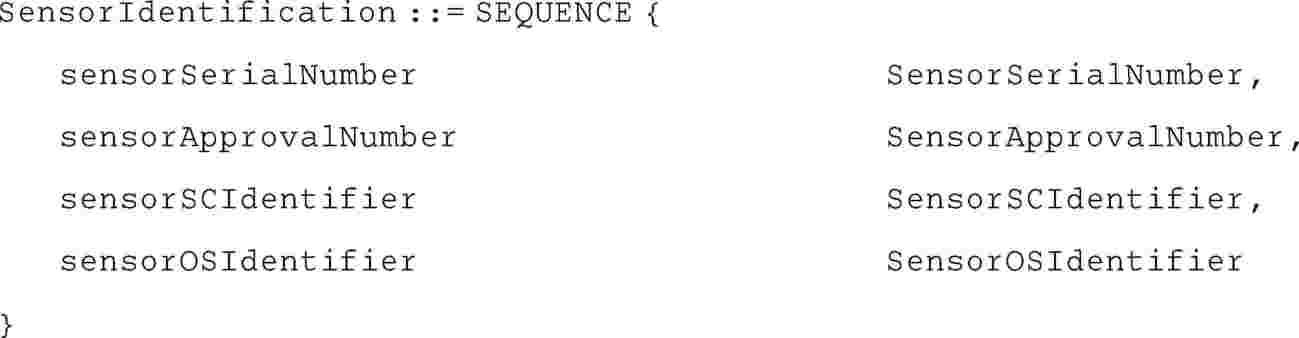
Broj tipskog odobrenja senzora.

Image

**Dodjela vrijednosti:** Nije određeno.

**2.93.   SensorIdentification**

Informacija sačuvana u senzoru kretanja koja se odnosi na identifikaciju senzora kretanja (zahtjev 077).



**sensorSerialNumber** je prošireni serijski broj senzora kretanja (uključujući kataloški broj i šifru proizvođača).

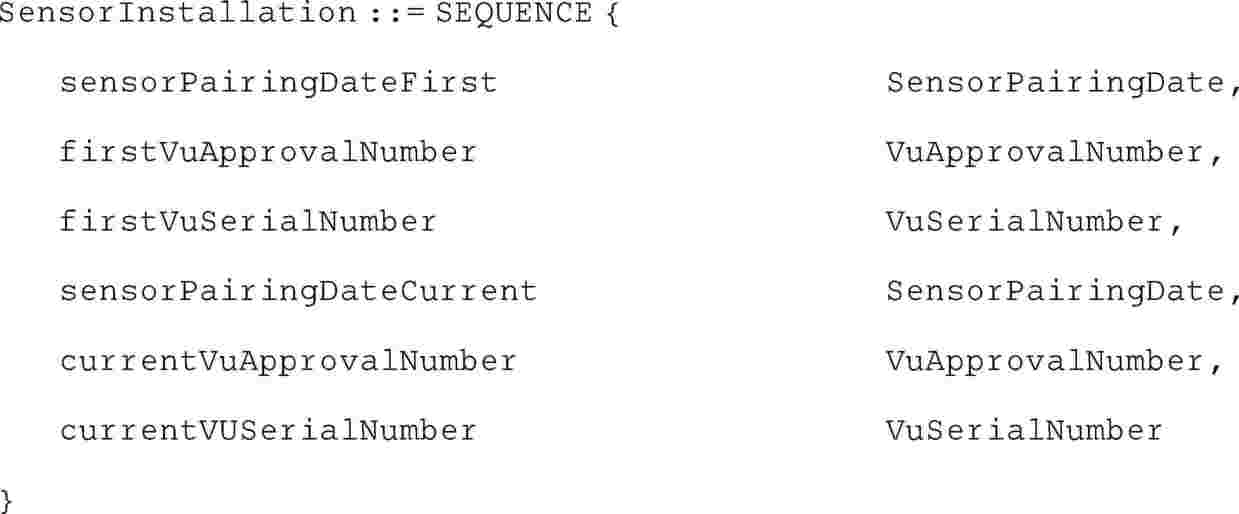
**sensorApprovalNumber** je broj tipskog odobrenja senzora kretanja.

**sensorSCIdentifier** je identifikator sigurnosnog sastavnog dijela senzora kretanja.

**sensorOSIdentifier** je identifikator operativnog sistema senzora kretanja.

**2.94.   SensorInstallation**

Informacija spremljena u senzoru kretanja koja se odnosi na ugradnju senzora kretanja (zahtjev 099).



**sensorPairingDateFirst** je datum prvog uparivanja senzora kretanja s jedinicom u vozilu.

**firstVuApprovalNumber** je broj tipskog odobrenja 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 broj tipskog odobrenja jedinice u vozilu s kojom je senzor kretanja trenutno uparen.

**currentVUSerialNumber** je serijski broj jedinice u vozilu s kojom je trenutno uparen senzor kretanja.

**2.95.   SensorInstallationSecData**

Informacija sačuvana na kartici radionice koja se odnosi na sigurnosne podatke potrebne za uparivanje senzora kretanja s jedinicama u vozilu (zahtjev 214).

Image

**Dodjela vrijednosti:** u skladu s ISO 16844-3.

**2.96.   SensorOSIdentifier**

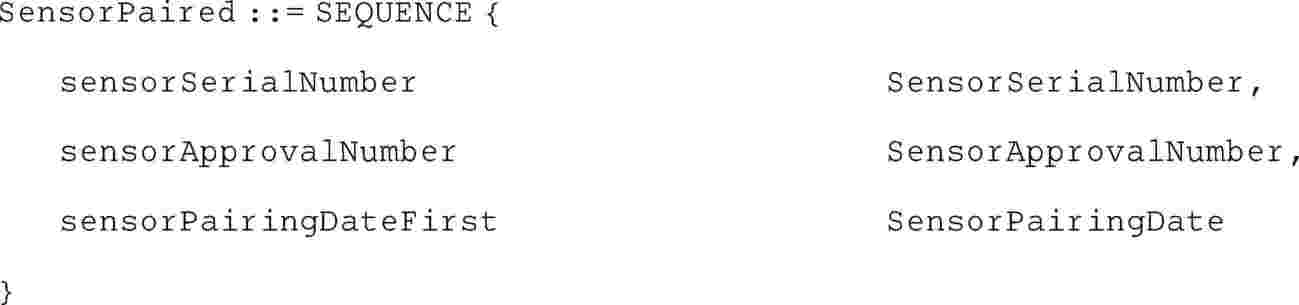
Identifikator operativnog sistema senzora kretanja.

Image

**Dodjela vrijednosti:** utvrđuje proizvođač.

**2.97.   SensorPaired**

Informacija spremljena u jedinici u vozilu koja se odnosi na identifikaciju senzora kretanja uparenog s jedinicom u vozilu (zahtjev 079).



**sensorSerialNumber** je serijski broj senzora kretanja trenutno uparenog s jedinicom u vozilu.

**sensorApprovalNumber** je broj tipskog odobrenja senzora kretanja koji je trenutno uparen s jedinicom u vozilu.

**sensorPairingDateFirst** je datum prvog uparivanja jedinice u vozilu sa senzorom kretanja koje je trenutno upareno s jedinicom u vozilu.

**2.98.   SensorPairingDate**

Datum uparivanja senzora kretanja s jedinicom u vozilu.

Image

**Dodjela vrijednosti:** Nije određeno.

**2.99.   SensorSerialNumber**

Serijski broj senzora kretanja.

Image

**2.100.   SensorSCIdentifier**

Identifikator sigurnosnog sastavnog dijela senzora kretanja.

Image

**Dodjela vrijednosti:** utvrđuje proizvođač dijela.

**2.101.   Signature**

Digitalni potpis.

Image

**Dodjela vrijednosti:** u skladu s Dodakom 11. ‚Zajednički sigurnosni mehanizmi’.

**2.102.   SimilarEventsNumber**

Broj sličnih događaja u određenom danu. (zahtjev 094).

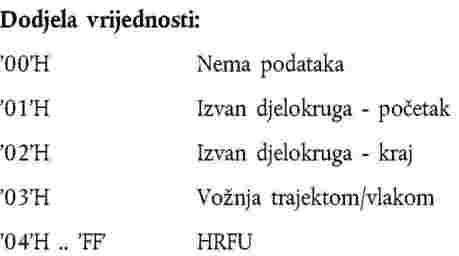
Image

**Dodjela vrijednosti:** 0 se ne koristi, 1 označava da se tog dana dogodio samo jedan događaj, 2 označava da su se dogodila 2 događaja te vrste (spremljen je samo jedan), … 255 označava da se tog dana dogodilo 255 ili više slučajeva takve vrste.

**2.103.   SpecificConditionType**

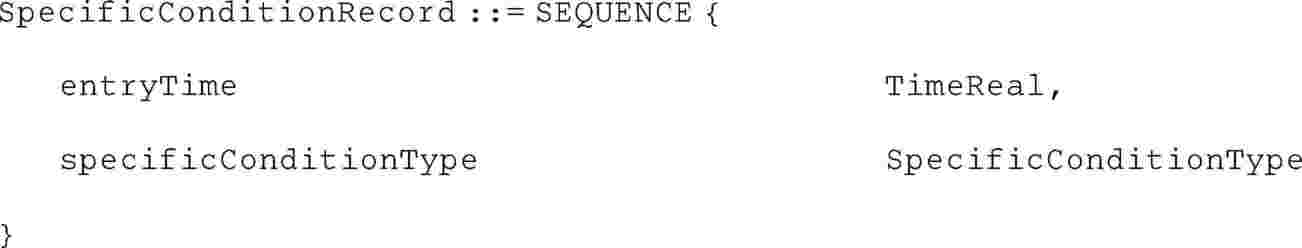
Šifra koja označava posebna stanja (zahtjevi 050b, 105a, 212a i 230a).

Image



**2.104.   SpecificConditionRecord**

Informacija sačuvana na kartici vozača, kartici radionice ili u jedinici u vozilu koja se odnosi na posebne uslove (zahtjevi 105a, 212a in 230a).



**entryTime** je datum i vrijeme unosa.

**specificConditionType** je šifra koja označava posebno stanje.

**2.105.   Speed**

Brzina vozila (km/h).

Image

**Dodjela vrijednosti:** kilometar na sat u djelatnom rasponu od 0 do 220 km/h.

**2.106.   SpeedAuthorised**

Najveća dopuštena brzina vozila (definicija bb).

Image

**2.107.   SpeedAverage**

Prosječna brzina u prethodno određenom trajanju (km/h).

Image

**2.108.   SpeedMax**

Najveća brzina izmjerena u prethodno određenom trajanju.

Image

**2.109.   TDesSessionKey**

Trojni ključ DES razmjene podataka.



**Dodjela vrijednosti:** nije podrobnije određeno.

**2.110.   TimeReal**

Šifra kombiniranog područja datuma i vremena u kojoj su datum i vrijeme izraženi kao broj sekundi nakon 00h00m00s na dan 1. siječnja 1970. GMT.

Image

**Dodjela vrijednosti – oktetni poredak:** Broj sekundi od ponoći 1. siječnja 1970. po GMT.

Najkasniji mogući datum i vrijeme su u 2106. godini

**2.111.   TyreSize**

Oznaka dimenzija guma.

Image

**Dodjela vrijednosti:** u skladu s Direktivom 92/23 (EEZ) od [31.3.1992., SL L 129, str. 95](https://eur-lex.europa.eu/legal-content/HR/AUTO/?uri=OJ:L:1992:129:TOC).

**2.112.   VehicleldentificationNumber**

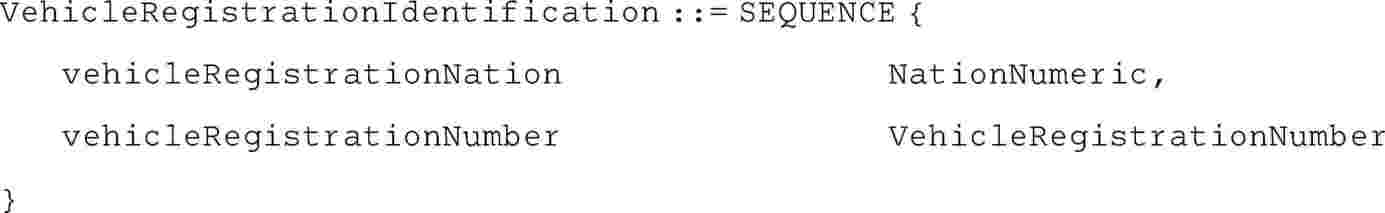
Identifikacijski broj vozila (VIN) koji se odnosi na vozilo kao cjelinu; obično serijski broj šasije ili broj okvira.

Image

**Dodjela vrijednosti:** kako je utvrđeno u ISO 3779.

**2.113.   VehicleRegistrationIdentification**

Identifikacija vozila jedinstvena za cijelu Europu (registracijska oznaka vozila i država članica registracije).



**vehicleRegistrationNation** je država u kojoj je vozilo registrovano.

**vehicleRegistrationNumber** je registracijska oznaka vozila (VRN).

**2.114.   VehicleRegistrationNumber**

Registracijski broj vozila (VRN). Registracijski broj dodjeljuje tijelo nadležno za registraciju.

VehicleRegistrationNumber: = SEQUENCE {

codePage INTEGER (0..255),

vehicleRegNumber OCTET STRING (SIZE(13))

}

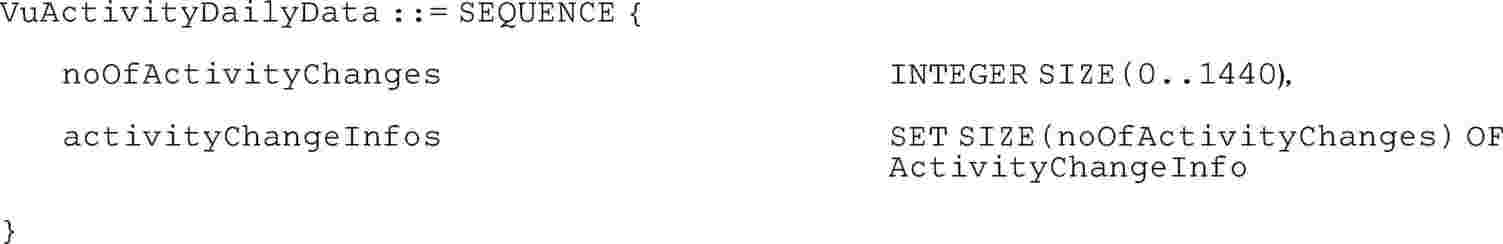
codePage utvrđuje niz znakova, definisanih u poglavlju 4.,

vehicleRegNumber je VRN šifriran određenim nizom znakova.

Dodjela vrijednosti: utvrđuje pojedina država”.

**2.115.   VuActivityDailyData**

Informacija sačuvana u jedinici vozila koja se odnosi na promjene aktivnosti i/ili promjene statusa vožnje i/ili promjene statusa kartice za određeni kalendarski dan (zahtjev 084) i na status otvora u 00:00 sati tog dana.



**noOfActivityChanges** je broj riječi ActivityChangelnfo u nizu activityChangeInfos.

**activityChangeInfos** je niz riječi ActivityChangeInfo pohranjen u jedinici vozila za određeni dan. Uvijek uključuje dvije riječi ActivityChangeInfo koje određuju status otvora u 00:00 tog dana.

**2.116.   VuApprovalNumber**

Broj tipskog odobrenja jedinice u vozilu.

Image

**Dodjela vrijednosti:** Nije određeno.

**2.117.   VuCalibrationData**

Informacija sačuvana u jedinici u vozilu koja se odnosi na kalibraciju tahografa (zahtjev 098).



**noOfVuCalibrationRecords** je broj zapisa sadržanih u nizu vuCalibrationRecords.

**vuCalibrationRecords** je niz zapisa o kalibraciji.

**2.118   VuCalibrationRecord**

Informacija spremljena u jedinici u vozilu, povezana s kalibracijom tahografa (zahtjev 098).



**calibrationPurpose** je svrha kalibracije.

**workshopName, workshopAddress** su naziv i adresa radionice.

**workshopCardNumber** identifikuje karticu radionice koja se koristi pri kalibraciji.

**workshopCardExpiryDate** je datum isteka važnosti kartice.

**vehicleIdentificationNumber** je VIN.

**vehicleRegistrationIdentification** sadrži registracijsku oznaku vozila i državu registracije vozila.

**wVehicleCharacteristicConstant** je karakteristični koeficijent vozila.

**kConstantOfRecordingEquipment** je konstanta tahografa.

**lTyreCircumference** je aktivni opseg guma točkova.

**tyreSize** je oznaka dimenzija guma na vozilu.

**authorisedSpeed** je dopuštena brzina vozila.

**oldOdometerValue, newOdometerValue** su staro i novo stanje brojača kilometara.

**oldTimeValue, newTimeValue** su stara i nova vrijednost datuma i vremena.

**nextCalibrationDate** je datum sljedeće kalibracije tipa naznačenog u CalibrationPurpose provedena od ovlaštenog tijela za nadzor.

**2.119   VuCardIWData**

Informacija spremljena u jedinici u vozilu povezana s ciklusima ubacivanja i vađenja kartice vozača ili kartice radionice u jedinici u vozilu (zahtjev 081).

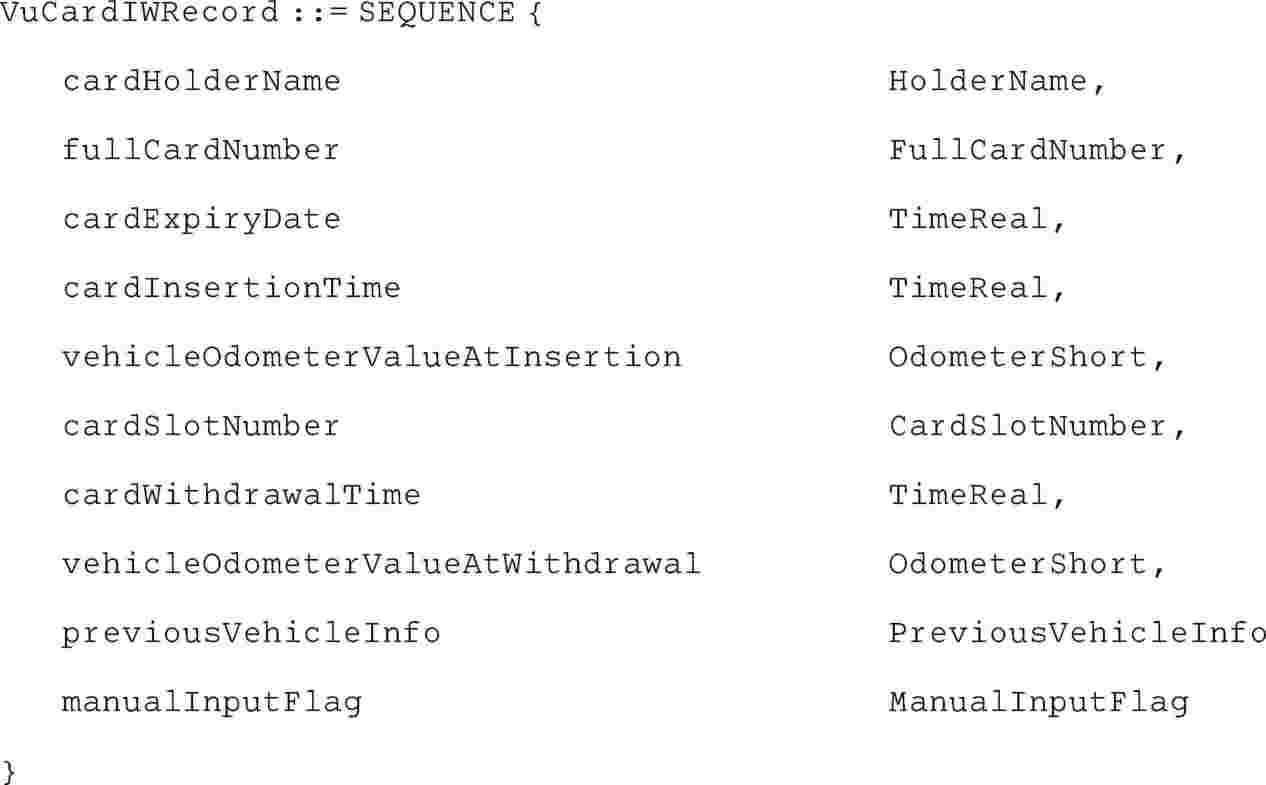


**noOfIWRecords** je broj zapisa u nizu vuCardIWRecords.

**vuCardIWRecords** je niz zapisa povezanih s ciklusima ubacivanja i vađenja kartice.

**2.120   VuCardIWRecord**

Informacija spremljena u jedinicu u vozilu, povezana s ciklusom ubacivanja i vađenja kartice vozača ili kartice radionice u jedinici u vozilu (zahtjev 081).



**cardHolderName** je prezime i ime(na) nosioca kartice vozača ili kartice radionice, sačuvanih na kartici.

**fullCardNumber** je vrsta kartice, država članica izdavaoc i broj kartice, sačuvanih na kartici.

**cardExpiryDate** je datum isteka kartice, pohranjen na kartici.

**cardInsertionTime** je datum i vrijeme ubacivanja.

**vehicleOdometerValueAtInsertion** je stanje brojača kilometara pri ubacivanju kartice.

**cardSlotNumber** je otvor u kojeg je umetnuta kartica.

**cardWithdrawalTime** je datum i vrijeme vađenja.

**vehicleOdometerValueAtWithdrawal** je stanje brojača kilometara pri vađenju kartice.

**previousVehicleInfo** sadrži podatke o vozilu koje je vozač prethodno koristio spremljene na kartici.

**manualInputFlag** je oznaka koja naznačuje je li je vlasnik kartice pri ubacivanju kartice ručno unio aktivnosti vozača.

**2.121.   VuCertificate**

Certifikat javnog ključa jedinice u vozilu.

Image

**2.122.   VuCompanyLocksData**

Informacija sačuvana u jedinici u vozilu, povezana s blokadama preduzeća (zahtjev 104).

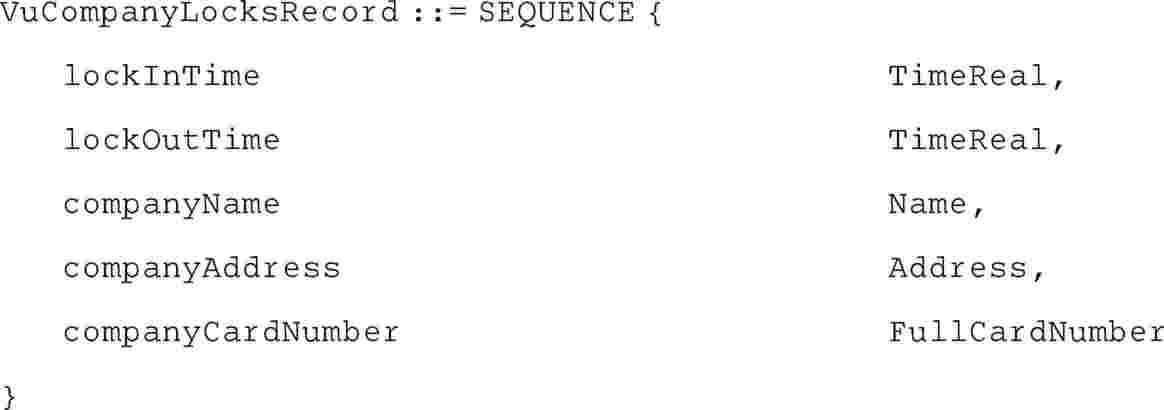


**noOfLocks** je broj zaključavanja naveden u vuCompanyLocksRecords.

**vuCompanyLocksRecords** je niz zapisa zaključavanja preduzeća.

**2.123.   VuCompanyLocksRecord**

Informacija sačuvana u jedinici u vozilu, povezana s jednim zaključavanjem preduzeća (zahtjev 104).



**lockInTime**, **lockOutTime** su datum i vrijeme zaključavanja i otključavanja podataka.

**companyName, companyAddress** su naziv i adresa preduzeća, povezani sa zaključavanjem podataka.

**companyCardNumber** identifikuje karticu korištenu pri zaključavanju.

**2.124.   VuControlActivityData**

Informacija sačuvana u jedinici u vozilu, povezana s nadzorom provedenim uz korištenje ove jedinice vozila (zahtjev 102).

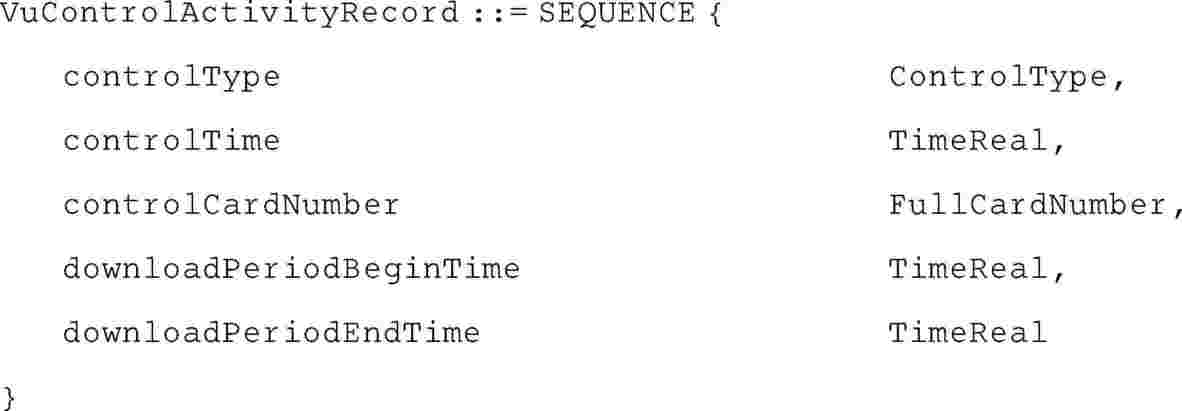


**noOfControls** je broj nadzora navedenih u vuControlActivityRecords.

**vuControlActivityRecords** je niz zapisa o aktivnostima nadzora.

**2.125.   VuControlActivityRecord**

Informacija sačuvana u jedinici u vozilu povezana s nadzorom provedenim uz korištenje ove jedinice vozila (zahtjev 102).



**controlType** je vrsta nadzora.

**controlTime** je datum i vrijeme nadzora.

**ControlCardNumber** identifikuje nadzornu karticu korištenu za nadzor.

**downloadPeriodBeginTime** je početak perioda za koje se obavlja preuzimanje podataka, ako je došlo do preuzimanja podataka.

**downloadPeriodEndTime** je kraj perioda za koje se obavlja preuzimanje podataka, ako je došlo do preuzimanja podataka.

**2.126.   VuDataBlockCounter**

Brojač pohranjen na kartici koji redom utvrđuje cikluse ubacivanja i vađenja kartice u jedinicama u vozilu.

Image

**Dodjela vrijednosti:** Redni broj, s najvećom vrijednošću 9 999, nakon čega opet kreće od 0.

**2.127.   VuDetailedSpeedBlock**

Informacija sačuvana u jedinici u vozilu, povezana s detaljnom brzinom vozila u minuti tokom koje se vozilo kretalo (zahtjev 093).



**speedBlockBeginDate** je datum i vrijeme prve vrijednosti brzine unutar bloka.

**speedsPerSecond** je kronološki slijed izmjerenih brzina svake sekunde u minuti koja počne u speedBlockBeginDate (uključeno).

**2.128.   VuDetailedSpeedData**

Informacija sačuvana u jedinici u vozilu povezana s podrobnim podacima o brzini vozila.

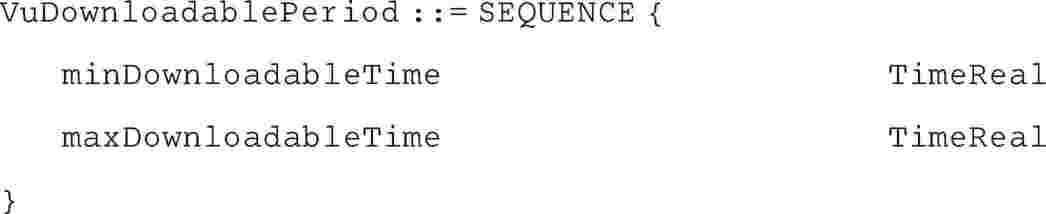


**noOfSpeedBlocks** je broj blokova brzina u nizu vuDetailedSpeedBlocks.

**vuDetailedSpeedBlocks** je niz detaljnih blokova brzina.

**2.129.   VuDownloadablePeriod**

Najstariji i najnoviji datum za koji jedinica u vozilu sadrži podatke vezane uz aktivnosti vozača (zahtjevi 081, 084 ili 087).

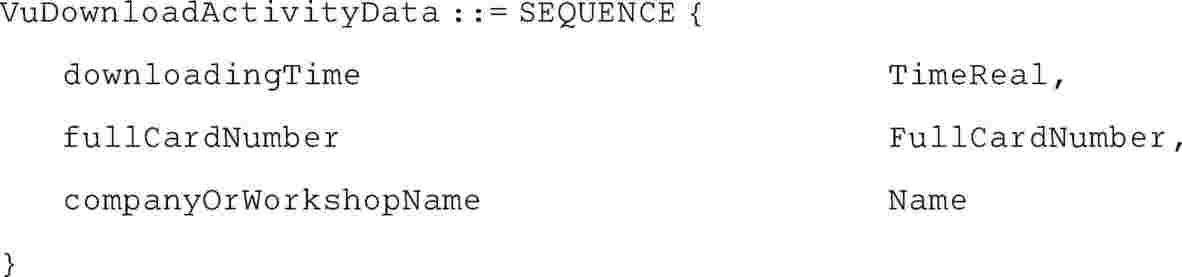


**minDownloadableTime** je najstariji datum i vrijeme arhivirani u jedinici vozila ubacivanja kartice ili promjene aktivnosti ili unosa mjesta.

**MaxDownloadableTime** je najnoviji datum i vrijeme arhivirani u jednici vozila vađenja kartice ili promjene aktivnosti ili unosa mjesta.

**2.130.   VuDownloadActivityData**

Informacija sačuvana u jedinici u vozilu povezana sa zadnjim preuzimanjem podataka iz iste (zahtjev 105).



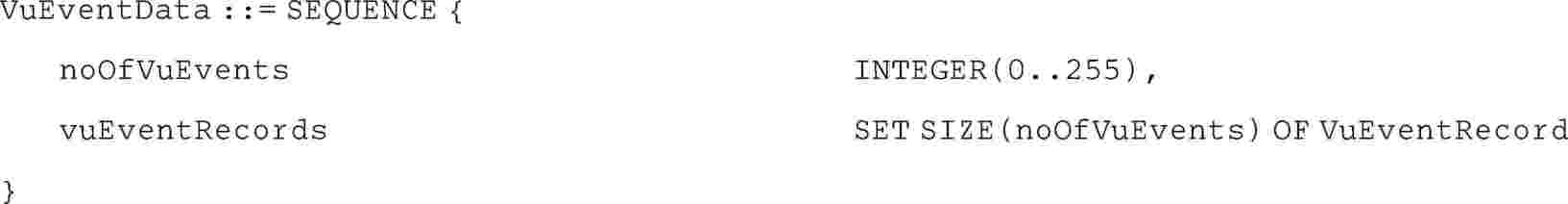
**downloadingTime** je datum i vrijeme preuzimanja podataka.

**fullCardNumber** identifikuje karticu korištenu za odobrenje preuzimanja podataka.

**companyOrWorkshopName** je naziv preduzeća ili radionice.

**2.131.   VuEventData**

Informacija sačuvana u jedinici u vozilu, povezana s događajima (zahtjev 094, osim u slučaju prekoračenja brzine).

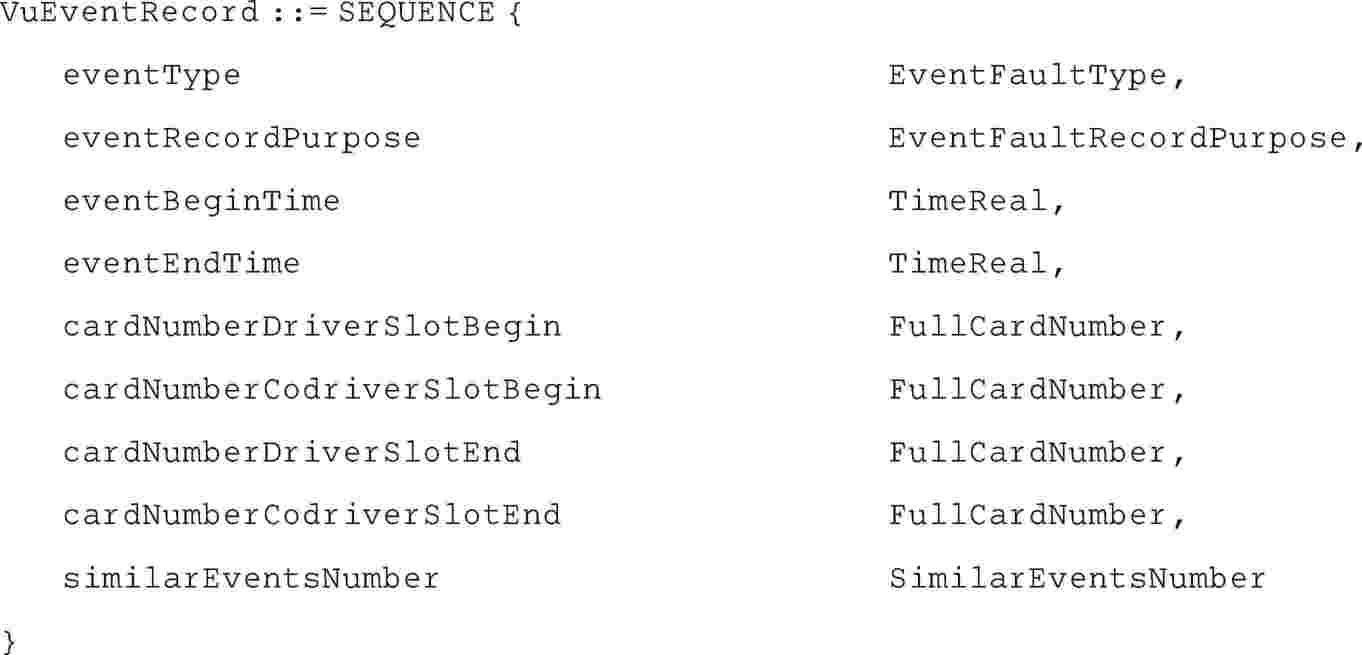


**noOfVuEvents** je broj događaja navedenih u nizu vuEventRecords.

**vuEventRecords** je niz zapisa događaja.

**2.132.   VuEventRecord**

Informacija sačuvana u jedinicu u vozilu povezana s događajem (zahtjev 094, osim u slučaju prekoračenja brzine).



**eventType** je vrsta događaja.

**eventRecordPurpose** je svrha s kojom je taj događaj zaevidentirajun.

**eventBeginTime** je datum i vrijeme početka događaja.

**eventEndTime** je datum i vrijeme kraja događaja.

**cardNumberDriverSlotBegin** identifikuje karticu umetnutu u otvor vozača na početku događaja.

**cardNumberCodriverSlotBegin** identifikuje karticu umetnutu u otvor suvozača na početku događaja.

**cardNumberDriverSlotEnd** identifikuje karticu umetnutu u otvor vozača na kraju događaja.

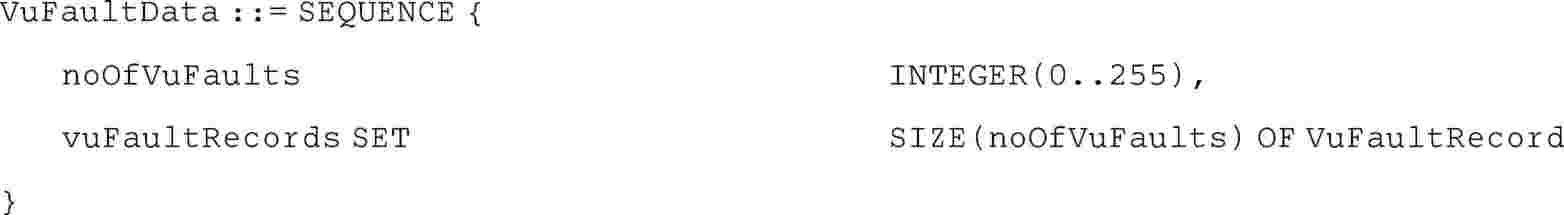
**cardNumberCodriverSlotEnd** identifikuje karticu umetnutu u otvor suvozača pri kraju događaja.

**similarEventsNumber** je broj sličnih događaja u tom danu.

Ovaj slijed se može koristiti za sve događaje, osim za događaje prekoračenja brzine.

**2.133.   VuFaultData**

Informacija sačuvana u jedinicu u vozilu, povezana s greškama (zahtjev 096).

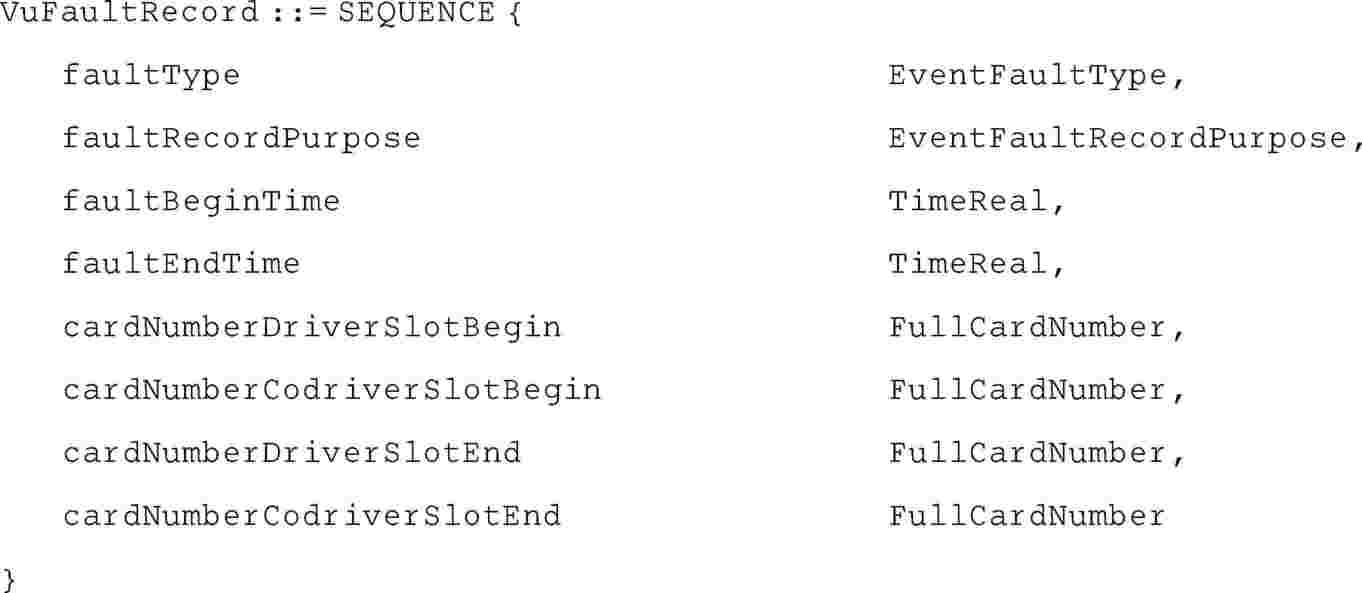


**noOfVuFaults** je broj grešaka navedenih u nizu vuFaultRecords.

**vuFaultRecords** je niz zapisa o greškama.

**2.134.   VuFaultRecord**

Informacija spremljena u jedinici u vozilu, povezana s pogreškom (zahtjev 096).



**faultType** je vrsta greške tahografa.

**faultRecordPurpose** je svrha s kojom je ta greška bila zaevidentirajuna.

**faultBeginTime** je datum i vrijeme početka greške.

**faultEndTime** je datum i vrijeme kraja greške.

**cardNumberDriverSlotBegin** identifikuje karticu umetnutu u otvor vozača na početku greške.

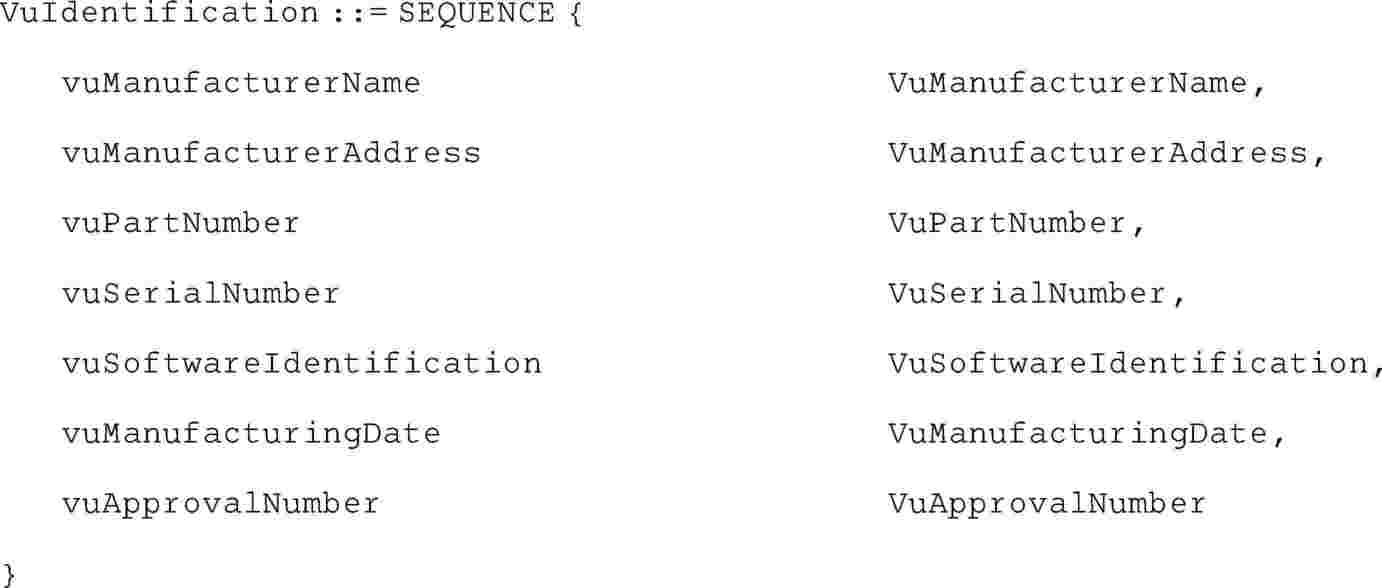
**cardNumberCodriverSlotBegin** identifikuje karticu umetnutu u otvor suvozača na početku greške.

**cardNumberDriverSlotEnd** identifikuje karticu umetnutu u otvor vozača na kraju greške.

**cardNumberCodriverSlotEnd** identifikuje karticu umetnutu u otvor suvozača na kraju greške.

**2.135.   VuIdentification**

Informacija sačuvana u jedinici u vozilu, povezana s identifikacijom jedinice u vozilu (zahtjev 075).



**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** identifikuje softver instaliran u jedinici u vozilu.

**vuManufacturingDate** je datum proizvodnje jedinice u vozilu.

**vuApprovalNumber** je broj tipskog odobrenja jedinice u vozilu.

**2.136.   VuManufacturerAddress**

Adresa proizvođača jedinice u vozilu.

Image

**Dodjela vrijednosti:** Nije određeno.

**2.137.   VuManufacturerName**

Naziv proizvođača jedinice u vozilu.

Image

**Dodjela vrijednosti:** Nije određeno.

**2.138.   VuManufacturingDate**

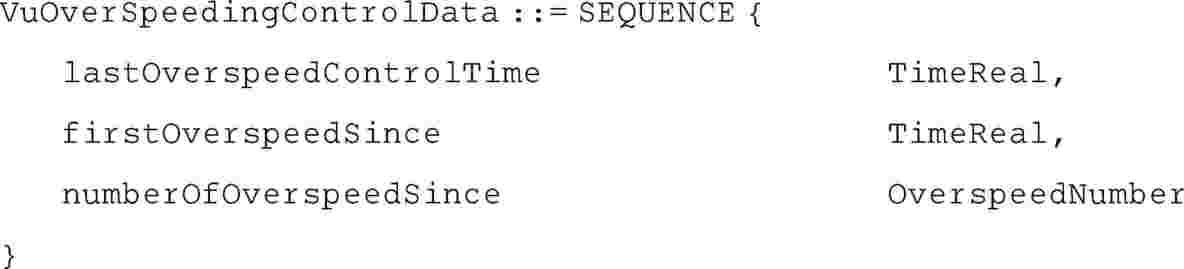
Datum proizvodnje jedinice u vozilu.

Image

**Dodjela vrijednosti:** Nije određeno.

**2.139.   VuOverSpeedingControlData**

Informacija sačuvana u jedinici u vozilu, povezana s događajima prekoračenja brzine nakon zadnje kontrole prekoračenja brzine (zahtjev 095).



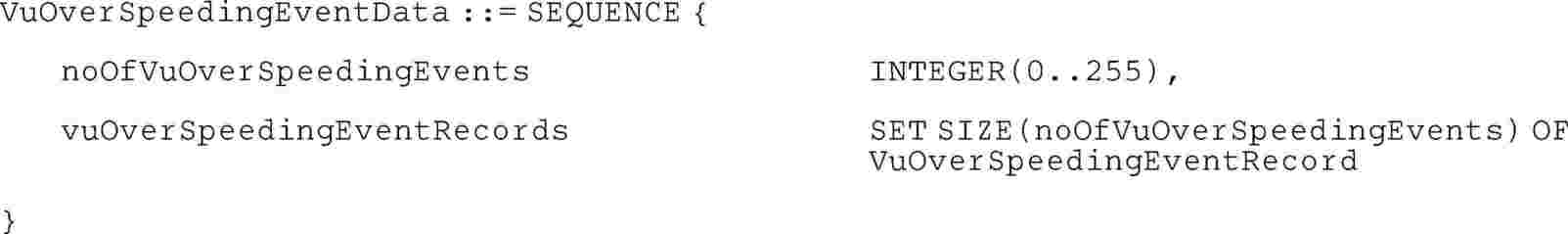
**lastOverspeedControlTime** je datum i vrijeme zadnje kontrole prekoračenja brzine.

**firstOverspeedSince** je datum i vrijeme prvog prekoračenja brzine nakon ove kontrole prekoračenja brzine.

**numberOfOverspeedSince** je broj događaja prekoračenja brzine od zadnje kontrole prekoračenja brzine.

**2.140.   VuOverSpeedingEventData**

Informacija sačuvana u jedinici u vozilu povezana s događajima prekoračenja brzine (zahtjev 094).

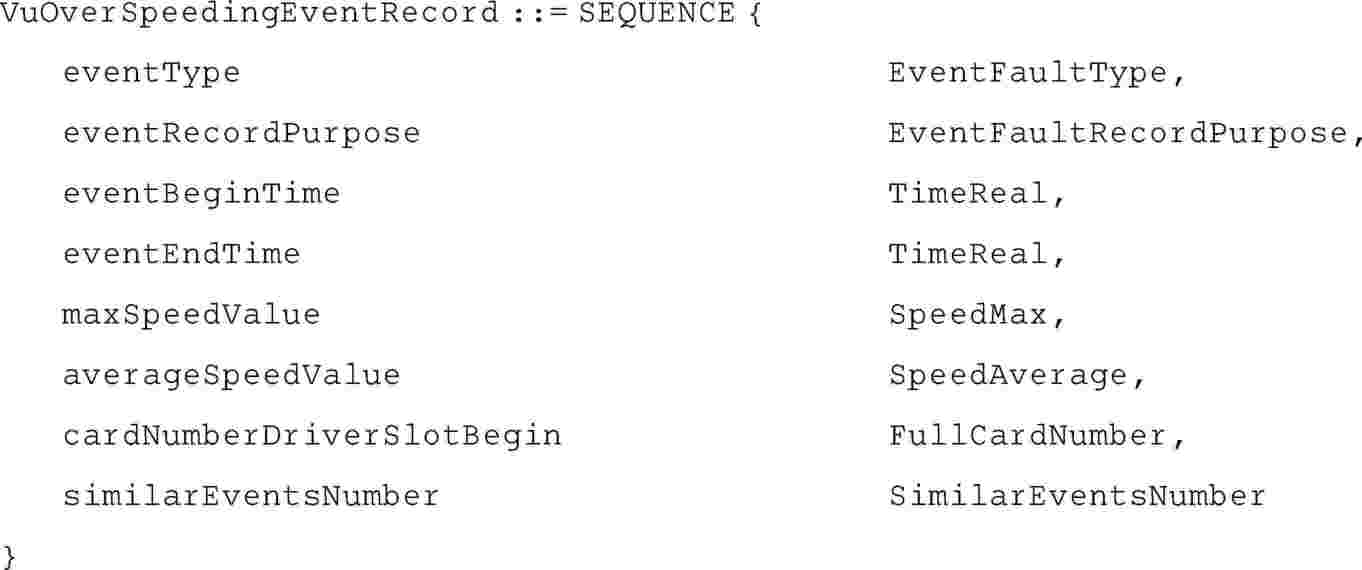


**noOfVuOverSpeedingEvents** je broj događaja navedenih u nizu vuOverSpeedingEventRecords.

**vuOverSpeedingEventRecords** je niz zapisa o događajima prekoračenja brzine.

**2.141.   VuOverSpeedingEventRecord**

Informacija sačuvana u jedinici u vozilu, povezana s događajima prekoračenja brzine (zahtjev 094).



**eventType** je vrsta događaja.

**eventRecordPurpose** je svrha zbog koje je taj događaj bio zaevidentirajun.

**eventBeginTime** je datum i vrijeme početka događaja.

**eventEndTime** je datum i vrijeme kraja događaja.

**maxSpeedValue** je najviša brzina izmjerena tokom događaja.

**averageSpeedValue** je aritmetička prosječna brzina izmjerena tokom događaja.

**cardNumberDriverSlotBegin** identifikuje karticu umetnutu u otvor vozača na početku događaja.

**similarEventsNumber** je broj sličnih događaja u tom danu.

**2.142.   VuPartNumber**

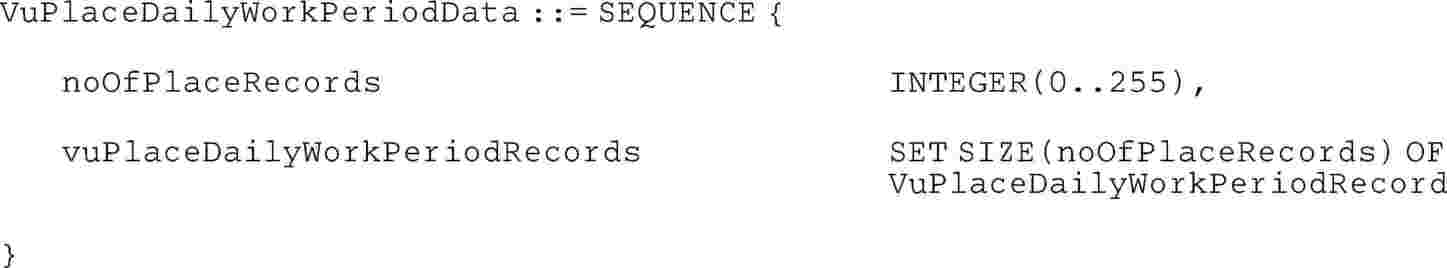
Kataloški broj jedinice u vozilu.

Image

**Dodjela vrijednosti:** određuje proizvođač jedinice vozila.

**2.143.   VuPlaceDailyWorkPeriodData**

Informacija sačuvana u jedinici u vozilu povezana s mjestima početka ili kraja dnevnih perioda aktivnosti vozača (zahtjev 087).

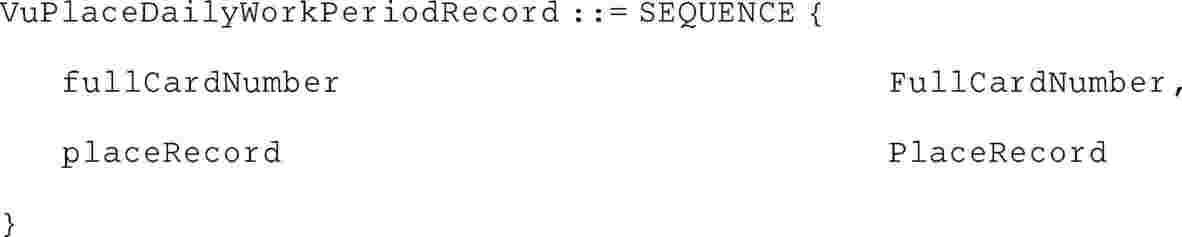


**noOfPlaceRecords** je broj zapisa navedenih u nizu vuPlaceDailyWorkPeriodRecords.

**vuPlaceDailyWorkPeriodRecords** je niz zapisa vezanih uz mjesta.

**2.144.   VuPlaceDailyWorkPeriodRecord**

Informacija spremljena u jedinici u vozilu povezana s mjestom početka ili kraja dnevnih perioda aktivnosti vozača (zahtjev 087).



**fullCardNumber** je vrsta kartice vozača, država članica izdavaoc kartice i broj kartice.

**placeRecord** sadrži informacije povezane s unesenim mjestom.

**2.145.   VuPrivateKey**

Privatni ključ jedinice u vozilu.

Image

**2.146.   VuPublicKey**

Javni ključ jedinice u vozilu.

Image

**2.147.   VuSerialNumber**

Serijski broj jedinice u vozilu (zahtjev 075).

Image

**2.148.   VuSoftInstallationDate**

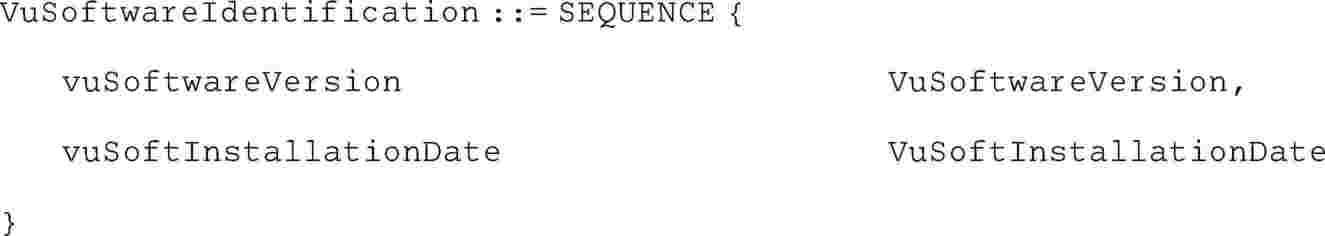
Datum ugradnje verzije softvera u jedinicu u vozilu.

Image

**Dodjela vrijednosti:** Nije određeno.

**2.149.   VuSoftwareIdentification**

Informacija spremljena u jedinici u vozilu, povezana s instaliranim softverom.



**vuSoftwareVersion** je broj verzije softvera instaliranog u jedinicu u vozilu.

**vuSoftInstallationDate** je datum instalacije softvera.

**2.150.   VuSoftwareVersion**

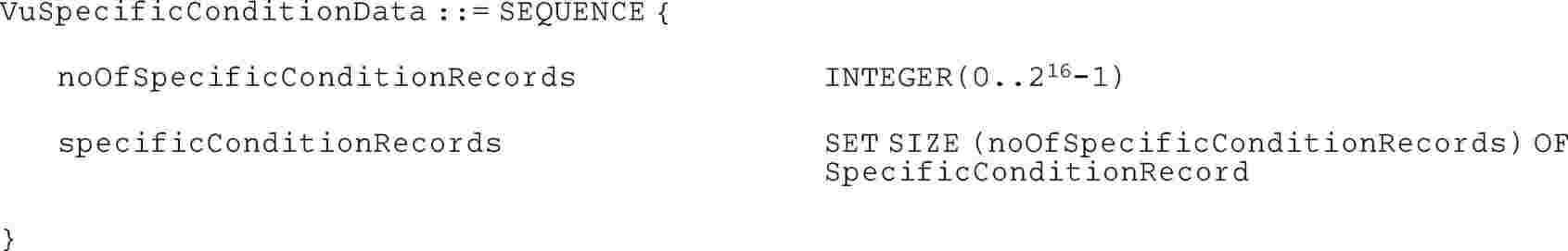
Verzija softvera jedinice u vozilu.

Image

**Dodjela vrijednosti:** Nije određeno.

**2.151.   VuSpecificConditionData**

Informacija sačuvana u jedinici u vozilu, povezana s posebnim stanjima.

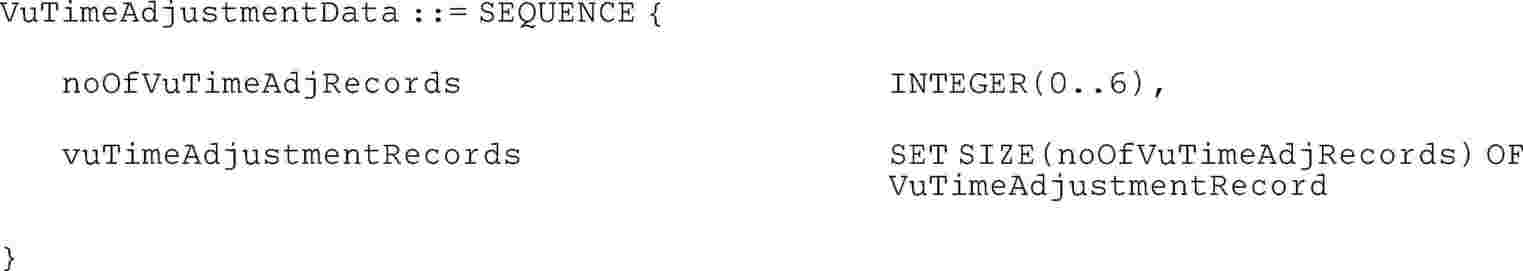


**noOfSpecificConditionRecords** je broj zapisa u nizu specificConditionRecords.

**specificConditionRecords** je niz zapisa povezanih s posebnim stanjima.

**2.152.   VuTimeAdjustmentData**

Informacija spremljena u jedinici u vozilu, povezana s podešenjima vremena provedenim van okvira redovnih kalibracija (zahtjev 101).

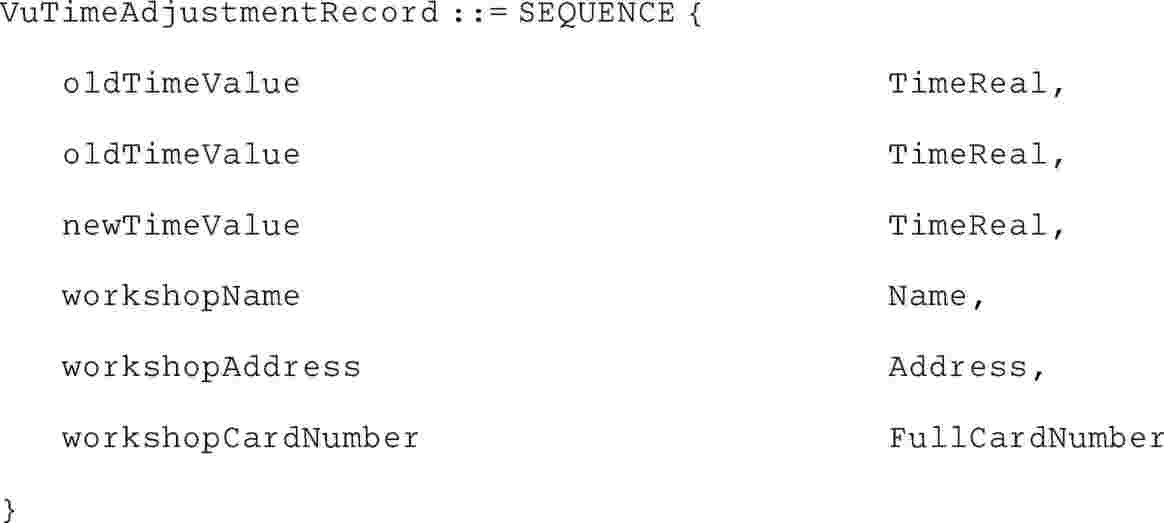


**noOfVuTimeAdjRecords** je broj zapisa u vuTimeAdjustmentRecords.

**vuTimeAdjustmentRecords** je niz zapisa o podešavanju vremena.

**2.153.   VuTimeAdjustmentRecord**

Informacija spremljena u jedinici u vozilu, povezana s podešavanjem vremena provedenim van okvira redovnih kalibrisanja (zahtjev 101).



**oldTimeValue, newTimeValue** su stara i nova vrijednost datuma i vremena.

**workshopName, workshopAddress** su naziv i adresa radionice.

**workshopCardNumber** identifikuje karticu radionice korištenu za podešavanje vremena.

**2.154.   W-VehicleCharacteristicConstant**

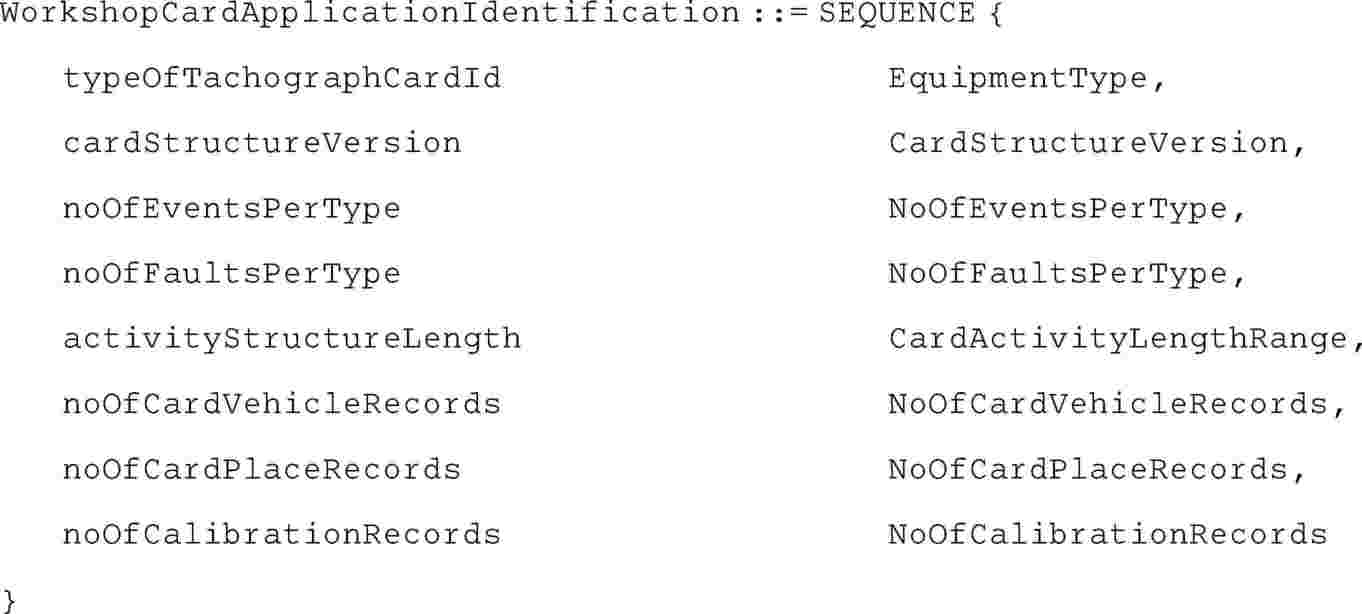
Karakteristični koeficijent vozila (definicija k).

Image

**Dodjela vrijednosti:** Impulsi po kilometru u djelatnom rasponu od 0 do 64 255 impulsa/km.

**2.155.   WorkshopCardApplicationIdentification**

Informacija sačuvana na kartici radionice, povezana s identifikacijom primjene kartice (zahtjev 190).



**typeOfTachographCardId** naznačuje vrstu primijenjene kartice.

**cardStructureVersion** naznačuje verziju strukture primijenjenu na kartici.

**noOfEventsPerType** je broj događaja po tipu događaja koje kartica može zaevidentirati.

**noOfFaultsPerType** je broj grešaka po tipu grešaka koje kartica može zaevidentirati.

**activityStructureLength** označava broj bajtova raspoloživih za čuvanje zapisa o aktivnosti.

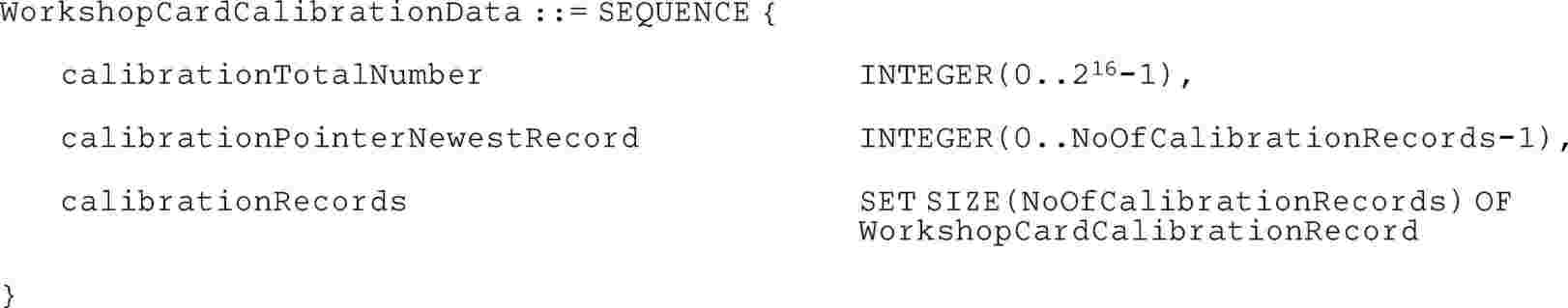
**noOfCardVehicleRecords** je broj zapisa vozila koje može sadržavati kartica.

**noOfCardPlaceRecords** je broj mjesta koje može zaevidentirati kartica.

**noOfCalibrationRecords** je broj zapisa kalibracija koje može sačuvati kartica.

**2.156.   WorkshopCardCalibrationData**

Informacija spremljena na kartici radionice, povezana s radioničkim radom s karticom (zahtjevi 227 i 229).



**calibrationTotalNumber** je ukupni broj kalibracija obavljenih s karticom.

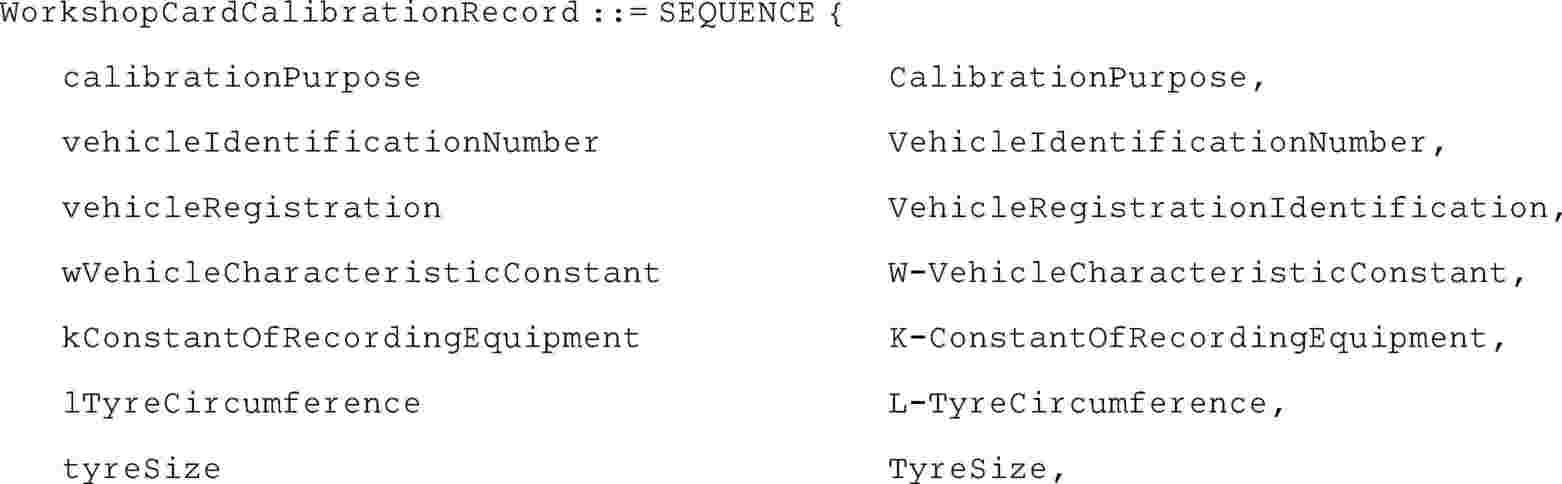
**calibrationPointerNewestRecord** je indeks zadnjeg ažuriranog zapisa kalibracije.

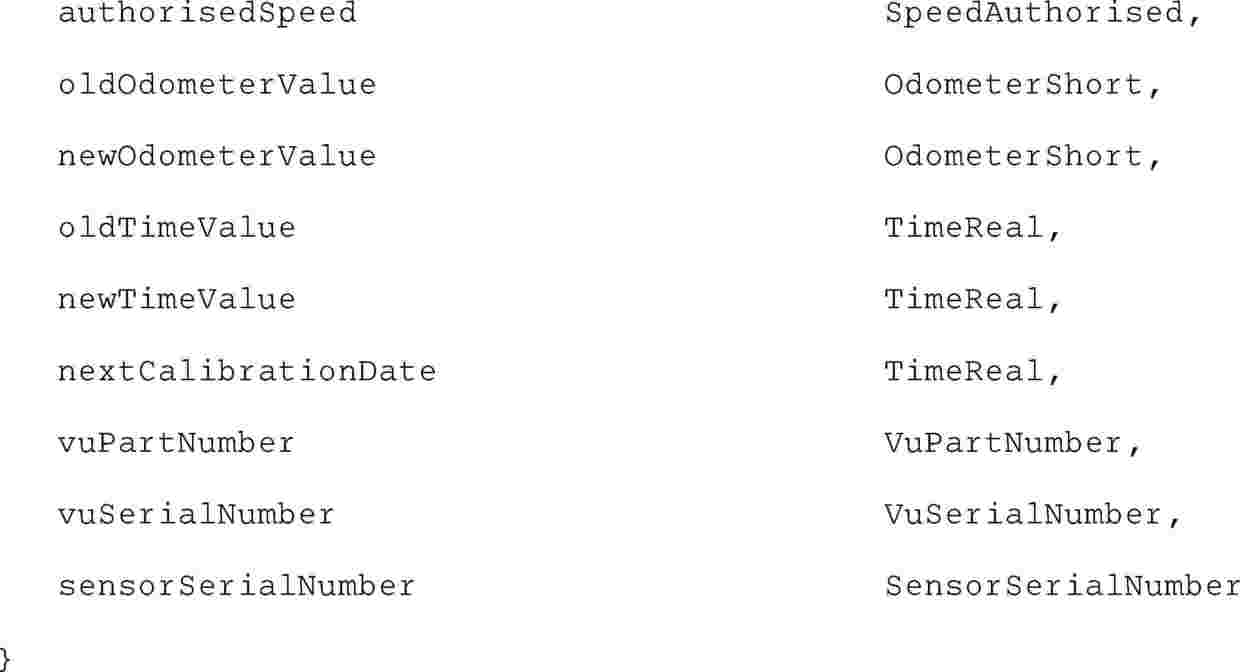
**Dodjela vrijednosti:** Broj koji odgovara brojaču evidencije kalibracije, počevši s ‚0’ za prvu pojavu zapisa kalibrisanja u strukturi.

**calibrationRecords** je niz zapisa koji sadrže informacije o kalibraciji i/ili podešavanju vremena.

**2.157.   WorkshopCardCalibrationRecord**

Informacija spremljena na kartici radionice povezana s obavljenim kalibrisanjem s tom karticom (zahtjev 227).





**calibrationPurpose** je svrha kalibracije.

**vehicleIdentificationNumber** je VIN.

**vehicleRegistration** sadrži registracijsku oznaku vozila i državu članicu registracije vozila.

**wVehicleCharacteristicConstant** je karakteristični koeficijent vozila.

**kConstantOfRecordingEquipment** je konstanta tahografa.

**lTyreCircumference** je aktivni opseg guma točkova.

**tyreSize** je oznaka dimenzija guma na vozilu.

**authorisedSpeed** je najviša dopuštena brzina vozila.

**oldOdometerValue, newOdometerValue** su staro i novo stanje brojača kilometara.

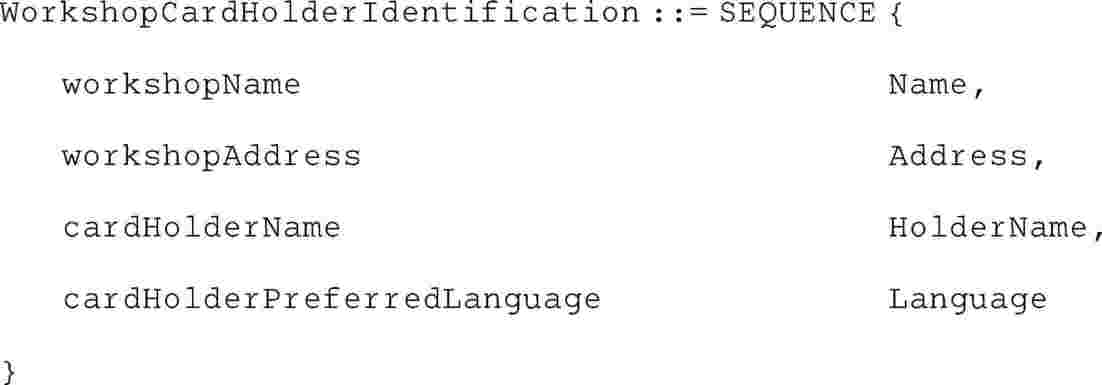
**oldTimeValue**, newTimeValue su stara i nova vrijednost datuma i vremena.

**nextCalibrationDate** je datum sljedeće kalibracije, tipa naznačenog u CalibrationPurpose pri ovlaštenom tijelu za kalibraciju.

**vuPartNumber, vuSerialNumber** i **sensorSerialNumber** su podakovni elementi za identifikaciju tahografa.

**2.158.   WorkshopCardHolderIdentification**

Informacija sačuvana na kartici radionice, povezana s identifikacijom nosioca kartice (zahtjev 216).



**workshopName** je naziv radionice nosioca kartice.

**workshopAddress** je adresa radionice nosioca kartice.

**cardHolderName** je prezime i ime(na) nosioca kartice (npr. ime mehaničara).

**cardHolderPreferredLanguage** je odabrani jezik nosioca kartice.

**2.159.   WorkshopCardPIN**

Osobni identifikacijski broj kontrolne kartice (zahtjev 213).

Image

**Dodjela vrijednosti:** PIN poznat nosiocu kartice, desno popunjeno ‚FF’ bajtima do 8 bajta.

**3.   DEFINICIJE RASPONA VRIJEDNOSTI I VELIČINA**

Definicija promjenjivih vrijednosti korištenih za definicije u stavu 2.

TimeRealRange::= 232-1

**3.1.   Definicije za karticu vozača:**

|  |  |  |
| --- | --- | --- |
| **Naziv promjenjive vrijednosti** | **Minimum** | **Maksimum** |
| Image | 5 544 bajta  (28 dana po 93 promjena aktivnosti na dan) | 13 776 bajta  (28 dana po 240 promjena aktivnosti na dan) |
| Image | 84 | 112 |
| Image | 84 | 200 |
| Image | 6 | 12 |
| Image | 12 | 24 |

**3.2.   Definicije za karticu radionice:**

|  |  |  |
| --- | --- | --- |
| **Naziv promjenjive vrijednosti** | **Minimum** | **Maksimum** |
| Image | 198 bajta  (1 dan s 93 promjena aktivnosti) | 492 bajta  (1 dan s 240 promjena aktivnosti) |
| Image | 6 | 8 |
| Image | 4 | 8 |
| Image | 3 | 3 |
| Image | 6 | 6 |
| Image | 88 | 255 |

**3.3.   Definicije za nadzornu karticu:**

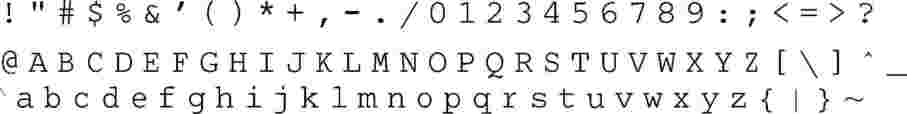
|  |  |  |
| --- | --- | --- |
| **Naziv promjenjive vrijednosti** | **Minimum** | **Maksimum** |
| Image | 230 | 520 |

**3.4.   Definicije za karticu prevoznika:**

|  |  |  |
| --- | --- | --- |
| **Naziv promjenjive vrijednosti** | **Minimum** | **Maksimum** |
| Image | 230 | 520 |

**4.   NIZOVI ZNAKOVA**

IA5Strings koriste ASCII znakove definirane u ISO/IEC 8824-1. Za čitljivost i lakši osvrt dodjela vrijednosti navedena je u nastavu. U slučaju nepodudarnosti ISO/IEC 8824-1 ima prednost pred ovom informativnom bilješkom.



Drugi nizovi znakova (Address, Name, VehicleRegistrationNumber) uz to koriste znakove definirane šiframa 192 do 255 u ISO/IEC 8859-1 (skup slova Latin1) ili u ISO/IEC 8859-7 (skup grčkih slova).

**5.   ŠIFRIRANJE**

Kad su šifrirani prema pravilima šifriranja ASN.1, sve definirane vrste podataka se moraju šifrirati prema ISO/IEC 8825-2 (usklađena inačica).

**Dodatak 2.**

**OPIS KARTICA TAHOGRAFA**

Sadržaj

1. UVOD …

1.1. Kratice …

1.2. Trimiteri …

2. ELEKTRIČNA I FIZIČKA OBELJEŽJA …

2.1. Napon napajanja i potrošnja struje …

2.2. Napon programiranja Vpp …

2.3. Generisanje i frekvencija sata …

2.4. Kontakt I/O …

2.5. Stanja kartice …

3. HARDVER I KOMUNIKACIJA …

3.1. Uvod …

3.2. Protokol prenosa …

3.2.1. Protokoli …

3.2.2. ATR …

3.2.3. PTS …

3.3. Uslovi pristupa (AC) …

3.4. Šifriranje podataka …

3.5. Pregled šifri naredbi i grešaka …

3.6. Opis naredbi …

3.6.1. Odabir datoteke …

3.6.1.1 Odabir po nazivu (AID) …

3.6.1.2. Odabir elementarne datoteke korištenjem njenog identifikatora datoteke …

3.6.2. Binarno čitanje …

3.6.2.1 Naredba bez sigurnog prenosa poruke …

3.6.2.2. Naredba sa sigurnim prenosom poruke …

3.6.3. Binarno ažuriranje …

3.6.3.1. Naredba bez sigurnog prenosa poruke …

3.6.3.2. Naredba sa sigurnim prenosom poruke …

3.6.4. Traži zahtjev za lozinku …

3.6.5. Provjeri …

3.6.6. Traži odgovor …

3.6.7. PSO: provjeri certifikat …

3.6.8. Unutarnja autentifikacija …

3.6.9. Spoljna autentifikacija …

3.6.10. Upravljanje sigurnosnim okruženjem …

3.6.11. PSO: funkcija kompresije podataka …

3.6.12. Komprimiraj datoteku …

3.6.13. PSO: proračunaj digitalni potpis …

3.6.14. PSO: provjeri digitalni potpis …

4. STRUKTURA KARTICA TAHOGRAFA …

4.1. Struktura kartice vozača …

4.2. Struktura kartice radionice …

4.3. Struktura kontrolne kartice …

4.4. Struktura kartice prevoznika …

**1.   UVOD**

**1.1.   Kratice**

Za potrebe ovog Dodatka, primjenjuju se sljedeće kratice:

|  |  |
| --- | --- |
| AC | uslovi pristupa |
| AID | identifikator aplikacije |
| ALW | uvijek |
| APDU | podaci jedinica aplikacijskog protokola (struktura naredbe) |
| ATR | odaziv na povrat u početno stanje |
| AUT | autentificirano |
| C6, C7 | kontakti br. 6 i 7 kartice opisani u ISO/IEC 7816-2 |
| cc | satni ciklusi |
| CHV | informacija o provjeri nosioca kartice |
| CLA | bajt razreda naredbe APDU |
| DF | namjenska datoteka; DF može sadržavati druge datoteke (EF ili DF) |
| EF | elementarna datoteka |
| ENC | šifrirano: pristub moguć samo šifriranjem podataka |
| etu | elementarna jedinica vremena |
| IC | integirsani krug |
| ICC | kartica s integirsanim krugom |
| ID | identifikator |
| IFD | uređaji sučelja |
| IFS | veličina informacijskog polja |
| IFSC | veličina informacijskog polja za karticu |
| IFSD | veličina informacijskog polja naprave (za terminal) |
| INS | bajt instrukcije APDU naredbe |
| Lc | dužina ulaznih podataka za naredbu APDU |
| Le | dužina očekivanih podataka (izlazni podaci za naredbu) |
| MF | glavna datoteka (temeljna DF) |
| P1-P2 | parametarski bajti |
| NAD | adresa čvora korištena u protokolu T = 1 |
| NEV | nikad |
| PIN | osobni identifikacijski broj |
| PRO SM | zaštićeno sigurnim prenosom poruka |
| PTS | odabir prenosa protokola |
| RFU | namijenjeno budućoj uporabi |
| RST | vraćanje u prijašnje stanje (kartice) |
| SM | siguran prenos poruka |
| SW1-SW2 | statusni bajti |
| TS | početni ATR znak |
| VPP | napon programiranja |
| XXh | vrijednost XX u heksadecimalnom zapisu |
| || | simbol ulančavanja 03||04 = 0304. |

**1.2.   Literatura**

U ovom su Dodatku korišteni sljedeći naslovi:

|  |  |
| --- | --- |
| EN 726-3 | Sistemi identifikacijskih kartica - Telekomunikacijske kartice s integirsanim krugom (krugovima) i terminali - Dio 3: Zahtjevi za karticu nezavisni od aplikacije. Prosinac, 1994. |
| ISO/IEC 7816-2 | Informacijska tehnologija - Identifikacijske kartice — Kontaktne kartice s integirsanim krugom (krugovima) - Dio 2: Dimenzije i položaj kontakata. Prvo izdanje: 1999. |
| ISO/IEC 7816-3 | Informacijska tehnologija - Identifikacijske kartice - Kontaktne kartice s integirsanim krugom (krugovima) - Dio 3: Elektronski signali i protokoli prenosa. 2.izdanje: 1997. |
| ISO/IEC 7816-4 | Informacijska tehnologija - Identifikacijske kartice — Kontaktne kartice s integirsanim krugom (krugovima) - Dio 4: Međugranske naredbe za razmjenu. Prvo izdanje: 1995 + 1. dopuna: 1997. |
| ISO/IEC 7816-6 | Informacijska tehnologija - Identifikacijske kartice - Kontaktne kartice s integirsanim krugovima - Dio 6: Međugranski podakovni elementi. Prvo izdanje: 1996 + 1. korekcija: 1998. |
| ISO/IEC 7816-8 | Informacijska tehnologija - Identifikacijske kartice - Kontaktne kartice s integirsanim krugom (krugovima) - Dio 8: Zaštitne međugranske naredbe. Prvo izdanje: 1999. |
| ISO/IEC 9797 | Informacijska tehnologija - Zaštitne tehnike - Mehanizam podakovne potpunosti upotrebom funkcije kriptografske provjere s blok šifarskim algoritmom. 2. izdanje: 1994. |

**2.   ELEKTRIČNA I FIZIČKA OBELJEŽJA**

TCS\_200  
Ako nije drugačije propisano, svi elektronski signali moraju biti u skladu s ISO/IEC 7816-3.

TCS\_201  
Položaj i dimenzije kontakata kartice moraju biti u skladu s ISO/IEC 7816-2.

**2.1.   Napon napajanja i potrošnja struje**

TCS\_202  
Kartica mora raditi prema specifikacijama unutar granica potrošnje naznačenim u ISO/IEC 7816-3.

TCS\_203  
Kartica mora raditi sa Vcc = 3 V (± 0,3 V) ili sa Vcc = 5 V (± 0,5 V).

Odabir napona se vrši prema ISO/IEC 7816-3.

**2.2.   Napon programiranja Vpp**

TCS\_204  
Kartica ne zahtijeva napon programiranja na pinu C6. Očekuje se da pin C6 nije priključen na IFD. Kontakt C6 se može priključiti na Vcc u kartici, ali ne i uzemljiti. Ovaj napon se ni u kojem slučaju ne smije obrađivati.

**2.3.   Generisanje i frekvencija sata**

TCS\_205  
Kartica radi u frekventnom području od 1 do 5 MHz. Unutar jedne razmjene podataka s karticom frekvencija sata može odstubati za ± 2 %. Frekvenciju sata generiše jedinica u vozilu a ne sama kartica. Radni ciklus se može izmjenjivati između 40 i 60 %.

TCS\_206  
U uslovima sadržanim u datoteci kartice EFICC, se može zaustaviti spoljni sat. Prvi bajt sadržaja datoteke EFICC šifrira uslove režima Clockstop (za pojedinosti pogledati EN 726-3).

|  |  |  |  |
| --- | --- | --- | --- |
| **Niska** | **Visoka** |  |  |
| **Bit 3** | **Bit 2** | **Bit 1** |
| 0 | 0 | 1 | Clockstop dopušten, nema povlaštene razine |
| 0 | 1 | 1 | Clockstop dopušten, povlaštena visoka nivo. |
| 1 | 0 | 1 | Clockstop dopušten, povlaštena niska nivo. |
| 0 | 0 | 0 | Clockstop nije dopušten |
| 0 | 1 | 0 | Clockstop dopušten samo na visokoj razini. |
| 1 | 0 | 0 | Clockstop dopušten samo na niskoj razini. |

Bitovi od 4 do 8 se ne koriste.

**2.4.   Kontakt I/O**

TCS\_207  
Kontakt I/O C7 se koristi za prijem podataka iz IFD i odašiljanje podataka u IFD. Tokom rada, samo kartica ili IFD mora biti u režimu odašiljanja. Ako su obje jedinice u režimu odašiljanja, to ne uzrokuje oštećenje kartice. Kad ne odašilje, kartica ulazi u režim prijema.

**2.5.   Stanja kartice**

TCS\_208  
Dok je priključeno napajanje kartica radi u dva stanja:

* radno stanje dok izvršava naredbe ili se spaja 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 za kartice tahografa i jedinice u vozilu kojima se osigurava ispravan rad i interoperabilnost.

Kartice tahografa 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 drugačije naznačeno, navedene naredbe su u cijelosti u skladu sa spomenutim normama.

**3.2.   Protokol prenosa**

TCS\_300  
Protokol prenosa je u skladu s ISO/IEC 7816-3. Konkretno, jedinica vozila mora raspoznati produženja vremena čekanja koje odašilje kartica.

**3.2.1.    Protokoli**

TCS\_301  
Kartica mora predvidjeti i protokol T = 0 i protokol T = 1.

TCS\_302  
T = 0 je standardni protokol, stoga je potrebna naredba PTS za prijelaz na protokol T = 1.

TCS\_303  
Naprave podržavaju neposrednu konvenciju u oba protokola, pa je stoga za karticu obavezna neposredna konvencija.

TCS\_304  
Bajt ‚Informacija o veličini kartičnog polja’ je prisutan pri ATR u znaku TA3. Ta vrijednost iznosi najmanje ‚F0h’ (= 240 bajta).

Na protokole se primjenjuju sljedeća ograničenja:

|  |  |
| --- | --- |
|  | TCS\_305 T = 0   * + Uređaji sučelja podržava odgovor na I/O nakon vršnog signala na RST od 400 cc.   + Uređaji sučelja čita znakove s razmakom od 12 etu.   + Uređaji sučelja čita pogrešan znak i njegovo ponavljanje ako su razmaci 13 etu. Ako je otkriven pogrešan znak, može se pojaviti signal greške na I/O između 1 etu i 2 etu. Uređaji podržava kašnjenje od 1 etu.   + Uređaji sučelja prihvaća 33-bajtni ATR (TS + 32).   + Ako je u ATR prisutan TC1, za znakove koje šalje uređaji sučelja prisutan je dodatni zaštitno vrijeme, iako znakovi koje šalje kartica još uvijek mogu biti razmaknuti 12 etu. Ovo takođe vrijedi i za znak ACK, kojeg kartica šalje nakon znaka P3 kojeg odašilje uređaji sučelja.   + Uređaji sučelja uzima u obzir znak NUL kojega odašilje kartica.   + Uređaji sučelja prihvaća komplementarne režime za ACK.   + Naredba traži odgovor te se ne može koristiti u režimu ulančavanja za dobivanje podataka čija bi dužina mogla prelaziti 255 bajta. |

|  |  |
| --- | --- |
|  | TCS\_306 T = 1   * + Bajt NAD: ne koristi se (NAD se postavlja na ‚00’).   + ABORT S-bloka: ne koristi se.   + Greška stanja VPP S-bloka: ne koristi se.   + Ukupna dužina ulančavanja podakovnog polja ne prelazi 255 bajta (što osigurava IFD).   + Veličinu podakovnog polja za uređaj (IFSD) navodi IFD odmah nakon ATR: IFD šalje zahtjev za IFS S-bloka nakon ATR, a kartica šalje natrag IFS S-bloka. Preporučena vrijednost za IFSD je 254 bajta.   + Kartica ne traži ponovno podešavanje IFS-a. |

**3.2.2.    ATR**

TCS\_307  
Uređaji provjerava bajte ATR prema ISO/IEC 7816-3. Ne vrši se provjera na povijesnim znakovima ATR.

**Primjer osnovnog biprotokola ATR** prema ISO/IEC 7816-3

|  |  |  |
| --- | --- | --- |
| **Znak** | **Vrijednost** | **Napomene** |
| TS | ‚3Bh’ | Označava neposrednu konvenciju |
| T0 | ‚85h’ | Prisutan TD1; prisutno 5 povijesnih bajtova |
| TD1 | ‚80h’ | Prisutan TD2; koristi se T = 0 |
| TD2 | ‚11h’ | Prisutan TA3; koristi se T = 1 |
| TA3 | ‚XXh’ (min. ‚F0h’) | Veličina informacijskog polja na kartici (IFSC) |
| TH1 do TH5 | ‚XXh’ | Povijesni znakovi |
| TCK | ‚XXh’ | Znak za provjeravanje (bez OR) |

TCS\_308  
Nakon odaziva na povrat u početno stanje (ATR) implicitno se odabire glavna datoteka (MF) i ona postaje tekući imenik.

**3.2.3.    PTS**

TCS\_309  
T = 0 je standardni protokol. Za postavljanje protokola T = 1 uređaj šalje kartici PTS (poznat i kao PPS).

TCS\_310  
Kako su oba protokola T = 0 i T = 1 obavezni, temeljni PTS za izmjenu protokola je obavezan za karticu.

Kako je naznačeno u ISO/IEC 7816-3, PTS se može koristiti za prijelaz na brzine prenosa podataka više od standardne brzine prenosa podataka koju predlaže kartica u ATR (bajt TA(1)), ako postoji.

Za karticu su više brzine prenosa podataka neobvezne.

TCS\_311  
Ako nije podržana niti jedna brzina prenosa podataka osim standardne (ili ako odabrana brzina prenosa podataka nije podržana), kartica ispravno odgovara na PTS prema ISO/IEC 7816-3 ispuštajući bajt PPS1.

Primjeri osnovnih PTS za odabir protokola su sljedeći:

|  |  |  |
| --- | --- | --- |
| **Znak** | **Vrijednost** | **Napomene** |
| PPSS | ‚FFh’ | Znak za početak |
| PPS0 | ‚00h’ ili ‚01h’ | Nema PPS1 do PPS3; ‚00h’ za odabir T0, ‚01h’ za odabir T1 |
| PK | ‚XXh’ | Znak provjere: ‚XXh’ = ‚FFh’ ako je PPS0 = ‚00h’  ‚XXh’ = ‚FEh’ ako je PPS0 = ‚01h’ |

**3.3.   Uslovi pristupa (AC)**

Uslovi pristupa (AC) za naredbe UPDATE\_BINARY i READ\_BINARY su određeni za svaku elementarnu datoteku.

TCS\_312  
AC tekuće datoteke moraju biti zadovoljene prije pristepena datoteci putem tih naredbi.

Definicije raspoloživih uslova pristupa su sljedeće:

* + ALW: Radnja je uvijek moguća i može se provesti bez ograničenja.
  + NEV: Radnja nije moguća nikada.
  + AUT: Pravo koje odgovara uspješnoj vanjskoj autentifikaciji mora biti otvoreno (vrši se naredbom EXTERNAL\_AUTHENTICATE).
  + PRO SM: Naredba se mora odaslati s dodatnim kriptografskim ispitnim zbirem putem sigurnog prenosa poruka (vidjeti Prilog 11.).
  + AUT i PRO-SM: (kombinirani).

Za naredbe obrade (UPDATE\_BINARY i READ\_BINARY) se na kartici mogu postaviti sljedeći uslovi pristupa:

|  |  |  |
| --- | --- | --- |
|  | **UPDATE\_BINARY** | **READ\_BINARY** |
| ALW | Da | Da |
| NEV | Da | Da |
| AUT | Da | Da |
| PRO SM | Da | Ne |
| AUT i PRO SM | Da | Ne |

Uslov pristupa PRO SM nije raspoloživ za naredbu READ\_BINARY. To znači da prisutstvo kriptografske provjere ispitnog zbira za naredbu READ nije nikad obavezno. No korištenjem vrijednosti ‚OC’ za razred, moguće je primijeniti naredbu READ\_BINARY sa sigurnosnim prenosom poruka, kako je opisano u stavu 3.6.2.

**3.4.   Šifriranje podataka**

Kada treba zaštititi povjerljivost podataka za čitanje iz datoteke, datoteka se označava kao ‚šifrirana’. Šifriranje se vrši putem sigurnog prenosa poruka (vidjeti Dodatak 11.).

**3.5.   Pregled šifri naredbi i grešaka**

Naredbe i umašina datoteka su izvedeni i usklađeni sa ISO/IEC 7816-4.

TCS\_313  
Ovaj dio opisuje sljedeće parove naredbi i odgovora APDU:

|  |  |
| --- | --- |
| **Naredba** | **INS** |
| SELECT FILE | A4 |
| READ BINARY | B0 |
| UPDATE BINARY | D6 |
| GET CHALLENGE | 84 |
| VERIFY | 20 |
| GET RESPONSE | C0 |
| PERFORM SECURITY OPERATION:   * VERIFY CERTIFICATE * COMPUTE DIGITAL SIGNATURE * VERIFY DIGITAL SIGNATURE * HASH | 2A |
| INTERNAL AUTHENTICATE | 88 |
| EXTERNAL AUTHENTICATE | 82 |
| MANAGE SECURITY ENVIRONMENT  SETTING A KEY | 22 |
| PERFORM HASH OF FILE | 2A |

TCS\_314  
Statusne riječi SW1 SW2 su uključene u svaku poruku odgovora i označivaju 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 | CX | Pogrešan CHV (PIN). ‚X’ osigurava brojač preostalih pokušaja. |
| 64 | 00 | Greška u izvedbi – Stanje postojane memorije nepromijenjeno. Greška potpunosti. |
| 65 | 00 | Greška u izvedbi – Stanje postojane memorije promijenjeno. |
| 65 | 81 | Greška u izvedbi – Stanje postojane memorije promijenjeno. Greška memorije |
| 66 | 88 | Sigurnosna greška:  pogrešan kriptografski ispitni zbir (prilikom sigurnosnog prenosa poruka) ili  pogrešan certifikat (prilikom provjere certifikata) ili  pogrešan kriptogram (prilikom vanjske autentifikacije) ili  pogrešan potpis (prilikom provjere potpisa) |
| 67 | 00 | Pogrešna dužina (pogrešan Lc ili Le) |
| 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 tekuće EF) |
| 69 | 87 | Nedostaju očekivani podakovni objekti sigurnog prenosa poruka |
| 69 | 88 | Neispravni podakovni objekti sigurnog prenosa poruka |
| 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 van EF) |
| 6C | XX | Pogrešna dužina, SW2 označava točnu dužinu. Podakovno polje ne uzvraća |
| 6D | 00 | Naredbena šifra nije podržana ili nije valjana |
| 6E | 00 | Razred nije podržan |
| 6F | 00 | Ostale greške provjere |

**3.6.   Opis naredbi**

U ovom su poglavlju opisane obavezne naredbe za kartice tahografa.

Dalje predmetne pojedinosti, povezane s obuhvaćenim kriptografskim radnjama su navedene u Dodatku 11. ‚Zajednički sigurnosni mehanizmi’.

Sve naredbe su opisane 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\_315  
Ako se zahtijevaju oba bajta dužine (Lc i Le), opisana naredba se mora podijeliti u dva dijela ako IFD koristi protokol T = 0: IFD šalje naredbu opisanu s P3 = Lc + podaci, a potom šalje naredbu GET\_RESPONSE (vidjeti točku 3.6.6.) uz P3 = Le.

TCS\_316  
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 sa P3 = La za čitanje podataka.

**3.6.1.    Odabir datoteke**

Ova naredba je u skladu s ISO/IEC 7816-4, ali ima ograničenu primjenu u usporedbi s naredbom definisanom u normi.

Naredba SELECT FILE se koristi:

* za odabir aplikacijske DF (obavezan odabir po imenu),
* za odabir elementarne datoteke koja odgovara ID predane datoteke.

**3.6.1.1.   Odabir po nazivu (AID)**

Ova naredba omogućava odabir aplikacijske DF na kartici.

TCS\_317  
Ova naredba može se izvoditi sa svakog mjesta u strukturi datoteke (poslije ATR ili u bilo koje drugo vrijeme).

TCS\_318  
Odabir aplikacije ponovo vraća tekuće sigurnosno okruženje. Nakon izvršenog biranja aplikacije ne bira se više niti jedan javni ključ, a ključ iz prethodne razmjene podataka više nije na raspolaganju za siguran prenos poruka. Gubi se i uslov pristupa AUT.

TCS\_319  
Poruka naredbe

|  |  |  |  |
| --- | --- | --- | --- |
| **Bajt** | **Dužina** | **Vrijednost** | **Opis** |
| CLA | 1 | ‚00h’ |  |
| INS | 1 | ‚A4h’ |  |
| P1 | 1 | ‚A4h’ | Odabir po nazivu (AID) |
| P2 | 1 | ‚0Ch’ | Ne očekuje se nikakav odgovor |
| Lc | 1 | ‚NNh’ | Broj bajtova poslanih na karticu (dužina AID): ‚06h’ za tahografsku aplikaciju |
| #6-#(5 + NN) | NN | ‚XX..XXh’ | AID: ‚FF 54 41 43 48 4F’ za tahografsku aplikaciju |

Za naredbu SELECT FILE nije potreban nikakav odgovor (nema Le u T = 1, ili se u T = 0 ne traži odgovor).

TCS\_320  
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 aplikacija koja odgovara AID, uzvraćeno stanje obrade je ‚6A82’,
* u T = 1, ako je prisutan bajt Le, uzvraćeno stanje obrade je ‚6700’,
* u T = 0, ako se traži odziv poslije naredbe SELECT FILE, uzvraćeno stanje je ‚6900’,
* ako se izabrana aplikacija smatra neispravnom (u atributima datoteke je otkrivena greška potpunosti), uzvraćeno stanje obrade je ‚6400’ ili ‚6581’.

**3.6.1.2.   Odabir elementarne datoteke korištenjem njenog identifikatora datoteke**

TCS\_321  
Poruka naredbe

|  |  |  |  |
| --- | --- | --- | --- |
| **Bajt** | **Dužina** | **Vrijednost** | **Opis** |
| CLA | 1 | ‚00h’ |  |
| INS’ | 1 | ‚A4h’ |  |
| P1 | 1 | ‚02h’ | Izbor EF u okviru tekuće DF |
| P2 | 1 | ‚0Ch’ | Ne očekuje se nikakav odgovor |
| Lc | 1 | ‚02h’ | Broj bajta poslanih na karticu |
| #6-#7 | 2 | ‚XXXXh’ | Identifikator datoteke |

Za naredbu SELECT FILE nije potreban nikakav odgovor (Kod T = 1 nema Le, ili se ne traži odgovor kod T = 0).

TCS\_322  
Poruka odgovora (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 FILE, uzvraćeno stanje je ‚6900’
* ako se izabrana datoteka smatra neispravnom (u atributima datoteke je otkrivena greška potpunosti), uzvraćeno stanje je ‚6400’ ili ‚6581’.

**3.6.2.    Binarno čitanje**

Ova naredba je u skladu s ISO/IEC 7816-4, ali ima ograničenu primjenu u usporedbi s naredbom utvrđenoj u normi.

Naredba Read Binary se koristi za čitanje podataka iz transparentne datoteke.

Odgovor kartice se sastoji od uzvraćanja pročitanih podataka koji se mogu neobvezno zatvoriti u strukturu sigurnog čitanja poruke.

TCS\_323  
Ova naredba se može izvesti samo ako sigurnosni status zadovoljava sigurnosne atribute utvrđene za EF za funkciju READ:

**3.6.2.1.   Naredba bez sigurnog prenosa poruke**

Ova naredba omogućava IFD-u čitanje podataka iz trenutno odabrane EF bez sigurnog prenosa poruka.

TCS\_324  
Čitanje podataka iz datoteke označene ‚Encrypted’ nije moguće preko ove naredbe

TCS\_325  
Poruka naredbe

|  |  |  |  |
| --- | --- | --- | --- |
| **Bajt** | **Dužina** | **Vrijednost** | **Opis** |
| CLA | 1 | ‚00h’ | Ne traži se siguran prenos poruke |
| INS | 1 | ‚B0h’ |  |
| P1 | 1 | ‚XXh’ | Pomak u bajtima od početka datoteke: najznačajniji bajt |
| P2 | 1 | ‚XXh’ | Pomak u bajtima od početka datoteke: najmanje značajan bajt |
| Le | 1 | ‚XXh’ | Dužina očekivanih podataka, broj bajtova koje treba pročitati |

Napomena: bit 8 u P1 mora biti postavljen na 0.

TCS\_326  
Poruka odgovora

|  |  |  |  |
| --- | --- | --- | --- |
| **Bajt** | **Dužina** | **Vrijednost** | **Opis** |
| #1-#X | X | ‚XX..XXh’ | Čitanje podataka |
| SW | 2 | ‚XXXXh’ | Statusne riječi (SW1, SW2) |

* Ako je naredba uspješna kartica uzvraća ‚9000’,
* ako EF nije izabrana, uzvraćeno stanje obrade je ‚6986’,
* ako kontrola pristupa odabrane datoteke nije zadovoljena, naredba se prekida s ‚6982’,
* ako pomak ne odgovara veličini EF (pomak > veličina EF), uzvraćeno stanje obrade je ‚6B00’,
* ako veličina podataka koje treba pročitati ne odgovara veličini EF (pomak + Le > veličina EF), stanje obrade je ‚6700’ ili ‚6Cxx’, pri čemu je ‚xx’ točna dužina,
* ako je otkrivena greška potpunosti unutar atributa datoteke, kartica će datoteku smatrati neispravnom i nepopravljivom, te je uzvraćeno stanje obrade ‚6400’ ili ‚6581’,
* ako je otkrivena greška potpunosti u sačuvanim podacima, kartica uzvraća tražene podatke, a uzvraćeno stanje obrade je ‚6281’.

**3.6.2.2.   Naredba sa sigurnim prenosom poruke**

Ova naredba omogućava IDF-u čitanje podataka iz trenutno odabranog EF uz siguran prenos poruka radi povjere potpunosti primljenih podataka i zaštite povjerljivosti podataka u slučaju da je EF označena s ‚Encrypted’

TCS\_327  
Naredbena poruka

|  |  |  |  |
| --- | --- | --- | --- |
| **Bajt** | **Dužina** | **Vrijednost** | **Opis** |
| CLA | 1 | ‚0Ch’ | Traži se siguran prenos poruka |
| INS | 1 | ‚B0h’ | INS |
| P1 | 1 | ‚XXh’ | P1 (pomak u bajtima od početka datoteke): najznačajniji bajt |
| P2 | 1 | ‚XXh’ | P2 (pomak u bajtima od početka datoteke): najmanje značajan bajt |
| Lc | 1 | ‚09h’ | Dužina ulaznih podatka za siguran prenos poruka |
| #6 | 1 | ‚97h’ | TLE: oznaka za određivanje očekivane dužine specifikacije |
| #7 | 1 | ‚01h’ | TLE: oznaka očekivane dužine |
| #8 | 1 | ‚NNh’ | Određivanje očekivane dužina (originalni Le): broj bajtova koje treba pročitati |
| #9 | 1 | ‚8Eh’ | TCC: oznaka za kriptografski kontrolni zbir |
| #10 | 1 | ‚04h’ | LCC: dužina sljedećeg kriptografskog kontrolnog zbira |
| #11-#14 | 4 | ‚XX..XXh’ | Kriptografski kontrolni zbir (4 najznačajnija bajta) |
| Le | 1 | ‚00h’ | Utvrđeno u ISO/IEC 7816-4 |

TCS\_328  
Poruka odgovora na poruku ako EF nije označen s ‚Encrypted’ i ako je format ulaza za siguran prenos poruka tačan:

|  |  |  |  |
| --- | --- | --- | --- |
| **Bajt** | **Dužina** | **Vrijednost** | **Opis** |
| #1 | 1 | ‚81h’ | TPV: oznaka za nešifrirane podatke |
| #2 | L | ‚NNh’ ili ‚81 NNh’ | LPV: dužina uzvraćenih podataka (= izvorni Le)  L je 2 bajta, ako je LPV < 127 bajta |
| #(2 + L)-#(1 + L+NN) | NN | ‚XX..XXh’ | Vrijednost nešifriranih podataka |
| #(2 + L+NN) | 1 | ‚8Eh’ | TCC: oznaka za kriptografski kontrolni zbir |
| #(3 + L+NN) | 1 | ‚04h’ | LCC: dužina sljedećeg kriptografskog kontrolnog zbira |
| #(4 + L+NN)-#(7 + L+NN) | 4 | ‚XX..XXh’ | Kriptografski kontrolni zbir (4 najznačajnija bajta) |
| SW | 2 | ‚XXXXh’ | Statusne riječi (SW1, SW2) |

TCS\_329  
Odgovor na poruku ako je EF označen kao ‚Encrypted’ i ako je ulazni format za siguran prenos poruka tačan:

|  |  |  |  |
| --- | --- | --- | --- |
| **Bajt** | **Dužina** | **Vrijednost** | **Opis** |
| #1 | 1 | ‚87h’ | TPI CG: oznaka za šifrirane podatke (kriptogram) |
| #2 | L | ‚MMh’ ili ‚81 MMh’ | LPI CG: dužina uzvraćenih šifriranih podataka (različita od izvorne Le naredbe zbog popunjenja)  L je 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 | ‚8Eh’ | TCC: oznaka za kriptografski kontrolni zbir |
| #(3 + L+MM) | 1 | ‚04h’ | LCC: dužina sljedećeg kriptografskog kontrolnog zbira |
| #(4 + L+MM)-#(7 + L+MM) | 4 | ‚XX..XXh’ | Kriptografski kontrolni zbir (4 najznačajnija bajta) |
| SW | 2 | ‚XXXXh’ | Statusne riječi (SW1, SW2) |

Uzvraćeni šifrirani podaci sadrže prvi bajt koji prikazuje korišteni režim popunjenja. Za tahografsku primjenu indikator popunjenja uvijek ima vrijednost ‚01h’, što znači da je primijenjen režim popunjenja utvrđen u ISO/IEC 7816-4 (jedan bajt koji ima vrijednost ‚80h’, iza kojeg slijedi nekoliko nultih bajtova: metoda 2 po ISO/IEC 9797).

Stanja ‚normalne’ obrade, opisana u naredbi READ BINARY bez sigurnog prenosa poruka (vidjeti točku 3.6.2.1.), mogu se uzvratiti tako da se koriste gore opisane strukture poruka odgovora, pod oznakom ‚99h’ (opisano u TCS\_335).

Osim toga mogu se dogoditi i neke greške posebno vezane uz siguran prenos poruka. U tom slučaju se stanje obrade jednostavno uzvraća bez uključivanja strukture sigurnog prenosa poruka.

TCS\_330  
Poruka odgovora kod netočnog ulaznog formata za siguran prenos poruka

|  |  |  |  |
| --- | --- | --- | --- |
| **Bajt** | **Dužina** | **Vrijednost** | **Opis** |
| SW | 2 | ‚XXXXh’ | Statusne riječi (SW1, SW2) |

* Ako ne postoji ključ tekuće razmjene podataka, uzvraća se stanje obrade ‚6A88’. To se može dogoditi ako još nije napravljen ključ razmjene podataka ili ako je valjanost ključa razmjene podataka istekla (u tom slučaju IFD mora ponovo pokrenuti postupak međusobne autentifikacije za postavljanje novog ključa za razmjenu podataka).
* Ako neki očekivani podakovni objekti (gore navedeni) nedostaju u formatu sigurnog prenosa poruka, uzvraća se stanje obrade ‚6987’: ova greška se događa ako nema očekivane oznake ili ako naredbodavni sadržaj nije pravilno izrađen.
* Ako neki podakovni objekti nisu tačni, uzvraćeno stanje obrade je ‚6988’: ova greška se događa ako su prisutne sve tražene oznake, ali su neke dužine različite od onih očekivanih.
* Ako ne uspije provjera kriptografskog kontrolnog zbira, uzvraćeno stanje obrade je ‚6688’.

**3.6.3.    Binarno ažuriranje**

Ova naredba je u skladu s ISO/IEC 7816-4, ali ima ograničenu primjenu u usporedbi s naredbom utvrđenoj u normi.

Poruka naredbe UPDATE BINARY započinje ažuriranjem (brisanje + pisanje) bitova koji su već sadržani u binarnom obliku EF, s bitovima danim u naredbi APDU.

TCS\_331  
Naredba se može izvoditi samo ako sigurnosni status zadovoljava sigurnosne atribute utvrđene za EF za funkciju UPDATE (Ako pristubna kontrola funkcije UPDATE obuhvaća PRO SM, tada u naredbu mora biti dodan siguran prenos poruka).

**3.6.3.1.   Naredba bez sigurnog prenosa poruke**

Ova naredba omogućava IFD-u upisivanje podataka u trenutno odabran EF bez da kartica provjerava potpunost primljenih podataka. Ovaj nešifrirani način je dopušten samo ako predmetna datoteka nije označena kao ‚Encrypted".

TCS\_332  
Poruka naredbe

|  |  |  |  |
| --- | --- | --- | --- |
| **Bajt** | **Dužina** | **Vrijednost** | **Opis** |
| CLA | 1 | ‚00h’ | Ne traži se siguran prenos poruka |
| INS | 1 | ‚D6h’ |  |
| P1 | 1 | ‚XXh’ |  |
| P2 | 1 | ‚XXh’ | Pomak u bajtovima od početka datoteke: najmanje značajan bajt |
| Lc | 1 | ‚NNh’ | Lc: dužina podataka koji se ažuriraju. Broj bajovta koje treba upisati |
| #6-#(5 + NN) | NN | ‚XX..XXh’ | Podaci koje treba upisati |

Napomena bit 8 u P1 mora biti postavljen na 0.

TCS\_333  
Poruka odgovora

|  |  |  |  |
| --- | --- | --- | --- |
| **Bajt** | **Dužina** | **Vrijednost** | **Opis** |
| SW | 2 | ‚XXXXh’ | Statusne riječi (SW1, SW2) |

* Ako je naredba uspješna kartica uzvraća ‚9000’,
* ako nije izabran EF, uzvraćeno stanje obrade je ‚6986’,
* ako nije udovoljeno pristubnoj kontroli za izabranu datoteku, naredba se prekida s ‚6982’,
* ako pomak nije kompatibilan s veličinom EF (pomak > veličina EF), uzvraćeno stanje obrade je ‚6B00’,
* ako veličina podataka koje treba upisati nije u skladu s veličinom EF (Offset + Lc > EF size) pomak + Le > veličina EF), uzvraćeni status obrade je ‚6700’,
* ako je otkrivena greška potpunosti atributa datoteke, kartica smatra da je datoteka neispravna i nepopravljiva, a uzvraćeno stanje obrade je ‚6400’ ili ‚6500’,
* ako zapisivanje nije uspješno, uzvraćeno stanje obrade je ‚6581’.

**3.6.3.2.   Naredba sa sigurnim prenosom poruke**

Ova naredba omogućava IFD-u upisivanje podataka u trenutno izabranu EF, a kartica provjerava potpunost primljenih podataka. Obzirom da nije tražena povjerljivost podataka, podaci nisu šifrirani.

TCS\_334  
Poruka naredbe

|  |  |  |  |
| --- | --- | --- | --- |
| **Bajt** | **Dužina** | **Vrijednost** | **Opis** |
| CLA | 1 | ‚0Ch’ | Siguran prenos poruka. Zatraženo |
| INS | 1 | ‚D6h’ | INS |
| P1 | 1 | ‚XXh’ | Pomak u bajtovima od početka datoteke: najznačajniji bajt |
| P2 | 1 | ‚XXh’ | Pomak u bajtovima od početka datoteke: najmanje značajan bajt |
| Lc | 1 | ‚XXh’ | Dužina polja zaštićenih podataka |
| #6 | 1 | ‚81h’ | TPV: oznaka za vrijednost nešifriranih podataka |
| #7 | L | ‚NNh’ ili ‚81 NNh’ | LPV: dužina odaslanih podataka  L je 2 bajta, ako je LPV > 127 bajtova |
| #(7 + L)-#(6 + L+NN) | NN | ‚XX..XXh’ | Vrijednost nešifriranih podataka (koje treba upisati) |
| #(7 + L+NN) | 1 | ‚8Eh’ | TCC: oznaka za kriptografski kontrolni zbir |
| #(8 + L+NN) | 1 | ‚04h’ | LCC: dužina sljedećeg kriptografskog kontrolnog zbira |
| #(9 + L+NN)-#(12 + L+NN) | 4 | ‚XX..XXh’ | Kriptografski kontrolni zbir (4 najznačajnija bajta) |
| Le | 1 | ‚00h’ | Kako je u utvrđeno u ISO/IEC 7816-4 |

TCS\_335  
Poruka odgovor pri pravilnom ulaznom formatu sigurnog prenosa poruka

|  |  |  |  |
| --- | --- | --- | --- |
| **Bajt** | **Dužina** | **Vrijednost** | **Opis** |
| #1 | 1 | ‚99h’ | TSW: oznaka za statusne riječi (koje treba zaštiti sa CC) |
| #2 | 1 | ‚02h’ | LSW: dužina uzvraćenih statusnih riječi |
| #3-#4 | 2 | ‚XXXXh’ | Statusne riječi (SW1, SW2) |
| #5 | 1 | ‚8Eh’ | TCC: oznaka za kriptografski kontrolni zbir |
| #6 | 1 | ‚04h’ | LCC: dužina sljedećeg kriptografskog kontrolnog zbira |
| #7-#10 | 4 | ‚XX..XXh’ | Kriptografski kontrolni zbir (4 najznačajnija bajta) |
| SW | 2 | ‚XXXXh’ | Statusne riječi (SW1, SW2) |

‚Redovna’ stanja obrade opisana za naredbu UPDATE BINARY bez sigurnog prenosa poruka (vidjeti točku 3.6.3.1.) se mogu uzvratiti tako da se koristi gore opisana struktura poruka odgovora.

Osim toga, mogu se dogoditi i neke greške karakteristične za siguran prenos poruka. U tom slučaju se stanje obrade jednostavno vraća bez uključivanja strukture sigurnog prenosa poruka.

TCS\_336  
Poruka odgovora ako je u sigurnom prenosu poruka došlo do greške

|  |  |  |  |
| --- | --- | --- | --- |
| **Bajt** | **Dužina** | **Vrijednost** | **Opis** |
| SW | 2 | ‚XXXXh’ | Statusne riječi (SW1, SW2) |

* Ako nema ključa tekuće razmjene podataka, uzvraćeno stanje obrade je ‚6A88’,
* ako neki očekivani podakovni objekti (gore navedeni) nedostaju u formatu sigurnog prenosa poruka, uzvraća se stanje obrade ‚6987’: ova greška se događa ako nedostaje očekivana oznaka ili ako naredbodavni sadržaj nije pravilno sastavljen,
* ako su neki podakovni objekti neispravni, uzvraćeno stanje obrade je ‚6988’: ova se greška događa ako postoje sve tražene oznake, ali su neke dužine različite od očekivanih,
* ako ne uspije provjera kriptografskih kontrolnih zbireva, stanje obrade je ‚6688’.

**3.6.4.    Traži zahtjev za lozinku**

Ova naredba je u skladu s ISO/IEC 7816-4, ali ima ograničenu primjenu u usporedbi s naredbom utvrđenom u normi.

Naredbom GET CHALLENGE se od kartice traži izdavanje zahtjeva za lozinku radi korištenja u sigurnosnom postubku u kojem se kartici šalju kriptogram ili šifrirani podaci.

TCS\_337  
Zahtjev za lozinku kojega izdaje kartica vrijedi samo za sljedeću naredbu koja koristi zahtjev za lozinku poslan kartici.

TCS\_338  
Poruka naredbe

|  |  |  |  |
| --- | --- | --- | --- |
| **Bajt** | **Dužina** | **Vrijednost** | **Opis** |
| CLA | 1 | ‚00h’ | CLA |
| INS | 1 | ‚84h’ | INS |
| P1 | 1 | ‚00h’ | P1 |
| P2 | 1 | ‚00h’ | P2 |
| Le | 1 | ‚08h’ | Le (dužina očekivanog zahtjeva za lozinku) |

TCS\_339  
Poruka odgovora

|  |  |  |  |
| --- | --- | --- | --- |
| **Bajt** | **Dužina** | **Vrijednost** | **Opis** |
| #1-#8 | 8 | ‚XX..XXh’ | Zahtjev za lozinku |
| 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 tačni, stanje obrade je ‚6A86’.

**3.6.5.    Provjeri**

Ova naredba je u skladu s ISO/IEC 7816-4, ali ima ograničenu primjenu u usporedbi s naredbom utvrđenom u normi.

Naredba Provjeri na kartici započinje usporedbu između CHV (PIN) podataka koji su poslani iz naredbe sa referentnih CHV arhiviranih na kartici.

Napomena: PIN koji unosi korisnik mora biti desno popunjen s bajtima ‚FFh’ do dužine od 8 bajtova IFD-a.

TCS\_340  
Ako je naredba uspješna, otvaraju se prava koja odgovaraju predočenju CHV, a brojač preostalih pokušaja CHV se pokreće iznova.

TCS\_341  
Neuspješna usporedba se registrira na kartici kako bi se ograničio broj daljnjih pokušaja korištenja referentnog CHV.

TCS\_342  
Poruka naredbe

|  |  |  |  |
| --- | --- | --- | --- |
| **Bajt** | **Dužina** | **Vrijednost** | **Opis** |
| CLA | 1 | ‚00h’ | CLA |
| INS | 1 | ‚20h’ | INS |
| P1 | 1 | ‚00h’ | P1 |
| P2 | 1 | ‚00h’ | P2 (provjereni CHV je implicitno poznat) |
| Lc | 1 | ‚08h’ | Dužina odaslane šifre CHV |
| #6-#13 | 8 | ‚XX..XXh’ | CHV |

TCS\_343  
Poruka odgovora

|  |  |  |  |
| --- | --- | --- | --- |
| **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 se smanjuje i uzvraća se status obrade ‚63CX’ (X > 0, pri čemu je X jednak brojaču preostalih pokušaja CHV. X = ‚F’, brojač preostalih pokušaja CHV je veći od ‚F’),
* ako se referentni CHV smatra neispravnim, uzvraćeno stanje obrade je ‚6400’ ili ‚6581’.

**3.6.6.    Traži odgovor**

Ova naredba je u skladu sa 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 izdana neposredno nakon naredbe za pripremu podataka, inače se podaci gube. Nakon izvršenja naredbe GET\_RESPONSE (osim ako nastubi greška ‚61xx’ ili ‚6Cxx’, vidjeti dolje), ranije pripremljeni podaci više nisu dostubni.

TCS\_344  
Poruka naredbe

|  |  |  |  |
| --- | --- | --- | --- |
| **Bajt** | **Dužina** | **Vrijednost** | **Opis** |
| CLA | 1 | ‚00h’ |  |
| INS | 1 | ‚C0h’ |  |
| P1 | 1 | ‚00h’ |  |
| P2 | 1 | ‚00h’ |  |
| Le | 1 | ‚XXh’ | Broj očekivanih bajtova |

TCS\_345  
Poruka odgovora

|  |  |  |  |
| --- | --- | --- | --- |
| **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 prekorači 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 dostubni 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 dostubni za iduću naredbu GET\_RESPONSE.
* Ako naredba nije podržana (protokol T = 1), kartica uzvraća ‚6D00’.

**3.6.7.    PSO: provjeri certifikat**

Ova naredba je u skladu s ISO/IEC 7816-8, ali ima ograničenu primjenu u usporedbi s naredbom utvrđenom u normi.

Naredbu VERIFY CERTIFICATE kartica koristi za dobivanje javnog ključa i provjeru njegove važnosti.

TCS\_346  
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) za MSE naredbe (vidjeti točku 3.6.10.) tako da koristi svoj identifikator ključa.

TCS\_347  
U svakom slučaju, naredba VERIFY CERTIFICATE koristi javni ključ koji je ranije odabran u sklopu MSE naredbe za otvaranje certifikata. Ovaj javni ključ mora biti onaj države članice ili evropski.

TCS\_348  
Poruka naredbe

|  |  |  |  |
| --- | --- | --- | --- |
| **Bajt** | **Dužina** | **Vrijednost** | **Opis** |
| CLA | 1 | ‚00h’ | CLA |
| INS | 1 | ‚2Ah’ | Izvedba sigurnosne operacije |
| P1 | 1 | ‚00h’ | P1 |
| P2 | 1 | ‚AEh’ | P2: podaci koji nisu šifrirani po BER-TLV (ulančavanje podakovnih elemenata) |
| Lc | 1 | ‚C2h’ | Lc: dužina certifikata, 194 bajtova |
| #6-#199 | 194 | ‚XX..XXh’ | Certifikat: ulančavanje podakovnih elemenata (opisano u Dodatku 11.) |

TCS\_349  
Poruka odgovora

|  |  |  |  |
| --- | --- | --- | --- |
| **Bajt** | **Dužina** | **Vrijednost** | **Opis** |
| SW | 2 | ‚XXXXh’ | Statusne riječi (SW1, SW2) |

* Ako je naredba uspješna, kartica uzvraća ‚9000’,
* ako provjera certifikata nije uspjela, uzvraća se stanje obrade ‚6688’. Postupak provjere i otvaranja certifikata opisan je u Dodatku 11.,
* ako u sigurnosnom okruženju nije prisutan javni ključ, uzvraća se stanje obrade ‚6A88’,
* ako se izabrani javni ključ (uporabljen za otvaranje certifikata) smatra oštećenim, uzvraćeno stanje obrade je ‚6400’ ili ‚6581’,
* ako je izabrani javni ključ (uporabljen za otvaranje certifikata) CHA.LSB (CertificateHolderAuthorisation.equipmentType) različit od ‚00’ (odnosno nije onaj države članice ili evropski), uzvraćeno stanje obrade je ‚6985’.

**3.6.8.    Unutarnja autentifikacija**

Ova naredba je u skladu s ISO/IEC 7816-4.

Primjenom INTERNAL AUTHENTICATE naredbe, IFD može autentifikovati karticu.

Postupak autentifikacije je opisan je u Dodatku 11. Obuhvaća sljedeća očitovanja:

TCS\_350  
Naredba INTERNAL AUTHENTICATE koristi privatni ključ kartice (izabran implicitno) za potpisivanje autentifikacijskih podataka, uključujući K1 (prvi element za dogovor o ključu za razmjenu podataka) i RND1, te koristi trenutno izabrani javni ključ (putem posljednje narede MSE) za šifriranje potpisa i oblikovanje autentifikacijskog tokena (podrobnije u Dodatku 11.).

TCS\_351  
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 kartici |
| #6-#13 | | 8 | ‚XX..XXh’ | Poziv uporabljen za autentifikaciju kartice |
| #14-#21 | 8 | ‚XX..XXh’ | VU.CHR (vidjeti Dodatak 11.) |
| Le | 1 | ‚80h’ | Dužina podataka koji se očekuju od kartice |

TCS\_352  
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 nema javnog ključa, uzvraćeno stanje obrade je ‚6A88’,

— ako u sigurnosnom okruženju nema privatnog ključa, uzvraćeno stanje obrade je ‚6A88’,

— ako VU.CHR ne odgovara identifikatoru trenutnog javnoga ključa, uzvraćeno stanje obrade je ‚6A88’,

— ako se izabrani privatni ključ smatra neispravnim, uzvraćeno stanje obrade je ‚6400’ ili ‚6581’.

TCS\_353  
Ako je naredba INTERNAL\_AUTHENTICATE uspješna, trenutačni ključ razmjene podataka, ako postoji, se briše i više nije dostuban. Za novi ključ razmjene podataka naredba EXTERNAL\_AUTHENTICATE treba biti uspješno izvršena.

**3.6.9.    Spoljna autentifikacija**

Ova naredba je u skladu s ISO/IEC 7816-4.

S naredbom EXTERNAL AUTHENTICATE kartica može autentifikovati IFD.

Postupak autentifikacije je opisan je u Dodatku 11. Sadrži sljedeća očitovanja:

TCS\_354  
Naredba GET CHALLENGE mora neposredno prethoditi naredbi EXTERNAL\_AUTHENTICATE. Kartica izdaje zahtjev za lozinku vana (RND3).

TCS\_355  
Provjera kriptograma koristi RND3 (zahtjev za lozinku koji šalje kartica), privatni ključ kartice (implicitno izabran) i javni ključ prethodno izabran naredbom MSE.

TCS\_356  
Kartica provjerava kriptogram; ako je tačan, otvara se pristubni uslov AUT.

TCS\_357  
Kriptogram ulaznih podataka nosi drugi element za dogovor o ključu razmjene podataka K2.

TCS\_358  
Poruka naredbe

|  |  |  |  |
| --- | --- | --- | --- |
| **Bajt** | **Dužina** | **Vrijednost** | **Opis** |
| CLA | 1 | ‚00h’ | CLA |
| INS | 1 | ‚82h’ | INS |
| P1 | 1 | ‚00h’ | P1 |
| P2 | 1 | ‚00h’ | P2 (javni ključ kojega treba koristiti je implicitno poznat, a prethodno je postavljen naredbom MSE) |
| Lc | 1 | ‚80h’ | Lc (dužina podataka poslanih na karticu) |
| #6-#133 | 128 | ‚XX..XXh’ | Kriptogram (vidjeti Dodatak 11.) |

TCS\_359  
Poruka odgovora

|  |  |  |  |
| --- | --- | --- | --- |
| **Bajt** | **Dužina** | **Vrijednost** | **Opis** |
| SW | 2 | ‚XXXXh’ | Statusne riječi (statusne riječi (SW1, SW2)) |

— Ako je naredba uspješna kartica uzvraća ‚9000’,

— ako u sigurnosnom okruženju nema javnog ključa, uzvraća se ‚6A88’,

— ako CHA trenutno postavljenog javnog ključa nije ulančavanje AID tahografskog programa i tipa opreme jedinice vozila, uzvraćeno stanje obrade je ‚6F00’ (vidjeti Dodatak 11.),

— ako u sigurnosnom okruženju nije prisutan nikakav privatni ključ, uzvraćeno stanje obrade je ‚6A88’,

— ako je provjera kriptograma pogrešna, uzvraćeno stanje obrade je ‚6688’,

— ako ovoj naredbi neposredno ne prethodi naredba GET CHALLENGE, uzvraćeno stanje obrade je ‚6985’,

— ako se izabrani privatni ključ smatra neispravnim, uzvraćeno stanje obrade je ‚6400’ ili ‚6581’.

TCS\_360  
Ako je naredba EXTERNAL AUTHENTICATE uspješna, i ako je prvi dio ključa razmjene podataka dostuban iz uspješnog ranije izvršenog INTERNAL AUTHENTICATE, ključ razmjene podataka je postavljen za buduće naredbe uz siguran prenos poruka.

TCS\_361  
Ako prvi dio ključa razmjene podataka nije dostuban iz prethodne naredbe INTERNAL AUTHENTICATE, onda se drugi dio ključa razmjene podataka, koji šalje IFD, ne arhivira na kartici. Tim se mehanizmom osigurava da se postupak međusobne autentifikacije obavlja redoslijedom utvrđenim u Dodatku 11.

**3.6.10.    Upravljanje sigurnosnim okruženjem**

Ova se naredba koristi za postavljanje javnoga ključa za potrebe autentifikacije.

Ova je naredba u skladu s normom ISO/IEC 7816-8. Primjena ove naredbe je ograničena u smislu odgovarajuće norme.

TCS\_362  
Ključ naveden u podakovnom polju MSE vrijedi za svaku datoteku DF tahografa.

TCS\_363  
Ključ naveden u podakovnom polju MSE ostaje tekući javni ključ do sljedeće ispravne naredbe MSE.

TCS\_364  
Ako navedeni ključ (već) nije na kartici, sigurno okruženje ostaje nepromijenjeno.

TCS\_365  
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 u vezi digitalnog potpisa) |
| Lc | 1 | ‚0Ah’ | Lc: dužina idućeg podakovnog polja |
| #6 | 1 | ‚83h’ | Oznaka za navođenje javnoga ključa u asimetričnim slučajevima |
| #7 | 1 | ‚08h’ | Dužina navedenog ključa (identifikatora ključa) |
| #8-#15 | 08h | ‚XX..XXh’ | Identifikator ključa utvrđen u Dodatku 11. |

TCS\_366  
Poruka odgovora

|  |  |  |  |
| --- | --- | --- | --- |
| **Bajt** | **Dužina** | **Vrijednost** | **Opis** |
| SW | 2 | ‚XXXXh’ | Statusne riječi (SW1, SW2) |

— Ako je naredba uspješna kartica uzvraća ‚9000’,

— ako navedeni ključ nije na kartici, uzvraćeno stanje obrade je ‚6A88’,

— ako nedostaju neki očekivani podakovni objekti u formatu sigurnog prenosa poruka, uzvraćeno stanje obrade je ‚6987’. To se može dogoditi ako nema oznake ‚83h’,

— ako su neki podakovni objekti netačni, uzvraćeno stanje obrade je ‚6988’. To se može dogoditi ako dužina identifikatora ključa nije ‚08h’,

— ako se izabrani ključ smatra neispravnim, uzvraćeno stanje obrade je ‚6400’ ili ‚6581’.

**3.6.11.    PSO: funkcija kompresije podataka**

Ova naredba služi za prenos na karticu rezultata proračuna kompresije podataka. Ova se naredba koristi za provjeru digitalnog potpisa.

Vrijednost funkcije kompresije se arhivira u EEPROM za iduću naredbu provjere digitalnog potpisa.

Ova naredba je u skladu s normom ISO/IEC 7816-8. Primjena ove naredbe je ograničena u odnosu na odgovarajuću normu.

TCS\_367  
Poruka naredbe

|  |  |  |  |
| --- | --- | --- | --- |
| **Bajt** | **Dužina** | **Vrijednost** | **Opis** |
| CLA | 1 | ‚00h’ | CLA |
| INS | 1 | ‚2Ah’ | Izvedba sigurnosne operacije |
| P1 | 1 | ‚90h’ | Vraćanje šifre funkcije kompresije podataka |
| P2 | 1 | ‚A0h’ | Oznaka: podakovno polje sadrži DO potreban za kompresiju podataka |
| Lc | 1 | ‚16h’ | Dužina Lc narednog podakovnog polja |
| #6 | 1 | ‚90h’ | Oznaka za šifru funkcije kompresije podataka |
| #7 | 1 | ‚14h’ | Dužina šifre funkcije kompresije podataka |
| #8-#27 | 20 | ‚XX..XXh’ | šifra funkcije kompresije |

TCS\_368  
Poruka odgovora

|  |  |  |  |
| --- | --- | --- | --- |
| **Bajt** | **Dužina** | **Vrijednost** | **Opis** |
| SW | 2 | ‚XXXXh’ | Statusne riječi (SW1, SW2) |

— Ako je naredba uspješna kartica uzvraća ‚9000’,

— ako nedostaju neki očekivani podakovni objekti (gore navedeni), uzvraća se stanje obrade ‚6987’. To se može dogoditi ako nema jedne od oznaka ‚90h’,

— ako neki podakovni objekti nisu tačni, uzvraćeno stanje obrade je ‚6988’. Ova se greška javlja ako postoji tražena oznaka, ali dužine različite od ‚14h’.

**3.6.12.    Komprimiraj datoteku**

Ova naredba nije u skladu s ISO/IEC 7816-8. Stoga bajt CLA ove naredbe ukazuje da slijedi vlasnička uporaba PERFORM SECURITY OPERATION/HASH.

TCS\_369  
Naredba izvrši kompresiju datoteke se koristi za komprimiranje podakovnog područja trenutno izabranog transparentnog EF.

TCS\_370  
Rezultat postubka komprimiranja se sprema na kartici. Nakon toga se može koristiti za ishođenje digitalnog potpisa datoteke korištenjem naredbe PSO-COMPUTE\_DIGITAL\_ SIGNATURE. Ovaj rezultat ostaje na raspolaganju za naredbu COMPUTE DIGITAL SIGNATURE do sljedeće uspješne naredbe Perform Hash of File.

TCS\_371  
Poruka naredbe

|  |  |  |  |
| --- | --- | --- | --- |
| **Bajt** | **Dužina** | **Vrijednost** | **Opis** |
| CLA | 1 | ‚80h’ | CLA |
| INS | 1 | ‚2Ah’ | Izvedba sigurnosne operacije |
| P1 | 1 | ‚90h’ | Oznaka: kompresija |
| P2 | 1 | ‚00h’ | P2: kompresija podataka trenutno odabrane transparentne datoteke |

TCS\_372  
Poruka odgovora

|  |  |  |  |
| --- | --- | --- | --- |
| **Bajt** | **Dužina** | **Vrijednost** | **Opis** |
| SW | 2 | ‚XXXXh’ | Statusne riječi (SW1, SW2) |

— Ako je naredba uspješna kartica uzvraća ‚9000’,

— ako nije izabrana niti jedna aplikacija, uzvraća se stanje obrade ‚6985’,

— ako se izabrani EF smatra neispravnim (greške potpunosti atributa datoteke ili sačuvanih podataka), uzvraćeno stanje obrade je ‚6400’ ili ‚6581’,

— ako izabrana datoteka nije transparentna, uzvraćeno stanje obrade je ‚6986’.

**3.6.13.    PSO: proračunaj digitalni potpis**

Ova se naredba koristi za proračun digitalnog potpisa iz šifre ranije proračunate funkcije kompresije podataka (vidjeti točku 3.6.12 PERFORM HASH of FILE).

Ova naredba je u skladu s normom ISO/IEC 7816-8. Primjena ove naredbe je ograničena u smislu predmetne norme.

TCS\_373  
Za proračun digitalnog potpisa se koristi privatni ključ kartice koji je kartici implicitno poznat.

TCS\_374  
Kartica izvodi digitalni potpis korištenjem metode popunjenja, u skladu sa PKCS1 (za pojedinosti vidjeti Dodatak 11.).

TCS\_375  
Poruka naredbe

|  |  |  |  |
| --- | --- | --- | --- |
| **Bajt** | **Dužina** | **Vrijednost** | **Opis** |
| CLA | 1 | ‚00h’ | CLA |
| INS | 1 | ‚2Ah’ | Izvedba sigurnosne radnje |
| P1 | 1 | ‚9Eh’ | Digitalni potpis koji treba uzvratiti |
| P2 | 1 | ‚9Ah’ | Oznaka: podakovno polje sadrži podatke koje treba potpisati. Ako nije obuhvaćeno podakovno polje, pretpostavlja se da su podaci već na kartici (komprimiranje datoteke). |
| Le | 1 | ‚80h’ | Dužina očekivanog potpisa |

TCS\_376  
Poruka odgovora

|  |  |  |  |
| --- | --- | --- | --- |
| **Bajt** | **Dužina** | **Vrijednost** | **Opis** |
| #1-#128 | 128 | ‚XX..XXh’ | Potpis prethodno proračunate funkcije komprimiranja |
| SW | 2 | ‚XXXXh’ | Statusne riječi (SW1, SW2) |

— Ako je naredba uspješna, kartica uzvraća ‚9000’,

— ako se implicitno izabrani privatni ključ smatra neispravnim, uzvraćeno stanje obrade je ‚6400’ ili ‚6581’.

**3.6.14.    PSO: provjeri digitalni potpis**

Ova naredba služi za provjeravanje digitalnog potpisa koji se pruža kao ulazni podatak, prema PKCS1 poruci, čija funkcija kompresije je poznata kartici. Kartica implicitno poznaje algoritam potpisa.

Ova naredba je u skladu s ISO/IEC 7816-8. Primjena ove naredbe je ograničena u usporedbi s odgovarajućom normom.

TCS\_377  
Naredba provjere digitalnog potpisa uvijek koristi javni ključ koji je odabran prethodnom naredbom upravljana sigurnim okruženjem i prethodnom šifrom kompresije unesenom naredbom PSO: funkcija kompresije.

TCS\_378  
Poruka naredbe

|  |  |  |  |
| --- | --- | --- | --- |
| **Bajt** | **Dužina** | **Vrijednost** | **Opis** |
| CLA | 1 | ‚00h’ | CLA |
| INS | 1 | ‚2Ah’ | Izvedba sigurnosne operacije |
| P1 | 1 | ‚00h’ |  |
| P2 | 1 | ‚A8h’ | Oznaka: podakovno polje sadrži DO mjerodavnu za provjeru |
| Lc | 1 | ‚83h’ | Dužina Lc narednog podakovnog polja |
| #28 | 1 | ‚9Eh’ | Oznaka za digitalni potpis |
| #29-#30 | 2 | ‚8180h’ | Dužina digitalnog potpisa (128 bajtova, šifriranih po ISO/IEC 7816-6) |
| #31-#158 |  | ‚XX..XXh’ | Sadržaj digitalnog potpisa |

TCS\_379  
Poruka odgovora

|  |  |  |  |
| --- | --- | --- | --- |
| **Bajt** | **Dužina** | **Vrijednost** | **Opis** |
| SW | 2 | ‚XXXXh’ | Statusne riječi (SW1, SW2) |

—Ako je naredba uspješna kartica uzvraća ‚9000’,

—ako ne uspije provjera potpisa, uzvraćeno stanje obrade je ‚6688’. Postupak provjeravanja je opisan ju Dodatku 11.,

—ako nije izabran javni ključ, uzvraćeno stanje obrade je ‚6A88’,

—ako nedostaju neki očekivani podakovni objekti (gore navedeni), uzvraćeno stanje obrade je ‚6987’. To se može dogoditi ako nema jedne od traženih oznaka,

—ako nema šifre funkcije komprimiranja za obradu naredbe (rezultat prethodne naredbe PSO: funkcija komprimiranja uzvraćeno stanje obrade je ‚6985’,

—ako su neki podakovni objekti netačni, uzvraćeno stanje obrade je ‚6988’. To se može dogoditi ako je dužina traženih podakovnih objekata netočna,

—ako se izabrani javni ključ smatra neispravnim, uzvraćeno stanje obrade je ‚6400’ ili ‚6581’.

**4.   STRUKTURA KARTICA TAHOGRAFA**

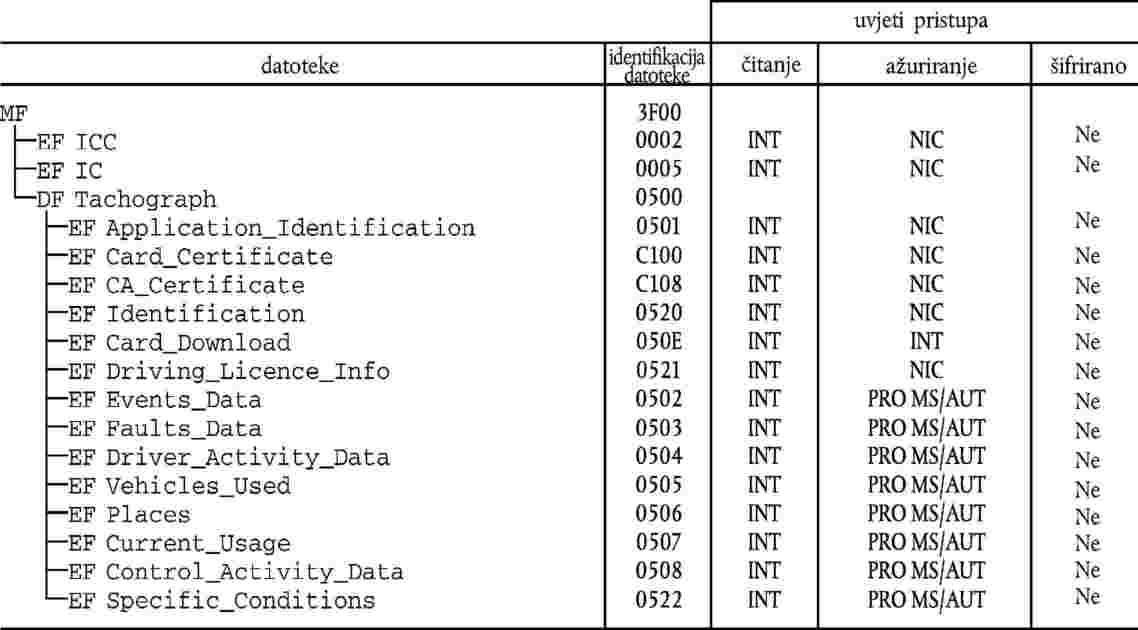
Ovaj stavak propisuje strukture datoteka kartica tahografa za pohranjivanje dostubnih podataka.

Ne propisuje obvezne unutarnje strukture koje ovise o proizvođaču kartice, npr. zaglavlja datoteke, niti pohranjivanje i postepene s podakovnim elementima potrebnim samo za internu upotrebu, kao npr. EuropeanPublicKey, CardPrivateKey, TDesSessionKey ili WorkshopCardPin.

Korisni memorijski kapacitet kartica tahografa iznosi najmanje 11 kilobajta. Mogu se koristiti i veći kapaciteti. U tom slučaju struktura kartice ostaje ista, ali se povećava broj zapisa nekih elemenata strukture. Ovaj stavak navodi najmanje i najveće vrijednosti brojeva ovih zapisa.

**4.1.    Struktura kartice vozača**

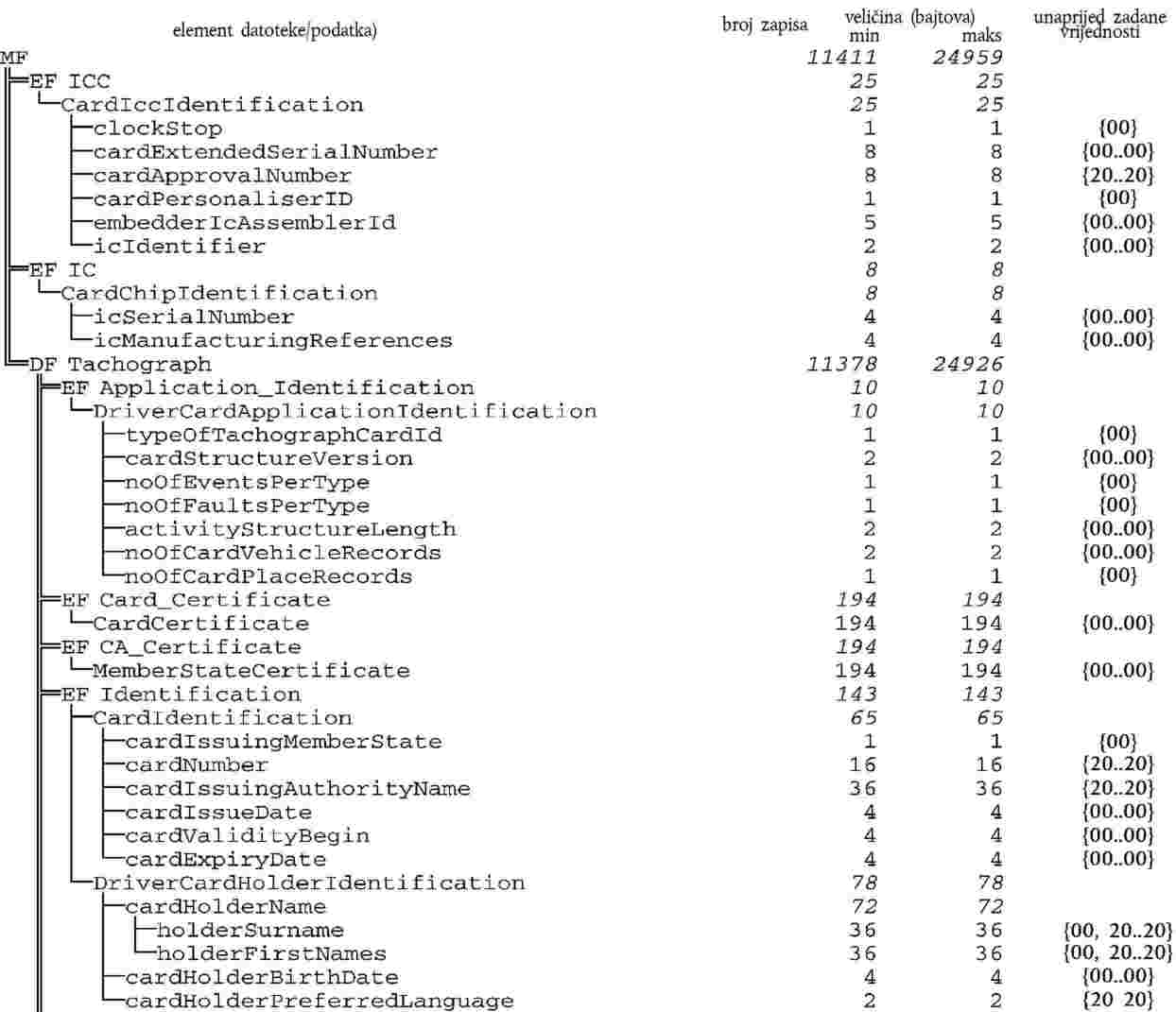
TCS\_400  
Kartica vozača nakon personalizacije mora imati sljedeću strukturu trajnih datoteka i uslove pristupa datoteci.

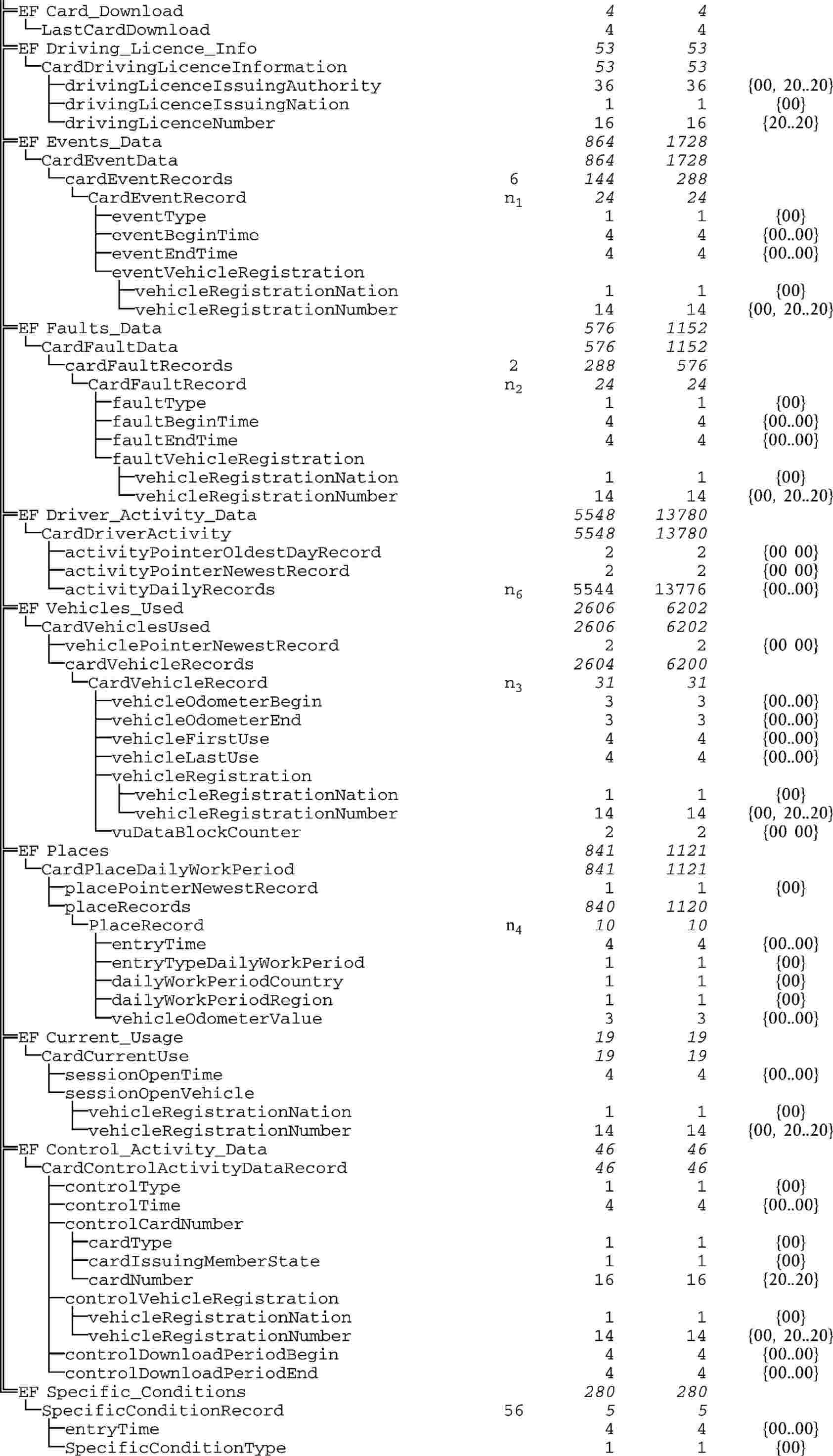


TCS\_401  
Strukture svih EF moraju biti transparentne.

TCS\_402  
Čitanje sa sigurnim prenosom poruke mora biti omogućeno za sve datoteke u DF Tahograf.

TCS\_403  
Kartica vozača mora imati sljedeću podakovnu strukturu:



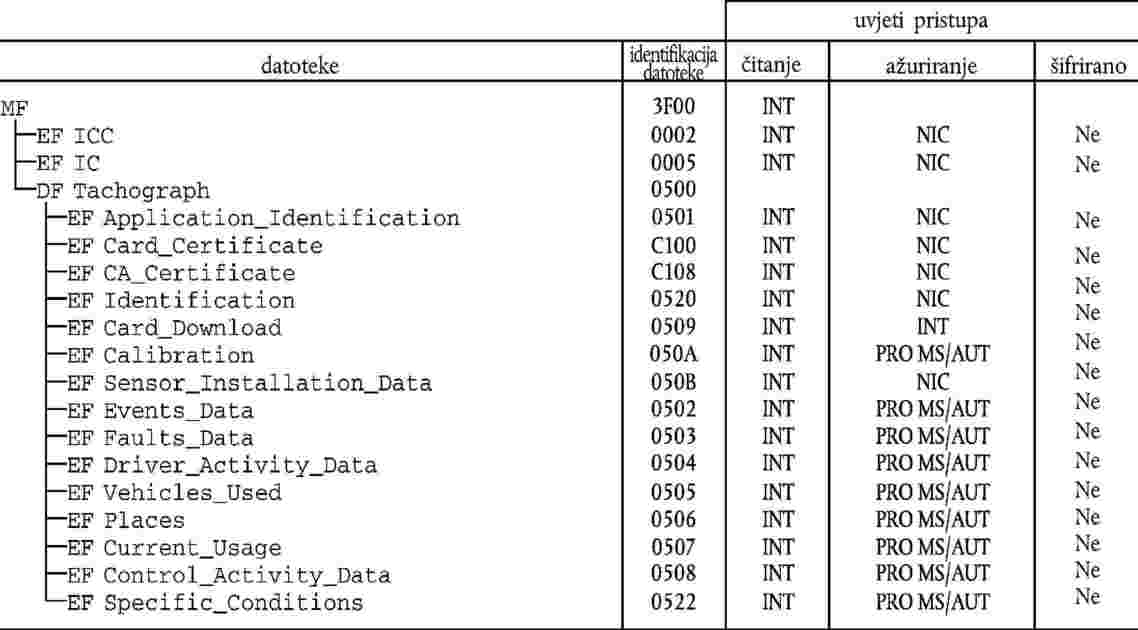


TCS\_404  
Sljedeće vrijednosti, koje se koriste za prikaz veličina u gornjoj tabeli, predstavljaju najmanje i najveće vrijednosti broja zapisa koje mora koristiti podaci struktura kartice vozača:

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | **min** | **maks** |
| Image | Image | **6** | 12 |
| Image | Image | **12** | 24 |
| Image | Image | **84** | 200 |
| Image | Image | **84** | 112 |
| Image | Image | 5 554 bajtova  (28 dana \* 93 promjene aktivnosti) | 13 776 bajtova  (28 dana \*240 promjene aktivnosti) |

**4.2.    Struktura kartice radionice**

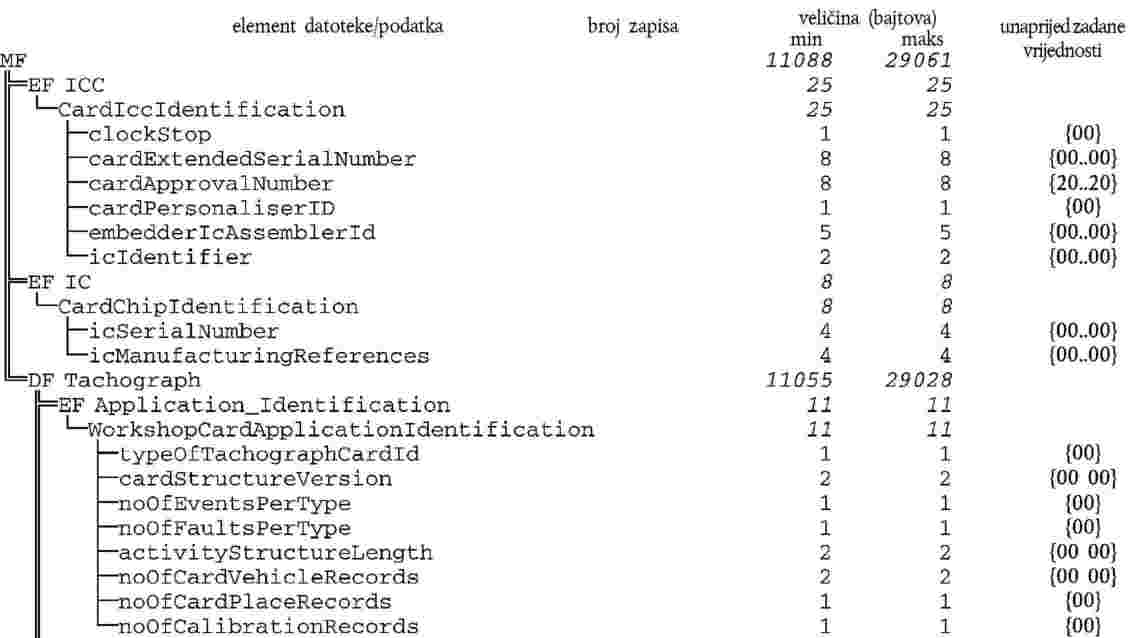
TCS\_405  
Kartica radionice nakon personalizacije mora imati sljedeću strukturu trajnih datoteka i sljedeće uslove pristupa datoteci:

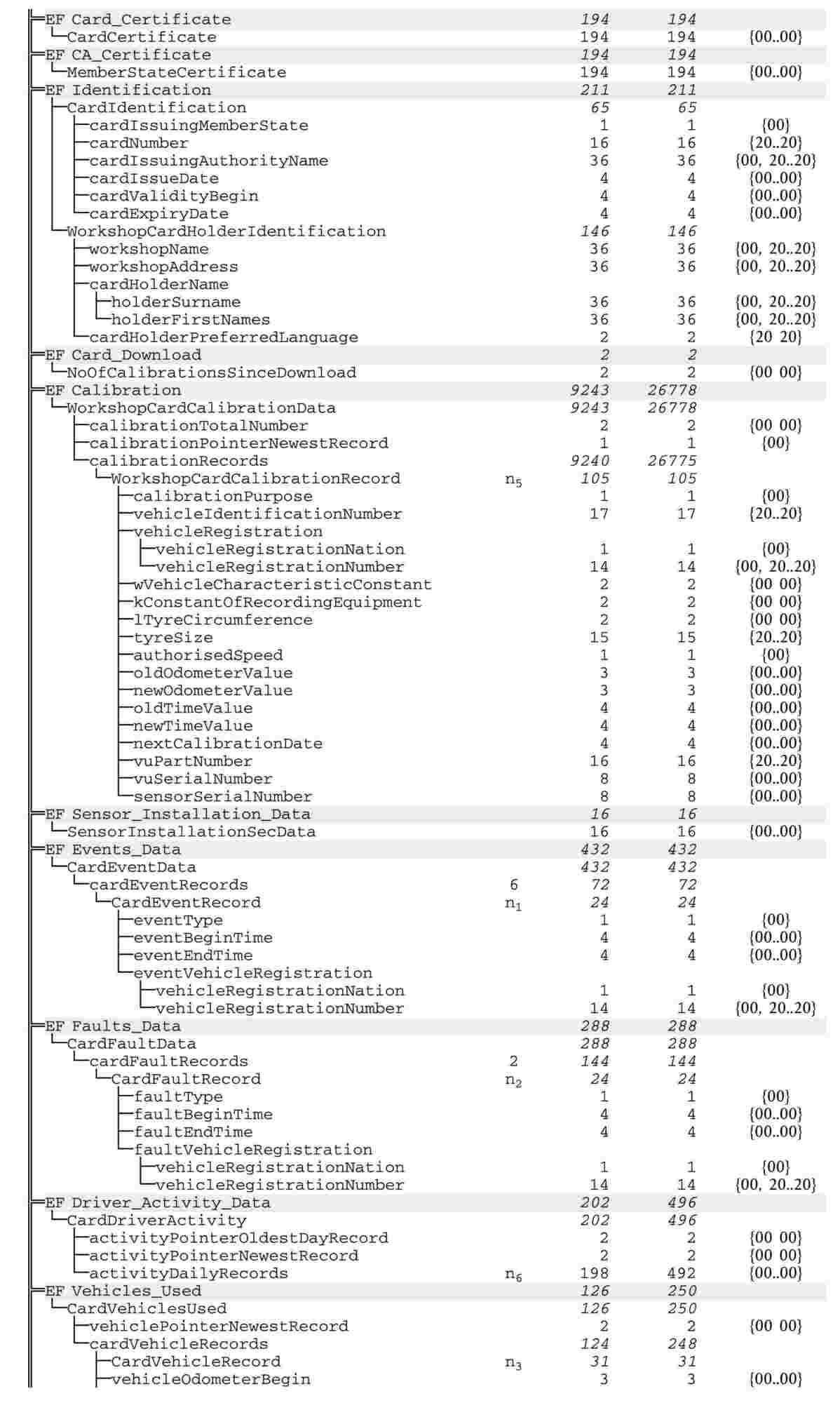


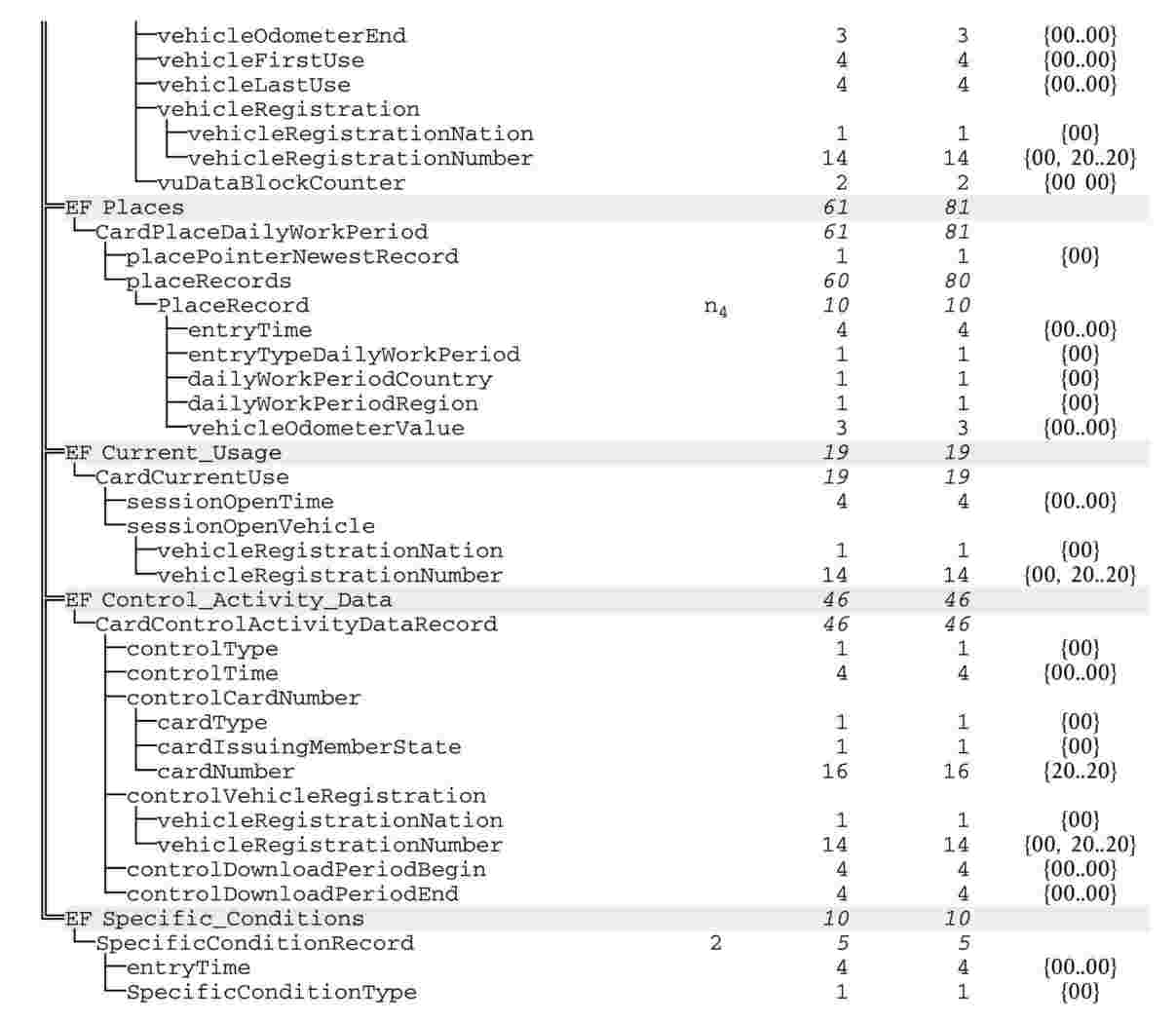
TCS\_406  
Strukture svih EF moraju biti transparentne.

TCS\_407  
Čitanje sa sigurnim prenosom poruke mora biti omogućeno za sve datoteke u DF Tahograf.

TCS\_408  
Kartica radionice mora imati sljedeću podakovnu strukturu:





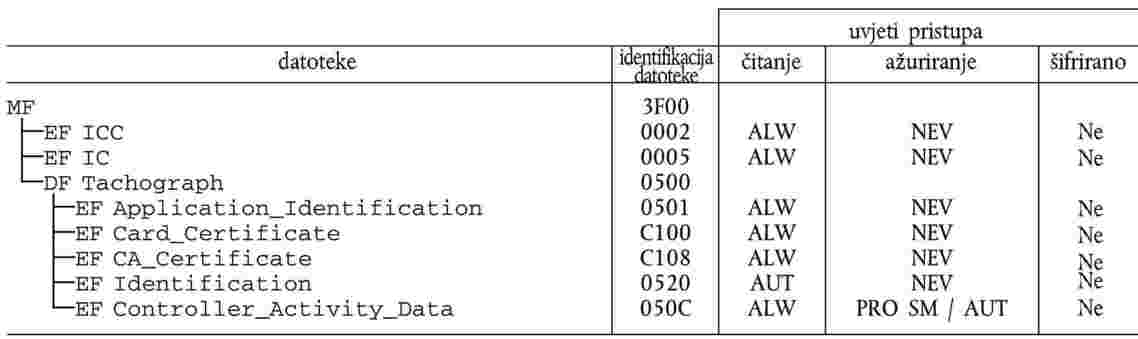


TCS\_409  
Sljedeće vrijednosti, koje se koriste za prikaz veličina u gornjoj tabeli, predstavljaju najmanje i najveće vrijednosti broja zapisa koje mora koristiti podaci struktura kartice radionice:

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | **min** | **maks** |
| Image | Image | **3** | 3 |
| Image | Image | **6** | 6 |
| Image | Image | **4** | 8 |
| Image | Image | **6** | 8 |
| Image | Image | **88** | 255 |
| Image | Image | 198 bajtova  (1 dan \* 93 promjene aktivnosti) | 492 bajtova  (1 dan \* 240 promjena aktivnosti) |

**4.3.    Struktura kontrolne kartice**

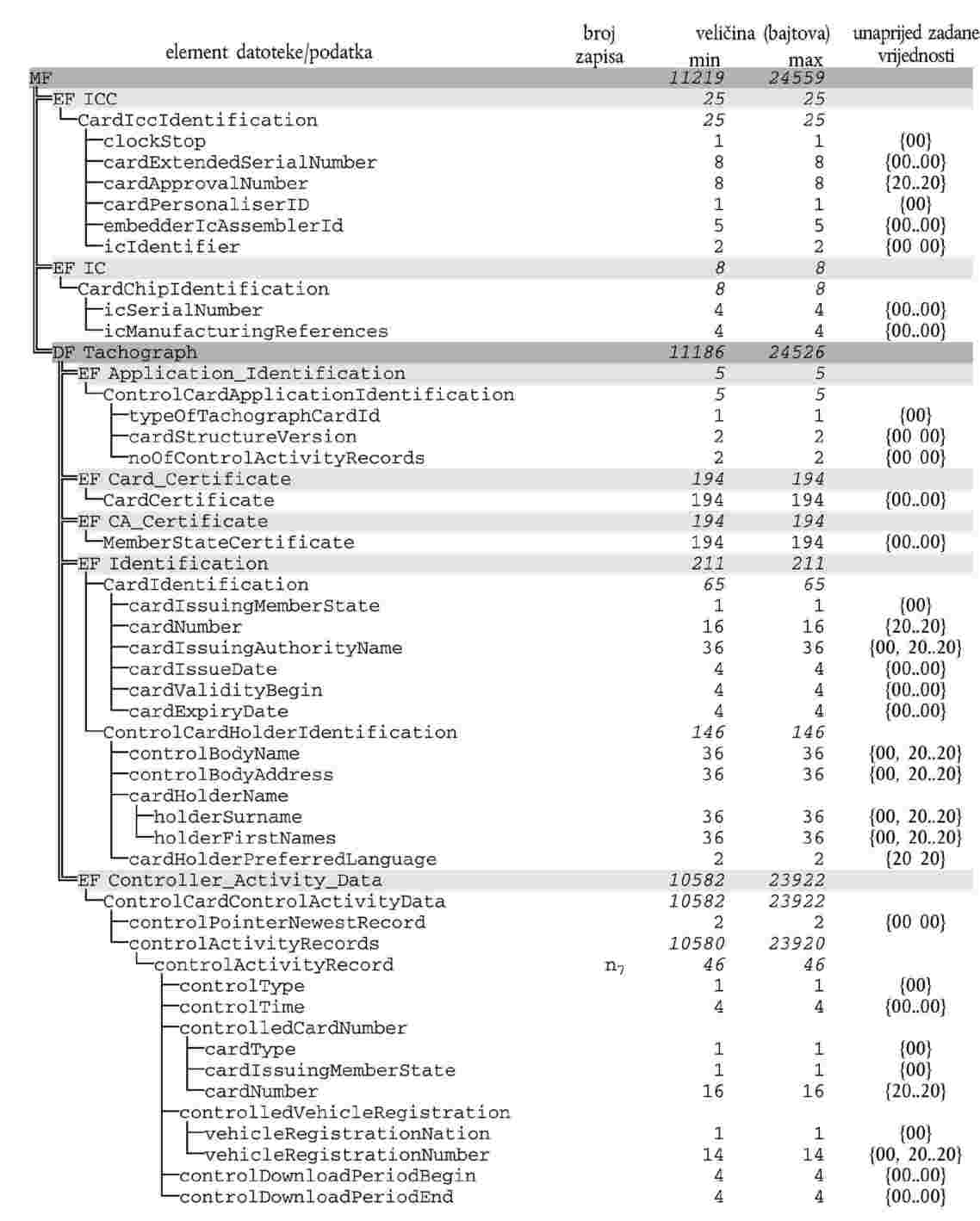
TCS\_410  
Nakon personalizacije kontrolna kartica mora imati sljedeću strukturu trajnih datoteka i uslove pristupa datoteci:



TCS\_411  
Strukture svih EF moraju biti transparentne.

TCS\_412  
Čitanje sa sigurnim prenosom poruke mora biti omogućeno za sve datoteke u DF Tahograf.

TCS\_413  
Kontrolna kartica mora imati sljedeću strukturu podataka:

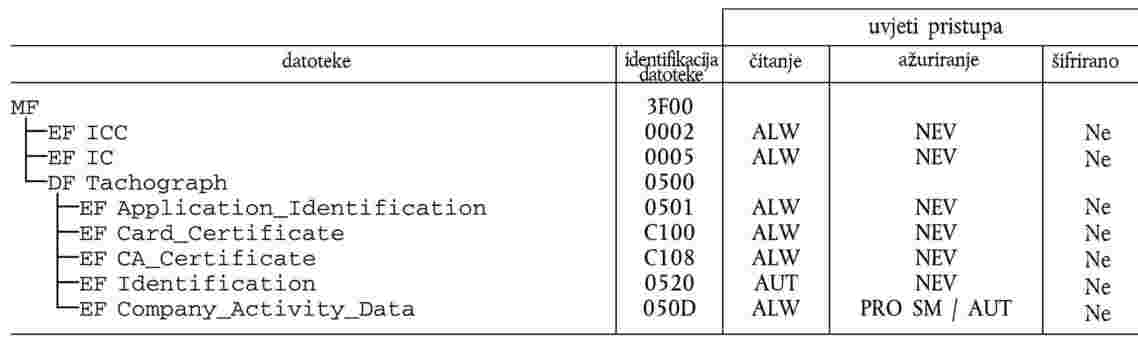


TCS\_414  
Sljedeće vrijednosti koje se koriste za prikaz veličina u gornjoj tabeli su najmanje i najveće vrijednosti koje mora imati podaci struktura kontrolne kartice.

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | **min** | **maks** |
| Image | Image | 230 | 520 |

**4.4.    Struktura kartice prevoznika**

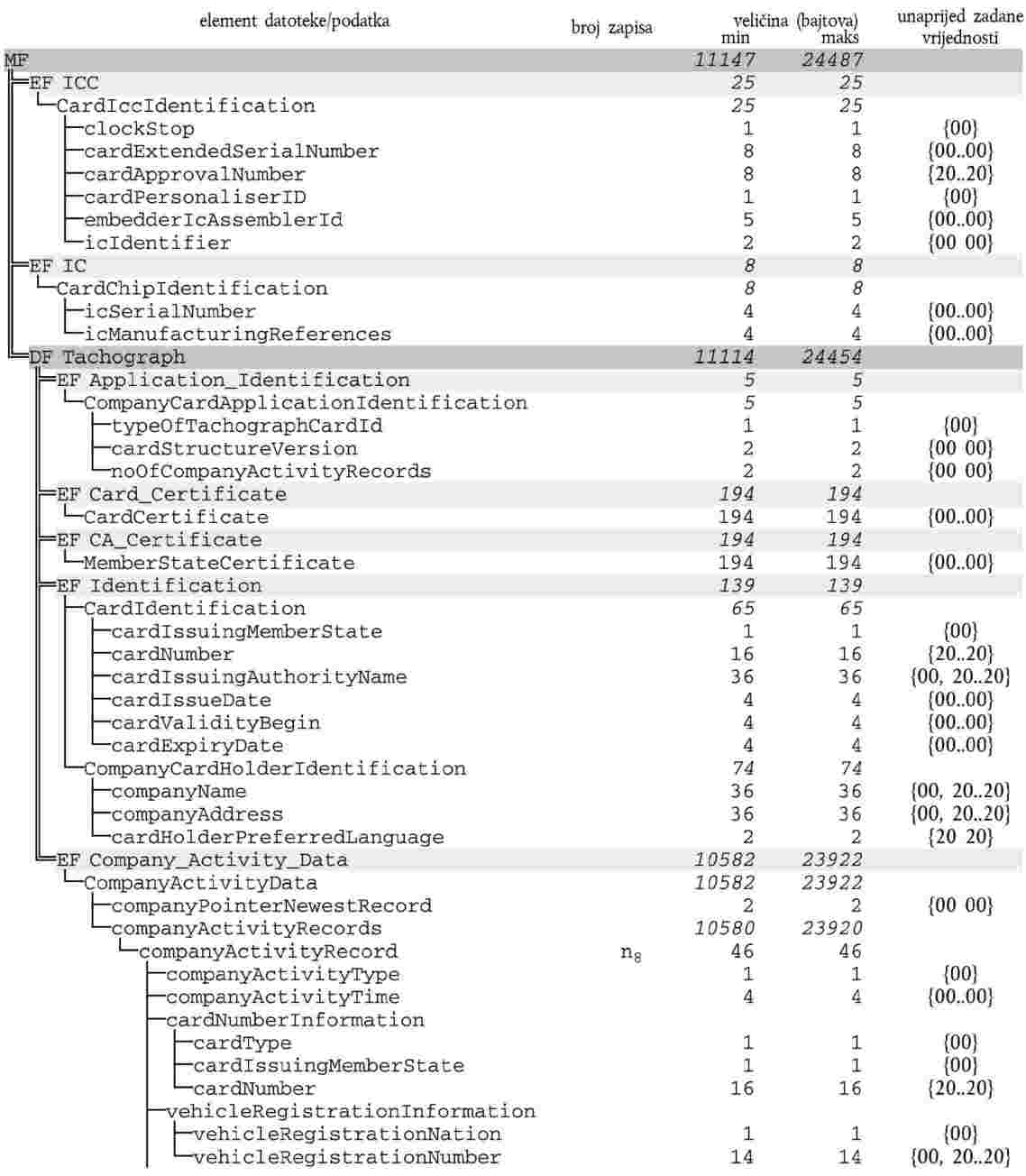
TCS\_415  
Kartica prevoznika nakon personalizacije mora imati sljedeću strukturu trajnih datoteka i sljedeće uslove pristupa datoteci:



TCS\_416  
Strukture svih EF moraju biti transparentne.

TCS\_417  
Čitanje sa sigurnim prenosom poruke mora biti omogućeno za sve datoteke u DF Tahograf.

TCS\_418  
Kartica prevoznika mora imati sljedeću podakovnu strukturu:





TCS\_419  
Sljedeće vrijednosti koje se koriste za prikaz veličina u gornjoj tabeli predstavljaju najmanje i najveće vrijednosti broja zapisa koje mora imati podaci struktura kartice prevoznika.

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | **min** | **maks** |
| Image | Image | 230 | 520 |

**Dodatak 3.**

**PIKTOGRAMI**

PIC\_001 Tahograf može koristiti sljedeće piktograme i kombinacije piktograma:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. | OSNOVNI PIKTROGRAMI   |  |  |  |  | | --- | --- | --- | --- | |  | **Osobe** | **Radnje** | **Načini rada** | | Image | Preduzeće |  | Prevoznički način | | Image | Nadzornik | Nadzor | Nadzorni način | | Image | Vozač | Vozač | Radni način | | Image | Radionica/Ispitno mjesto | Ispitivanje/kalibracija | Kalibracijski način | | Image | Proizvođač |  |  |  |  |  |  | | --- | --- | --- | |  | **Aktivnosti** | **Trajanje** | | Image | Pripravnost | Period tekuće pripravnosti | | Image | Vožnja | Vrijeme neprekidne vožnje | | Image | Odmor | Period tekućeg odmora | | Image | Rad | Period tekućeg rada | | Image | Pauza | Ukupno vrijeme pauza | | Image | Nepoznato |  |  |  |  |  | | --- | --- | --- | |  | **Oprema** | **Funcije** | | Image | Otvor vozača |  | | Image | Otvor suvozača |  | | Image | Kartica |  | | Image | Sat |  | | Image | Prikaz | Prikazivanje | | Image | Vanjsko čuvanje | Preuzimanje podataka | | Image | Napajanje |  | | Image | Pisač/Ispis | Ispisivanje | | Image | Senzor |  | | Image | Dimenzije guma |  | | Image | Vozilo/Jedinica vozila |  |  |  |  | | --- | --- | |  | **Posebni uslovi** | | Image | Van djelokruga | | Image | Boravak na trajektu/vlaku |  |  |  |  |  | | --- | --- | --- | --- | |  | **Razno** |  |  | | Image | Događaji | Image | Greške | | Image | Početak dnevnog perioda aktivnosti | Image | Kraj dnevnog perioda aktivnosti | | Image | Mjesto | Image | Ručni unos aktivnosti vozača | | Image | Osiguranje | Image | Brzina | | Image | Vrijeme | Image | Ukupno/sažetak |  |  |  | | --- | --- | |  | **Oznake** | | Image | Dnevno | | Image | Tjedno | | Image | dva tjedna | | Image | Od ili do | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 2. | KOMBINACIJE PIKTOGRAMA   |  |  |  |  | | --- | --- | --- | --- | |  | **Razno** |  |  | | Image  Image | Mjesto nadzora |  |  | | Image  Image | Mjesto početka dnevnog perioda aktivnosti | Image  Image | Mjesto kraja dnevnog perioda aktivnosti | | Image  Image | Od vremena | Image  Image | Do vremena | | Image  Image | U vozilu |  |  | | Image  Image | Početak aktivnosti van djelokruga | Image  Image | Kraj aktivnosti van djelokruga |  |  |  | | --- | --- | |  | **Kartice** | | Image  Image | Kartica vozača | | Image  Image | Kartica prevoznika | | Image  Image | Kontrolna kartica | | Image  Image | Kartica radionice | | Image  - - - | Bez kartice |  |  |  | | --- | --- | |  | **Vožnja** | | Image  Image | Vožnja u posadi | | Image  Image | Vrijeme vožnje u nedelja dana | | Image  Image | Vrijeme vožnje u dva tjedna |  |  |  | | --- | --- | |  | **Ispisi** | | Image  Image  Image | Dnevni ispis aktivnosti vozača s kartice | | Image  Image  Image | Dnevni ispis aktivnosti svih vozača iz jedinice u vozilu | | Image  Image  Image  Image | Ispis događaja i grešaka s kartice | | Image  Image  Image  Image | Ispis događaja i grešaka iz jedinice vozila | | Image  Image  Image | Ispis tehničkih podataka | | Image  Image  Image | Ispis prekoračenja brzine |  |  |  | | --- | --- | |  | **Događaji** | | Image  Image | Ubacivanje nevažeće kartice | | Image  Image  Image | Sukob kartica | | Image  Image  Image | Preklapanje vremena | | Image  Image  Image | Vožnja bez odgovarajuće kartice | | Image  Image  Image | Ubacivanje kartice tokom vožnje | | Image  Image  Image | Zadnja razmjena podataka s karticom nije pravilno završena | | Image  Image | Prekoračenje brzine | | Image  Image | Prekid napajanja | | Image  Image | Greška podataka kretanja | | Image  Image | Proboj zaštite | | Image  Image | Podešavanje vremena (u radionici) | | Image  Image | Kontrola prekoračenja brzine |  |  |  | | --- | --- | |  | **Greške** | | Image  Image  Image | Greška kartice (otvor vozača) | | Image  Image  Image | Greška kartice (otvor suvozača) | | Image  Image | Greška prikaza | | Image  Image | Greška preuzimanja podataka | | Image  Image | Greška pisača | | Image  Image | Greška senzora | | Image  Image | Interna greška jedinice vozila |  |  |  | | --- | --- | |  | **Postupak ručnog unosa** | | Image  Image  Image | I dalje isto dnevno period aktivnosti? | | Image  Image | Kraj prethodnog perioda aktivnosti? | | Image  Image  Image | Potvrdi ili unesi mjesto kraja perioda aktivnosti | | Image  Image  Image | Unesi vrijeme početka | | Image  Image  Image | Unesi mjesto početka perioda aktivnosti. | |

Napomena: Dodatne kombinacija piktograma za formiranje bloka ispisa ili identifikatora zapisa su utvrđene u Dodatku 4.

**Dodatak 4.**

**ISPISI**

SADRŽAJ

|  |  |
| --- | --- |
| 1. | Uopšteno |

|  |  |
| --- | --- |
| 2. | Specifikacija Podakovnog Bloka |

|  |  |
| --- | --- |
| 3. | Specifikacija Ispisa |

|  |  |
| --- | --- |
| 3.1. | Aktivnosti vozača iz dnevnog ispisa kartice |

|  |  |
| --- | --- |
| 3.2. | Aktivnosti vozača iz dnevnog ispisa jedinice vozila |

|  |  |
| --- | --- |
| 3.3. | Događaji i greške iz ispisa kartice |

|  |  |
| --- | --- |
| 3.4. | Događaji i greške iz ispisa jedinice vozila |

|  |  |
| --- | --- |
| 3.5. | Ispis tehničkih podataka |

|  |  |
| --- | --- |
| 3.6. | Ispis prekoračenja brzine |

**1.   UOPŠTENO**

Svaki ispis nastaje povezivanjem raznih podakovnih blokova koji se identifikujeju identifikatorom bloka.

Jedan podakovni blok sadrži jedan ili više zapisa, koji se mogu identifikujeti pomoću identifikatora zapisa.

PRT\_001  
Ako identifikator zapisa neposredno prethodi identifikatoru bloka, identifikator zapisa se ne ispisuje.

PRT\_002  
Ako je neka podaci stava nepoznata ili se ne smije ispisati radi zaštite prava na pristub podacima, umjesto nje se ispisuju praznine.

PRT\_003  
Ako je sadržaj cijelog reda nepoznat ili ga ne treba ispisivati, tada se izostavlja cijeli red.

PRT\_004  
Numerička podaci polja se ispisuju u desnom poravnanju, s razmakom za tisuće i milijune i bez vodećih nula.

PRT\_005  
Polja s podakovnim nizovima se ispisuju u lijevom poravnanju i pune prazninama do dužine podakovnog elementa ili se skraćuju na dužinu podakovnog elementa prema potrebi (imena i adrese).

**2.   SPECIFIKACIJA PODAKOVNOG BLOKA**

U ovom poglavlju se koriste sljedeći dogovoreni formati evidentirajunja:

|  |  |
| --- | --- |
| — | Podebljano tiskana slova označivaju običan tekst koji se ispisuje (ispis ostaje u normalnim slovima), |

|  |  |
| --- | --- |
| — | Normalna slova stoje za varijable (piktogrami ili podaci), koji se kod ispisa zamjenjuju njihovim vrijednostima, |

|  |  |
| --- | --- |
| — | Imena varijabli su nadopunjena podcrtavanjem za prikaz dužine podakovnog elementa raspoložive za primjenu, |

|  |  |
| --- | --- |
| — | Datumi su prikazani u formatu ‚dd/mm/gggg’ (dan, mjesec, godina). Može se koristiti i oblik ‚dd.mm.gggg’, |

|  |  |
| --- | --- |
| — | Izraz ‚Identifikator kartice’ označava slog koji se sastoji od sljedećeg: vrsta kartice prikazana kombinacijom piktograma, šifra države članice izdavaoca, kosa crta i broj kartice s indeksom zamjene i indeksom obnavljanja odvojenim razmakom:  Image |

PRT\_006  
Za ispise se koriste sljedeći podatkovni blokovi i/ili zapisi podataka, u skladu sa sljedećim značenjima i formatima:

1

|  |  |
| --- | --- |
| **Datum i vrijeme ispisa dokumenta** | Image  dd/mm/yyyy hh:mm **(UTC)** |

**2.   *Vrsta ispisa***

|  |  |
| --- | --- |
| Identifikator bloka | Image |
| Kombinacija piktograma i ispisa (vidjeti Dodatak 3.), Podešenje ograničivača brzine (samo pri ispisu prekoračenja brzine) | Picto xxx **km/h** |

**3.   *Identifikacija vlasnika kartice***

|  |  |
| --- | --- |
| Identifikator bloka. P = piktogram „osoba” | P |
| Prezime vlasnika kartice | P Last\_Name |
| Ime(na) vlasnika kartice (ako postoji) | First\_Name |
| Identifikacija kartice | Card\_Identification |
| Datum isteka valjanosti kartice (ako postoji) | dd/mm/yyyy |
| U slučaju neosobne kartice koja ne sadrži prezime vlasnika kartice, umjesto toga se tiska naziv preduzeća, radionice ili nadzornog tijela. | |

**4.   *Identifikacija vozila***

|  |  |
| --- | --- |
| Identifikator bloka | Image |
| VIN | Image  VIN |
| Država članica registracije i registracijski broj vozila (VRN) | Nat/VRN |

**5.   *Identifikacija jedinice vozila (JV)***

|  |  |
| --- | --- |
| Identifikator bloka | Image |
| Naziv proizvođača JV | Image  VU\_Manufacturer |
| Kataloški broj JV | VU\_Part\_Number |

**6.   *Zadnja kalibracija tahografa***

|  |  |
| --- | --- |
| Identifikator bloka | Image |
| Naziv radionice | Image  Last\_Name |
| Identifikacija kartice radionice | Card\_Identification |
| Datum kalibracije | Image  dd/mm/yyyy |

**7.   *Zadnji nadzor (od strane službenika za nadzor)***

|  |  |
| --- | --- |
| Identifikator bloka | Image |
| Identifikacija nadzorne kartice | Card\_Identification |
| Datum, vrijeme i vrsta nadzora | Image  dd/mm/yyyy hh:mm pppp |
| Vrsta nadzora: Do četiri piktograma. Vrsta nadzora može biti (kombinacija) sljedećeg:  Image:Preuzimanje podataka s karticeImage:Preuzimanje podataka s JVImage:IspisImage:Prikaz | |

**8.   *Aktivnosti vozača pohranjene na kartici prema redoslijedu nastajanja***

|  |  |
| --- | --- |
| Identifikator bloka | Image |
| 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.   *Period u kojem kartica nije bila umetnuta***

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  | | --- | --- | | 8.1.a | Identifikator zapisa (početak periode) | |  |
| |  |  | | --- | --- | | 8.1.b | *Nepoznato period*. Vrijeme početka, trajanje | | Image  : hh:mm hhhmm |
| |  |  | | --- | --- | | 8.1.c | *Ručno unesena aktivnost* | | A: hh:mm hhhmm |
| Piktogram aktivnosti, vrijeme početka, trajanje. |  |

**8.2.   *Umetanje kartice u otvor S***

|  |  |
| --- | --- |
| Identifikator zapisa; S = piktogram otvora | S |
| Država članica registracije vozila i registracijski broj vozila (VRN) | Image  Nat/VRN |
| Stanje brojača kilometara vozila pri umetanju kartice | x xxx xxx **km** |

**8.3.   *Aktivnost (dok je kartica bila umetnuta)***

|  |  |
| --- | --- |
| Piktogram aktivnosti, vrijeme početka, trajanje, stanje posade (piktogram posade ako je stanje CREW, prazno ako je SINGLE) | A: hh:mm hh**h**mm  Image  Image |
| |  |  | | --- | --- | | 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 VU, po otvoru, hronološkim redom***

|  |  |
| --- | --- |
| Identifikator bloka | Image |
| Datum upita (kalendarski dan ispisa) | dd/mm/yyyy |
| Brojač kilometara vozila u 00:00 i 24:00 | x xxx xxx – x xxx xxx **km** |

**10.   *Aktivnosti koje se obavljaju u otvoru 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.   *Period kada u otvoru S nema kartice***

|  |  |
| --- | --- |
| Identifikator zapisa |  |
| Nije umetnuta kartica | Image  Image  - - - |
| Brojač kilometara vozila na početku periode. | x xxx xxx **km** |

**10.2.   *Umetanje kartice***

|  |  |
| --- | --- |
| Identifikator zapisa o umetanju kartice |  |
| Prezime vozača | Image  Last\_Name |
| Ime vozača | First\_Name |
| Identifikacija kartice vozača | Card\_Identification |
| Datum isteka kartice vozača | dd/mm/yyyy |
| Država članica registracije i registracijska oznaka prethodno korištenog vozila | Image  Image  Nat/VRN |
| Datum i vrijeme vađenja kartice iz prethodnog vozila | dd/mm/yyyy hh:mm |
| Prazna crta |  |
| 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. koristi očitanje podataka brojača kilometara od zadnjeg dostubnog umetanja kartice. |  |

**10.3.   *Aktivnost***

|  |  |
| --- | --- |
| Piktogram aktivnosti, vrijeme početka, trajanje, status posade (piktogram posade ako je CREW, prazno ako je SINGLE) | A ÷ hh:mm hhhmm  Image  Image |
| 10.3.a Posebno stanje. Vrijeme unosa, piktogram posebnog stanja (ili kombinacija piktograma). | hh:mm - - - pppp |

**10.4.   *Vađenje kartice ili kraj periode „bez kartice”***

|  |  |
| --- | --- |
| Brojač kilometara vozila pri vađenju kartice ili na kraju periode „bez kartice” i prijeđena udaljenost od umetanja kartice ili od početka periode „bez kartice”. | x xxx xxx **km;** x xxx **km** |

**11.   *Dnevni sažetak***

|  |  |
| --- | --- |
| Identifikator bloka | Image |

**11.1.   *Dnevni sažetak JV za periode bez kartice u otvoru vozača***

|  |  |
| --- | --- |
| Identifikator bloka | 1  Image  Image  - - - |

**11.2.   *Dnevni sažetak JV za periode bez kartice u otvoru suvozača***

|  |  |
| --- | --- |
| Identifikator bloka | 2  Image  Image  - - - |

**11.3.   *Dnevni sažetak JV po vozaču***

|  |  |
| --- | --- |
| Identifikator zapisa |  |
| Prezime vozača | Image  Last\_Name |
| Ime(na) vozača | First\_Name |
| Identifikacija kartice vozača | Card\_Identification |

**11.4.   *Unos mjesta gdje dnevno period rada počinje i/ili završava***

|  |  |
| --- | --- |
| pi = piktogram početka/završetka, vremena, države, regije, stanje brojača kilometara | pihh:mm Cou Reg |
| Brojač kilometara | x xxx xxx **km** |

**11.5.   *Aktivnosti ukupno (s kartice)***

|  |  |
| --- | --- |
| Ukupno trajanje vožnje, prijeđena udaljenost | Image  hh**h**mm x xxx **km** |
| Ukupno trajanje rada i pripravnosti | Image  hh**h**mm  Image  hh**h**mm |
| Ukupno trajanje odmora i nepoznato | Image  hh**h**mm  Image  hh**h**mm |
| Ukupno trajanje aktivnosti posade | Image  Image  hh**h**mm |

**11.6.   *Aktivnosti ukupno (periode bez kartice u otvoru vozača)***

|  |  |
| --- | --- |
| Ukupno trajanje vožnje, prijeđena udaljenost | Image  hh**h**mm x xxx **km** |
| Ukupno trajanje rada i pripravnosti | Image  hh**h**mm  Image  hh**h**mm |
| Ukupno trajanje odmora | Image  hh**h**mm |

**11.7.   *Aktivnosti ukupno (period bez kartice u otvoru suvozača)***

|  |  |
| --- | --- |
| Ukupno trajanje rada i pripravnosti | Image  hh**h**mm  Image  hh**h**mm |
| Ukupno trajanje odmora | Image  hh**h**mm |

**11.8.   *Aktivnosti ukupno (po vozaču, uključuje oba otvora)***

|  |  |
| --- | --- |
| Ukupno trajanje vožnje, prijeđena udaljenost | Image  hh**h**mm x xxx **km** |
| Ukupno trajanje rada i pripravnosti | Image  hh**h**mm  Image  hh**h**mm |
| Ukupno trajanje odmora | Image  hh**h**mm |
| Ukupno trajanje aktivnosti posade | Image  Image  hh**h**mm |
| Ako se traži dnevni ispis za tekući dan, informacije o dnevnom sažetku računaju se iz dostubnih podataka u vrijeme ispisa. | |

**12.   *Događaji i/ili pogreške arhivirani na kartici***

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  | | --- | --- | | 12.1. | Identifikator bloka pet zadnjih „Događaja i pogrešaka” s kartice | | Image  Image  Image |
| |  |  | | --- | --- | | 12.2. | Identifikator bloka svi zabilježeni „Događaji” na kartici | | - - - - - - - - - - -  Image  Image  - - - - - - - - - |

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  | | --- | --- | | 12.3. | Identifikator bloka sve zabilježene „Pogreške” na kartici | | Image  Image |

**12.4.   *Zapis Događaja i/ili pogreške***

|  |  |
| --- | --- |
| Identifikator zapisa |  |
| Piktogram događaj/pogreška, svrha zapisa, datum i vrijeme početka | Pic (p) dd**/**mm**/**yyyy hh:mm |
| Dodatna šifra događaja/pogreške (ako postoji), trajanje | Image  xx hh**h**mm |
| Država članica registracije i registracijska oznaka vozila (VRN) u kojem se dogodio događaj ili pogreška | Image  Nat/VRN |

**13.   *Događaji i/ili pogreške, otprije arhivirani ili još uvijek traju u JV***

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  | | --- | --- | | 13.1. | Identifikator bloka zadnjih pet „Događaja i pogrešaka” iz JV | | Image  Image  Image |
| |  |  | | --- | --- | | 13.2. | Identifikator bloka otprije zabilježeni ili još uvijek traju „Događaji” u JV | | Image  Image |
| |  |  | | --- | --- | | 13.3. | Identifikator bloka otprije zabilježeni ili još uvijek traju „Pogreške” u JV | | Image  Image |

**13.4.   *Zapis događaja i/ili pogreške***

|  |  |
| --- | --- |
| Identifikator zapisa |  |
| Piktogram događaja/pogreške, svrha zapisa, datum i vrijeme početka, | Pic (p) dd/mm/yyyy hh:mm |
| Dodatna šifra događaja/pogreške (ako postoji), broj sličnih događaja tog dana, trajanje | Image  xx (xxx) hh**h**mm |
| Identifikacija kartica umetnutih na početku ili na kraju događaja ili pogreške (do četiri reda bez ponavljanja istih brojeva kartica dva puta) | Card\_Identification  Card\_Identification  Card\_Identification  Card\_Identification |
| Slučaj kad nije bila umetnuta nijedna kartica | Image  - - - |
| Svrha zapisa (p) je numerička šifra koja objašnjava zašto je događaj ili pogreška zabilježena, a šifrirana u skladu s podatkovnim elementom EventFaultRecordPurpose. | |

**14.   *Identifikacija JV***

|  |  |
| --- | --- |
| Identifikator bloka | Image |
| Naziv proizvođača JV | Image  Name |
| Adresa proizvođača JV | Address |
| Kataloški broj JV | PartNumber |
| Homologacijski broj JV | Apprv |
| Serijski broj JV | S/N |
| Godina proizvodnje JV | Yyyy |
| Verzija programa u JV i datum instalacije | **V** xxxx dd/mm/yyyy |

**15.   *Identifikacija senzora***

|  |  |
| --- | --- |
| Identifikator bloka | Image |
| Serijski broj senzora | Image  S/N |
| Homologacijski broj senzora | Apprv |
| Datum prve ugradnje senzora | dd/mm/yyyy” |

**3.   SPECIFIKACIJE ISPISA**

U ovom se poglavlju koriste sljedeći dogovoreni zapisi:

|  |  |
| --- | --- |
| Image | Ispis bloka ili broja zapisa N |
| Ispis bloka ili broja zapisa N ponovljeno onoliko puta koliko je potrebno |
| Ispis bloka ili zapisa X i/ili Y prema potrebi ponavljajući onoliko puta koliko je potrebno |

**3.1.   Aktivnosti vozača iz dnevnog ispisa kartice**

PRT\_007  
Dnevni ispis vozačevih aktivnosti s kartice mora biti u skladu sa sljedećim formatom:

|  |  |
| --- | --- |
| 1. | Datum i vrijeme ispisa dokumenta |
| 2. | Vrsta ispisa |
| 3. | Identifikacija nadzornika (ako je nadzorna kartica umetnuta u VU) |
| 3. | Identifikacija vozača (iz kartice koja je predmet ispisa) |
| 4. | Identifikacija vozila (vozilo iz kojeg se uzima ispis) |
| 5. | Identifikacija JV (JV iz koje se uzima ispis) |
| 6. | Zadnja kalibracija JV |
| 7. | Zadnji nadzor kojemu je pregledavani vozač bio podvrgnut |
| 8. | Razdjelnik aktivnosti vozača |
| 8.a | Stanje izvan područja primjene na početku tog 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. | Aktivnosti ukupno |
| 12.1. | Događaji ili pogreške s razdjelnika kartice |
| 12.4. | Zapisi događaja/pogrešaka (zadnjih pet događaja ili pogrešaka arhiviranih na kartici) |
| 13.1. | Događaji ili pogreške s razdjelnika JV |
| 13.4. | Zapisi događaja/pogrešaka (zadnjih pet događaja ili pogrešaka arhiviranih ili tekućih u JV) |
| 21.1. | Mjesto nadzora |
| 21.2. | Potpis nadzornika |
| 21.5. | Potpis vozača” |

**3.2. Aktivnosti vozača iz dnevnog ispisa JV moraju biti u skladu sa sljedećim formatom:**

PRT\_008

The driver activities from VU daily printout shall be in accordance with the following format:

|  |  |
| --- | --- |
| 1. | Datum i vrijeme ispisa dokumenta |
| 2. | Vrsta ispisa |
| 3. | Identifikacija vlasnika kartice (za sve kartice umetnute u JV) |
| 4. | Identifikacija vozila (vozilo iz kojeg se uzima ispis) |
| 5. | Identifikacija JV (JV iz koje se uzima ispis) |
| 6. | Zadnja kalibracija JV |
| 7. | Zadnji nadzor na ovom tahografu |
| 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 periode bez kartice u prorezu vozača |
| 11.4. | Mjesta unijeta hronološkim redom |
| 11.6. | Aktivnosti ukupno |
| 11.2. | Sažetak periode bez kartice u otvoru suvozača |
| 11.4. | Mjesta unijeta hronološkim redom |
| 11.8. | Aktivnosti ukupno |
| 11.3. | Sažetak aktivnosti za vozača, uključena oba otvora |
| 11.4. | Mjesta koja je taj vozač unio hronološkim redom |
| 11.7. | Aktivnosti ukupno za tog vozača |
| 13.1. | Razdjelnik događaja i pogrešaka |
| 13.4. | Zapisi događaja/pogrešaka (zadnjih pet događaja ili pogrešaka od ranije arhiviranih ili koje još traju u JV) |
| 21.1. | Mjesto nadzora |
| 21.2. | Potpis nadzornika |
| 21.3. | Od vremena (prostor na kojem vozač naznači da je bio bez kartice |
| 21.4. | Do vremena koje se odnosi na njega) |
| 21.5. | Potpis vozača” |

**3.3.   Događaji i greške iz ispisa kartice**

PRT\_009  
Događaji i greške iz ispisa kartice moraju biti u skladu sa sljedećim formatom:

|  |  |
| --- | --- |
| Image | Datum i vrijeme ispisa dokumenta |
| Vrsta ispisa |
| Identifikacija kontrolora (ako je u jedinicu vozila umetnuta kontrolna kartica) |
| Identifikacija vozača (iz kartice za koju se radi ispis) |
| Identifikacija vozila (vozilo za koje se radi ispis) |
| Razdvajatelj događaja |
| Zapisi događaja (svi događaji arhivirani na kartici) |
| Razdvajatelj grešaka |
| Zapisi o greškama (sve greške sačuvane na kartici) |
| Mjesto nadzora |
| Potpis kontrolora |
| Potpis vozača |

**3.4.   Događaji i greške iz ispisa jedinice vozila**

PRT\_10  
Događaji i greške iz ispisa jedinice vozila moraju biti u skladu sa sljedećim formatom:

|  |  |
| --- | --- |
| Image | Datum i vrijeme ispisa dokumenta |
| Vrsta ispisa |
| Identifikacija nosioca kartice (za sve kartice umetnute u jedinicu vozila) |
| Identifikacija vozila (vozilo za koje se radi ispis) |
| Razdvajatelj događaja |
| Zapisi događaja (svi događaji arhivirani ili koji se trenutno događaju u jedinici vozila) |
| Razdvajatelj grešaka |
| Zapisi o greškama (sve greške sačuvane ili se trenutno događaju u jedinici vozila) |
| Mjesto nadzora |
| Potpis kontrolora |
| Potpis vozača |

**3.5.   Ispis tehničkih podataka**

PRT\_011  
Ispis tehničkih podataka mora biti u skladu sa sljedećim formatom:

|  |  |
| --- | --- |
| Image | Datum i vrijeme ispisa dokumenta |
| Vrsta ispisa |
| Identifikacija nosioca kartice (za sve kartice umetnute u jedinicu vozila) |
| Identifikacija vozila (vozilo iz kojeg se radi ispis) |
| Identifikacija jedinice vozila |
| Identifikacija senzora |
| Razdvajatelj podataka o kalibraciji |
| Zapisi kalibracije (svi raspoloživi zapisi hronološkim redom) |
| Razdvajatelj podešavanja vremena |
| Zapisi o podešavanju vremena (svi raspoloživi zapisi od zapisa o podešavanju vremena i od zapisa o kalibraciji) |
| Najnoviji događaj i greška zapisani u jedinici vozila |

**3.6.   Ispis prekoračenja brzine**

PRT\_012  
Ispis prekoračenja brzine mora biti u sljedećem formatu:

|  |  |
| --- | --- |
| Image | Datum i vrijeme ispisa dokumenta |
| Vrsta ispisa |
| Identifikacija nosioca kartice (za sve kartice umetnute u jedinicu vozila) |
| Identifikacija vozila (vozilo iz kojeg se radi ispis) |
| Informacije o kontroli prekoračenja brzine |
| Identifikator podataka o prekoračenju brzine |
| Prvo prekoračenje brzine poslije zadnje kalibracije |
| Identifikator podataka o prekoračenju brzine |
| 5 najtežih prekoračenja brzine u zadnjih 365 dana |
| Identifikator podataka o prekoračenju brzine |
| Najteže prekoračenje brzine za svaki od posljednjih 10 dana napauza |
| Mjesto nadzora |
| Potpis kontrolora |
| Potpis vozača |

**Dodatak 5.**

**PRIKAZ**

U ovom se Dodatku koriste sljedeći dogovorni oblici evidentirajunja:

|  |  |
| --- | --- |
| — | podebljano tiskana slova označivaju običan teksta za prikaz (prikaz je u normalnim slovima), |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| — | normalna slova označivaju promjenjive varijable (piktogrami ili podaci), koji se za prikaz zamjenjuju njihovim vrijednostima:   |  |  |  | | --- | --- | --- | | dd mm gggg | : | dan, mjesec, godina, | | hh | : | sati, | | mm | : | minute, | | D | : | piktogram trajanje, | | EF | : | kombinacija piktograma događaja ili grešaka, | | O | : | piktogram načina rada. | |

DIS\_001  
Tahograf prikazuje podatke primjenom sljedećeg formata:

|  |  |
| --- | --- |
| **Podaci** | Image |
| **standardni prikaz** | |
| Lokalno vrijeme | Image |
| Način rada | Image |
| Podaci o vozaču | Image |
| Podaci o suvozaču | Image |
| Uključeno stanje ‚Van nadležnosti | Image |
| **Upozorenje** | |
| Prekoračenje vremena neprekidne vožnje | Image |
| Događaj ili greška | Image |
| **Ostali prikazi** | |
| UTC datum | Image |
| vrijeme | Image |
| Neprekidno vrijeme vožnje i ukupno vrijeme pauze vozača | Image |
| Neprekidno vrijeme vožnje i ukupno vrijeme pauze suvozača | Image |
| Ukupno vrijeme vožnje vozača za protekli i tekući nedelja | Image |
| Ukupno vrijeme vožnje suvozača za protekli i tekući nedelja | Image |

**Dodatak 6.**

**SPOLJNA SUČELJA**

SADRŽAJ

|  |  |
| --- | --- |
| 1. | Hardver |

|  |  |
| --- | --- |
| 1.1. | Utičnica |

|  |  |
| --- | --- |
| 1.2. | Raspored kontakata |

|  |  |
| --- | --- |
| 1.3. | Blok dijagram |

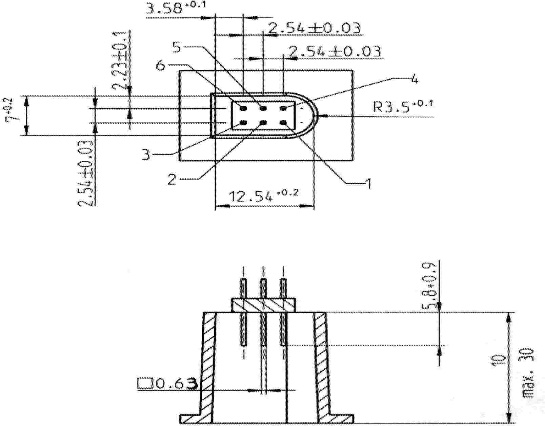
|  |  |
| --- | --- |
| 2. | Sučelje za preuzimanje Podataka |

|  |  |
| --- | --- |
| 3. | Sučelje Kalibracije |

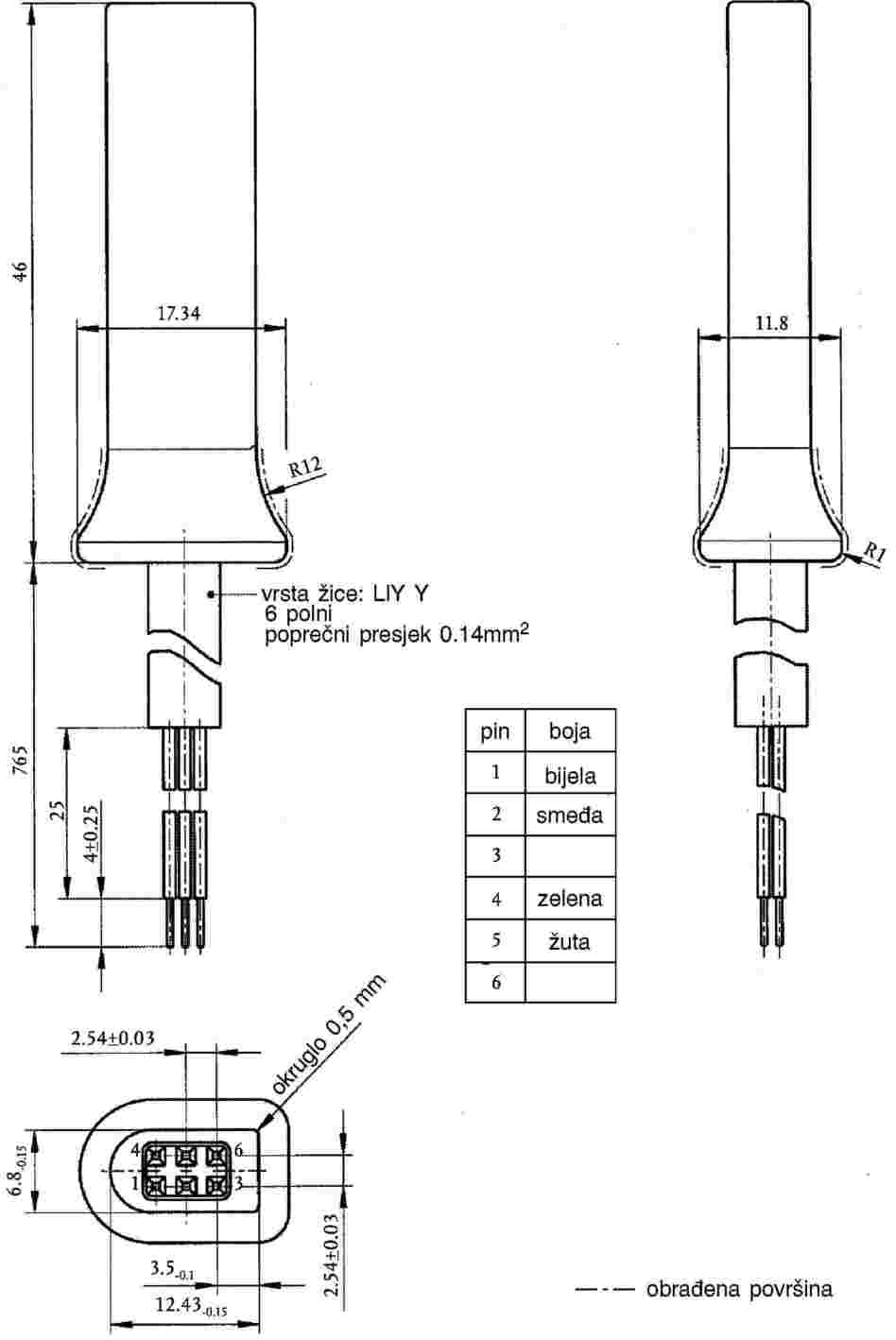
**1.   HARDVER**

**1.1.   Utičnica**

INT\_001  
Utičnica za preuzimanje podataka/kalibraciju je 6-pinski konektor, koji je dostuban s prednje strane tahografa bez potrebe isključivanja bilo kojeg dijela tahografa, i koji udovoljava sljedećem nacrtu (sve dimenzije su izražene u milimetrima):



Sljedeći dijagram prikazuje tipičan utikač za 6-pinsko uparivanje:



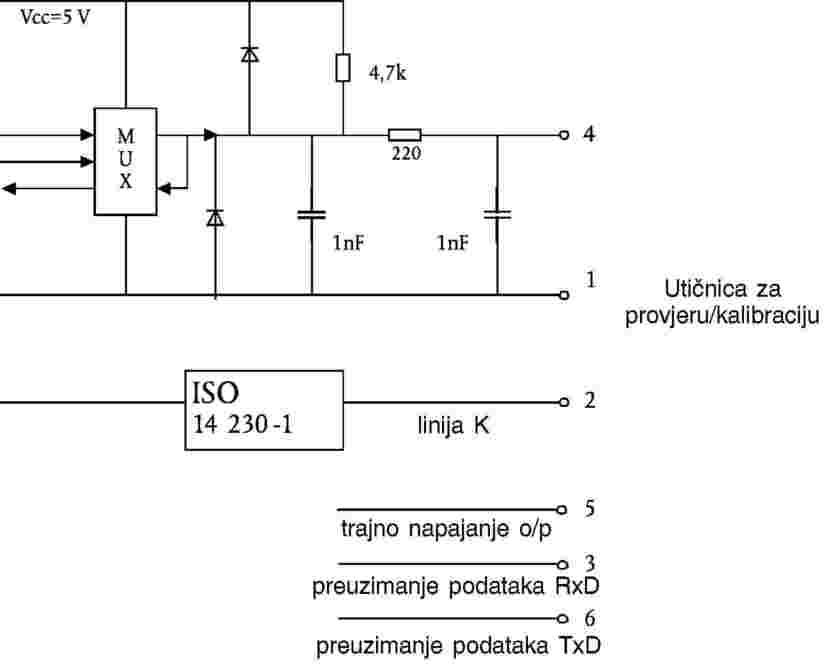
**1.2.   Raspored kontakata**

INT\_002  
Kontakti se raspoređuju prema sljedećoj tablici:

|  |  |  |
| --- | --- | --- |
| **Pin** | **Opis** | **Napomena** |
| 1 | Akumulator - minus | Priključeno na negativni pol akumulatora vozila |
| 2 | Podaci komunikacija | Linija K (po ISO 14 230-1) |
| 3 | RxD – preuzimanje podataka | Unos podataka u tahograf |
| 4 | Ulazno/izlazni signal | Kalibracija |
| 5 | Stalni izlaz napajanja | Raspon napona je onaj koji je na vozilu minus 3 V kako bi se omogućio pad napona na zaštitnim strujnim krugovima  Izlaz 40 mA |
| 6 | TxD - preuzimanje podataka | Izlaz podataka iz tahografa |

**1.3.   Blok dijagram**

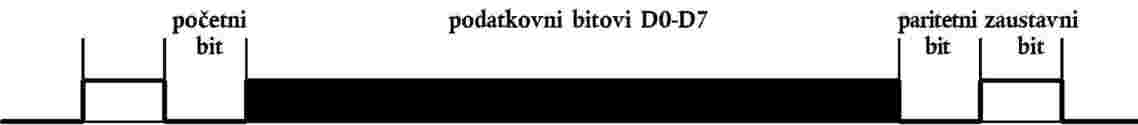
INT\_003  
Blok dijagram udovoljava sljedećem

:

**2.   SUČELJE ZA PREUZIMANJE PODATAKA**

INT\_004  
Sučelje za preuzimanje podataka udovoljava specifikacijama RS232.

INT\_005Sučelje za preuzimanje podataka koristi jedan početni bit, 8 podakovnih bitova, s LSB (najmanje značajnim bitom) na početku, jedan parno paritetni bit i 1 zaustavni bit.



Kod prenosa numeričkih podataka sastavljenih od više bajtova, najznačajniji bajt se prenosi prvi, a najmanje značajan bajt posljednji.

INT\_006  
Brzine prenosa podataka moraju biti prilagodljive od 9 600 bps do 115 200 bps. Prenos se mora postići pri najvišoj mogućoj brzini prenosa, kod čega je početna brzina prenosa podataka nakon početka komunikacije postavljena na 9 600 bps.

**3.   SUČELJE KALIBRACIJE**

INT\_007  
Podaci komunikacija mora zadovoljiti ISO 14 230-1 Drumska vozila – dijagnostički sistemi – protokol s ključnom riječi 2000 - Dio 1.: Fizički nivo, Prvo izdanje: 1999.

INT\_008  
Ulazno/izlazni signal mora zadovoljiti sljedećem električnom opisu:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Parametar** | **Minimalno** | **Tipično** | **Maksimalno** | **Napomena** |
| Ulow (in) |  |  | 1,0 V | I = 750 μΑ |
| Uhigh (in) | 4 V |  |  | I = 200 μΑ |
| Frekvencija |  |  | 4 kHz |  |
| Ulow (in) |  |  | 1,0 V | I = 1 mA |
| Uhigh (out) | 4 V |  |  | I = 1 mA |

INT\_009  
Ulazno/izlazni signal mora zadovoljiti sljedećim vremenskim dijagramima:

|  |  |
| --- | --- |
| signal senzora (out) | Image |
| ispitni signal (in) | Image |
| signal UTC sata (out) | Image |

**Dodatak 7.**

**PROTOKOLI PREUZIMANJA PODATAKA**

SADRŽAJ

|  |  |
| --- | --- |
| 1. | Uvod … |

|  |  |
| --- | --- |
| 1.1. | Područje primjene … |

|  |  |
| --- | --- |
| 1.2. | Skraćenice i zabilješke … |

|  |  |
| --- | --- |
| 2. | Preuzimanje podataka s jedinice vozila … |

|  |  |
| --- | --- |
| 2.1. | Postupak preuzimanja podataka … |

|  |  |
| --- | --- |
| 2.2. | Protokol preuzimanja podataka … |

|  |  |
| --- | --- |
| 2.2.1. | Struktura poruke … |

|  |  |
| --- | --- |
| 2.2.2. | Vrste poruka … |

|  |  |
| --- | --- |
| 2.2.2.1. | Zahtjev za početak komunikacije (SID 81) … |

|  |  |
| --- | --- |
| 2.2.2.2. | Pozitivan odgovor za početak komunikacije (SID C1) … |

|  |  |
| --- | --- |
| 2.2.2.3. | Zahtjev za početak dijagnostičkog procesa (SID 10) … |

|  |  |
| --- | --- |
| 2.2.2.4. | Pozitivan odgovor za početak dijagnostike (SID 50) … |

|  |  |
| --- | --- |
| 2.2.2.5. | Servis upravljanja vezom (SID 87) … |

|  |  |
| --- | --- |
| 2.2.2.6. | Pozitivan odgovor na zahtjev za upravljanje vezom (SID C7) … |

|  |  |
| --- | --- |
| 2.2.2.7. | Zahtjev za prihvat podataka (SID 35) … |

|  |  |
| --- | --- |
| 2.2.2.8. | Pozitivan odgovor na zahtjev za prihvat podataka (SID 75) … |

|  |  |
| --- | --- |
| 2.2.2.9. | Zahtjev za prenos podataka (SID 36) … |

|  |  |
| --- | --- |
| 2.2.2.10. | Pozitivan odgovor za prenos podataka (SID 76) … |

|  |  |
| --- | --- |
| 2.2.2.11. | Zahtjev za prekid prenosa (SID 37) … |

|  |  |
| --- | --- |
| 2.2.2.12. | Pozitivan odgovor na zahtjev za prekid prenosa (SID 77) … |

|  |  |
| --- | --- |
| 2.2.2.13. | Zahtjev za prekid komunikacije (SID 82) … |

|  |  |
| --- | --- |
| 2.2.2.14. | Pozitivan odgovor na zahtjev za prekid komunikacije (SID C2) … |

|  |  |
| --- | --- |
| 2.2.2.15. | Potvrda dijela poruke (SID 83) … |

|  |  |
| --- | --- |
| 2.2.2.16. | Negativan odgovor (SID 7F) … |

|  |  |
| --- | --- |
| 2.2.3. | Protok poruke … |

|  |  |
| --- | --- |
| 2.2.4. | Vremenski termini … |

|  |  |
| --- | --- |
| 2.2.5. | Obrada grešaka … |

|  |  |
| --- | --- |
| 2.2.5.1. | Faza početka komunikacije … |

|  |  |
| --- | --- |
| 2.2.5.2. | Faza komunikacije … |

|  |  |
| --- | --- |
| 2.2.6. | Sadržaj poruke odgovora … |

|  |  |
| --- | --- |
| 2.2.6.1. | Pozitivan odgovor za prenos pregleda podataka … |

|  |  |
| --- | --- |
| 2.2.6.2. | Pozitivan odgovor za prenos podataka o aktivnostima … |

|  |  |
| --- | --- |
| 2.2.6.3. | Pozitivan odgovor za prenos podataka o događajima i greškama … |

|  |  |
| --- | --- |
| 2.2.6.4. | Pozitivan odgovor za prenos detaljnih podataka o brzini … |

|  |  |
| --- | --- |
| 2.2.6.5. | Pozitivan odgovor za prenos tehničkih podataka … |

|  |  |
| --- | --- |
| 2.3. | Čuvanje datoteke ESM … |

|  |  |
| --- | --- |
| 3. | PROTOKOL PREUZIMANJA PODATAKA S KARTICE TAHOGRAFA … |

|  |  |
| --- | --- |
| 3.1. | Područje primjene … |

|  |  |
| --- | --- |
| 3.2. | Definicije … |

|  |  |
| --- | --- |
| 3.3. | Preuzimanje podataka s kartice … |

|  |  |
| --- | --- |
| 3.3.1. | Slijed inicijalizacije … |

|  |  |
| --- | --- |
| 3.3.2. | Slijed za nepotpisane datoteke podataka… |

|  |  |
| --- | --- |
| 3.3.3. | Slijed za potpisane datoteke podataka … |

|  |  |
| --- | --- |
| 3.3.4. | Slijed vraćanja brojača kalibracija u početno stanje … |

|  |  |
| --- | --- |
| 3.4. | Format spremanja podataka … |

|  |  |
| --- | --- |
| 3.4.1. | Uvod … |

|  |  |
| --- | --- |
| 3.4.2. | Format datoteke … |

|  |  |
| --- | --- |
| 4. | Preuzimanje podataka s kartice tahografa preko jedinice u vozilu … |

**1.   UVOD**

Ovaj Dodatak navodi postubke za obavljanje različitih vrsta preuzimanja podataka na spoljni medij za čuvanje, zajedno s protokolima koje treba provesti kako bi se osigurao ispravan prenos podataka i potpuna shodnost formata preuzetih podataka koji omogućava svakom kontroloru da pregleda takve podatke i da može kontrolisati njihovu vjerodostojnost i potpunost prije analize.

**1.1.   Područje primjene**

Podaci se mogu preuzeti na ESM:

* iz jedinice u vozilu posebnom namjenskom opremom (IDE) priključenom na jedinicu vozila,
* s kartice tahografa putem IDE opremljenom uređajem kartičnog sučelja (IFD),
* s kartice tahografa preko jedinice u vozilu putem IDE priključenim na jedinicu vozila.

Da bi se omogućila provjera vjerodostojnosti i potpunosti preuzetih podataka sačuvanih na ESM, podaci se preuzimaju potpisom stavljenim shodno Dodatku 11. Zajednički sigurnosni mehanizmi. Identifikacija uređaja izvora (jedinica vozila ili kartica) i njegovi sigurnosni certifikati (države članice i opreme) se takođe preuzimaju. Onaj ko provjerava podatke mora nezavisno posjedovati povjerljiv evropski javni ključ.

DDP\_001  
Podaci preuzeti tokom jednog procesa preuzimanja podataka se moraju sačuvati u ESM unutar jedne datoteke.

**1.2.   Skraćenice i zabilješke**

U ovom se Dodatku koriste sljedeće skraćenice:

|  |  |
| --- | --- |
| AID | identifikator aplikacije |
| ATR | odziv na vraćanje u početno stanje |
| CS | bajt kontrolnog zbira |
| DF | namjenska datoteka |
| DS\_ | dijagnostički proces |
| EF | elementarna datoteka |
| ESM | spoljni medij za čuvanje podataka |
| FID | identifikator datoteke (ID datoteke) |
| FMT | formatni bajt (prvi bajt glave poruke) |
| ICC | kartica s integirsanim sklopom |
| IDE | posebna namjenska oprema: Oprema koja se koristi za preuzimanje podataka na ESM (npr. osobno računalo) |
| IFD | uređaj sučelja |
| KWP | protokol s ključnom riječi 2000 |
| LEN | bajt dužine (posljednji bajt glave poruke) |
| PPS | protokol biranja parametra |
| PSO | izvođenje sigurnosne radnje |
| SID | identifikator službe |
| SRC | izvorni bajt |
| TGT | ciljni bajt |
| TLV | vrijednost dužine oznake |
| TREP | parametar odziva prenosa |
| TRTP | parametar zahtjeva za prenos |
| VU | jedinica u vozilu. |

**2.   PREUZIMANJE PODATAKA S JEDINICE VOZILA**

**2.1.   Postupak preuzimanja podataka**

Za preuzimanje podataka s jedinice vozila operator mora obaviti sljedeće radnje:

* umetnuti svoju karticu tahografa unutar otvora jedinice vozila (16),
* priključiti IDE na priključnicu za preuzimanje podataka jedinice vozila,
* uspostaviti vezu između IDE i jedinice vozila,
* odabrati na IDE podatke za preuzimanje i poslati zahtjev u jedinicu vozila,
* zaključiti sesiju preuzimanja podataka.

**2.2.   Protokol preuzimanja podataka**

Protokol je strukturiran na načelu nadređen-podređen, kod čega IDE ima nadređenu, a jedinica vozila podređenu ulogu.

Struktura, vrste i protok poruka su načelno utemeljena na protokolu ključne riječi 2000 (KWP) (ISO 14230-2 Drumska vozila – Dijagnostički sistemi – Protokol ključne riječi 2000 - Dio 2.: Nivo podakovnih veza).

Aplikacijska nivo se u načelu temelji na sadašnjem nacrtu ISO 14229-1 (Drumska vozila – Dijagnostički sistemi – Dio 1. Dijagnostičke službe, verzija 6. od 22. veljače 2001.).

**2.2.1.    Struktura poruke**

DDP\_002  
Sve poruke koje se razmjenjuju između IDE i jedinice vozila su formatirane u strukturi koja se sastoji od tri dijela:

* glava koju čini formatni bajt (FMT), ciljni bajt (TGT), izvorni bajt (SRC) i moguće bajt za dužinu (LEN),
* podakovno polje koje čine bajt identifikatora službe (SID) i promjenjiv broj podakovnih bajtova koji može obuhvaćati neobavezni bajt dijagnostičkog procesa (DS) ili neobavezni bajt parametara prenosa (TRTP ili TREP),
* kontrolni zbir kojega čini bajt kontrolnog zbira (CS).

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Zaglavlje** | | | | **Podakovno polje** | | | | | **Kontrolni zbir** |
| FMT | TGT | SRC | LEN | SID | Podaci | … | … | … | CS |
| 4 bajta | | | | najviše 225 bajtova | | | | | 1 bajt |

Bajt TGT i SRC predstavljaju fizičku adresu primatelja i tvorca poruke. Vrijednosti su F0 Hex za IDE i EE Hex za jedinicu vozila.

Bajt LEN je dužina dijela podakovnog polja.

Bajt ispitnog zbira je 8-bitni zbir serije modula 256 svih bajtova poruke s izuzekom samog CS.

Bajtovi FMT, SID, DS\_, TRTP i TREP su definirani u nastavu ovog dokumenta.

DDP\_003  
Kada su podaci koje prenosi poruka duži od prostora koji je raspoloživ u dijelu podakovnog polja, poruka se u stvarnosti šalje u nekoliko dijelova poruke. Svaki dio poruke nosi glavu, isti SID, TREP i 2-bajtni brojač dijelova poruke koji označava broj dijelova poruke u cjelokupnoj poruci. Kako bi se omogućilo provjeravanje grešaka i prekid, IDE potvrđuje svaki dio poruke. IDE može primiti dio poruke, tražiti da se ona ponovo prenese, zahtijevati od jedinice vozila da ponovo počne ili prekine prenos.

DDP\_004  
Ako posljednji dio poruke sadrži točno 255 bajtova u podakovnom polju, zadnji dio poruke se mora staviti s praznim podakovnim poljem (osim SID TREP i brojača dijelova poruke) kako bi se označio kraj poruke.

Primjer:

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | |  |  |  |  |  | | --- | --- | --- | --- | --- | | Zaglavlje | SID | TREP | Poruka | CS | | 4 bajta | Više od 255 bajtova | | |  | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | ce se prenijeti kao:   |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | |  | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | Zaglavlje | SID | TREP | 00 | 01 | Dio poruke1 | CS | | 4 bajta | 255 bajtova | | | | |  | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | |  | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | Zaglavlje | SID | TREP | 00 | 01 | Dio poruke 2 | CS | | 4 bajta | 255 bajtova | | | | |  | |  |  |  | | --- | --- | |  | … |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | |  | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | Zaglavlje | SID | TREP | xx | yy | Dio poruke n | CS | | 4 bajta | Manje od 255 bajtova | | | | |  | | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | ili kao:   |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | |  | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | Zaglavlje | SID | TREP | 00 | 01 | Dio poruke1 | CS | | 4 bajta | 255 bajtova | | | | |  | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | |  | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | Zaglavlje | SID | TREP | 00 | 02 | Dio poruke2 | 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 vozila i IDE zahtijeva razmjenu osam različitih vrsta poruka.

Sljedeća tabela prikazuje sažeti prikaz takvih poruka.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Struktura poruke**  **IDE -> <- VU** | | **Najviše 4 bajta Zaglavlje** | | | | **Najviše 255 bajtova Podaci** | | | **1 bajt Kontrolni zbir** |
| **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 | 9B |
| Zahtjev za početak dijagnostičkog procesa | | 80 | EE | F0 | 02 | 10 | 81 |  | F1 |
| Pozitivan odgovor za početak dijagnostike | | 80 | F0 | EE | 02 | 50 | 81 |  | 31 |
| Parametri kontrolne veze | |  | | | | | | | |
|  | Provjera brzine prenosa podataka (faza 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 zahtjev za provjeru brzine prenosa podataka | | 80 | F0 | EE | 02 | C7 |  | 01 | 28 |
| Prelazna brzina prenosa podataka (faza 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 | |  |  |  |  |  |  |  |  |
|  | Pregled | 80 | EE | F0 | 02 | 36 | 01 |  | 97 |
|  | Aktivnosti | 80 | EE | F0 | 06 | 36 | 02 | Datum | CS |
| Događaji i greške | 80 | EE | F0 | 02 | 36 | 03 |  | 99 |
| Detaljna brzina | 80 | EE | F0 | 02 | 36 | 04 |  | 9A |
| Tehnički podaci | 80 | EE | F0 | 02 | 36 | 05 |  | 9B |
|  | Preuzimanje podataka sa kartice | 80 | EE | F0 | 02 | 36 | 06 |  | 9C |
| Pozitivan odgovor za prenos podataka | | 80 | F0 | EE | Len | 76 | TREP | Podatak | 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 |  |  | El |
| Pozitivan odgovor na za prekid komunikacije | | 80 | F0 | EE | 01 | C2 |  |  | 21 |
| Potvrda dijela poruke | | 80 | EE | F0 | Len | 83 |  | Podatak | CS |
| Negativni odgovori | |  | | | | | | | |
| Opšti odbacivanje | | 80 | F0 | EE | 03 | 7F | Sid Req | 10 | CS |
| Servis nije podržan | | 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 | FO | EE | 03 | 7F | Sid Req | 13 | CS |
| Neispravni uslovi ili greška slijeda zahtjeva | | 80 | F0 | EE | 03 | 7F | Sid Req | 22 | CS |
| Zahtjev van dosega | | 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 dostubni | | 80 | F0 | EE | 03 | 7F | Sid Req | FA | CS |
| * Sid Req = Sid odgovarajućeg zahtjeva. * TREP = TRTP odgovarajućeg zahtjeva. * Osjenčana polja označivaju da se ne prenosi ništa. * Izraz prihvat (s gledišta IDE) se koristi zbog usklađenosti s ISO 14229. Znači isto što i preuzimanje podataka (s gledišta VU). * Potencijalni 2-bitni brojači dijelova poruke nisu prikazani u ovoj tablici. | | | | | | | | | |

**2.2.2.1.   Zahtjev za početak komunikacije (SID 81)**

DDP\_005  
Ovu poruku izdaje IDE za uspostavljanje komunikacijske veze s jedinicom vozila. Početne komunikacije se uvijek obavljaju pri brzini od 9 600 bauda (dok se brzina prenosa podataka eventualno ne promijeni korištenjem odgovarajućih servisa za upravljanje vezom).

**2.2.2.2.   Pozitivan odgovor za početak komunikacije (SID C1)**

DDP\_006  
Ovu poruku izdaje jedinica vozila kao pozitivan odgovor na zahtjev za početak komunikacije. Ona sadrži 2 ključna bajta ‚EA’,8F’ koji označivaju da jedinica podržava protokol sa zaglavljem koje sadrži podatke o ciljanom,izvoru i dužini.

**2.2.2.3.   Zahtjev za početak dijagnostičkog procesa (SID 10)**

DDP\_007  
Poruku sa zahtjevom za početak dijagnostičkog procesa šalje IDE kako bi zahtijevao novi dijagnostički proces sa jedinicom vozila. Podfunkcija ‚zadani proces’ (81 Hex) označava da je potrebno otvoriti standardni dijagnostički proces.

**2.2.2.4.   Pozitivan odgovor za početak dijagnostike (SID 50)**

DDP\_008  
Pozitivan odgovor na poruku za početak dijagnostike šalje jedinica vozila kao pozitivan odgovor na zahtjev za početak dijagnostičkog procesa.

**2.2.2.5.   Servis upravljanja vezom (SID 87)**

DDP\_052  
Servis kontrole veze koristi IDE da bi započela s promjenom brzine prenosa podataka. Ovo se odvija u dva koraka. U prvom koraku IDE predlaže promjenu brzine prenosa podataka navodeći novu brzinu. Po primitku pozitivne poruke iz jedinice vozila, IDE odašilje potvrdu promjene brzine prenosa podataka u jedinicu vozila (drugi korak). IDE potom prelazi na novu brzinu prenosa podataka. Po primitku potvrde jedinica vozila 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 izdaje jedinica vozila kao pozitivan odgovor na zahtjev za servis upravljanja vezama (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 izdaje IDE kako bi je jedinica vozila obavijestila da je radnja prihvata podatka zatražena. Za zadovoljavanje uslova ISO14229, obuhvaćeni su podaci koji sadrže pojedinosti o adresi, veličini i formatu zahtijevanih podataka. Obzirom da ih IDE ne poznaje prije prihvata podatka, adresa memorije se postavlja 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 šalje jedinica vozila kako bi ukazala IDE da je jedinica vozila spremna za preuzimanje podataka. Za udovoljavanje zahtjeva ISO 14229, podaci su obuhvaćeni u ovoj poruci s pozitivnim odgovorom, ukazujući IDE da će dalje poruke s pozitivnim odgovorom na zahtjev za prenos podataka sadržavati najviše 00FFh bajtova.

**2.2.2.9.   Zahtjev za prenos podataka (SID 36)**

DDP\_011  
Zahtjev za prenos podataka šalje IDE da bi jedinica vozila ukazala na vrstu podataka koje treba preuzeti. Jednobajtni parametar zahtjeva za prenos podataka (TRTP) označava vrstu prenosa.

Postoji šest vrsta prenosa podataka:

* pregled (TRTP 01),
* aktivnosti navedenog dana (TRTP 02),
* događaji i greške (TRTP 03),
* detaljna brzina (TRTP 04),
* tehnički podaci (TRTP 05),
* preuzimanje podataka sa kartice (TRTP 06).

DDP\_054  
IDE mora obavezno zahtijevati prenos pregleda podataka (TRTP 01) tokom procesa preuzimanja podataka obzirom da će samo to osigurati da se certifikati jedinice vozila zaevidentiraju unutar preuzete datoteke (i omogućiti provjeru digitalnog potpisa).

U drugom slučaju (TRTP 02) poruka sa zahtjevom za prenos podataka obuhvaća oznaku kalendarskog dana (u formatuImage ) za kojega treba preuzeti podatke.

**2.2.2.10.   Pozitivan odgovor za prenos podataka (SID 76)**

DDP\_012  
Pozitivan odgovor za prenos podataka šalje jedinica vozila 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), jedinica vozila će poslati podatke koji pomažu operatoru IDE da izabere podatke koje želi dalje preuzeti. Informacija sadržana u ovoj poruci je sljedeća:

* sigurnosni certifikati,
* identifikacija vozila,
* tekući datum i vrijeme jedinice vozila,
* najstariji i najraniji datum za koje je moguće preuzeti podatke (podaci iz jedinice vozila),
* oznaka prisustva kartice u jedinici vozila,
* prethodno preuzimanje podataka za potrebe preduzeća,
* zaključavanja podataka preduzeća,
* prethodni nadzor.

**2.2.2.11.   Zahtjev za prekid prenosa (SID 37)**

DDP\_013  
Zahtjev za prijekid prenosa šalje IDE kako bi obavijestio jedinicu vozila 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 prijekid prenosa šalje jedinica vozila kako bi potvrdila zahtjev za prekid prenosa.

**2.2.2.13.   Zahtjev za prekid komunikacije (SID 82)**

DDP\_015  
Poruka sa zahtjevom za prekid komunikacije šalje IDE za prekid komunikacijske veze s jedinicom vozila.

**2.2.2.14.   Pozitivan odgovor na zahtjev za prekid komunikacije (SID C2)**

DDP\_016  
Poruku s pozitivnim odgovorom na prekid komunikacije šalje jedinica vozila za potvrdu zahtjeva za prekid komunikacije.

**2.2.2.15.   Potvrda dijela poruke (SID 83)**

DDP\_017  
Potvrdu dijela poruke šalje IDE za potvrdu primitka svakog dijela poruke koji se prenosi u više dijelova poruka. Podakovno polje sadrži SID koji se prima sa jedinice vozila i 2-bajtnu šifru kako slijedi:

* MsgC + 1 potvrđuje ispravan prijem broja dijela poruke MsgC.
* Zahtjev šalje IDE prema jedinici vozila da pošalje sljedeći dio poruke.
* MsgC ukazuje na problem s prijemom broja dijela poruke MsgC.
* Zahtjev ponovno šalje IDE prema jedinici vozila da pošalje dio poruke.
* FFFF zahtijeva kraj poruke.

Ovim se postubkom može služiti IDE za okončanje prenosa poruke iz jedinice vozila iz bilo kojeg razloga.

Posljednji dio neke poruke (bajt LEN < 255) se može potvrditi korištenjem bilo koje od ovih šifri ili se ne mora potvrditi.

Odgovori jedinice vozila koji se sastoje od više dijelova poruke su sljedeći:

* pozitivan odgovor na prenos podataka (SID 76)

**2.2.2.16.   Negativan odgovor (SID 7F)**

DDP\_018  
Poruku s negativnim odgovorom jedinica vozila šalje kao odgovor na gore navedene poruke zahtjeva ako jedinica vozila ne može udovoljiti zahtjevu. Podaci polja poruke sadrže SID odgovore (7F), SID zahtjeva i šifru koja označava razlog za negativan odgovor. Na raspolaganju su sljedeće šifre:

* 10 opšti odbacivanje

Radnja se ne može obaviti zbog razloga koji nije dolje naveden

* 11 servis nije podržan

SID zahtjeva nije razumljiv

* 12 podfunkcija se ne podržava

DS\_ ili TRTP zahtjeva nije razumljiv ili nema daljnjih dijelova poruke koje treba prenijeti

* 13 neispravna dužina poruke

Dužina primljene poruke je pogrešna

* 22 uslovi nisu ispravni ili greška slijeda zahtjeva

Zahtijevani servis nije aktivan ili slijed poruka zahtjeva nije ispravan

* 31 zahtjev van djelokruga

Zapis parametra zahtjeva (podakovno polje) nije valjan

* 50 prihvat podataka se ne prihvaća

Zahtjev se ne može izvršiti (jedinica vozila u neprimjerenom režimu rada ili unutarnja greška jedinice vozila)

* 78 čekanje na odgovor

Zahtijevana radnja se ne može pravovremeno dovršiti i jedinica vozila nije spremna za prihvaćanje drugog zahtjeva

* FA podaci nisu dostubni

Podakovni objekt zahtjeva za prenos podataka nije dostuban u jedinici vozila (npr. nije umetnuta kartica, …)

**2.2.3.    Protok poruke**

Tipičan protok poruke tokom redovnog postubka preuzimanja podataka je sljedeći:

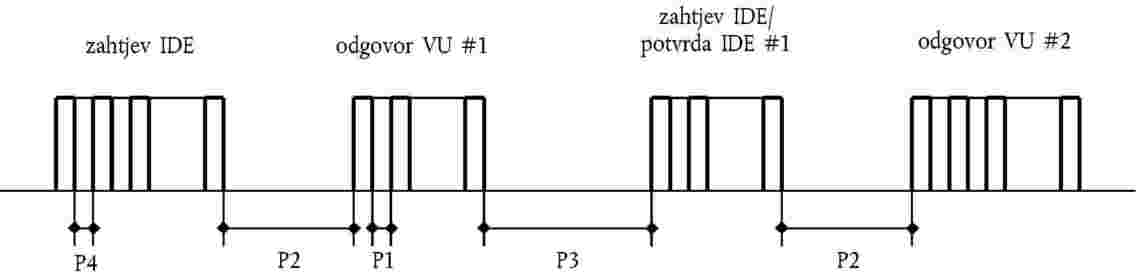
|  |  |  |
| --- | --- | --- |
| **IDE** |  | **VU** |
| Zahtjev za početak komunikacije | Image |  |
|  | Image | Pozitivan odgovor |
| Zahtjev za početak dijagnostičke aktivnosti | Image |  |
|  | Image | Pozitivan odgovor |
| Zahtjev za prihvat podataka | Image |  |
|  | Image | Pozitivan odgovor |
| Zahtjev za prenos pregleda podataka | Image |  |
|  | Image | Pozitivan odgovor |
| Zahtjev za podatke #2 | Image |  |
|  | Image | Pozitivan odgovor #1 |
| Potvrda dijela poruke #1 | Image |  |
|  | Image | Pozitivan odgovor #2 |
| Potvrda dijela poruke #2 | Image |  |
|  | Image | Pozitivni odgovor #m |
| Potvrda dijela poruke #m | Image |  |
|  | Image | Pozitivan odgovor (podakovno polje < 255 bajtova) |
| Potvrda dijela poruke (neobvezno) | Image |  |
| … | | |
| Zahtjev za prenos podataka #n | Image |  |
|  | Image | Pozitivan odgovor |
| Zahtjev za prekid prenosa | Image |  |
|  | Image | Pozitivan odgovor |
| Zahtjev za prekid komunikacije | Image |  |
|  | Image | Pozitivan odgovor |

**2.2.4.    Vremenski termini**

DDP\_019  
Tokom redovnog rada mjerodavni su vremenski parametri prikazani na sljedećoj slici:

**Slika 1.**

**Protok poruke, vremenski termini**



Gdje je:

P1= međubajtno vrijeme za odgovor VU.

P2= vrijeme između kraja zahtjeva IDE i početka odziva VU, ili između kraja potvrde IDE i početka sljedećeg odgovora VU.

P3= vrijeme između kraja odziva VU i početka novog zahtjeva IDE ili između kraja odgovora VU i početka potvrde IDE, ili između kraja zahtjeva IDE i početka novog zahtjeva IED ako VU ne odgovori.

P4= međubajtno vrijeme za zahtjev IDE.

P5= produžena vrijednost P3 za preuzimanje podataka s kartice.

Dopuštene vrijednosti vremenskih parametara su prikazane u sljedećoj tablici (prošireni niz parametara tempiranja KWP, koriste 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[(17)](https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex:32002R1360#ntr17-L_2002207HR.01014801-E0002) |
| P3 | 10 | 5 000 |
| P4 | 5 | 20 |
| P5 | 10 | 20 minuta |

**2.2.5.    Obrada grešaka**

Ako tokom razmjene poruka dođe do greške, shema protoka poruke se mijenja zavisno o tome koja oprema je ustanovila grešku i o poruci koja uzrokuje grešku.

Na slikama 2. i 3. prikazani su postubci obrade greške za jedinicu vozila odnosno IDE.

**2.2.5.1.   Faza početka komunikacije**

DDP\_020  
Ako IDE ustanovi grešku u fazau početka komunikacije, zbog vremena ili zbog protoka bitova, čekat će u trajanju od P3 min prije ponovnog izdavanja zahtjeva.

DDP\_021  
Ako jedinica vozila ustanovi grešku u slijedu koji dolazi iz IDE, ona neće poslati odgovor i čekat će u trajanju od najviše P3 drugu poruku sa zahtjevom za početak komunikacije.

**2.2.5.2.   Faza komunikacije**

Mogu se odrediti dva različita područja obrade grešaka:

|  |  |
| --- | --- |
| 1. | Jedinica vozila utvrđuje grešku prenosa iz IDE.  DDP\_022 Za svaku primljenu poruku jedinica vozila mora ustanoviti greške proteka vremena, greške bajtnih formata (npr. kršenje početnog i zaustavnog bita) i okvirne greške (pogrešan broj primljenih bajtova, pogrešan bajt kontrolnog zbira).  DDP\_023 Ako jedinica vozila uoči jednu od gore spomenutih grešaka, ona ne šalje nikakav odgovor i zanemaruje primljenu poruku.  DDP\_024 Jedinica vozila može ustanoviti ostale greške u formatu ili sadržaju primljene poruke (npr. poruka se ne podržava) čak i ako poruka udovoljava zahtjevima dužine i ispitnog zbira; u tom slučaju jedinica vozila mora odgovoriti IDE porukom s negativnim odgovorom koja navodi narav greške.  **Slika 2.**  **Obrada grešaka u jedinici vozila**  Image |

|  |  |
| --- | --- |
| 2. | IDE uočava grešku prenosa iz jedinice vozila.  DDP\_025 Za svaku primljenu poruku IDE mora ustanoviti vremenske greške, greške u formatu bajtova (npr. kršenja početnog i završnog bita) i okvirne greške (pogrešan broj primljenih bajtova, pogrešan bajt kontrolnog zbira).  DDP\_026 IDE mora uočiti greške slijeda, npr. neispravan korak povećanja brojača dijelova poruke za naredne primljene poruke.  DDP\_027 Ako IDE utvrdi grešku ili nema odgovora iz jedinice vozila u vremenu P2max, poruka sa zahtjevom će se ponovo poslati u najviše tri prenosa ukupno. Za potrebe ovog uočavanja greške, potvrda dijela poruke će se smatrati zahtjevom upućenim jedinici vozila.  DDP\_028 IDE mora čekati u trajanju od najmanje P3min prije početka svakog prenosa; period čekanja se mjeri od posljednjeg proračunatog javljanja zaustavnog bita nakon otkrivanja greške.  **Slika 3.**  **Obrada grešaka u IDE**  Image |

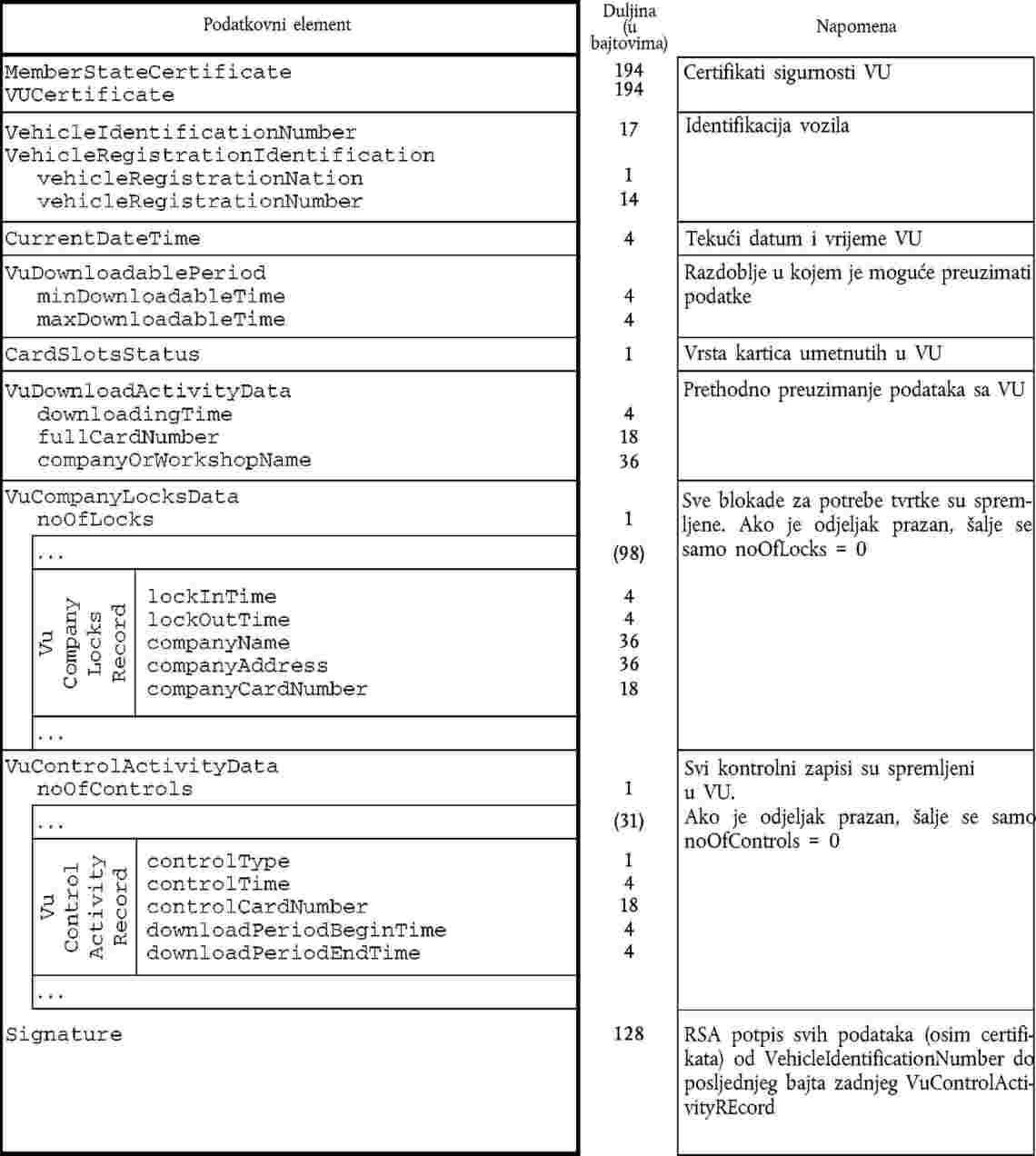
**2.2.6.    Sadržaj poruke odgovora**

Ovaj stavak navodi sadržaj podakovnih polja različitih poruka s pozitivnim odgovorom.

Podakovni elementi su definirani u rječnika podataka Dodatka 1..

**2.2.6.1.   Pozitivan odgovor za prenos pregleda podataka**

DDP\_029  
Podakovno polje poruke ‚pozitivnog odgovora za prenos pregleda podataka’ mora pružiti sljedeće podatke sljedećim redom prema SID 76h, TREP 01h i odgovarajućem prelamanju i brojanju dijelova poruke:



**2.2.6.2.   Pozitivan odgovor za prenos podataka o aktivnostima**

DDP\_030  
Podakovno polje poruke ‚pozitivnog odgovora za prenos podataka o aktivnostima’ pruža sljedeće podatke sljedećim redom prema SID 76h, TREP 02h i odgovarajućem prelamanju i brojanju dijelova poruke:



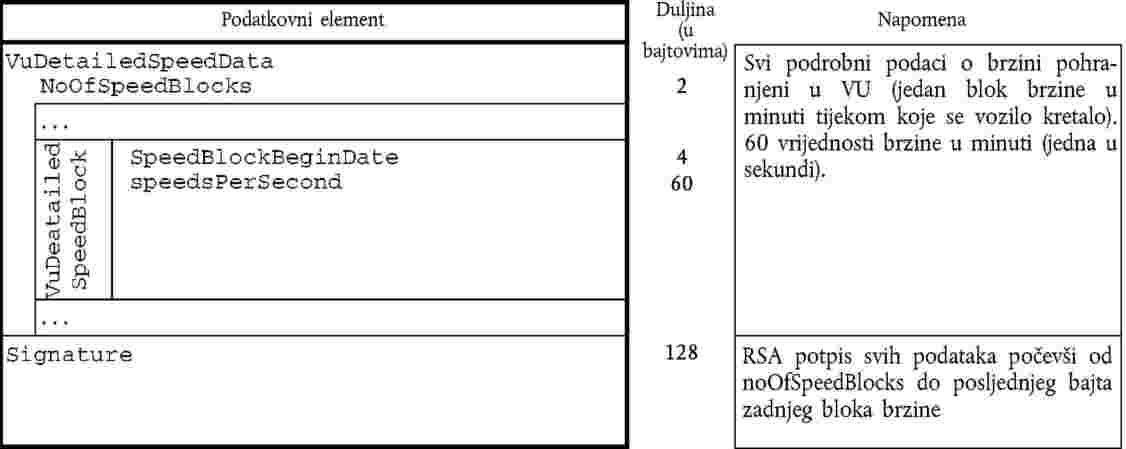
**2.2.6.3.   Pozitivan odgovor za prenos podataka o događajima i greškama**

DDP\_031  
Podakovno polje poruke ‚pozitivnog odgovora za prenos podataka o događajima i greškama’ pruža sljedeće podatke sljedećim redom prema SID 76h, TREP 03h i odgovarajućem prelamanju i brojanju dijelova poruke:



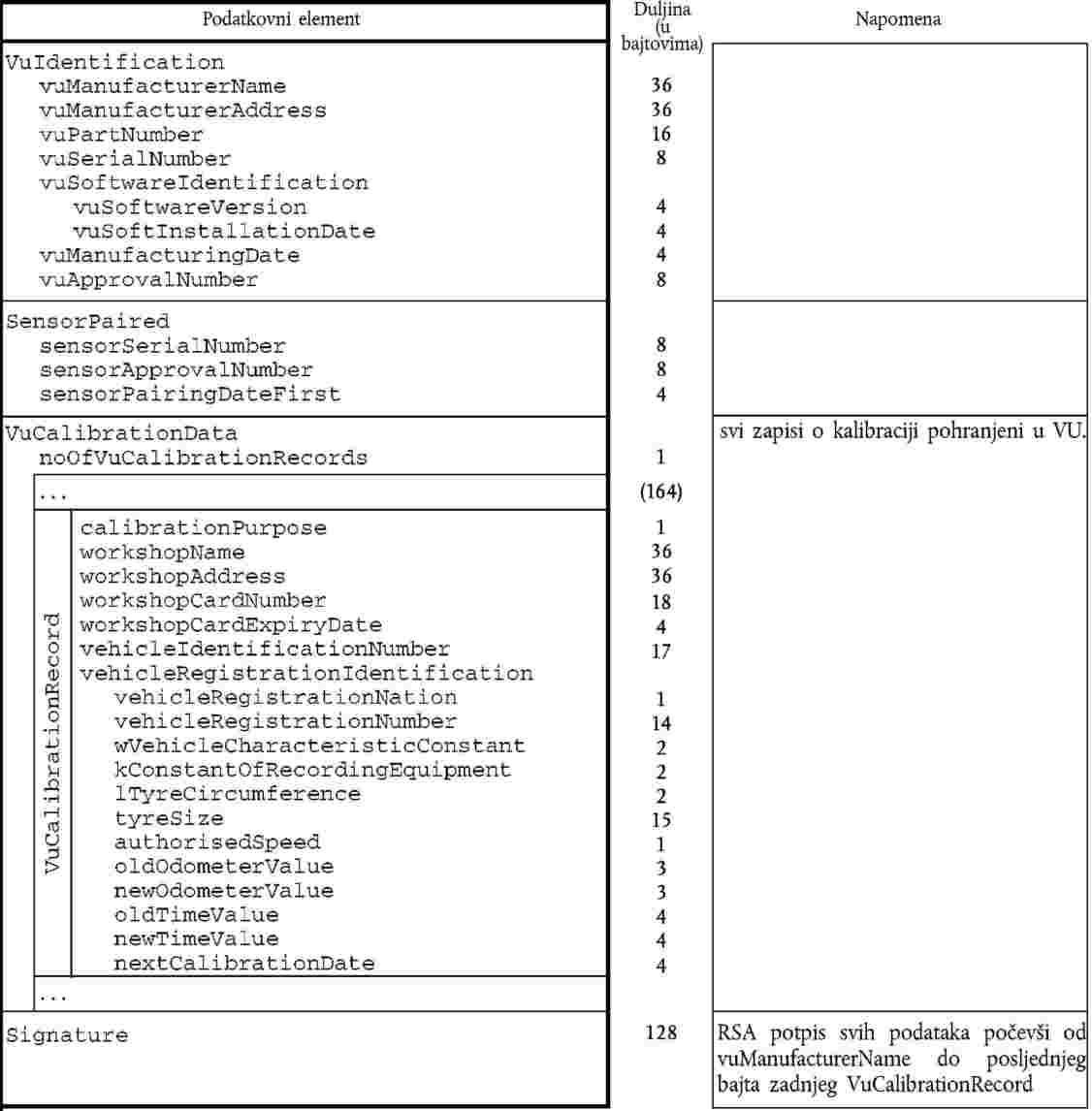
**2.2.6.4.   Pozitivan odgovor za prenos detaljnih podataka o brzini**

DDP\_032  
Podakovno polje poruke ‚pozitivan odgovor za prenos detaljnih podataka o brzini’ pruža sljedeće podatke sljedećim redom prema SID 76h, TREP 04h i odgovarajućem prelamanju i brojanju dijelova poruke:



**2.2.6.5.   Pozitivan odgovor za prenos tehničkih podataka**

DDP\_033  
Podakovno polje ‚pozitivnog odgovora za prenos tehničkih podataka’ pruža sljedeće podatke sljedećim redom prema SID 76h, TREP 05h i odgovarajućem prelamanju i brojanju dijelova poruke:



**2.3.   Čuvanje datoteke ESM**

DDP\_034  
Ako je proces preuzimanja podataka obuhvatio i prenos podataka iz jedinice vozila, IDE mora sačuvati unutar jedne fizičke datoteke sve podatke koje je primio sa jedinicie vozila tokom procesa preuzimanja podataka u okviru poruka s pozitivnim odgovorom na zahtjev za prenos podataka. Arhivirani podaci ne sadrže glave 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 KARTICE TAHOGRAFA**

**3.1.   Područje primjene**

Ovaj stavak opisuje direktno preuzimanje podataka s kartice tahografa na IDE. IDE nije dio sigurnog okruženja; stoga se ne vrši nikakva autentifikacija između kartice i IDE.

**3.2.   Definicije**

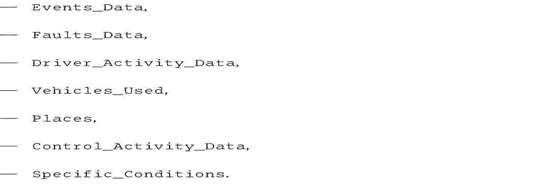
Proces preuzimanja podataka: Svaki put se obavlja preuzimanje podataka s ICC. Proces obuhvaća cjelokupan postupak od vraćanja u početno stanje ICC od strane IFD do stavljanja van pogona ICC (izvlačenje kartice ili sljedeće vraćanje u početno stanje).

Potpisana podaci datoteka: Datoteka se prenosi na IFD u običnom tekstu. Na ICC se datoteka sažima i potpisuje, a potpis se prenosi na IFD.

**3.3.   Preuzimanje podataka s kartice**

DDP\_035  
Preuzimanje podataka s kartice tahografa obuhvaća sljedeće korake:

* preuzimanje zajedničkih podataka kartice u EF Ovi podaci su neobvezni i nisu zaštićeni digitalnim potpisom,
* preuzimanje Ovaj podatak nije zaštićen digitalnim potpisom,
* bvezno je preuzeti ove datoteke u svakom procesu preuzimanja podataka.
* preuzimanje drugih podataka aplikacije EF (unutar DF ) osim EF Ovi podaci su zaštićeni digitalnim potpisom,
* obavezno je preuzeti najmanje u svakom procesu preuzimanja podataka,
* prilikom preuzimanja podataka s kartice vozača takođe je obvezno preuzeti sljedeće EF:



— prilikom preuzimanja podataka s kartice vozača, ažuriranje ,

— prilikom preuzimanja podataka s kartice radionice, vraćanje u početno stanje brojača kalibracija u EF Card\_Download.

**3.3.1.    Slijed inicijalizacije**

DDP\_036  
IDE započinje sljedećim slijedom:

|  |  |  |  |
| --- | --- | --- | --- |
| **Kartica** | **Smjer** | **IDE/IFD** | **Značenje/napomene** |
|  | Image | Vraćanje hardvera u početno stanje |  |
| ATR | Image |  |  |

Može se koristiti PPS za prijelaz na veću brzinu prenosa podataka ako ICC to podržava.

**3.3.2.    Slijed za nepotpisane podakovne datoteke**

DDP\_037  
Slijed prenosaImage je sljedeći:

|  |  |  |  |
| --- | --- | --- | --- |
| **Kartica** | **Smjer** | **IDE/IFD** | **Značenje/napomene** |
|  | Image | Odabir datoteke | Odabrati datoteku selektirajući je pomoću identifikatora datoteka |
| OK | Image |  |  |
|  | Image | Binarno čitanje | Ako datoteka sadrži više podataka nego što je veličina međumemorije čitača ili kartice, naredbu treba ponoviti dok se ne pročita cijela datoteka. |
| Podaci sa datoteke  OK | Image | Čuvanje podataka u ESM | prema 3.4. (Format spremanja podataka) |

Napomena: Prije biranjaImage EF, mora se odabrati tahografska aplikacija (odabir putem AID).

**3.3.3.    Slijed za potpisane podakovne datoteke**

DDP\_038  
Koristi se sljedeći slijed za svaku od sljedećih datoteka koju treba preuzeti sa njihovim potpisom:

|  |  |  |  |
| --- | --- | --- | --- |
| **Kartica** | **Smjer** | **IDE/IFD** | **Značenje/napomene** |
|  | Image | Odabir datoteke |  |
| OK | Image |  |  |
|  | Image | Sažimanje datoteke | Proračunava vrijednost sažimanja nad sadržajem podataka odabrane datoteke korištenjem propisanog algoritma funkcije sažimanja prema Prilogu 11. Ova naredba nije ISO-naredba. |
| Proračun vrijednosti sažimanja datoteke i privremeno pohranjivanje vrijednost sažimanja |  |  |  |
| OK | Image |  |  |
|  | Image | Binarno čitanje | Ako datoteka sadrži više podataka nego što je veličina međumemorije čitača ili kartice, naredbu treba ponoviti dok se ne pročita cijela datoteka. |
| Podaci datoteke  OK | Image | Čuvanje primljenih podataka u ESM | prema 3.4. (Format za čuvanje podataka |
| OK | Image | PSO: Proračun digitalnog potpisa |  |
| Zaštitna radnja ‚proračuna digitalnog potpisa’ korištenjem privremeno sačuvane vrijednosti sažimanja |  |  |  |
| Potpis  OK | Image | Stavljanje podataka uz prethodno sačuvane podatke na ESM | prema 3.4. (Format za čuvanje podataka) |

**3.3.4.    Slijed vraćanja brojača kalibracija u početno stanje**

DDP\_039  
Slijed vraćanja u početno stanje brojačaImage na kartici radionice je sljedeći:

|  |  |  |  |
| --- | --- | --- | --- |
| **Kartica** | **Smjer** | **IDE/IFD** | **Značenje/napomene** |
|  | Image | Image | Odabir pomoću identifikatora datoteke |
| OK | Image |  |  |
|  | Image | Binarno ažuriranje  Image |  |
| Vraćanje broja preuzimanja podataka s kartice u početno stanje |  |  |  |
| OK | Image |  |  |

**3.4.   Format spremanja podataka**

**3.4.1.    Uvod**

DDP\_040  
Preuzeti podaci se moraju pohranjivati u skladu sa sljedećim uslovima:

* podatke se sprema transparentno. To znači da se poredak bajtova kao i poredak bitova unutar bajtova koji se prenose s kartice mora očuvati tokom pohranjivanja,
* svi podaci s kartice koji su preuzeti tokom procesa preuzimanja se spremaju u jednoj datoteci na ESM.

**3.4.2.    Format datoteke**

DDP\_041  
Format datoteke je niz više TLV objekata.

DDP\_042  
Znak za EF je FID plus dodatak ‚00’.

DDP\_043  
Znak potpisa EF 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 je rezervirana za buduću upotrebu.

DDP\_045  
Ako datoteka nije preuzeta, ništa što se odnosi na datoteku se ne smije sačuvati (nikakva oznaka i nikakva nulta dužina).

DDP\_046  
Potpis se arhivira kao sljedeći objekt TLV direktno nakon TLV objekta koji sadrži podatke datoteke.

|  |  |  |
| --- | --- | --- |
| **Definicija** | **Značenje** | **Dužina** |
| FID (2 bajta) || ‚00’ | Oznaka za EF (FID) | 3 bajta |
| FID (2 bajta) || ‚01’ | Znak za potpis EF(FID) | 3 bajta |
| XX XX | Dužina polja vrijednosti | 2 bajta |

Primjer podataka u preuzetoj datoteci na ESM:

|  |  |  |
| --- | --- | --- |
| **Oznaka:** | **Dužina:** | **Vrijednost** |
| Image | Image | Image |
| Image | Image | Image |
|  |  | … |
| Image | Image | Image |
| Image | Image | Image |

**4.   PREUZIMANJE PODATAKA S KARTICE TAHOGRAFA PREKO JEDINICE U VOZILU**

DDP\_047  
Jedinica vozila mora omogućiti preuzimanje sadržaja kartice vozača umetnute u priključeni IDE.

DDP\_048  
IDE mora poslati poruku ‚zahtjev za prenos podataka s kartice’ na jedinicu vozila za pokretanje tog načina rada (vidjeti 2.2.2.9.).

DDP\_049  
Jedinica vozila potom mora preuzeti sve podatke sa kartice, datoteku po datoteku, u skladu s protokolom preuzimanja s kartice definisanim u stavu 3. i dostaviti sve podatke primljene s kartice na IDE unutar odgovarajućeg formata datoteke TLV (vidjeti 3.4.2.) i komprimirane unutar poruke ‚pozitivan odgovor za prenos podataka’.

DDP\_050  
IDE mora vratiti podatke s kartice iz poruke ‚pozitivan odgovor za prenos podataka’ (uklanjanje svih zaglavlja, SID, TREP, brojača dijelova poruke i kontrolnih zbireva) i sačuvati ih u jednu fizičku datoteku kako je opisano u stavu 2.3.

DDP\_051  
Jedinica vozila nakon toga, prema potrebi, ažurira datotekuImage na kartici vozača.

**Dodatak 8.**

**PROTOKOL KALIBRACIJE**

SADRŽAJ

1. Uvod …

2. Izrazi, definicije i literatura …

3. Pregled servisa …

3.1. Raspoloživi servisi …

3.2. Šifre odziva …

4. Servis komunikacije …

4.1. Servis StartCommunication …

4.2. Servis StopCommunication …

4.2.1. Opis poruke …

4.2.2. Format poruka …

4.2.3. Određivanje parametara …

4.3. Servis TesterPresent …

4.3.1. Opis poruka …

4.3.2. Format poruka …

5. Servis upravljanja …

5.1. Servis StartDiagnosticSession …

5.1.1. Opis poruka …

5.1.2. Format poruka …

5.1.3. Određivanje parametara …

5.2. Servis SecurityAccess …

5.2.1. Opis poruka …

5.2.2. Format poruka – SecurityAccess – requestSeed …

5.2.3. Formati poruka – SecurityAccess – sendKey …

6. Servis prenosa podataka …

6.1. Servis ReadDataByIdentifier …

6.1.1. Opis poruka …

6.1.2. Format poruka …

6.1.3. Opis parametara …

6.2. Servis WriteDataByIdentifier …

6.2.1. Opis poruka …

6.2.2. Format poruka …

6.2.3. Određivanje parametara …

7. Upravljanje ispitnim impulsima – funkcionalna jedinica za upravljanje ulazom/izlazom …

7.1. Opis poruka …

7.1.1. Opis poruka …

7.1.2. Format poruka …

7.1.3. Određivanje parametara …

8. Formati datarecords …

8.1. Rasponi prenesenih parametara …

8.2. Formati dataRecords …

**1.   UVOD**

Ovaj Dodatak 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. Takođe opisuje upravljanje linijom ulazno/izlaznih signala na utičnici za kalibraciju.

Uspostavljanje komunikacije K-linijom je opisano u odjeljku 4. ‚Servis komunikacije’.

Ovaj Prilog upotrebljava pojam dijagnostičkih ‚aktivnost’ za određivanje opsega upravljanja putem K-linije u različitim uslovima. Standardna aktivnost je ‚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 aktivnosti se opisuje u odjeljku 5. ‚Servis upravljanja’.

CPR\_001  
‚ECUProgrammingSession’ omogućava upisivanje podataka u jedinicu u vozilu. Kod upisa podataka za kalibraciju (zahtjevi 097 i 098), jedinica u vozilu takođe mora biti u načinu rada KALIBRACIJA.

Prenos podataka putem K-linije je opisan u odjeljku 6. ‚Servis prenosa podataka’. Formati prenesenih podataka su detaljno izloženi u odjeljku 8. ‚Formati dataRecords’.

CPR\_002  
‚ECUAdjustmentSession’ omogućava izbor kalibracijskog načina rada preko U/I signala sučelja K-linije. Upravljanje kalibrisanjem U/I signala je opisano u odjeljku 7. ‚Upravljanje ispitnim impulsima – funkcionalna jedinica upravljanja ulazom/izlazom’.

CPR\_003  
U ovom dokumentu se ‚tt’ odnosi na adresu ispitnog uređaja.Iako može postojati povlaštena adresa ispitnih uređaja, jedinica vozila se ispravno odaziva na svaku adresu ispitnog uređaja. Fizička adresa jedinice vozila je 0xEE.

**2.   IZRAZI, DEFINICIJE I LITERATURA**

Protokoli, poruke i šifre greške se u načelu temelje na dosadašnjem nacrtu ISO 14229-1 (Drumska vozila - dijagnostički sistemi - dio 1.: dijagnostički servis, inačica 6. od 22. veljače 2001.).

Za identifikatore servisa, zahtjevi za servise i odzive, te za standardne parametre koriste se bajtno šifriranje i heksadecimalne vrijednosti.

Izraz ‚ispitni uređaj’ se odnosi na uređaj koji se koristi za upisivanje podataka za programiranje/kalibraciju jedinice vozila.

Izrazi ‚korisnik’ i ‚poslužitelj’ se odnose na ispitni uređaj odnosno jedinicu vozila.

Izraz ECU označava ‚elektronsku upravljačku jedinicu’ i odnosi se na jedinicu vozila.

**Literatura:**

|  |  |  |
| --- | --- | --- |
| ISO 14230-2 | : | Drumska vozila - Dijagnostički sistemi – Protokol s ključnim riječima 2000. - Dio 2: Nivo podakovnih veza. Prvo izdanje: 1999. Vozila - dijagnostički sistemi |

**3.   PREGLED SERVISA**

**3.1.   Raspoloživi servisi**

Sljedeća tabela daje pregled servisa koje će biti dostubni na tahografu i koji su definirani u ovom dokumentu.

CPR\_004  
Tabela prikazuje servise koji su dostubni u aktiviranoj dijagnostičkom procesu.

—Prvi stubac navodi servise koji su dostubni,

—drugi stubac obuhvaća broj tačke ovog Priloga ako je servis detaljnije definiran,

—treći stubac pridružuje vrijednosti identifikatora servisa za poruke zahtjeva,

—četvrti stubac navodi servise ‚StandardDiagnosticSession’ (SD) koje moraju biti ugrađene u svaku jedinicu vozila,

—peti stubac navodi servisne procese ‚ECUAdjustmentSession’ (ECUAS) koji moraju biti ugrađeni da bi se upravljalo U/I signalnom linijom u utičnici za kalibraciju na prednjoj strani jedinice vozila,

—šesti stubac navodi servise ‚ECUProgrammingSession’ (ECUPS) koji moraju biti ugrađeni da bi se programiralo parametre u jedinici vozila.

Tabela 1.

**Tabela s pregledom vrijednosti identifikatora servisa**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | | **Dijagnostički procesi** | | |
| **Naziv servisa za dijagnostiku** | **Dio br.** | **Zahtijevana Sid vrijednost** | **SD** | **ECUAS** | **ECUPS** |
| StartCommunication | 4.1. | 81 | Image | Image | Image |
| StopCommunication | 4.2. | 82 | Image |  |  |
| TesterPresent | 4.3. | 3E | Image | Image | Image |
| StartDiagnosticSession | 5.1. | 10 | Image | Image | Image |
| SecurityAccess | 5.2. | 27 | Image | Image | Image |
| ReadDataByIdentifier | 6.1. | 22 | Image | Image | Image |
| WriteDataByIdentifier | 6.2. | 2E |  |  | Image |
| InputOutputControlByIdentifier | 7.1. | 2F |  | Image |  |
| |  |  | | --- | --- | | Image | Ovaj simbol označava da je servis obavezan u ovom dijagnostičkom procesu.  Izostanak simbola označava da ovaj servis nije dozvoljen u ovom dijagnostičkom procesu. | | | | | | |

**3.2.   Šifre odziva**

Šifre odziva se definiraju za svaki servis.

**4.   SERVIS KOMUNIKACIJE**

Neki servisi su potrebni za uspostavljanje i održavanje komunikacije. Oni se ne javljaju na izvršnom nivou. Raspoloživi servisi su navedeni u sljedećoj tablici:

Tabela 2.

**Servisi komunikacije**

|  |  |
| --- | --- |
| **Naziv servisa** | **Opis** |
| StartCommunication | Korisnik zahtjeva početak komunikacijskog procesa s poslužiteljem (poslužiteljima) |
| StopCommunication | Korisnik zahtijeva prekid tekućeg komunikacijskog procesa |
| TesterPresent | Korisnik poručuje poslužitelju da je još uvijek prisutan |

CPR\_005  
Servis StartCommunication se koristi da bi započela komunikacija. Da bi se obavio neki servis, komunikaciju se mora pokrenuti, a komunikacijski parametri moraju biti primjereni željenom načinu rada.

**4.1.   Servis StartCommunication**

CPR\_006  
Po prijemu znaka primitiva StartCommunication, jedinica vozila mora provjeriti može li se zahtijevana komunikacijska veza pokrenuti u trenutačnim uslovima. Važeći uslovi za početak komunikacijske veze su opisani u dokumentu ISO 14230-2.

CPR\_007  
Potom jedinica vozila mora obaviti sve potrebne radnje za početak komunikacijske veze i šalje primitiv odziva StartCommunication s odabranim pozitivnim parametrima odziva.

CPR\_008  
Ako jedinica vozila koja je već pokrenuta (i započela je dijagnostičku aktivnost) primi novi zahtjev StartCommunication (npr. zbog ispravljanja greške u dijagnostičkom uređaju) zahtjev mora biti prihvaćen i jedinica vozila se mora ponovo pokrenuti.

CPR\_009  
Ako zbog nekog razloga komunikacijska veza ne može biti pokrenuta, jedinica vozila će i dalje raditi kao i neposredno prije pokušaja pokretanja komunikacijske veze.

CPR\_010  
Poruka sa zahtjevom StartCommunication mora biti fizički naslovljena.

CPR\_011  
Inicijalizacija jedinice vozila za servise se obavlja u postubku ‚brze inicijalizacije’:

|  |  |
| --- | --- |
| — | prije svake aktivnosti postoji period neaktivnosti sabirnice, |

|  |  |
| --- | --- |
| — | dijagnostički uređaj potom šalje obrazac za inicijalizaciju, |

|  |  |
| --- | --- |
| — | svi podaci koji su potrebni za uspostavljanje komunikacije su sadržani u odzivu jedinice vozila. |

CPR\_012  
Po završetku inicijalizacije,

|  |  |
| --- | --- |
| — | svi komunikacijski parametri se postavljaju na vrijednosti definirane u tablici 4. prema ključnim bajtovima, |

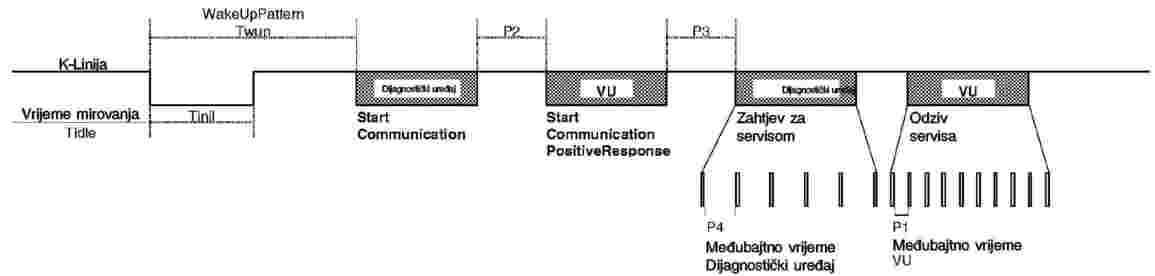
|  |  |
| --- | --- |
| — | jedinica vozila čeka na prvi zahtjev dijagnostičkog uređaja, |

|  |  |
| --- | --- |
| — | jedinica vozila je u standardnom dijagnostičkom načinu rada, tj. StandardDiagnosticSession, |

|  |  |
| --- | --- |
| — | U/I signalna linija kalibracije je u standardnom načinu rada, tj. u načinu rada van pogona. |

CPR\_014  
Brzina podataka na K-liniji mora biti 10 400 Bauda.

CPR\_016  
Brza inicijalizacija započinje kada dijagnostički uređaj prenese obrazac pobude (Wup) na K-liniji. Obrazac započinje nakon vremena mirovanja na K-liniji u vremenu smanjene aktivnosti Tinil. Ispitna jedinica prenosi prvi bit servisa StartCommunication nakon perioda Twup i prvog prekida.



CPR\_017  
Vremenski termini za prvo pokretanje i uopšteno termini veze su navedeni u tabelama u nastavu. Postoje različite mogućnosti za period mirovanja:

|  |  |
| --- | --- |
| — | prvi prenos nakon uključivanja Tidle = 300 ms. |

|  |  |
| --- | --- |
| — | nakon okončanja servisa StopCommunication, Tidle = P3 min. |

|  |  |
| --- | --- |
| — | nakon prekida komunikacije zbog isteka vremena P3 max, Tidle = 0. |

Tabela 3.

**Vremenski termini za brzo pokretanje**

|  |  |  |  |
| --- | --- | --- | --- |
| **Parametar** | | **najmanja vrijednost** | **najveća vrijednost** |
| Tinil | 25 ± 1 ms | 24 ms | 26 ms |
| Twup | 50 ± 1 ms | 49 ms | 51 ms |

Tabela 4.

**Vremenski termini komunikacije**

|  |  |  |  |
| --- | --- | --- | --- |
| **Vremenski parametar** | **Opis parametra** | **Donje granične vrijednosti (ms)** | **Gornje granične vrijednosti (ms)** |
| **najmanja** | **najveća** |
| P1 | Međubajtna vrijednost za odziv jedinice vozila | 0 | 20 |
| P2 | Vrijeme između zahtjeva dijagnostičkog uređaja i odziva VU ili dva odziva VU | 25 | 250 |
| P3 | Vrijeme između kraja odziva VU i početka novog zahtjeva dijagnostičkog uređaja | 55 | 5 000 |
| P4 | Međubajtno vrijeme za zahtjev dijagnostičkog uređaja | 5 | 20 |

CPR\_018  
Format poruka za brzo pokretanje je naveden u sljedećim tabelama:

Tabela 5.

**Poruka StartCommunication zahtjeva**

|  |  |  |  |
| --- | --- | --- | --- |
| **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 | Zahtjev za servis StarCommunication | 81 | SCR |
| #5 | Kontrolni zbir | 00-FF | CS |

Tabela 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 | Id servisa StartCommunication s pozitivnim odgovorom | C1 | SCRPR |
| #6 | Bajt ključa 1 | EA | KB1 |
| #7 | Bajt ključa 2 | 8F | KB 2 |
| #8 | Kontrolni zbir | 00-FF | CS |

CPR\_019  
Nema negativnog odgovora na poruku StartCommunication zahtjeva, ako nema poruke s pozitivnim odgovorom za prenos, tada se jedinica vozila ne pokreće, ništa se ne prenosi i ona nastavlja s redovnim radom.

**4.2.   Servis StopCommunication**

**4.2.1.    Opis poruke**

Svrha ove razine servisne komunikacije je okončanje komunikacijske aktivnosti.

CPR\_020  
Po prijemu znaka primitiva StopCommunication, jedinica vozila mora provjeriti omogućavaju li prevladavajući uslovi okončanje ove komunikacije. U tom slučaju jedinica vozila mora obaviti sve radnje potrebne za okončanje ove komunikacije.

CPR\_021  
Ako je moguće okončati komunikaciju, jedinica vozila mora izdati primitiv odziva StopCommunication s odabranim parametrima pozitivnog odgovora prije okončanja komunikacije.

CPR\_022  
Ako se komunikacija iz nekog razloga ne može okončati, jedinica vozila mora izdati primitiv odziva StopCommunication s odabranim parametrom negativnog odgovora.

CPR\_023  
Ako jedinica vozila ustanovi istek vremena P3max, komunikacija se okončava bez izdavanja primitiva bilo kakvog odgovora.

**4.2.2.    Format poruka**

CPR\_024  
Formati poruke za primitive StopCommunication se navode u sljedećim tabelama:

Tabela 7.

**Poruka StopCommunication zahtjeva**

|  |  |  |  |
| --- | --- | --- | --- |
| **Bajt #** | **Naziv parametra** | **Heksadecimalna vrijednost** | **Mnemonik** |
| #1 | Formatni bajt – fizičko adresiranje | 80 | FMT |
| #2 | Bajt ciljne adrese | EE | TGT |
| #3 | Bajt adrese izvora | tt | SRC |
| #4 | Bajt za dodatnu dužinu | 01 | LEN |
| #5 | Id servisa StopCommunication zahtjeva | 82 | SPR |
| #6 | Kontrolni zbir | 00-FF | CS |

Tabela 8.

**StopCommunication poruka s pozitivnim odgovorom**

|  |  |  |  |
| --- | --- | --- | --- |
| **Bajt #** | **Naziv parametra** | **Heksadecimalna vrijednost** | **Mnemonik** |
| #1 | Formatni bajt – fizičko adresiranje | 80 | FMT |
| #2 | Bajt ciljne adrese | tt | TGT |
| #3 | Bajt adrese izvora | EE | SRC |
| #4 | Bajt za dodatnu dužinu | 01 | LEN |
| #5 | Servis StopCommunication s pozitivnim odgovorom | C2 | SPRPR |
| #6 | Kontrolni zbir | 00-FF | CS |

Tabela 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 adrese izvora | EE | SRC |
| #4 | Bajt za dodatnu dužinu | 03 | LEN |
| #5 | Id servisa negativnog odgovora | 7F | NR |
| #6 | Identifikacija servisa StopCommuinication zahtjeva | 82 | SPR |
| #7 | responseCode = generalReject | 10 | RC\_GR |
| #8 | Kontrolni zbir | 00-FF | CS |

**4.2.3.    Određivanje parametara**

Ovaj servis ne zahtijeva nikakvo određivanje parametara.

**4.3.   Servis TesterPresent**

**4.3.1.    Opis poruka**

Servis TesterPresent koristi dijagnostički uređaj kako bi ukazao poslužitelju da je još uvijek prisutan, kako bi spriječila automatsko vraćanje poslužitelja u redovan rad i moguće prekidanje komunikacije. Ovaj poslani servis povremeno održava dijagnostički proces/komunikaciju aktivnim ponovnim postavljanjem sata P3 prilikom svakog primitka zahtjeva za ovaj servis.

**4.3.2.    Format poruka**

CPR\_079  
Format poruka za primitive TesterPresent je prikazan u sljedećim tabelama:

Tabela 10.

**Poruka TesterPresent zahtjeva**

|  |  |  |  |
| --- | --- | --- | --- |
| **Bajt #** | **Naziv parametra** | **Heksadecimalna vrijednost** | **Mnemonik** |
| #1 | Formatni bajt – fizičko adresiranje | 80 | FMT |
| #2 | Bajt ciljne adrese | EE | TGT |
| #3 | Bajt adrese izvora | tt | SRC |
| #4 | Bajt za dodatnu dužinu | 02 | LEN |
| #5 | Id servisa TesterPresent zahtjeva | 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 mora odgovoriti porukom sa sljedećim pozitivnim odgovorom. Ako je postavljen na ‚ne’, poslužitelj ne šalje nikakav odgovor.

Tabela 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 adrese izvora | EE | SRC |
| #4 | Bajt za dodatnu dužinu | 01 | LEN |
| #5 | Id servisa TesterPresent s pozitivnim odgovorom | 7E | TPPR |
| #6 | Kontrolni zbir | 00-FF | CS |

CPR\_081  
Servis mora podržavati sljedeće šifre negativnih odgovora:

Tabela 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 adrese izvora | EE | SRC |
| #4 | Bajt za dodatnu dužinu | 03 | LEN |
| #5 | Id službe negativnog odgovora | 7F | NR |
| #6 | Identifikacija službe TesterPresent zahtjeva | 3E | TP |
| #7 | responseCode = [SubFunctionNotSupported-InvalidFormat | 12 | RC\_SFNS\_IF |
| incorrectMessageLength] | 13 | RCJML |
| #8 | Kontrolni zbir | 00-FF | CS |

**5.   SERVIS UPRAVLJANJA**

Raspoloživi servisi su navedeni u sljedećoj tabeli:

Tabela 13.

**Servisi upravljanja**

|  |  |
| --- | --- |
| **Naziv servisa** | **Opis** |
| StartDiagnosticSession | Korisnik zahtijeva pokretanje dijagnostičkog procesa s VU |
| SecurityAccess | Korisnik zahtijeva pristepene funkcijama koje su ograničene na ovlaštene korisnike |

**5.1.   Servis StartDiagnosticSession**

**5.1.1.    Opis poruka**

CPR\_025  
Servis StartDiagnosticSession se koristi kako bi omogućio dijagnostičke procese u poslužitelju. Dijagnostički proces omogućava poseban skup servisa prema tablici 17. Proces može proizvođačima vozila omogućiti posebne servise koje nisu dio ovog dokumenta. Sprovođenjena pravila moraju odgovarati sljedećim zahtjevima:

|  |  |
| --- | --- |
| — | uvijek je samo jedan dijagnostički proces aktivan u jedinici vozila, |

|  |  |
| --- | --- |
| — | prilikom uključenja jedinica vozila mora uvijek pokrenuti StandardDiagnosticSession. Ako nije pokrenut niti jedan drugi dijagnostički proces, StandardDiagnosticSession mora biti aktivan sve dok je uključena jedinica vozila, |

|  |  |
| --- | --- |
| — | ako je ispitni uređaj zatražio dijagnostički proces koji je već aktivan, jedinica vozila mora poslati poruku s pozitivnim odgovorom, |

|  |  |
| --- | --- |
| — | kada god ispitni uređaj zatraži novi dijagnostički proces, jedinica vozila mora najprije poslati poruku StartDiagnosticSession s pozitivnim odgovorom prije nego li novi proces postane aktivan u jedinici vozila. Ako jedinica vozila nije u stanju započeti zatraženi novi dijagnostički proces, ona će odgovoriti porukom StartDiagnosticSession s negativnim odgovorom, te će se nastaviti odvijati tekući proces. |

CPR\_026  
Dijagnostički proces započinje samo ako je uspostavljena komunikacija između korisnika i jedinice vozila.

CPR\_027  
Vremenski parametri opisani u tablici 4. moraju biti aktivni nakon uspješne StartDiagnosticSession s parametrom diagnosticSession postavljenim na ‚StandardDiagnosticSession’ u poruci zahtjeva ako je prethodno bio aktivan drugi dijagnostički proces.

**5.1.2.    Format poruka**

CPR\_028  
Formati poruka za primitive StartDiagnosticSession su prikazani u sljedećim tabelama:

Tabela 14.

**Poruka StartDiagnosticSession zahtjeva**

|  |  |  |  |
| --- | --- | --- | --- |
| **Bajt #** | **Naziv parametra** | **Heksadecimalna vrijednost** | **Mnemonik** |
| #1 | Formatni bajt – fizičko adresiranje | 80 | FMT |
| #2 | Bajt ciljne adrese | EE | TGT |
| #3 | Bajt adrese izvora | tt | SRC |
| #4 | Bajt za dodatnu dužinu | 02 | LEN |
| #5 | Id servisa StartDiagnosticSession zahtjeva | 10 | STDS |
| #6 | diagnosticSession = (jedna vrijednost iz tablice 17.) | XX | DS\_… |
| #7 | Kontrolni zbir | 00-FF | CS |

Tabela 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 adrese izvora | EE | SRC |
| #4 | Dodatni bajt za dužinu | 02 | LEN |
| #5 | ID servisa pozitivnog odziva StartDiagnosticSession | 50 | STDSPR |
| #6 | DiagnosticSession = (ista vrijednost kao u bajtu #6 u tabeli 14.) | XX | DS\_… |
| #7 | Kontrolni zbir | 00-FF | CS |

Tabela 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 adrese izvora | EE | SRC |
| #4 | Bajt za dodatnu dužinu | 03 | LEN |
| #5 | Id servisa negativnog odgovora | 7F | NR |
| #6 | Id servis StartDiagnosticSession zahtjeva | 10 | STDS |
| #7 | ResponseCode = (subFunctionNotSupported[(18)](https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex:32002R1360#ntr18-L_2002207HR.01016801-E0001) | 12 | RC\_SFNS |
| incorrectMessageLength[(19)](https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex:32002R1360#ntr19-L_2002207HR.01016801-E0002) | 13 | RC\_IML |
| conditionsNotCorrect[(20)](https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex:32002R1360#ntr20-L_2002207HR.01016801-E0003)) | 22 | RC\_CNC |
| #8 | Kontrolni zbir | 00-FF | CS |

**5.1.3.    Određivanje parametara**

CPR\_029  
Parametar diagnosticSession (DS\_) koristi servis StartDiagnosticSession za odabir posebnog postubka jednog ili više poslužitelja. U ovom dokumentu su opisani sljedeći dijagnostički procesi:

Tabela 17.

**Određivanje vrijednosti diagnosticSession**

|  |  |  |
| --- | --- | --- |
| **Heksadecimalna vrijednost** | **Opis** | **Mnemonik** |
| 81 | StandardDiagnosticSession  Ovaj dijagnostički proces uključuje sve servise navedene u tablici 1. stubcu 4. ‚SD’. Ovi servisi omogućavaju čitanje svih podataka s poslužitelja (VU). Ovaj dijagnostički proces je aktivan nakon što je uspješno obavljeno pokretanje između korisnika (dijagnostičkog uređaja) i poslužitelja (VU). Preko ovog dijagnostičkog procesa mogu se memorirati drugi dijagnostički procesi navedeni u ovoj tački. | SD |
| 85 | ECUProgrammingSession  Ovaj dijagnostički proces uključuje sve servise navedene u tablici 1. stubcu 6. ‚ECUPS’. Ovi servisi podržavaju programiranje memorije poslužitelja (VU). Preko ovog dijagnostičkog procesa se mogu memorirati drugi dijagnostički procesi navedeni u ovoj tački. | ECUPS |
| 87 | ECUAdjustmentSession  Ovaj dijagnostički proces uključuje sve servise navedene u tablici 1. stubcu 5. ‚ECUAS’. Ovi servisi podržavaju upravljanje ulazom/izlazom poslužitelja (VU). Preko ovog dijagnostičkog procesa se mogu memorirati drugi dijagnostički procesi navedeni u ovoj tački. | ECUAS |

**5.2.   Servis SecurityAccess**

Upisivanje podataka kalibracije ili pristub ulazu/izlazu liniji kalibracije nije moguće osim ako je jedinica vozila u načinu rada KALIBRACIJA. Pored unošenja važeće kartice radionice u jedinicu vozila, u jedinicu vozila je potrebno upisati odgovarajući PIN prije dobivanja dozvole za pristub načinu rada KALIBRACIJA.

Servis SecurityAccess osigurava način upisivanja PIN-a i ukazivanje dijagnostičkom uređaju je li jedinica vozila u načinu rada KALIBRACIJA ili nije.

Dopušteno je upisivanje PIN-a na neki drugi način.

**5.2.1.    Opis poruka**

Servis SecurityAccess se sastoji od SecurityAccess poruke ‚requestSeed’, nakon čega može slijediti SecurityAccess poruka ‚sendKey’. Servis SecurityAccess se mora obavljati nakon servisa StartDiagnosticSession.

CPR\_033  
Dijagnostički uređaj može koristiti SecurityAccess poruku ‚requestSeed’ za provjeru je li je jedinica u vozilu spremna za prihvaćanje PIN-a.

CPR\_034  
Ako je jedinica u vozilu već u načinu rada KALIBRACIJA, ona odgovara na zahtjev upućivanjem ‚signala’ od 0x0000 korištenjem servisa SecurityAccess s pozitivnim odgovorom.

CPR\_035  
Ako je jedinica u vozilu spremna prihvatiti PIN za provjeru putem kartice radionice, ona odgovara na zahtjev slanjem ‚signala’ koje je veće od 0x0000 korištenjem servisa SecurityAccess s pozitivnim odgovorom.

CPR\_036  
Ako jedinica u vozilu nije spremna prihvatiti PIN iz dijagnostičkog uređaja, bilo zato što umetnuta kartica radionice nije valjana ili zato što kartica radionice nije umetnuta, ili stoga što jedinica u vozilu očekuje PIN na neki drugi način, ona mora odgovoriti na zahtjev negativnim odgovorom sa šifrom odziva koji je postavljen na conditionsNotCorrectOrRequestSequenceError.

CPR\_037  
Dijagnostički uređaj može potom koristiti SecurityAccess poruku ‚sendKey’ za slanje PIN-a jedinici u vozilu. Da bi se dalo vremena za provođenje postubka autentifikacije kartice, jedinica vozila mora koristiti šifru negativnog odgovora requestCorrectlyReceived-ResponsePending kako bi se produžilo vrijeme za davanje odgovora. Međutim, dopušteno vrijeme odziva ne smije biti duže od pet minuta. Čim se zahtijevani servis okonča, jedinica vozila mora poslati poruku s pozitivnim odgovorom ili poruku s negativnim odgovorom sa šifrom odgovora koja je različita od ove. Jedinica vozila može ponavljati šifru requestCorrectlyReceived-ResponsePending s negativnim odgovorom do okončanja traženog servisa i do upućivanja poruke s konačnim odgovorom.

CPR\_038  
Jedinica u vozilu mora odgovarati na ovaj zahtjev korištenjem servisa SecurityAccess s pozitivnim odgovorom samo kada je u načinu rada KALIBRACIJA.

CPR\_039  
U sljedećim slučajevima, jedinica u vozilu se odaziva na ovaj zahtjev negativnim odgovorom sa šifrom odgovora postavljenom na:

|  |  |
| --- | --- |
| — | subFunctionNot supported: nepravilan format parametra podfunkcije (accessType), |

|  |  |
| --- | --- |
| — | conditionsNotCorrectOrRequestSequenceError: jedinica u vozilu nije spremna za prihvaćanje unosa PIN, |

|  |  |
| --- | --- |
| — | invalidKey: PIN nije valjan i broj pokušaja provjere PIN-a nije premašen, |

|  |  |
| --- | --- |
| — | exceededNumberOfAttempts: PIN nije valjan 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’ je prikazan u sljedećim tabelama:

Tabela 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 adrese izvora | tt | SRC |
| #4 | Bajt za dodatnu dužinu | 02 | LEN |
| #5 | Id servisa SecurityAccess zahtjeva | 27 | SA |
| #6 | accessType – requestSeed | 7D | AT\_RSD |
| #7 | Kontrolni zbir | 00-FF | CS |

Tabela 19.

**Poruka SecurityAccess – 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 adrese izvora | EE | SRC |
| #4 | Bajt za dodatnu dužinu | 04 | LEN |
| #5 | Id servisa SecurityAccess s pozitivnim odgovorom | 67 | SAPR |
| #6 | accessType – requestSeed | 7D | AT\_RSD |
| #7 | SeedHigh | 00-FF | SEEDH |
| #8 | SeedLow | 00-FF | SEEDL |
| #9 | Kontrolni zbir | 00-FF | CS |

Tabela 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 adrese izvora | EE | SRC |
| #4 | Bajt za dodatnu dužinu | 03 | LEN |
| #5 | Id servisa negativnog odgovora | 7F | NR |
| #6 | Id servisa SecurityAccess zahtjeva | 27 | SA |
| #7 | responseCode = (conditionsNotCorrectOrRequestSequenceError | 22 | RC\_CNC |
| incorrectMessageLength] | 13 | RC\_IML |
| #8 | Kontrolni zbir | 00-FF | CS |

**5.2.3.    Formati poruka – SecurityAccess – sendKey**

CPR\_041  
Formati poruka za SecurityAccess primitive ‚sendKey’ su prikazani u sljedećim tabelama:

Tabela 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 adrese izvora | tt | SRC |
| #4 | Bajt za dodatnu dužinu | m + 2 | LEN |
| #5 | Id servisa SecurityAccess zahtjeva | 27 | SA |
| #6 | accessType – sendKey | 7E | AT\_SK |
| #7 do #m + 6 | Key#1 (viši) | xx | KEY |
| … | … |  |
| Key #m (niži, m mora biti najmanje 4, a najviše 8) | xx |  |
| #m + 7 | Kontrolni zbir | 00-FF | CS |

Tabela 22.

**Poruka SecurityAccess – 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 adrese izvora | EE | SRC |
| #4 | Bajt za dodatnu dužinu | 02 | LEN |
| #5 | Id servisa SecurityAccess s pozitivnim odgovorom | 67 | SAPR |
| #6 | accessType – sendKey | 7E | AT\_SK |
| #7 | Kontrolni zbir | 00-FF | CS |

Tabela 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 adrese izvora | EE | SRC |
| #4 | Bajt za dodatnu dužinu | 03 | LEN |
| #5 | Id servisa negativnog odgovora | 7F | NR |
| #6 | Id servisa SecurityAccess zahtjeva | 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.   SERVIS PRENOSA PODATAKA**

Raspoloživi servisi su opisani u sljedećoj tablici:

Tabela 24.

**Servisi prenosa podataka**

|  |  |
| --- | --- |
| **Naziv servisa** | **Opis** |
| ReadDataByldentifier | Korisnik zahtjeva prenos tekuće vrijednosti zapisa koji je dostuban za recordDataldentifier |
| WriteDataByldentifier | Korisnik zahtijeva upisivanje zapisa kojem je pristubio recordDataldentifier |

**6.1.   Servis ReadDataByIdentifier**

**6.1.1.    Opis poruka**

CPR\_050  
Servisom ReadDataByIdentifier se služi korisnik za traženje vrijednosti podakovnog zapisa iz poslužitelja. Podatke prepoznaje recordDataIdentifier. Odgovornost proizvođača jedinice vozila je da udovolji uslovima poslužitelja prilikom obavljanja servisa.

**6.1.2.    Format poruka**

CPR\_051  
Formati poruka za primitive ReadDataByIdentifier su prikazani u sljedećim tabelama:

Tabela 25.

**Poruka ReadDataByIdentifier zahtjeva**

|  |  |  |  |
| --- | --- | --- | --- |
| **Bajt #** | **Naziv parametra** | **Heksadecimalna vrijednost** | **Mnemonik** |
| #1 | Formatni bajt – fizičko adresiranje | 80 | FMT |
| #2 | Bajt ciljne adrese | EE | TGT |
| #3 | Bajt adrese izvora | tt | SRC |
| #4 | Bajt za dodatnu dužinu | 03 | LEN |
| #5 | Id servisa ReadDataByldentifier zahtjeva | 22 | RDBI |
| #6 i #7 | recordDataldentifier = (vrijednost iz tablice 28.) | xxxx | RDI\_… |
| #8 | Kontrolni zbir | 00-FF | CS |

Tabela 26.

**Poruka ReadDataByldentifier s pozitivnim odgovorom**

|  |  |  |  |
| --- | --- | --- | --- |
| **Bajt #** | **Naziv parametra** | **Heksadecimalna vrijednost** | **Mnemonik** |
| #1 | Formatni bajt – fizičko adresiranje | 80 | FMT |
| #2 | Bajt ciljne adrese | tt | TGT |
| #3 | Bajt adrese izvora | EE | SRC |
| #4 | Bajt za dodatnu dužinu | m + 3 | LEN |
| #5 | Id servisa ReadDataByldentifier s pozitivnim odgovorom | 62 | RDBIPR |
| #6 i #7 | recordDataldentifier = (ista vrijednost kao bajtovi #6 i #7 iz tabele 25.) | xxxx | RDI\_… |
| #8 do #m + 7 | dataRecordO = (data#l | xx | DREC\_DATA1 |
| : | : | : |
| data#m) | xx | DREC\_DATAm |
| #m + 8 | Kontrolni zbir | 00-FF | CS |

Tabela 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 adrese izvora | EE | SRC |
| #4 | Bajt za dodatnu dužinu | 03 | LEN |
| #5 | Id servisa negativnog odgovora | 7F | NR |
| #6 | Id servisa ReadDataByIdentifier zahtjeva | 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 recordDataldentifier (RDI\_) u poruci ReadDataByldentifier zahtjeva prepoznaje podakovni zapis.

CPR\_053  
Vrijednosti recordDataIdentifier definirane ovim dokumentom prikazuje tabela u nastavu.

Tabelu recordDataldentifier čine četiri stubca i više redova.

|  |  |
| --- | --- |
| — | Prvi stubac (Heksadecimalna vrijednost) obuhvaća ‚heksadecimalnu vrijednost’ dodijeljenu recordDataldentifier opisanom u trećem stubcu. |

|  |  |
| --- | --- |
| — | Drugi stubac (Podakovni element) prikazuje podakovni element iz Dodatka 1. na kojem se temelji recordDataldentifier (ponekad je potrebno prešifriranje). |

|  |  |
| --- | --- |
| — | Treći stubac (Opis) navodi odgovarajući naziv recordDataldentifier. |

|  |  |
| --- | --- |
| — | Četvrti stubac (Mnemonik) navodi mnemonik ovog recordDataldentifier. |

Tabela 28.

**Određivanje vrijednosti recordDataldentifier**

|  |  |  |  |
| --- | --- | --- | --- |
| **Heksadecimalna vrijednost** | **Podakovni element** | **Naziv recordDataldentifier**  **(vidjeti format u tački 8.2.)** | **Mnemonik** |
| F90B | Image | TimeDate | RDI\_TD |
| F912 | Image | HighResolutionTotalVehicleDistance | RDI\_HRTVD |
| F918 | Image | Kfactor | RDI\_KF |
| F91C | Image | LfactorTyreCircumference | RDI\_LF |
| F91D | Image | WvehicleCharacteristicFactor | RDI\_WVCF |
| F921 | Image | TyreSize | RDI\_TS |
| F922 | Image | NextCalibrationDate | RDI\_NCD |
| F92C | Image | SpeedAuthorised | RDI\_SA |
| F97D | Image | RegisteringMemberState | RDI\_RMS |
| F97E | Image | VehicleRegistrationNumber | RDI\_VRN |
| F190 | Image | VIN | RDI\_VIN |

CPR\_054  
Parametar dataRecord (DREC\_) koristi ReadDataByldentifier poruka s pozitivnim odgovorom za pružanje korisniku (dijagnostičkom uređaju) vrijednosti podakovnog zapisa kojeg je prepoznao recordDataIdentifier. Formati podataka su opisani u odjeljku 8. Mogu se ugraditi dodatni korisnički neobvezni dataRecords uključujući posebne ulazne, unutarnje i izlazne podatke, ali nisu definirani u ovom dokumentu.

**6.2.   Servis WriteDataByIdentifier**

**6.2.1.    Opis poruka**

CPR\_056  
Servis WriteDataByIdentifier korisnik koristi za upisivanje vrijednosti podakovnih zapisa u poslužitelj. Podatke prepoznaje recordDataldentifier. Odgovornost je proizvođača jedinice vozila da udovolji uslovima poslužitelja prilikom obavljanja ovog serisa. Za ažuriranje parametara navedenih u tablici 28., jednica vozila mora biti u načinu rada KALIBRACIJA.

**6.2.2.    Format poruka**

CPR\_057  
Formati poruka za primitive WriteDataByIdentifier su navedeni u sljedećim tabelama:

Tabela 29.

**Poruka WriteDataByIdentifier zahtjeva**

|  |  |  |  |
| --- | --- | --- | --- |
| **Bajt #** | **Naziv parametra** | **Heksadecimalna vrijednost** | **Mnemonik** |
| #1 | Formatni bajt – fizičko adresiranje | 80 | FMT |
| #2 | Bajt ciljne adrese | EE | TGT |
| #3 | Bajt adrese izvora | tt | SRC |
| #4 | Bajt za dodatnu dužinu | m+3 | LEN |
| #5 | Id servisa WriteDataByIdentifier zahtjeva | 2E | WDBI |
| #6 i #7 | recordDataIdentifier = (vrijednost iz tabele 28.) | xxxx | RDI\_… |
| #8 do #m + 7 | dataRecord() = (data#l | xx | DREC\_DATA1 |
| : |  |  |
| data#m) | xx | DREC\_DATAm |
| #m+8 | Kontrolni zbir | 00-FF | CS |

Tabela 30.

**Poruka WriteDataByIdentifier s pozitivnom odgovorom**

|  |  |  |  |
| --- | --- | --- | --- |
| **Bajt #** | **Naziv parametra** | **Heksadecimalna vrijednost** | **Mnemonik** |
| #1 | Formatni bajt – fizičko adresiranje | 80 | FMT |
| #2 | Bajt ciljne adrese | tt | TGT |
| #3 | Bajt adrese izvora | EE | SRC |
| #4 | Bajt za dodatnu dužinu | 03 | LEN |
| #5 | Id servisa WriteDataByIdentifier s pozitivnim odgovorom | 6E | WDBIPR |
| #6 i #7 | recordDataIdentifier = (ista vrijednost kao i bajti #6 i #7 iz tabele 29.) | xxxx | RDI\_… |
| #8 | Kontrolni zbir | 00-FF | CS |

Tabela 31.

**WriteDataByIdentifier poruka s negativnim odgovorom**

|  |  |  |  |
| --- | --- | --- | --- |
| **Bajt #** | **Naziv parametra** | **Heksadecimalna vrijednost** | **Mnemonik** |
| #1 | Formatni bajt – fizičko adresiranje | 80 | FMT |
| #2 | Bajt ciljne adrese | tt | TGT |
| #3 | Bajt adrese izvora | EE | SRC |
| #4 | Bajt za dodatnu dužinu | 03 | LEN |
| #5 | Id servisa negativnog odgovora | 7F | NR |
| #6 | Id servisa WriteDataByIdentifier zahtjeva | 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.    Određivanje parametara**

Parametar recordDataIdentifier (RDI\_) je određen u tablici 28.

Parametar dataRecord (DREC\_) koristi poruka WriteDataByIdentifier zahtjeva za davanje poslužitelju (VU) vrijednosti podakovnih zapisa koje je prepoznao recordDataIdentifier. Formati podataka su navedeni u odjeljku 8.

**7.   UPRAVLJANJE ISPITNIM IMPULSIMA – FUNKCIONALNA JEDINICA ZA UPRAVLJANJE ULAZOM/IZLAZOM**

Raspoloživi servisi su navedeni u sljedećoj tablici:

Tabela 32.

**Funkcionalna jedinica za upravljanje ulazom/izlazom**

|  |  |
| --- | --- |
| **Naziv usluge** | **Opis** |
| InputOutputControlByIdentifier | Korisnik zahtijeva upravljanje ulazom/izlazom koje je specifično za poslužitelj |

**7.1.   Opis poruka**

**7.1.1.    Opis poruka**

Postoji veza putem priključka na prednjoj strani tahografa koja omogućava upravljanje ili praćenje ispitnih impulsa korištenjem odgovarajuće dijagnostičke opreme.

CPR\_058  
Ova linija kalibracije U/I signala se može konfigurirati naredbom iz K-linije korištenjem servisa InputOutputControlByIdentifier za odabir tražene funkcije ulaza ili izlaza za liniju. Raspoloživa stanja linije su:

|  |  |
| --- | --- |
| — | van pogona, |

|  |  |
| --- | --- |
| — | speedSignalInput, pri čemu se linija kalibracije U/I signala koristi za ulaz signala brzine (ispitni signal) koji nadomješta signal brzine senzora kretanja, |

|  |  |
| --- | --- |
| — | realTimeSpeedSignalOutputSensor, pri čemu se linija kalibracije signala U/I koristi za izlaz signala brzine senzora kretanja, |

|  |  |
| --- | --- |
| — | RTCOutput, pri čemu se linija kalibracije U/I signala koristi za izlaz signala UTC sata. |

CPR\_059  
Jedinica u vozilu je morala pristubiti postubku podešavanja i mora biti u načinu rada KALIBRACIJA za konfiguraciju stanja linije. Prilikom izlaza iz postubka podešavanja ili načina rada KALIBRACIJA, jedinica u vozilu mora osigurati da se linija kalibracije U/I signala vrati u stanje ‚van pogona’ (standardno).

CPR\_060  
Ako se impulsi brzine primaju u liniju ulaza signala brzine u realnom vremenu jedinice vozila dok je linija kalibracije U/I signala postavljena na ulaz, linija kalibracije U/I signala se mora postaviti na izlaz ili vratiti u stanje van pogona.

CPR\_061  
Redoslijed je sljedeći:

|  |  |
| --- | --- |
| — | uspostaviti komunikaciju od strane servisa StartCommunication, |

|  |  |
| --- | --- |
| — | ući u postupak kalibracije putem servisa StartDiagnosticSession Service i biti u načinu rada KALIBRACIJA (redoslijed ove dvije operacije nije bitan), |

|  |  |
| --- | --- |
| — | promjena stanja izlaza od strane servisa InputOutputControlByIdentifier. |

**7.1.2.    Format poruka**

CPR\_062  
Formati poruka za InputOutputControlByIdentifier su prikazani u sljedećim tabelama:

Tabela 33.

**Poruka zahtjeva InputOutputControlByIdentifier**

|  |  |  |  |
| --- | --- | --- | --- |
| **Bajt #** | **Naziv parametra** | **Heksadecimalne vrijednost** | **Mnemonik** |
| #1 | Formatni bajt – fizičko adresiranje | 80 | FMT |
| #2 | Bajt ciljne adrese | EE | TGT |
| #3 | Bajt adrese izvora | tt | SRC |
| #4 | Bajt za dodatnu dužinu | xx | LEN |
| #5 | Sid InputOutputControlByIdentifier zahtjeva | 2F | IOCBI |
| #6 i #7 | InputOutputIdentifier = (CalibrationInputOutput) | F960 | IOI\_CIO |
| #8 ili # #8 do #9 | ControlOptionRecord = ( |  | COR\_… |
| inputOutputControlParameter – jedna vrijednost iz tabele 36. | xx | IOCP\_… |
| controlState – jedna vrijednost iz tabele 38. (vidjeti donju napomenu)) | xx | CS\_… |
| #9 ili #10 | Kontrolni zbir | 00-FF | CS |
| Napomena: Parametar controlState je prisutan samo u nekim slučajevima (vidjeti točku 7.1.3.). | | | |

Tabela 34.

**InputOutputControlByIdentifier poruka s pozitivnim odgovorom**

|  |  |  |  |
| --- | --- | --- | --- |
| **Bajt #** | **Naziv parametra** | **Heksadecimalna vrijednost** | **Mnemonik** |
| #1 | Formatni bajt – fizičko adresiranje | 80 | FMT |
| #2 | Bajt ciljne adrese | tt | TGT |
| #3 | Bajt adrese izvora | EE | SRC |
| #4 | Bajt za dodatnu dužinu | xx | LEN |
| #5 | SId InputOutputControlByIdentifier s pozitivnim odgovorom | 6F | IOCBIPR |
| #6 i #7 | inputOutputIdentifier = (CalibrationInputOutput) | F960 | IOI\_CIO |
| #8 ili # #8 do #9 | controlStatusRecord = ( |  | CSR\_ |
| inputOutputControlParameter (ista vrijednost kao bajt #8 u tabeli 33.) | xx | IOCP\_… |
| controlState (ista vrijednost kao bajt #9 u tablici 33.)) (ako je primjenjivo) | xx | CS\_… |
| #9 ili #10 | Kontrolni zbir | 00-FF | CS |

Tabela 35.

**InputOutputControlByIdentifier poruka s negativnim odgovorom**

|  |  |  |  |
| --- | --- | --- | --- |
| **Bajt #** | **Naziv parametra** | **Heksadecimalna vrijednost** | **Mnemonik** |
| #1 | Formatni bajt – fizičko adresiranje | 80 | FMT |
| #2 | Bajt ciljne adrese | tt | TGT |
| #3 | Bajt adrese izvora | EE | SRC |
| #4 | Bajt za dodatnu dužinu | 03 | LEN |
| #5 | Id servisa negativnog odgovora | 7F | NR |
| #6 | SId InputOutputControIByIdentifier zahtjeva | 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.    Određivanje parametara**

CPR\_064  
Parametar inputOutputControlParameter (IOCP\_) je određen u sljedećoj tablici:

Tabela 36.

**Određivanje vrijednosti inputOutputControlParameter**

|  |  |  |
| --- | --- | --- |
| **Heksadecimalna vrijednost** | **Opis** | **Mnemonik** |
| 00 | ReturnControlToECU  Ova vrijednost upozorava poslužitelja (VU) da dijagnostički uređaj više ne upravlja linijom kalibracije U/I signala. | RCTECU |
| 01 | ResetToDefault  Ova vrijednost upozorava poslužitelja (VU) da se od njega zahtijeva povrat linije kalibracije U/I signala u standardno stanje. | RTD |
| 03 | ShortTermAdjustment  Ova vrijednost upozorava poslužitelja (VU) da se od njega traži podešavanje linije kalibracije U/I signala sa vrijednošću obuhvaćenom parametrom controlState. | STA |

CPR\_065  
Parametar controlState je prisutan samo kada je inputOutputControlParameter postavljen na ShortTermAdjustment i određen je u sljedećoj tablici:

Tabela 37.

**Određivanje vrijednosti controlState**

|  |  |  |
| --- | --- | --- |
| **Način rada** | **Heksadecimalna vrijednost** | **Opis** |
| Stavi van pogona | 00 | U/I linija je van pogona (standardno stanje) |
| Stavi u pogon | 01 | Stavlja u pogon U/I liniju kalibracije kao speedSignalInput |
| Stavi u pogon | 02 | Stavlja u pogon U/I liniju kalibracije kao TimeSpeedSignalOutputSensor |
| Stavi u pogon | 03 | Stavlja u pogon U/I liniju kalibracije kao RTCOutput |

**8.   FORMATI DATARECORDS**

Ova tačka opisuje:

|  |  |
| --- | --- |
| — | opšta pravila koja se moraju primijeniti na raspon parametara koje jedinica u vozilu prenosi dijagnostičkom uređaju, |

|  |  |
| --- | --- |
| — | formate koji se moraju koristiti za podatke koji se prenose putem servisa prenosa podataka opisanih u odjeljku 6. |

CPR\_067  
jedinica vozila mora podržavati sve utvrđene parametre.

CPR\_068  
Podaci koje jedinica vozila prenosi dijagnostičkom uređaju kao odgovor na poruku zahtjeva moraju biti izmjereni podaci (tj. tekuća vrijednost traženog parametra kojega je jednica vozila izmjerila ili uočila).

**8.1.   Rasponi prenesenih parametara**

CPR\_069  
Tabela 38. određuje raspone koja se koriste za određivanje važnosti prenesenog parametra.

CPR\_070  
Vrijednosti u rasponu ‚indikator greške’ omogućavaju jedinici u vozilu da odmah upozori da valjan parametarski podatak trenutno nije dostuban zbog neke greške tahografa.

CPR\_071  
Vrijednosti u rasponu ‚nije dostuban’ omogućavaju jedinici u vozilu da prenese poruku koja sadrži parametar koji nije dostuban ili ga taj modul ne podržava. Vrijednosti u području ‚nije traženo’ omogućavaju uređaju da prenese poruku naredbe i odredi one parametre kod kojih se odziv s prijemnika ne očekuje.

CPR\_072  
Ako greška sastavnog dijela spriječi prenos valjanog podatka za parametar, umjesto podatka za takav parametar treba koristiti indikator greške opisan tablici 38. Međutim, ako izmjeren ili proračunan podatak daje ispravnu vrijednost, ali premašuje definirani raspon parametra, ne smije se koristiti indikator greške. Podatke treba prenositi upotrebljavajući odgovarajuće najmanje ili najveće vrijednosti parametra.

Tabela 38.

**Rasponi dataRecords**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Naziv raspona** | **1 bajt**  **(heksadecimalna vrijednost)** | **2 bajta**  **(heksadecimalna vrijednost)** | **4 bajta**  **(heksadecimalna vrijednost)** | **ASCII** |
| Ispravni signal | 00 do FA | 0000 do FAFF | 00000000 do FAFFFFFF | 1 do 254 |
| Specifičan indikator parametra | FB | FB00 do FBFF | FB000000 do FBFFFFFF | niti jedan |
| Rezervirani rasponi za buduće bitove indikatora | FC do FD | FC00 do FDFF | FC000000 do FDFFFFFF | niti jedan |
| Indikator greške | FE | FE00 do FEFF | FE000000 do FEFFFFFF | 0 |
| Nije raspoloživ ili zatražen | FF | FF00 do FFFF | FF000000 do FFFFFFFF | FF |

CPR\_073  
Za parametre šifrirane u ASCII, ASCII znak ‚\*’ je rezerviran kao razdjelnik.

**8.2.   Formati dataRecords**

Dolje navedene tablice 39. do 42. detaljno prikazuju formate koji se moraju koristiti putem servisa ReadDataByIdentifier i WriteDataByIdentifier.

CPR\_074  
Tabela 39. daje dužinu, razlučivost i radno područje za svaki parametar koji je identifikujeo recordDataldentifier:

Tabela 39.

**Format dataRecords**

|  |  |  |  |
| --- | --- | --- | --- |
| **Naziv parametra** | **Dužina podatka**  **(u bajtovima)** | **Razlučivost** | **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 6,255 impulsa/m |
| LfactorTyreCircumference | 2 | uvećanje 0,125 10-3/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 tabeli 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 tabeli 42.) | |
| VIN | 17 | ASCII | ASCII |

CPR\_075  
Tabela 40. opisuje formate različitih bajtova parametra TimeDate:

Tabela 40.

**Podrobni format TimeDate (vrijednost recordDataIdentifier value # F90B)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Bajt** | **Određivanje parametra** | **Razlučivost** | **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 | mjesec 1 do 12 |
| 5 | Dan | uvećanje 0,25 dana/bit, pomak 0 dana (vidjeti napomenu ispod tabele 41.) | 0,25 do 31,75 dana |
| 6 | Godina | uvećanje 1 godina/bit, pomak + 1985 godina (vidjeti napomenu ispod tabele 41.) | godina 1985. do 2235. |
| 7 | Lokalni pomak minuta | uvećanje 1 min/bit, pomak -125 min | -59 do +59 min |
| 8 | Lokalni pomak sati | uvećanje 1 h/bit, pomak -125 h | -23 do + 23 h |

CPR\_076  
Tabela 41. detaljno opisuje formate različitih bajtova parametra NextCalibrationDate:

Tabela 41.

**Podroban format NextCalibrationDate (vrijednost „recordDataIdentifier value # F922)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Bajt** | **Određivanje parametra** | **Razlučivost** | **Radno područje** |
| 1 | Mjesec | uvećanje 1 mjesec/bit, pomak 0 mjeseci | mjesec 1 do 12 |
| 2 | Dan | uvećanje 0,25 dana/bit, pomak 0 dana (vidjeti donju napomenu) | 0,25 do 31,75 dana |
| 3 | Godina | uvećanje 1 godina/bit, +1985 godina (vidjeti donju napomenu) | godina 1985 do 2235 |
| Napomena u vezi s korištenja parametra ‚Dan’:   |  |  | | --- | --- | | 1. | Vrijednost 0 u datumu je prazna vrijednost. Vrijednosti 1, 2, 3 i 4 se koriste za označivanje prvog dana u mjesecu; 5, 6, 7 i 8 određuju drugi dan u mjesecu itd. |  |  |  | | --- | --- | | 2. | Ovaj parametar ne utiče niti mijenja gornji parametar sati. |   Napomena u vezi korištenja bajta parametra ‚Godina’:   |  |  | | --- | --- | |  | Vrijednost 0 za godinu određuje 1985. godinu; vrijednost 1 određuje 1986.; itd. | | | | |

CPR\_078  
Tabela 42. opisuje formate različitih bajtova parametra VehicleRegistrationNumber:

Tabela 42.

**Podroban format parametra VehicleRegistrationNumber (vrijednost recordDataIdentifier value # F97E)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Bajt** | **Označivanje parametra** | **Razlučivost** | **Radno područje** |
| 1 | Kodna stranica (određena u Dodatku 1.) | ASCII | 01 do 0A |
| 2 do 14 | Registarska oznaka vozila (određena u Dodatku 1.) | ASCII | ASCII |

**Dodatak 9.**

**TIPSKO ODOBRENJE – POPIS NAJMANJEG OBIMA OBVEZNIH ISPITIVANJA**

SADRŽAJ

1. Uvod …

1.1. Tipsko odobrenje …

1.2. Literatura …

2. Funkcionalna ispitivanja jedinice u vozilu …

3. Funkcionalna ispitivanja senzora kretanja …

4. Funkcionalna ispitivanja kartica tahografa …

5. Ispitivanja interoperabilnosti …

**1.   UVOD**

**1.1.   Tipsko odobrenje**

EEZ tipsko odobrenje tahografa (ili njegov dio) ili karticu tahografa se temelji na:

|  |  |
| --- | --- |
| — | atestiranju sigurnosti koje sprovodi ITSEC vlast, u donosu na sigurnosni cilj koji u potpunosti udovoljava Dodatku 10. ovom Prilogu, |

|  |  |
| --- | --- |
| — | potvrđivanje funkcionalnosti koje sprovodi tijelo države članice koje potvrđuje da ispitivani predmet udovoljava zahtjevima ovog Priloga u smislu izvršenih funkcija, tačnosti mjerenja i obelježja okruženja, |

|  |  |
| --- | --- |
| — | potvrđivanje interoperabilnosti koju obavlja nadležno tijelo koje potvrđuje da je tahograf (ili kartica tahografa) u cijelosti interoperabilan/interoperabilna sa zahtijevanim modelom kartice tahografa (ili tahografa) (vidjeti poglavlje VIII. ovog Priloga). |

ISO 16844-3:2004, Cor 1:2006 Cestovna vozila - Ssstemi tahografa - Dio 3.: Sučelje senzora kretanja (s jedinicama vozila).

Ovaj Dodatak propisuje najmanji obim ispitivanja koji tijelo države članice mora obaviti tokom funkcionalnih ispitivanja, te koji najmanji obim ispitivanja mora obaviti nadležno tijelo tokom ispitivanja interoperabilnosti. Postubci koji se provode za obavljanje ispitivanja ili vrsta ispitivanja nisu podrobnije propisani.

Ovaj Dodatak ne obuhvaća ispitivanje karakteristika sigurnosti. Ako se neka ispitivanja neophodna za tipsko odobrenje obavljaju tokom procjene sigurnosti i postubka ispitivanja, tada takva ispitivanja ne treba ponavljati. U tom slučaju mogu se kontrolisati samo rezultati takvih sigurnosnih ispitivanja. Za informaciju, zahtjevi koje treba ispitati tokom ispitivanja sigurnosti (ili koji su blisko povezani sa ispitivanjima koje treba obaviti) su u ovom Dodatku označeni sa ‚\*’.

Ovaj Dodatak razmatra odvojeno tipsko odobrenje senzora kretanja i jedinice u vozilu, kao sastavne dijelove tahografa. Interoperabilnost svakog modela senzora kretanja i svakog modela jedinice u vozilu nije obveza, stoga se tipsko odobrenje za senzor kretanja može izdati samo u kombinaciji s tipnim odobrenje za jedinicu u vozilu i obrnuto.

**1.2.   Literatura**

U ovom su Dodatku korišteni sljedeći izvori:

|  |  |
| --- | --- |
| IEC 68-2-1 | Ispitivanje u odnosu na okruženje - Dio 2.: Ispitivanja - Ispitivanje A: Hladno. 1990 + Izmjena 2.: 1994. |
| IEC 68-2-2 | Ispitivanje u odnosu na okruženje - Dio 2.: Ispitivanja - Ispitivanje B: Suho i toplo. 1974 + Izmjena 2.: 1994. |
| IEC 68-2-6 | Osnovni postubci ispitivanja u odnosu na okruženje – Metode ispitivanja – Fc ispitivanje i smjernice: Vibracije (sinusoidalne). 6. izdanje: 1985. |
| IEC 68-2-14 | Osnovni postubci ispitivanja u odnosu na okruženje – Metode ispitivanja – N ispitivanje: Promjena temperature. Izmjena 1.: 1986. |
| IEC 68-2-27 | Osnovni postubci ispitivanja u odnosu na okruženje – Metode ispitivanja – Ea ispitivanje i smjernice: Udaranje. 3. izdanje: 1987. |
| IEC 68-2-30 | Osnovni postubci ispitivanja u odnosu na okruženje – Metode ispitivanja – Db ispitivanje i smjernice: Vlažno toplinsko, ciklično ispitivanje (12 + 12 – satni ciklus). Izmjena 1.: 1985. |
| IEC 68-2-35 | Osnovni postupak ispitivanja u odnosu na okruženje – Metode ispitivanja – Fda ispitivanje: Nasumične vibracije širokog pojasa visoke ponovljivosti. Izmjena 1.: 1983. |
| IEC 529 | Stepeni zaštite koje osiguravaju kućišta (pravilnik IP). 2. izdanje: 1989. |
| IEC 61000-4-2 | Elektromagnetna kompatibilnost (EMC) – Postubci ispitivanja i mjerenja – Ispitivanje otpornosti na elektrostatsko pražnjenje: 1995./Izmjena 1.:1998. |
| ISO 7637-1 | Drumska vozila – Elektro smetnje zbog provođenja i spajanja – Dio 1.: Putnička vozila i laka privredna vozila nazivnog napona napajanja 12 V – Prelazna električna provodljivost u vodovima napajanja. 2. izdanje: 1990. |
| ISO 7637-2 | Drumska vozila – Elektro smetnje zbog provođenja i spajanja – Dio 2.: Privredna vozila nazivnog napona napajanja 24 V – Prelazna električna provodljivost u vodovima napajanja. Prvo izdanje: 1990. |
| ISO 7637-3 | Drumska vozila – Elektro smetnje zbog provođenja i spajanja – Dio 3.: Vozila s naponom napajanja 12V ili 24 V – Prijelazni elektro prenos s kapacitivnim i induktivnim spojevima putem vodića koji nisu vodovi napajanja. Prvo izdanje: 1995. + ispravak 1.: 1995. |
| ISO/IEC 7816-1 | Identifikacijske kartice – Kontaktne kartice s integirsanim krugom/krugovima – Dio 1.: Fizička obelježja. Prvo izdanje: 1998. |
| ISO/IEC 7816-2 | Informacijska tehnologija - Identifikacijske kartice – Kontaktne kartice s integirsanim krugom/krugovima – Dio 2.: Dimenzije i mjesto kontakata. Prvo izdanje: 1999. |
| ISO/IEC 7816-3 | Informacijska tehnologija - Identifikacijske kartice – Kontaktne kartice s integirsanim krugom/krugovima – Dio 3.: Elektronski signali i protokol prenosa. 2. izdanje: 1997. |
| ISO/IEC 10373 | Identifikacijske kartice – Metode ispitivanja. Prvo izdanje: 1993. |

**2.   FUNKCIONALNA ISPITIVANJA JEDINICE U VOZILU**

|  |  |  |  |
| --- | --- | --- | --- |
| **Br.** | **Ispitivanje** | **Opis** | **Predmetni zahtjevi** |
| 1. | **Administrativni pregled** | | |
| 1.1. | Dokumentacija | Ispravnost dokumentacije |  |
| 1.2. | Rezultati ispitivanja proizvođača | Rezultati ispitivanja proizvođača obavljenih tokom sklapanja. Dokumentacijski iskazi | 070,071,073 |
| 2. | **Vizualni pregled** | | |
| 2.1. | Shodnost s dokumentacijom | |  |
| 2.2. | Identifikacija/oznake | | 168, 169 |
| 2.3. | Materijali | | 163 do 167 |
| 2.4. | Pečaćenje | | 251 |
| 2.5. | Spoljna sučelja | |  |
| 3. | **Funkcionalna ispitivanja** | | |
| 3.1. | Predviđene funkcije | | 002, 004, 244 |
| 3.2. | Načini rada | | 006\*, 007\*, 008\*, 009\*, 106, 107 |
| 3.3. | Funkcije i prava na pristub podacima | | 010\*, 01l\*, 240, 246, 247 |
| 3.4. | Praćenje ubacivanja i vađenja kartica | | 013, 014, 015\*, 016\*, 106 |
| 3.5. | Mjerenje brzine i udaljenosti | | 017 do 026 |
| 3.6. | Mjerenje vremena (pokus se obavlja na 20 °C) | | 027 do 032 |
| 3.7. | Praćenje aktivnosti vozača | | 033 do 043, 106 |
| 3.8. | Praćenje statusa vožnje | | 044, 045, 106 |
| 3.9. | Ručni unos | | 046 do 050b |
| 3.10. | Upravljanje zaključavanjem podataka preduzeća | | 051 do 055 |
| 3.11. | Praćenje djelatnosti nadzora | | 056,057 |
| 3.12. | Otkrivanje događaja i/ili grešaka | | 059 do 069, 106 |
| 3.13. | Identifikacijski podaci o uređaju | | 075\*, 076\*, 079 |
| 3.14. | Podaci o ubacivanju i vađenju vozačke kartice | | 081\* do 083\* |
| 3.15. | Podaci o aktivnostima vozača | | 084\* do 086\* |
| 3.16. | Podaci o mjestima | | 087\* do 089\* |
| 3.17. | Podaci o brojaču kilometara | | 090\* do 092\* |
| 3.18. | Podrobni podaci o brzini | | 093\* |
| 3.19. | Podaci o događajima | | 094\*, 095 |
| 3.20. | Podaci o greškama | | 096\* |
| 3.21. | Podaci o kalibraciji | | 097\*, 098\* |
| 3.22. | Podaci o podešavanju vremena | | 100\*, 101\* |
| 3.23. | Podaci o nadzornim aktivnostima | | 102\*, 103\* |
| 3.24. | Podaci o zaključavanju podataka preduzeća | | 104\* |
| 3.25. | Podaci o aktivnosti preuzimanja podataka | | 105\* |
| 3.26. | Podaci o posebnim uslovima | | 105a\*, 105b\* |
| 3.27. | Zapisivanje i čuvanje na karticama tahografa | | 108, 109\*, 109a\*, 110\*, 111, 112 |
| 3.28. | Prikaz | | 072, 106, 113 do 128, PIC\_001, DIS\_001 |
| 3.29. | Ispis | | 072, 106, 129 do 138, PIC\_001, PRT\_001 do PRT\_012 |
| 3.30. | Upozorenje | | 106, 139 do 148, PIC\_001 |
| 3.31. | Preuzimanje podataka na spoljni uređaj | | 072, 106, 149 do 151 |
| 3.32. | Izlaz podataka na dodatne vanjske uređaje | | 152, 153 |
| 3.33. | Kalibracija | | 154\*, 155\*, 156\*, 245 |
| 3.34. | Podešavanje vremena | | 157\*, 158\* |
| 3.35. | Neometanje dodatnih funkcija | | 003, 269 |
| 3.36. | Sučelje senzora kretanja | | 001a, 099” |
| 3.37 | Provjeriti detektira li, bilježi li i arhivira li JV događaj(e) i/ili pogrešku(-e) koje je definisao proizvođač JV, kada povezani senzor kretanja reagira na magnetska polja koja ometaju detekciju kretanja vozila, zahtjev 161a.” | |  |
| 4. | **Ispitivanja u odnosu na okolinu** | | |
| 4.1. | Temperatura | Provjerava funkcionalnost putem:   |  |  | | --- | --- | | — | IEC 68-2-1, Ad ispitavanje, trajanje testa 72 sata pri niskoj temperaturi (- 20 °C), 1 h u radu, 1 h van rada, |  |  |  | | --- | --- | | — | IEC 68-2-2, Bd ispistivanje, trajanje testa 72 sata pri visokoj temperaturi (+ 70 °C), 1 h u radu, 1 h van rada, |   Temperaturni ciklusi: provjeravanje može li jedinica u vozilu izdržati brze promjene temperature okoline putem Na ispitivanja IEC 68-2-14, 20 ciklusa, svaki s temperaturom koja se kreće od niske temperature (- 20 °C) do visoke temperature (+ 70 °C) i 2 sata držanja na niskoj i na visokoj temperaturi  Može se obaviti skraćena serija ispitivanja (između onih propisanih u tački 3. ove tablice) pri niskoj temperaturi, viskoj temperaturi i tokom temperaturnih ciklusa. | 159 |
| 4.2. | Vlaga | Provjerava može li jedinica u vozilu izdržati cikličnu vlažnost (toplo ispitivanje) putem IEC 68-2-30, pokus Db, šest ciklusa u trajanju od 24 sata, pri svakom primjena temperature od + 25 °C do + 55 °C i relativna vlažnost od 97 % pri + 25 °C i od 93 % pri + 55 °C | 160 |
| 4.3. | Vibracije | 1.Sinusoidalne vibracije:   * provjerava može li jedinica u vozilu izdržati sinusoidalne vibracije sa sljedećim obilježjima: * konstantan pomak između 5 i 11 Hz: vršna amplituda 10 mm * konstantno ubrzanje između 11 i 300 Hz: 5 g   Ovaj zahtjev se provjerava putem IEC 68-2-6, Fc ispitivanje, uz minimalno trajanje ispitivanja od 3 × 12 sati (12 sati po osi)  2.Nasumične vibracije:   * provjerava se može li jedinica u vozilu izdržati nasumične vibracije sa sljedećim obilježjima: * frekvencija 5-150 Hz, nivo 0,02 g2/Hz   Ovaj zahtjev se provjerava putem IEC 68-2-35, Ffda ispitivanje, uz minimalno trajanje ispitivanja od 3 × 12 sati (12 sati po osi), 1 sat u radu, 1 sat van rada  Dva gore opisana ispitivanja se obavljaju na dva različita uzorka tipa uređaja koji se ispituje | 163 |
| 4.4. | Zaštita od vode i stranih tijela | Provjerava je li indeks zaštite jedinice u vozilu usklađen IEC 529 i iznosi najmanje IP 40, kada je ugrađena u radnom stanju na vozilo | 164, 165 |
| 4.5. | Prednaponska zaštita | Provjerava može li jedinica u vozilu izdržati snagu napajanja od:  izvedbe od 24V: 34 V pri + 40 °C 1 sat  izvedbe od 12V: 17 V pri + 40 °C 1 sat | 161 |
| 4.6. | Zaštita od zamjene polariteta | Provjerava može li jedinica u vozilu izdržati inverziju svojeg napajanja. | 161 |
| 4.7. | Zaštita od krakog spoja | Provjerava jesu li signali ulaza i izlaza zaštićeni od krakog spoja u odnosu na napajanje i uzemljenje | 161 |
| 5. | **EMC ispitivanja** | | |
| 5.1. | Emitiranje zračenja i osjetljivost | Shodnost s Direktivom 95/54/EEZ | 162 |
| 5.2. | Elektrostatičko pražnjenje | Shodnost s IEC 61000-4-2, ± 2 kV (nivo 1) | 162 |
| 5.3. | Provođenje prijelazne osjetljivosti pri napajanju | Za izvedbu od 24V: shodnost s ISO 7637-2:   |  |  | | --- | --- | |  | puls 1a: Vs = - 100 V, Ri = 10 ohm |  |  |  | | --- | --- | |  | puls 2: Vs = + 100 V, Ri = 10 ohm |  |  |  | | --- | --- | |  | puls 3a: Vs = - 100 V, Ri = 50 ohm |  |  |  | | --- | --- | |  | puls 3b: Vs = + 100 V, Ri = 50 ohm |  |  |  | | --- | --- | |  | puls 4: Vs = - 16 V, Va = - 12 V, t6 = 100 ms |  |  |  | | --- | --- | |  | puls 5: Vs = + 120 V, Ri = 2,2 ohm, td = 250 ms |   Za izvedbu 12V: shodnost s ISO 7637-1:   |  |  | | --- | --- | |  | puls 1: Vs = - 100 V, Ri = 10 ohm |  |  |  | | --- | --- | |  | puls 2: Vs = + 100 V, Ri = 10 ohm |  |  |  | | --- | --- | |  | puls 3a: Vs = - 100 V, Ri = 50 ohm |  |  |  | | --- | --- | |  | puls 3b: Vs = + 100 V, Ri = 50 ohm |  |  |  | | --- | --- | |  | puls 4: Vs = - 6 V, Va = - 5 V, t6 = 15 ms |  |  |  | | --- | --- | |  | puls 5: Vs = + 65 V, Ri = 3 Ohm, td = 100 ms |   Puls 5 se ispituje samo za jedinice u vozilima namijenjenima ugradnji na vozila na kojima se ne sprovodi jedinstvena spoljna zaštita od rasterećenja | 162 |

**3.   FUNKCIONALNA ISPITIVANJA SENZORA KRETANJA**

|  |  |  |  |
| --- | --- | --- | --- |
| **Br.** | **Pokus** | **Opis** | **Predmetni zahtjevi** |
| 1. | **Administrativni pregled** | | |
| 1.1. | Dokumentacija | Pravilnost dokumentacije |  |
| 2. | **Vizualni pregled** | | |
| 2.1. | Shodnost s dokumentacijom | |  |
| 2.2. | Identifikacija/oznake | | 169, 170 |
| 2.3. | Materijali | | 163 do 167 |
| 2.4. | Pečaćenje | | 251 |
| 3. | **Funkcionalni pokusi** | | |
| 3.1. | Identifikacijski podaci za senzor | | 077\* |
| 3.2. | Senzor kretanja – uparivanje jedinice u vozilu | | 099\*, 155 |
| 3.3. | Detektiranje kretanja | |  |
| Tačnost mjerenja kretanja | | 022 do 026 |
| 3.4. | Sučelje jedinice vozila | | 001a |
| 3.5 | Provjeriti da je senzor kretanja neosjetljiv na magnetsko polje. Alternativno, provjeriti da senzor kretanja reagira na magnetska polja koja ometaju detekciju kretanja vozila tako da povezana JV može detektirati, zabilježiti i pohraniti greške senzora | | 161a |
| 4. | **Ispitivanja u odnosu na okolinu** | | |
| 4.1. | Radna temperatura | Provjerava se funkcionalnost (određeno u ispitivanju br. 3.3.) u temperaturnom intrevalu [- 40 °C; + 135 °C] prema:   |  |  | | --- | --- | | — | IEC 68-2-1, Ad ispitivanje, trajanje ispitivanja 96 sati pri najnižoj temperaturi Tomin |  |  |  | | --- | --- | | — | IEC 68-2-2, Bd ispitivanje, trajanje ispitivanja 96 sati pri najvišoj temperaturi Tomax | | 159 |
| 4.2. | Temperaturni ciklusi: | Provjerava se funkcionalnost (određeno u ispitivanje br. 3.3.) prema IEC 68-2-14 Na ispitivanje, 20 ciklusa, svaki s temperaturnom koja se izmjenjuje od najniže temperature (- 40 °C) do najviše temperature (+ 135 °C) i 2 sata održavanja na najnižoj i na najvišoj temperaturi  Može se provesti skraćena serija ispitivanja (među onima koji su određeni u ispitivanju 3.3.) na najnižoj temperaturi, najvišoj temperaturi i tokom temperaturnih ciklusa | 159 |
| 4.3. | Ciklusi vlažnosti | Provjerava se funkcionalnost (određeno u ispitivanju br. 3.3.) putem IEC 68-2-30, Db ispitivanje, šest 24-satnih ciklusa, svaka temperatura se mijenja od + 25 °C do + 55 °C, relativna vlažnost od 97 % pri + 25 °C i od 93 % pri + 55 °C | 160 |
| 4.4. | Vibracije | Provjerava se funkcionalnost (određeno u ispitivanju br. 3.3.) putem IEC 68-2-6, Fc ispitivanje, s trajanjem ispitivanja od 100 ciklusa frekvencije:  konstantan pomak između 10 i 57 Hz: 1,5 mm amplituda vršno konstantno ubrzanje između 57 i 500 Hz: 20 g | 163 |
| 4.5. | Mehanički udar | Provjerava se funkcionalnost (određeno u ispitivanju br. 3.3.) putem IEC 68-2-27 Ea ispitivanje, 3 udarca u oba smjera 3 okomite osi | 163 |
| 4.6. | Zaštita od vode i stranih tijela | Provjerava se iznosi li pokazatelj zaštite senzora kretanja prema IEC 529 najmanje IP 64, kada je ugrađen u radnom stanju na vozilo | 165 |
| 4.7. | Zaštita od zamjene polariteta | Provjerava se može li senzor kretanja izdržati inverziju svog energetskog napajanja | 161 |
| 4.8. | Zaštita od krakog spoja | Provjerava se jesu li signali ulaza i izlaza zaštićeni od krakog spoja u odnosu na napajanje i uzemljenje | 161 |
| 5. | **EMC** | | |
| 5.1. | Emitiranje zračenja i osjetljivost | Provjerava shodnosti s Direktivom 95/54/EEZ | 162 |
| 5.2. | Elektrostatičko pražnjenje | Shodnost s IEC 61000-4-2, ± 2 kV (nivo 1) | 162 |
| 5.3. | Provedena prelazna osjetljivosti na vodićima napajanja | Shodnost s ISO 7637-3 (nivo III) | 162 |

**4.   FUNKCIONALNA ISPITIVANJA KARTICA TAHOGRAFA**

|  |  |  |  |
| --- | --- | --- | --- |
| **Br.** | **Pokus** | **Opis** | **Predmetni zahtjevi** |
| 1. | **Administrativni pregled** | | |
| 1.1. | Dokumentacija | Pravilnost dokumentacije |  |
| 2. | **Vizualni pregled** | | |
| 2.1. |  | Osigurava da su sva obelježja zaštite i vidljivi podaci ispravno tiskani na kartici i da su sukladni | 171 do 181 |
| 3. | **Fizičko ispitivanje** | | |
| 3.1. |  | Provjerava se dimenzija kartice i položaj kontakata | 184  ISO/IEC 7816-1  ISO/IEC 7816-2 |
| 4. | **Ispitivanje protokola** | | |
| 4.1. | ATR | Provjerava se shodnost ATR | ISO/IEC 7816-3  TCS 304, 307, 308 |
| 4.2. | T = 0 | Provjerava se shodnost protokola T = 0 | ISO/IEC 7816-3  TCS 302, 303, 305 |
| 4.3. | PTS | Provjerava se shodnost PTS naredbe postavljanjem na T = 1 sa T = 0 | ISO/IEC 7816-3  TCS 309 do 311 |
| 4.4. | T = l | Provjerava se shodnost protokola T = 1 | ISO/IEC 7816-3  TCS 303,/306 |
| 5. | **Struktura kartice** | | |
| 5.1. |  | Ispituje se je li podaci struktura kartice sukladna provjerom prisustva obveznih datoteka na kartici i uslova pristepenu istima | TCS 312  TCS 400\*, 401, 402, 403\*, 404, 405\*, 406, 407, 408\*, 409, 410\*, 411, 412, 413\*, 414, 415\*, 416, 417, 418\*, 419 |
| 6. | **Funkcionalna ispitivanja** | | |
| 6.1. | Normalna obrada | Ispituje se najmanje jednom svaka dopuštena upotreba naredbe (npr. ispitati naredbu UPTDATE BINARY sa CLA = ‚00’, CLA = OC’ i s različitim parametrima P1, P2 i Lc)  Provjerava se na kartici jesu li radnje stvarno obavljene (npr.: čitanjem datoteke na kojoj je izvedena naredba) | TCS 313 do TCS 379 |
| 6.2. | Poruke greške | Ispituje se najmanje jednom svaka poruka greške (kako je definisano u Dodatku 2.) za svaku naredbu  Ispituje se najmanje jednom svaka generička greška (osim grešaka potpunosti ‚6400’ koje su provjerene tokom ispitivanja sigurnosti) |  |
| 7. | **Ispitivanja u odnosu na okolina** | | |
| 7.1. |  | Osigurava se da kartice rade unutar graničnih uslova koju su određeni shodno ISO/IEC 10373. | 185 do 188  ISO/IEC 7816-1 |

**5.   ISPITIVANJA INTEROPERABILNOSTI**

|  |  |  |
| --- | --- | --- |
| **Br.** | **Pokus** | **Opis** |
| 1. | Uzajamna autentifikacija | Provjerava se odvija li se uzajamna autentifikacija između jedinice u vozilu i kartice tahografa normalno |
| 2. | Ispitivanje upisivanja/očitavanja | Izvodi se scenarij tipičnog rada jedinice u vozilu. Scenarij mora biti prilagođen vrsti kartice koja se ispituje i obuhvaća upisivanje u čim je moguće više EF na kartici.  Provjera se vrši preuzimanjem podataka s kartice i provjerom da su svi odgovarajući zapisi obavljeni pravilno  Provjerava se dnevni ispis kartice i mogu li svi odgovarajući zapisi biti pravilno očitani |

**Dodatak 10.**

**GENERIČKI SIGURNOSNI CILJEVI**

Ovaj Dodatak propisuje najmanji obavezan sadržaj sigurnosnih ciljeva senzora kretanja, jedinice u vozilu i kartice tahografa.

Kako bi definisali sigurnosne ciljeve u odnosu na koje mogu zatražiti certifikate sigurnosti, proizvođači moraju prema potrebi dopuniti i popuniti dokumente, bez izmjena ili brisanja postojećih opasnosti, ciljeva, načina postepena i propisanih funkcija za provodbu sigurnosti.

**SADRŽAJ**

**Generički sigurnosni cilj senzora kretanja**

1. Uvod …

2. Kratice, definicije i literatura…

2.1. Kratice …

2.2. Definicije …

2.3. Literatura …

3. Obrazloženje proizvoda …

3.1. Opis i način korištenja senzora kretanja …

3.2. Životni vijek senzora kretanja …

3.3. Opasnosti …

3.3.1. Opasnosti u odnosu na politiku upravljanja pristubom …

3.3.2. Opasnosti u odnosu na projektovanje …

3.3.3. Opasnosti vezane uz rad …

3.4. Sigurnosni ciljevi …

3.5. Sigurnosni ciljevi informatičke tehnologije …

3.6. Fizička sredstva, osoblje ili načini postepena …

3.6.1. Projektovanje opreme …

3.6.2. Isporuka opreme …

3.6.3. Generisanje i isporuka sigurnosnih podataka …

3.6.4. Ugradnja, kalibracija i kontrola tahografa …

3.6.5. Nadzor nad sprovođenjem zakona …

3.6.6. Nadograđivanje softvera …

4. Funkcije sprovođenje sigurnosti …

4.1. Identifikacija i autentifikacija …

4.2. Upravljanje pristubom …

4.2.1. Politika upravljanja pristubom …

4.2.2. Prava na pristub podacima …

4.2.3. Struktura datoteke i uslovi pristupa …

4.3. Odgovornost …

4.4. Revizija …

4.5. Tačnost …

4.5.1. Politika upravljanja informacijskim tokom …

4.5.2. Unutarnji prenos podataka …

4.5.3. Potpunost arhiviranih podataka …

4.6. Pouzdanost servisa …

4.6.1. Ispitivanja …

4.6.2. Softver …

4.6.3. Fizička zaštita …

4.6.4. Prekidi napajanja …

4.6.5. Uslovi povrata u početno stanje …

4.6.6. Dostubnost podataka …

4.6.7. Višestruka primjena …

4.7. Razmjena podataka …

4.8. Kriptografska podrška …

5. Određivanje sigurnosnih mehanizama …

6. Minimalna otpornost sigurnosnih mehanizama …

7. Nivo sigurnosti …

8. Obrazloženje …

**Generički sigurnosni cilj jedinice u vozilu**

1. Uvod …

2. Kratice, definicije i literatura …

2.1. Kratice …

2.2. Definicije …

2.3. Literatura …

3. Obrazloženje proizvoda …

3.1. Opis jedinice u vozilu i način upotrebe …

3.2. Životni vijek jedinice u vozilu …

3.3. Opasnosti …

3.3.1. Opasnosti u odnosu na politiku identifikacije i upravljanja pristubom …

3.3.2. Opasnosti u odnosu na projektovanje …

3.3.3. Opasnosti vezane uz rad …

3.4. Sigurnosni ciljevi …

3.5. Sigurnosni ciljevi informatičke tehnologije …

3.6. Fizička sredstva, osoblje ili načini postepena …

3.6.1. Projektovanje opreme …

3.6.2. Isporuka opreme i stavljanje u pogon …

3.6.3. Generisanje i isporuka sigurnosnih podataka …

3.6.4. Isporuka kartica …

3.6.5. Ugradnja, kalibracija i kontrola tahografa …

3.6.6. Rad opreme …

3.6.7. Nadzor nad sprovođenjem zakona …

3.6.8 Nadogradnja programa …

4. Funkcije sprovođenje sigurnosti …

4.1. Identifikacija i autentifikacija …

4.1.1. Identifikacija i autentifikacija senzora kretanja …

4.1.2. Identifikacija i autentifikacija korisnika …

4.1.3. Daljinska identifikacija i autentifikacija preduzeća …

4.1.4. Identifikacija i autentifikacija upravljačke naprave …

4.2. Upravljanje pristubom …

4.2.1. Politika upravljanja pristubom …

4.2.2. Prava pristupa funkcijama …

4.2.3. Prava na pristub podacima …

4.2.4. Struktura datoteke i uslovi pristupa …

4.3. Odgovornost …

4.4. Revizija …

4.5. Ponovno korištenje predmeta …

4.6 Tačnost …

4.6.1. Politika upravljanja tokom informacija …

4.6.2. Unutarnji prenos podataka …

4.6.3. Potpunost arhiviranih podataka …

4.7. Pouzdanost servisa …

4.7.1. Ispitivanja …

4.7.2. Softver …

4.7.3. Fizička zaštita …

4.7.4. Prekidi napajanja …

4.7.5. Uslovi povrata u početno stanje …

4.7.6. Dostubnost podataka …

4.7.7. Višestruke aplikacije …

4.8. Razmjena podataka …

4.8.1. Razmjena podataka sa senzorom kretanja …

4.8.2. Razmjena podataka sa karticama tahografa …

4.8.3. Razmjena podataka s spoljnim medijima za čuvanje podataka (funkcija preuzimanja podataka) …

4.9. Kriptografska podrška …

5. Određivanje sigurnosnih mehanizama …

6. Minimalna otpornost sigurnosnih mehanizama …

7. Nivo sigurnosti …

8. Obrazloženje …

**Generički sigurnosni cilj kartice tahografa**

1. Uvod …

2. Kratice, definicije i literatura …

2.1. Kratice …

2.2. Definicije …

2.3. Literatura …

3. Obrazloženje proizvoda …

3.1. Opis kartice tahografa i način korištenja …

3.2. Životni vijek kartice tahografa …

3.3. Opasnosti …

3.3.1. Krajnji ciljevi …

3.3.2. Putovi napada …

3.4. Sigurnosni ciljevi …

3.5. Sigurnosni ciljevi informatičke tehnologije …

3.6. Fizička sredstva, osoblje ili načini postepena …

4. Funkcije sprovođenje sigurnosti …

4.1. Udovoljavanje profilu zaštite …

4.2. Identifikacija i autentifikacija korisnika …

4.2.1. Identifikacija korisnika …

4.2.2. Autentifikacija korisnika …

4.2.3. Neuspjela autentifikacija …

4.3. Upravljanje pristubom …

4.3.1. Politika upravljanja pristubom …

4.3.2. Funkcije upravljanja pristubom …

4.4. Odgovornost …

4.5. Revizija …

4.6. Tačnost …

4.6.1. Potpunost arhiviranih podataka …

4.6.2. Temeljna autentifikacija podataka …

4.7. Pouzdanost servisa …

4.7.1. Ispitivanja …

4.7.2. Softver …

4.7.3. Napajanje …

4.7.4. Uslovi povrata u početno stanje …

4.8. Razmjena podataka …

4.8.1. Razmjena podataka s jedinicom u vozilu …

4.8.2. Isporučivanje podataka jedinici van vozila (funkcija preuzimanja podataka) …

4.9. Kriptografska podrška …

5. Određivanje sigurnosnih mehanizama …

6. Tražena najmanja otpornost mehanizama …

7. Nivo sigurnosti …

8. Obrazloženje …

**GENERIČKI SIGURNOSNI CILJ SENZORA KRETANJA**

**1.   Uvod**

Ovaj dokument sadrži opis senzora kretanja, opasnosti koje mora prevladati i sigurnosnih ciljeva koje mora postići, propisuje tražene funkcije sprovođenje sigurnosti, te navodi zahtijevanu najmanju otpornost sigurnosnih mehanizama i zahtijevanu razinu sigurnosti za razvoj i ocjenu.

Zahtjevi iz ovog dokumenta su oni iz teksta Priloga I.B. U pogledu jasnoće čitanja ponekad dolazi do ponavljanja zahtjeva u tekstu Priloga I.B i zahtjeva u vezi sigurnosnih ciljeva. Ako postoje dvojbe između zahtjeva u vezi sigurnosnog cilja i zahtjeva iz teksta Priloga I.B na koji se poziva navedeni zahtjev u vezi sigurnosnog cilja, vrijedi zahtjev iz teksta Priloga I.B.

Zahtjevi iz teksta Priloga I.B na koje se ne pozivaju sigurnosni ciljevi ne podliježu funkcijama sprovođenje sigurnosti.

Jednoznačne oznake se pripisuju opasnostima, ciljevima, načinima postepena i SEF specifikacijama u svrhu pronalaženja dokumentacije razvoja i ocjene.

**2.   Kratice, definicije i literatura**

**2.1.    Kratice**

|  |  |
| --- | --- |
| ROM | Stalna memorija |
| SEF | Funkcija sprovođenje sigurnosti |
| TBD | Odredit će se |
| TOE | Predmet vrednovanja |
| VU | Jedinica u vozilu. |

**2.2.    Definicije**

|  |  |
| --- | --- |
| Digitalni tahograf | Uređaj za belježenje |
| Jedinica | Uređaji priključena na senzor kretanja |
| Podaci o kretanju | Podaci koji se razmjenjuju sa VU, koji iskazuju brzinu i pređenu udaljenost |
| Fizički odvojeni dijelovi | Fizički sastavni dijelovi senzora kretanja koji su raspoređeni u vozilu nasuprot fizičkih sastavnih dijelova koji su spojeni u kućištu senzora kretanja |
| Sigurnosni podaci | Posebni podaci potrebni za podržavanje funkcija sprovođenje sigurnosti (npr. kriptografski ključevi) |
| Sistem | Oprema, osoblje ili organizacije koji su na bilo koji način povezani s tahografom |
| Korisnik | Čovjek-korisnik senzora kretanja (kada se ne koristi u izrazu ‚korisnički podaci’) |
| Korisnički podaci | Svi podaci, drugačiji od podatka o kretanju ili sigurnosti, koje upisuje ili sprema senzor kretanja |

**2.3.    Literatura**

|  |  |
| --- | --- |
| ITSEC | Kriterijum vrednovanja sigurnosti informatičke tehnologije ITSEC 1991. |

**3.   Obrazloženje proizvoda**

**3.1.    Opis i način korištenja senzora kretanja**

Senzor kretanja je namijenjen ugradnji u vozila za drumski prevoz. Namijenjen je pružanju sigurnih podataka jedinici vozila o kretanju vozila, iskazujući brzinu i pređenu udaljenost vozila.

Senzor kretanja je u mehaničkom sučelju s dijelom vozila koji se kreće, a čije kretanje može predstavljati brzinu vozila i pređenu udaljenost. Može biti smješten u mjenjaču vozila ili u bilo kojem drugom dijelu vozila.

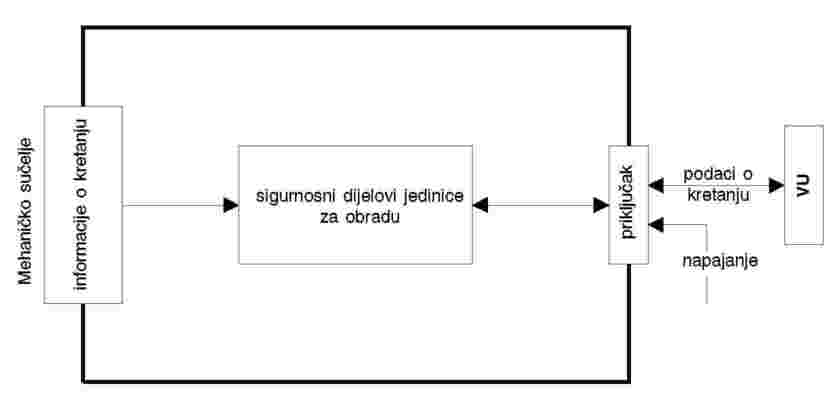
U svom radnom načinu rada, senzor kretanja je povezan s jedinicom vozila.

Takođe, on može biti povezan i s posebnom opremom koja služi za upravljanje (određuje proizvođač).

Sljedeća slika prikazuje tipični senzor kretanja:

**Slika 1.**

**Tipični senzor kretanja**

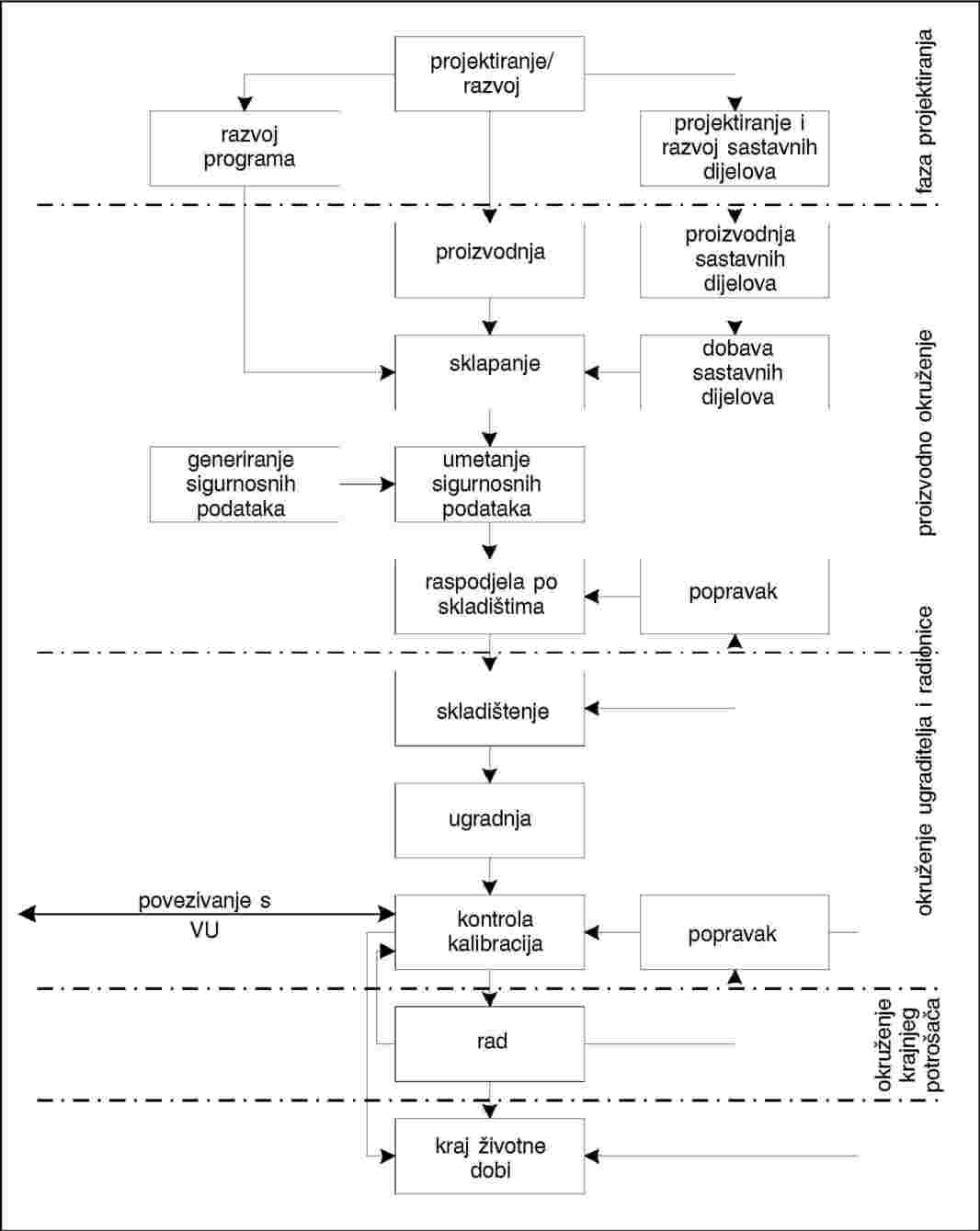


**3.2.    Životni vijek senzora kretanja**

Tipičan životni vijek senzora kretanja opisuje sljedeća slika:

**Slika 2.**

**Tipični životni vijek senzora kretanja**



**3.3.    Opasnosti**

Ovaj stavak opisuje opasnosti s kojima se može suočiti senzor kretanja.

**3.3.1.   Opasnosti u odnosu na politiku upravljanja pristubom**

|  |  |
| --- | --- |
| T.Access | Korisnici mogu pokušati pristubiti funkcijama za koje nemaju dozvolu. |

**3.3.2.   Opasnosti u odnosu na projektovanje**

|  |  |
| --- | --- |
| T. Faults | Greške mašinane opreme, programa i komunikacijskih postupaka mogu senzor kretanja dovesti u nepredviđeno stanje koje ugrožava njegovu sigurnost |
| T.Tests | Korištenje neprovjerenih načina ispitivanja ili postojećih ‚stražnjih ulaza’ može ugroziti sigurnost senzora kretanja |
| T.Design | Korisnici mogu pokušati steći nezakonite spoznaje o projektu bilo iz materijala proizvođača (putem krađe, mita,…) ili putem obrnutog inženjerstva |

**3.3.3.   Opasnosti vezane uz rad**

|  |  |
| --- | --- |
| T.Environment | Korisnici mogu ugroziti sigurnost senzora kretanja putem djelovanja iz neposredne okoline (toplinsko, elektromagnetsko, optičko, kemijsko, mehaničko, …) |
| T.Hardware | Korisnici mogu pokušati preraditi mašinanu opremu senzora kretanja |
| T.Mechanical\_Origin | Korisnici mogu pokušati uticat na ulazne podatke osjetila kretanja (npr. odvrtanjem s mjenjača, …) |
| T.Motion\_Data | Korisnici mogu pokušati promijeniti podatke o kretanju vozila (dodavanje, izmjena, brisanje, reprodukcija signala) |
| T.Power\_Supply | Korisnici mogu pokušati poremetiti sigurnosne ciljeve senzora kretanja izmjenom (prekidom, smanjenjem, povećanjem) napajanja |
| T.Security\_Data | Korisnici mogu pokušati steći nezakonito saznanje o sigurnosnim podacima u opremi tokom generisanja sigurnosnih podataka ili prevoza ili skladištenja |
| T.Software | Korisnici mogu pokušati izmijeniti program senzora kretanja |
| T.Stored\_Data | Korisnici mogu pokušati izmijeniti spremljene podatke (sigurnosni ili korisnički podaci). |

**3.4.    Sigurnosni ciljevi**

Glavni sigurnosni cilj sistema digitalnog tahografa je sljedeći:

|  |  |
| --- | --- |
| O.Main | Podaci koje provjeravaju kontrolna tijela moraju biti dostubni i u potpunosti i točno odražavati aktivnosti vozača i vozila koji su pod nadzorom u smislu vožnje, rada, vremena pripravnosti i odmora i u smislu brzine vozila |

Sigurnosni cilj senzora kretanja koji doprinosi sveukupnom sigurnosnom cilju je stoga:

|  |  |
| --- | --- |
| O.Sensor\_Main | Podaci koje prenosi senzor kretanja moraju biti dostubni VU kako bi VU omogućili da odredi potpuno i točno kretanje vozila u smislu brzine i pređene udaljenosti. |

**3.5.    Sigurnosni ciljevi informatičke tehnologije**

Posebni sigurnosni ciljevi informatičke tehnologije za senzor kretanja koji doprinose njegovom glavnom sigurnosnom cilju su sljedeći:

|  |  |
| --- | --- |
| O.Access | Senzor kretanja mora nadzirati pristub priključenih jedinica funkcijama i podacima |
| O.Audit | Senzor kretanja mora provjeravati pokušaje ugrožavanje njegove sigurnosti i treba ih proslijediti do odgovarajućih jedinica |
| O.Authentication | Senzor kretanja mora autentifikovati priključene jedinice |
| O.Processing | Senzor kretanja mora osigurati da je obrada ulaznih podataka za izvođenje podataka o kretanju točna |
| O.Reliability | Senzor kretanja mora osigurati pouzdan servis |
| O.Secured\_Data\_Exchange | Senzor kretanja mora osiguravati razmjenu podataka s VU. |

**3.6.    Fizička sredstva, osoblje ili načini postepena**

Ovaj stavak opisuje fizičke zahtjeve, uslove za osoblje ili načine postepena koji doprinose sigurnosti senzora kretanja.

**3.6.1.   Projektovanje opreme**

|  |  |
| --- | --- |
| M.Development | Projektanti senzora kretanja moraju voditi računa da se dodjela odgovornosti tokom projektovanja vrši na način koji održava sigurnost IT |
| M.Manufacturing | Proizvođači senzora kretanja moraju osigurati da se odgovornosti tokom izrade dodijeli na način koji održava sigurnost IT, te da tokom postubka izrade senzor bude zaštićen od fizičkih napada koji bi mogli ugroziti sigurnost IT. |

**3.6.2.   Isporuka opreme**

|  |  |
| --- | --- |
| M.Delivery | Proizvođači senzora kretanja, proizvođači vozila i ugradioci ili radionice moraju osigurati da se rukovanje senzorom kretanja obavlja na način koji održava sigurnost IT. |

**3.6.3.   Generisanje i isporuka sigurnosnih podataka**

|  |  |
| --- | --- |
| M.Sec\_Data\_Generation | Algoritmi za generisanje sigurnosnih podataka moraju biti dostubni samo ovlašćenim i povjerljivim osobama |
| M.Sec\_Data\_Transport | Sigurnosni podaci moraju se dobivati, prenositi i unositi u senzor kretanja tako da se očuva njegova vlastita povjerljivost i potpunost. |

**3.6.4.   Ugradnja, kalibracija i kontrola tahografa**

|  |  |
| --- | --- |
| M.Approved\_Workshops | Ugradnju, kalibriranje i popravak tahografa mogu obavljati pouzdani i ovlašćeni ugradioci ili radionice. |
| M.Mechanical\_Interface | Sredstva za otkrivanje neovlaštenog interveniranja u mehaničko sučelje trebaju biti osigurana (npr. pečaćenje) |
| M.Regular\_Inpections | Tahograf se mora periodično nadzirati i kalibrirati. |

**3.6.5.   Nadzor nad sprovođenjem zakona**

|  |  |
| --- | --- |
| M.Controls | Nadzor nad sprovođenjem zakona se mora obavljati redovito i nasumice, te mora obuhvaćati ispitivanja sigurnosti. |

**3.6.6.   Nadograđivanje softvera**

|  |  |
| --- | --- |
| M.Software\_Upgrade | Prije ugradnje u senzor kretanja, izmjene programa moraju biti atestirane sa stanovišta sigurnosti. |

**4.   Funkcije sprovođenje sigurnosti**

**4.1.    Identifikacija i autentifikacija**

UIA\_101  
Senzor kretanja mora moći utvrditi, za svaku interakciju, identitet svake jedinice na koju je bio priključen.

UIA\_102  
Identitet priključene jedinice se sastoji od:

* grupe jedinica:
* VU,
* dijagnostičkog uređaja,
* ostalog
* ID jedinice (samo VU).

UIA\_103  
ID priključene VU jedinice se sastoji od broja odobrenja VU i serijskog broja VU.

UIA\_104  
Senzor kretanja mora biti sposobno autentifikovati svaku VU ili dijagnostički uređaj koji je priključen:

— prilikom priključenja jedinice,

— prilikom obnove napajanja.

UIA\_105  
Senzor kretanja mora biti sposoban za periodično ponovno autentificiranje VU na koju je priključen.

UIA\_106  
Senzor kretanja mora prepoznati i spriječiti korištenje podataka za autentifikaciju koji su kopirani i već upotrijebljeni.

UIA\_107  
Nakon utvrđivanja uzastopnih neuspješnih pokušaja autentifikacije (broj određuje proizvođač, ali ne smije biti veći od 20), SEF mora:

— generisati revizijski zapis događaja,

— upozoriti jedinicu,

— nastaviti predavati podatke o kretanju u neosiguranom načinu rada.

**4.2.    Upravljanje pristubom**

Pristubni dijagnostički uređaji osiguravaju da podaci učitani iz, stvoreni u ili promjenjeni u TOE, mogu obaviti samo oni koji su za to ovlašćeni i kartice trgovačkog društva”

**4.2.1.   Politika upravljanja pristubom**

ACC\_101  
Senzor kretanja mora upravljati pravima na pristub funkciji i podacima.

**4.2.2.   Prava na pristub podacima**

ACC\_102  
Senzor kretanja mora osigurati da se identifikacijski podaci senzora kretanja mogu upisati samo jednom (zahtjev 078).

ACC\_103  
Senzor kretanja mora prihvatiti i/ili sačuvati korisničke podatke samo iz autentificiranih jedinica.

ACC\_104  
Senzor kretanja mora provesti odgovarajuća prava pristupa čitanju i upisivanju sigurnosnih podataka.

**4.2.3.   Struktura datoteke i uslovi pristupa**

ACC\_105  
Struktura programa i podakovnih datoteka te uslovi pristupa se moraju osmisliti u postubku proizvodnje i potom blokirati u odnosu na sve buduće promjene ili brisanja.

**4.3.    Odgovornost**

ACT\_101  
Senzor kretanja mora u svojoj memoriji čuvati identifikacijske podatke senzora kretanja (zahtjev 077).

ACT\_102  
Senzor kretanja mora u svojoj memoriji čuvati ugradne podatke (zahtjev 099).

ACT\_103  
Senzor kretanja mora imati mogućnost davanja podataka o odgovornosti autentificiranim jedinicama na njihov zahtjev.

**4.4.    Revizija**

AUD\_101  
Senzor kretanja mora, u slučajevima ugroze njegove sigurnosti, generisati revizijske zapise događaja.

AUD\_102  
Slučajevi koji utiču na sigurnost senzora kretanja su sljedeći:

— pokušaji narušavanja sigurnosti,

— neuspješna autentifikacija,

— greška potpunosti sačuvanih podataka,

— greška pri unutarnjem prenosu podataka,

— neovlašteno otvaranje kućišta,

— sabotaža mašinane opreme

— hardversko manipuliranje.

AUD\_103  
Revizijski zapisi moraju obuhvatiti sljedeće podatke:

— datum i vrijeme događaja,

— vrsta događaja,

— identitet priključene jedinice.

Ako zahtijevani podaci nisu dostubni, daje se odgovarajući standardni znak (TBD od proizvođača).

AUD\_104  
Senzor kretanja mora poslati generišene revizijske zapise u VU u trenutku njihovog generisanja i može ih takođe sačuvati u memoriju.

AUD\_105  
Ako senzor kretanja spremi revizijske zapise, on osigurava da se 20 revizijskih zapisa održava nezavisno o veličini kapaciteta za čuvanje revizija, te mora moći isporučiti sačuvane revizijske zapise autentificiranim jedinicama na njihov zahtjev.

**4.5.    Tačnost**

**4.5.1.   Politika upravljanja informacijskim tokom**

ACR\_101  
Senzor kretanja mora osigurati da se podaci o kretanju mogu obrađivati i izvoditi samo iz mehaničkog ulaza u osjetilo.

**4.5.2.   Unutarnji prenos podataka**

Zahtjevi iz ovog stava vrijede samo ako senzor kretanja koristi fizički odvojene dijelove.

ACR\_102  
Ako se podaci prenose između fizički odvojenih dijelova senzora kretanja, podaci moraju biti zaštićeni od promjena.

ACR\_103  
Prilikom utvrđivanja greške prenosa podataka tokom unutrašnjeg prenosa, prenos se ponavlja i SEF mora generisati revizijski zapis o događaju.

**4.5.3.   Potpunost arhiviranih podataka**

ACR\_104  
Senzor kretanja mora provjeriti korisničke podatke sačuvane u njegovoj memoriji u smislu grešaka potpunosti.

ACR\_105  
Po otkrivanju greške potpunosti arhiviranih korisničkih podataka, SEG mora generisati revizijski zapis.

**4.6.    Pouzdanost servisa**

**4.6.1.   Ispitivanja**

RLB\_101  
Sve naredbe, aktivnosti ili mjesta ispitivanja karakteristična za potrebe ispitivanja u fazi proizvodnje moraju biti stavljeni van funkcije ili uklonjeni prije kraja faze proizvodnje. Ne smije biti moguće njihovo obnavljanje za kasniju upotrebu.

RLB\_102  
Senzor kretanja mora sprovoditi samoispitivanja tokom početnog pogona, te tokom redovnog rada kako bi provjerio ispravnost svog rada. Samoispitivanja senzora kretanja moraju obuhvaćati provjeru potpunosti sigurnosnih podataka i provjeru potpunosti pohranjenog izvršnog logaritma (ako nije u ROM-u).

RLB\_103  
Po otkrivanju unutarnje greške tokom samoispitivanja, SEF mora generisati revizijski zapis (greška osjetila).

**4.6.2.   Softver**

RLB\_104  
Ne smije postojati mogućnost analiziranja ili ispravljanja programa senzora kretanja na terenu.

RLB\_105  
Unos podataka iz spoljnih izvora se ne smije prihvatiti kao izvršni kod.

**4.6.3.   Fizička zaštita**

RKB\_106  
Ako je senzor kretanja projektovan tako da se može otvarati, senzor kretanja mora detektirati svako otvaranje kućišta, čak i bez vanjskog napajanja u trajanju od najmanje 6 mjeseci. U tom slučaju SEF mora generisati revizijski zapis o događaju (prihvatljivo je da se revizijski zapis generiše i spremi nakon ponovnog priključenja napajanja).

Ako je senzor kretanja osmišljen tako da se ne može otvoriti, projektira se tako da se pokušaji neovlaštene fizičke intervencije mogu lako utvrditi (npr. vizualnim pregledom).

RLB\_107  
Senzor kretanja mora detektirati određeni (određuje proizvođač) utjecaj na hardverske komponente.

RLB\_108  
U gore opisanom slučaju, SEF mora generisati revizijski zapis i senzor kretanja mora: (određuje proizvođač).

**4.6.4.   Prekidi napajanja**

RLB\_109  
Senzor kretanja mora održavati sigurno stanje tokom prekida ili kolebanja napajanja.

**4.6.5.   Uslovi povrata u početno stanje**

RLB\_110  
Prilikom prekida napajanja, ili ako se operacija prekine prije dovršetka, ili u nekim drugim uslovima povrata u početno stanje, senzor kretanja se mora na pravilan način vratiti u početno stanje.

**4.6.6.   Dostubnost podataka**

RLB\_111  
Senzor kretanja mora osigurati dobivanje pristupa izvorima podataka na zahtjev i da se izvori podataka ne traže i ne zadržavaju bez potrebe.

**4.6.7.   Višestruka primjena**

RLB\_112  
Ako senzor kretanja osigurava primjenu podataka drukčiju od tahografske primjene, svi programi se moraju fizički i/ili logički odvojiti jedni od drugih. Ovi programi ne koriste sigurnosne podatke zajednički. Samo jedan posao smije biti aktivan u određenom trenutku.

**4.7.    Razmjena podataka**

DEX\_101  
Senzor kretanja mora isporučiti VU podatke o kretanju s pridruženim sigurnosnim obilježjima, kako bi VU bila u mogućnosti provjeriti njihovu potpunost i autentičnost.

**4.8.    Kriptografska podrška**

Zahtjevi iz ovog stava vrijede samo prema potrebi, zavisno o korišćenim sigurnosnim mehanizmima i o rješenjima proizvođača.

CSP\_101  
Svaka kriptografska radnja koju obavlja senzor kretanja mora biti u skladu s propisanim algoritmom i propisanom dužinom ključa.

CSP\_102  
Ako senzor kretanja generiše kriptografske ključeve, to mora biti u skladu s propisanim algoritmima generisanja kriptografskih ključeva i propisanim veličinama kriptografskog ključa.

CSP\_103  
Ako senzor kretanja raspodjeljuje kriptografske ključeve, to mora biti u skladu s propisanim metodama raspodjele ključeva.

CSP\_104  
Ako senzor kretanja pristubi kriptografskim ključevima, to mora biti u skladu s utvrđenim metodama pristupa kriptografskim ključevima.

CSP\_105  
Ako senzor kretanja uništi kriptografske ključeve, to mora biti u skladu s utvrđenim metodama uništenja kriptografskih ključeva.

**5.   Određivanje sigurnosnih mehanizama**

Sigurnosne mehanizme koji zadovoljavaju funkcije sprovođenje sigurnosti senzora kretanja određuju proizvođači senzora kretanja.

**6.   Minimalna otpornost sigurnosnih mehanizama**

Minimalna otpornost sigurnosnih mehanizama senzora kretanja je ‚visoka’, kako je određeno u (ITSEC).

**7.   Nivo sigurnosti**

Ciljna nivo sigurnosti senzora kretanja je nivo ITSEC E3, kako je određeno u (ITSEC).

**8.   Obrazloženje**

Sljedeće matrice logički obrazlažu SEF iskazivanjem:

— koji SEF ili sredstva suzbijaju koje opasnosti,

— koji SEF ispunjavaju koje sigurnosne ciljeve IT.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  | **Opasnosti** | | | | | | | | | | **Ciljevi IT** | | | | | | | | |
| **Dostubnost** | **Greške** | **Ispitivanja** | **Konstrukcija** | **Okruženje** | **Hardver** | **Mechanical\_Origin** | **Motion\_Data** | **Power\_Supply** | **Security\_Data** | | **Softver** | **Stored\_Data** | **Dostubnost** | **Revizija** | **Autentifikacija** | **Obrada** | **Pouzdanost** | **Secured\_Data\_Exchange** |
| Fizička sredstva, osoblje i načini postepena | | | | | | | | | | | | | | | | | | | | | |
| Razvoj | | |  | x | x | x |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |
| Proizvodnja | | |  |  | x | x |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |
| Isporuka | | |  |  |  |  |  | x |  |  |  |  | | x | x |  |  |  |  |  |  |
| Generisanje sigurnosnih podataka | | |  |  |  |  |  |  |  |  |  | x | |  |  |  |  |  |  |  |  |
| Prenos sigurnosnih podataka | | |  |  |  |  |  |  |  |  |  | x | |  |  |  |  |  |  |  |  |
| Ovlaštene radionice | | |  |  |  |  |  |  | x |  |  |  | |  |  |  |  |  |  |  |  |
| Mehaničko sučelje | | |  |  |  |  |  |  | x |  |  |  | |  |  |  |  |  |  |  |  |
| Redovna kontrola | | |  |  |  |  |  | x | x |  | x |  | | x |  |  |  |  |  |  |  |
| Nadzor nad sprovođenjem zakona | | |  |  |  |  | x | x | x |  | x | x | | x |  |  |  |  |  |  |  |
| Nadogradnja programa | | |  |  |  |  |  |  |  |  |  |  | | x |  |  |  |  |  |  |  |
| Funkcije sprovođenje sigurnosti | | | | | | | | | | | | | | | | | | | | | |
| Identifikacija i autentifikacija | | | | | | | | | | | | | | | | | | | | | |
| UIA\_101 Identifikujenje jedinica | | | x |  |  |  |  |  |  | x |  |  | |  |  | x |  | x |  |  | x |
| UIA\_102 Identitet jedinica | | | x |  |  |  |  |  |  |  |  |  | |  |  | x |  | x |  |  |  |
| UIA\_103 Identitet VU | | |  |  |  |  |  |  |  |  |  |  | |  |  |  | x |  |  |  |  |
| UIA\_104 Autentifikacija jedinica | | | x |  |  |  |  |  |  | x |  |  | |  |  | x |  | x |  |  | x |
| UIA\_105 Ponovna autentifikacija | | | x |  |  |  |  |  |  | x |  |  | |  |  | x |  | x |  |  | x |
| UIA\_106 Nekrivotvoriva autentifikacija | | | x |  |  |  |  |  |  | x |  |  | |  |  | x |  | x |  |  |  |
| UIA\_107 Neuspjela autentifikacija | | |  |  |  |  |  |  |  | x |  |  | |  |  |  | x |  |  | x |  |
| Upravljanje pristubom | | | | | | | | | | | | | | | | | | | | | |
| ACC\_101 Politika upravljanja pristubom | | | x |  |  |  |  |  |  |  |  | x | |  | x | x |  |  |  |  |  |
| ACC\_102 ID senzora kretanja | | |  |  |  |  |  |  |  |  |  |  | |  | x | x |  |  |  |  |  |
| ACC\_103 Korisnički podaci | | |  |  |  |  |  |  |  |  |  |  | |  | x | x |  |  |  |  |  |
| ACC\_104 Sigurnosni podaci | | |  |  |  |  |  |  |  |  |  | x | |  | x | x |  |  |  |  |  |
| ACC\_105 Struktura datoteke i uslovi pristupa | | | x |  |  |  |  |  |  |  |  | x | |  | x | x |  |  |  |  |  |
| Odgovornost | | | | | | | | | | | | | | | | | | | | | |
| ACT\_101 ID podaci o senzoru kretanja | | |  |  |  |  |  |  |  |  |  |  | |  |  |  | x |  |  |  |  |
| ACT\_102 Podaci o povezivanju | | |  |  |  |  |  |  |  |  |  |  | |  |  |  | x |  |  |  |  |
| ACT\_103 Podaci o odgovornosti | | |  |  |  |  |  |  |  |  |  |  | |  |  |  | x |  |  |  |  |
| Revizija | | | | | | | | | | | | | | | | | | | | | |
| AUD\_101 Revizijski zapisi | | |  |  |  |  |  |  |  |  |  |  | |  |  |  | x |  |  |  |  |
| AUD\_102 Popis revizijskih događaja | | | x |  |  |  | x | x |  |  |  |  | |  | x |  | x |  |  |  |  |
| AUD\_103 Revizijski podaci | | |  |  |  |  |  |  |  |  |  |  | |  |  |  | x |  |  |  |  |
| AUD\_104 Revizijski alati | | |  |  |  |  |  |  |  |  |  |  | |  |  |  | x |  |  |  |  |
| AUD\_105 Čuvanje revizijskih zapisa | | |  |  |  |  |  |  |  |  |  |  | |  |  |  | x |  |  |  |  |
| Tačnost | | | | | | | | | | | | | | | | | | | | | |
| ACR\_101 Politika upravljanja informacijskim tokom | | |  |  |  |  |  |  |  | x |  |  | |  |  |  |  |  | x | x |  |
| ACR\_102 Unutarnji prenosi | | |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  | x | x |  |
| ACR\_103 Unutarnji prenosi | | |  |  |  |  |  |  |  |  |  |  | |  |  |  | x |  |  |  |  |
| ACR\_104 Potpunost sačuvanih podataka | | |  |  |  |  |  |  |  |  |  |  | |  | x |  |  |  |  | x |  |
| ACR\_105 Potpunost sačuvanih podataka | | |  |  |  |  |  |  |  |  |  |  | |  | x |  | x |  |  |  |  |
| Pouzdanost | | | | | | | | | | | | | | | | | | | | | |
| RLB\_101 Ispitivanja u proizvodnji | | |  |  | x | x |  |  |  |  |  |  | |  |  |  |  |  |  | x |  |
| RLB\_102 Samoispitivanja | | |  | x |  |  |  | x |  |  | x |  | | x |  |  |  |  |  | x |  |
| RLB\_103 Samoispitivanja | | |  |  |  |  |  | x |  |  | x |  | | x |  |  | x |  |  |  |  |
| RLB\_104 Analiza programa | | |  |  |  | x |  |  |  |  |  |  | | x |  |  |  |  |  | x |  |
| RLB\_105 Instalacija programa | | |  |  |  |  |  |  |  |  |  |  | | x |  |  |  |  | x | x |  |
| RLB\_106 Otvaranje kućišta | | |  |  |  | x | x | x |  |  |  | x | | x | x |  |  |  |  | x |  |
| RLB\_107 Nedopuštena preinaka hardvera | | |  |  |  |  |  | x |  |  |  |  | |  |  |  |  |  |  | x |  |
| RLB\_108 Nedopuštena preinaka hardvera | | |  |  |  |  |  | x |  |  |  |  | |  |  |  | x |  |  |  |  |
| RLB\_109 Prekidi napajanja | | |  |  |  |  |  |  |  |  | x |  | |  |  |  |  |  |  | x |  |
| RLB\_110 Povrat u početno stanje | | |  | x |  |  |  |  |  |  |  |  | |  |  |  |  |  |  | x |  |
| RLB\_111 Dostubnost podataka | | |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  | x | x |  |
| RLB\_112 Višestruki programi | | |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  | x |  |
| Razmjena podataka | | | | | | | | | | | | | | | | | | | | | |
| DEX\_101 Isporuka sigurnosnih podataka o kretanju | | |  |  |  |  |  |  |  | x |  |  | |  |  |  |  |  |  |  | x |
| Kriptografska podrška | | | | | | | | | | | | | | | | | | | | | |
| CSP\_101 Algoritmi | | |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  | x | x |
| CSP\_102 Generisanje ključeva | | |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  | x | x |
| CSP\_103 Raspodjela ključeva | | |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  | x | x |
| CSP\_104 Dostubnost ključeva | | |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  | x | x |
| CSP\_105 Uništenje ključeva | | |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  | x | x |

**GENERIČKI SIGURNOSNI CILJ JEDINICE U VOZILU**

**1.   Uvod**

Ovaj dokument sadrži opis jedinice u vozilu, opasnosti koje mora prevladati i sigurnosnih ciljeva koje mora postići, propisuje tražene funkcije sprovođenje sigurnosti, te navodi zahtijevanu najmanju otpornost sigurnosnih mehanizama i zahtijevanu razinu sigurnosti za razvoj i ocjenjivanje.

Zahtjevi iz ovog dokumenta su oni iz teksta Priloga I.B. U svrhu jasnoće čitanja ponekad dolazi do ponavljanja zahtjeva u tekstu Priloga I.B i zahtjeva u vezi sa sigurnosnim ciljevima. Ako postoje dvojbe između zahtjeva u vezi sa sigurnosnim ciljevima i zahtjeva iz Priloga I.B na koji se poziva navedeni zahtjev u vezi sa sigurnosnim ciljem, vrijedi zahtjev iz teksta Priloga I.B.

Zahtjevi iz teksta Priloga I.B na koje se ne pozivaju sigurnosni ciljevi ne podliježu funkcijama sprovođenje sigurnosti.

Jednoznačne oznake se pripisuju opasnostima, ciljevima, načinima postepena i specifikacijama SEF u svrhu pronalaženja dokumentacije razrade i ocjene.

**2.   Kratice, definicije i literatura**

**2.1.    Kratice**

|  |  |
| --- | --- |
| PIN | Osobni identifikacijski broj |
| ROM | Stalna memorija |
| SEF | Funkcija sprovođenje sigurnosti |
| TBD | Odredit će se |
| TOE | Predmet vrednovanja |
| VU | Jedinica u vozilu. |

**2.2.    Definicije**

|  |  |
| --- | --- |
| Digitalni tahograf | Uređaj za belježenje |
| Podaci o kretanju | Podaci koji se razmjenjuju sa senzorom kretanja, koji iskazuju brzinu i pređenu udaljenost |
| Fizički odvojeni dijelovi | Fizički sastavni dijelovi VU koji su raspoređeni u vozilu naspram fizičkih sastavnih dijelova koji su spojeni u kućištu VU |
| Sigurnosni podaci | Posebni podaci potrebni za podržavanje funkcija sprovođenje sigurnosti (npr. kriptografski ključevi) |
| Sistem | Oprema, osoblje ili organizacije koji su na bilo koji način povezani s tahografom |
| Korisnik | Korisnici su čovjek-korisnik opreme. Uobičajeni korisnici jedinice u vozilu obuhvaćaju vozače, kontrolore, radionice i preduzeća |
| Korisnički podaci | Svi podaci, drugačiji od sigurnosnih podataka, koje se zapisuje ili sprema u VU, prema zahtjevu u poglavlju III.12. |

**2.3.    Literatura**

|  |  |
| --- | --- |
| ITSEC | Kriterijum vrednovanja sigurnosti informatičke tehnologije ITSEC 1991. |

**3.   Obrazloženje proizvoda**

**3.1.    Opis jedinice u vozilu i način upotrebe**

VU je namijenjena ugradnji u vozila za drumski prevoz. Njezina namjena je zapisivanje, čuvanje, reprodukcija, ispis i isporuka podataka koji se odnose na aktivnosti vozača.

Povezana je sa senzorom kretanja s kojim razmjenjuje podatke o kretanju vozila.

Korisnici se identifikujeju u odnosu na VU korištenjem kartica tahografa.

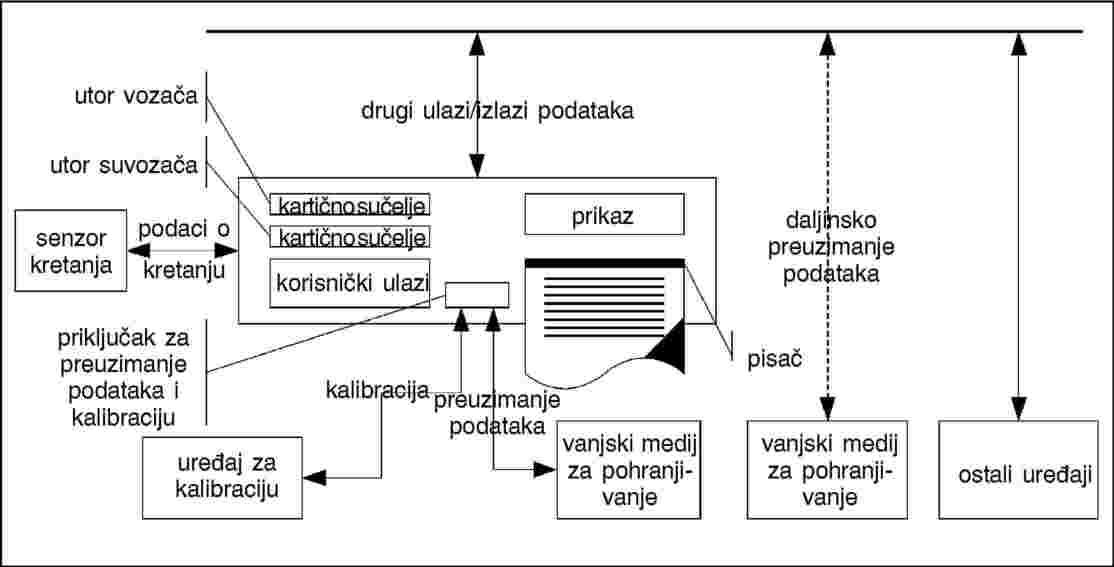
VU zapisuje i sprema podatke o aktivnosti korisnika u svoju memoriju podataka, te takođe zapisuje podatke o aktivnosti korisnika na kartice tahografa.

VU predaje podatke na prikaz, štampač i vanjske uređaje.

Radno okruženje jedinice u vozilu kada je ugrađena u vozilo je opisana sljedećom slikom:

**Slika 1.**

**Radno okruženje VU**



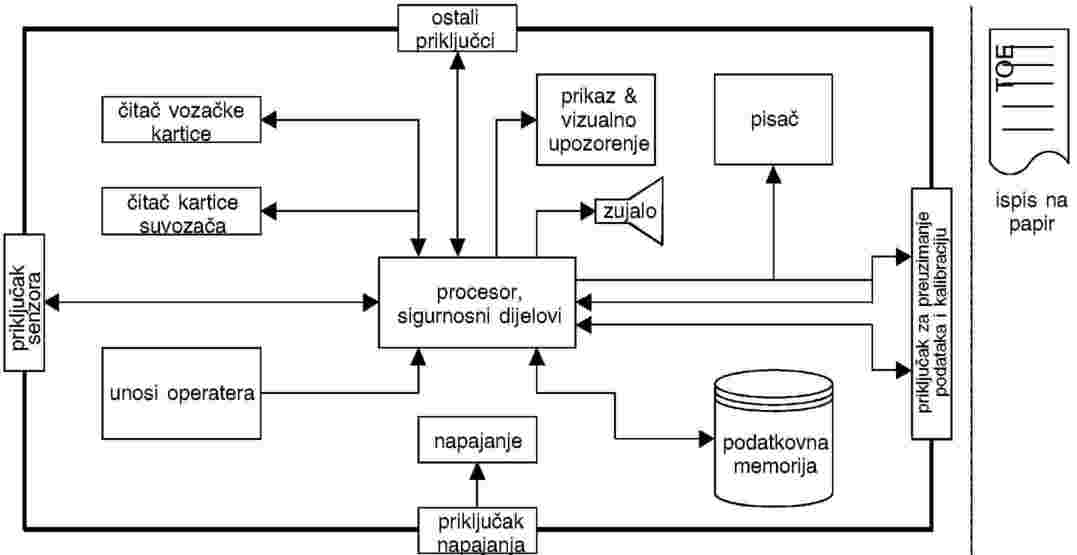
Opšta obelježja VU, funkcije i načini rada su opisani u poglavlju II. Priloga I.B.

Funkcionalni zahtjevi za VU su propisani u poglavlju III. Priloga I.B.

Tipična VU je opisana na sljedećoj slici:

**Slika 2.**

**Tipična VU […] neobavezno**



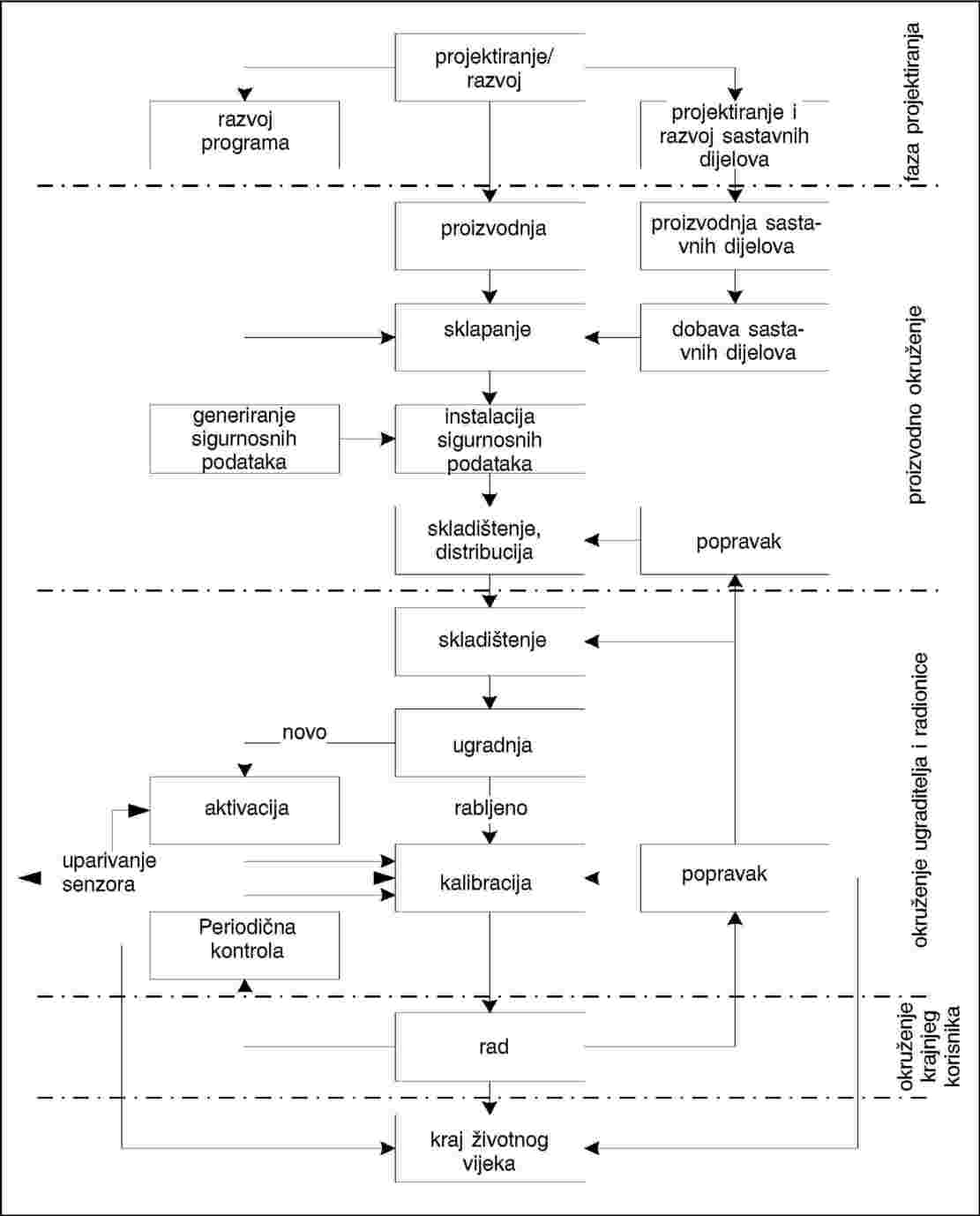
Treba naglasiti da iako je mehanizam pisača dio TOE, to nije i papirnati ispis.

**3.2.    Životni vijek jedinice u vozilu**

Tipični životni vijek VU opisuje sljedeća slika:

**Slika 3.**

**Tipični životni vijek VU**



**3.3.    Opasnosti**

Ovaj stavak opisuje opasnosti kojima je izložena VU.

**3.3.1.   Opasnosti u odnosu na politiku identifikacije i upravljanja pristubom**

|  |  |
| --- | --- |
| T.Access | Korisnici mogu pokušati pristubiti funkcijama za koje nemaju dopuštenje (npr. funkcija kolibracije dostupna vozačima) |
| T.Identification | Korisnici mogu pokušati koristiti nekoliko identifikacija ili nikakvu identifikaciju. |

**3.3.2.   Opasnosti u odnosu na projektovanje**

|  |  |
| --- | --- |
| T.Faults | Greške hardvera, softvera i komunikacijskih postupaka mogu VU dovesti u nepredviđeno stanje koje ugrožava njezinu sigurnost |
| T.Tests | Korištenje neprovjerenih načina ispitivanja ili postojećih ‚stražnjih vrata’ može ugroziti sigurnost VU |
| T.Design | Korisnici mogu pokušati steći nezakonite spoznaje o projektu bilo iz materijala proizvođača (putem krađe, mita,…) ili putem obrnutog inženjerstva |

**3.3.3.   Opasnosti vezane uz rad**

|  |  |
| --- | --- |
| T.Calibration\_Parameters | Korisnici mogu pokušati koristiti pogrešno kalibriran uređaj (putem izmjene podataka kalibracije ili organizacijskih slabosti). |
| T.Card\_Data\_Exchange | Korisnici mogu pokušati izmijeniti podatke dok se razmjenjuju između VU i kartica tahografa (dodavanje, izmjena, brisanje, reprodukcija signala) |
| T.Clock | Korisnici mogu pokušati učiniti izmjenu na unutarnjem satu |
| T.Environment | Korisnici mogu ugroziti sigurnost VU putem djelovanja iz okruženja (toplinski, elektromagnetski, optički, kemijski, mehanički, …) |
| T.Fake\_Devices | Korisnici mogu pokušati priključiti krivotvorene uređaje na VU (senzor kretanja, pametne kartice) |
| T.Hardware | Korisnici mogu pokušati izmijeniti hardver VU |
| T.Motion\_Data | Korisnici mogu pokušati izmijeniti podatke o kretanju vozila (dodavanje, izmjena, brisanje, reprodukcija signala) |
| T.Non\_Activated | Korisnici mogu koristiti opremu koja nije aktivirana |
| T.Output\_Data | Korisnici mogu pokušati izmijeniti isporuku podataka (ispis, prikaz ili preuzimanje podataka) |
| T.Power\_Supply | Korisnici mogu pokušati poremetiti sigurnosne ciljeve VU izmjenom napajanja (prekid, smanjenje, povećanje) |
| T.Security\_Data | Korisnici mogu pokušati steći nezakonito saznanje o sigurnosnim podacima tokom generisanja podataka ili prenosa ili instalacije u opremi |
| T.Software | Korisnici mogu pokušati izmijeniti softver VU |
| T.Stored\_Data | Korisnici mogu pokušati izmijeniti spremljene podatke (sigurnosni ili korisnički podaci). |

**3.4.    Sigurnosni ciljevi**

Glavni sigurnosni cilj sistema s digitalnim tahografom je sljedeći:

|  |  |
| --- | --- |
| O.Main | Podaci koje provjeravaju kontrolna tijela moraju biti na raspolaganju i u potpunosti i točno odražavati aktivnosti vozača i vozila koji su pod nadzorom u smislu vožnje, rada, vremena pripravnosti i odmora i u smislu brzine vozila |

Zato su sigurnosni ciljevi VU koji doprinose opštim sigurnosnom cilju sljedeći:

|  |  |
| --- | --- |
| O.VU\_Main | Podaci koji se mjere i zapisuju i potom provjeravaju od strane kontrolnih tijela moraju biti dostubni i točno odražavati aktivnosti nadziranih vozača i vozila u smislu vožnje, rada, vremena pripravnosti i odmora i u smislu brzine vozila |
| O.VU\_Export | VU mora biti u stanju isporučiti podatke u spoljni medij za čuvanje na način koji omogućava provjeru njihove potpunosti i autentičnosti. |

**3.5.    Sigurnosni ciljevi informatičke tehnologije**

Posebni sigurnosni ciljevi informatičke tehnologije VU koji doprinose njenom glavnom sigurnosnom cilju su sljedeći:

|  |  |
| --- | --- |
| O.Access | VU mora nadzirati korisnički pristub funkcijama i podacima |
| O.Accountability | VU mora prikupiti točne podatke u vezi odgovornosti |
| O.Audit | VU mora ispitati pokušaje narušavanja sigurnosti sistema i ići njihovim tragom do odgovarajućih korisnika |
| O.Authentication | VU mora autentifikovati priključene jedinice (kada između jedinica trebaju postojati pouzdane veze) |
| O.Integrity | VU mora održavati potpunost arhiviranih podataka |
| O.Output | VU mora osigurati da izlazni podaci točno odražavaju izmjerene ili sačuvane podatke. |
| O.Processing | VU mora osigurati da obrada ulaza za izvođenje korisničkih podataka bude točna |
| O.Reliability | VU mora osigurati pouzdane servise |
| O.Secured\_Data\_Exchange | VU mora osiguravati razmjenu podataka sa senzorom kretanja i karticama tahografa. |

**3.6.    Fizička sredstva, osoblje ili načini postepena**

Ovaj stavak opisuje fizičke i kadrovske zahtjeve ili zahtjeve za postupak koji doprinose sigurnosti VU.

**3.6.1.   Projektovanje opreme**

|  |  |
| --- | --- |
| M.Development | Projektanti VU moraju voditi računa da se dodjela odgovornosti tokom projektovanja vrši na način koji održava sigurnost IT |
| M.Manufacturing | Proizvođači VU moraju osigurati da se odgovornosti tokom izrade dodijele na način koji održava sigurnost IT, te da tokom postubka izrade VU bude zaštićena od fizičkih napada koji bi mogli ugroziti sigurnost IT. |

**3.6.2.   Isporuka opreme i stavljanje u pogon**

|  |  |
| --- | --- |
| M.Delivery | Proizvođači VU, proizvođači vozila i radionice ili servisi moraju osigurati da se rukovanje s VU koja nije stavljena u pogon obavlja na način koji održava sigurnost IT. |
| M.Activation | Proizvođači vozila i ugradioci ili radionice moraju VU staviti u pogon nakon njezine ugradnje prije nego što vozač vozila napusti poslovni prostor u kojem je izvršena ugradnja. |

**3.6.3.   Generisanje i isporuka sigurnosnih podataka**

|  |  |
| --- | --- |
| M.Sec\_Data\_Generation | Algoritmi generisanja sigurnosnih podataka moraju biti dostubni samo ovlašćenim i pouzdanim osobama. |
| M.Sec\_Data\_Transport | Sigurnosni podaci moraju se generisati , prenositi i unositi u VU tako da se očuva njihovu povjerljivost i potpunost. |

**3.6.4.   Isporuka kartica**

|  |  |
| --- | --- |
| M.Card\_Availability | Kartice tahografa moraju biti dostubne i isporučivati se samo ovlašćenim osobama |
| M.Driver\_Card\_Uniqueness | Vozači u jednom trenutku smiju imati samo jednu valjanu vozačku karticu |
| M.Card\_Traceability | Mora postojati mogućnost praćenja kartica (bijeli popisi, crni popisi), a crne popise se mora koristiti tokom sigurnosnih revizija. |

**3.6.5.   Ugradnja, kalibracija i kontrola tahografa**

|  |  |
| --- | --- |
| M.Approved\_Workshops | Ugradnju, kalibraciju i popravak tahografa moraju obavljati pouzdani i ovlašćeni ugradioci ili radionice |
| M.Regular\_Inpections | Tahograf se mora periodično nadzirati i kalibrirati |
| M.Faithful\_Calibration | Ovlašćeni ugradioci i radionice moraju upisati odgovarajuće parametre vozila u tahograf tokom kalibracije. |

**3.6.6.   Rad opreme**

|  |  |
| --- | --- |
| M.Faithful\_Drivers | Vozači se moraju pridržavati pravila i postubati odgovorno (npr. koristiti svoje vozačke kartice, pravilno odabrati svoju djelatnost kod ručnog biranja, …). |

**3.6.7.   Nadzor nad sprovođenjem zakona**

|  |  |
| --- | --- |
| M.Controls | Nadzor nad sprovođenjem zakona se mora obavljati redovito i nasumice, te mora obuhvaćati ispitivanja sigurnosti. |

**3.6.8.   Nadogradnja programa**

|  |  |
| --- | --- |
| M.Software\_Upgrade | Prije ugradnje u VU, izmjene programa moraju biti atestirane sa stanovišta sigurnosti. |

**4.   Funkcije sprovođenje sigurnosti**

**4.1.    Identifikacija i autentifikacija**

**4.1.1.   Identifikacija i autentifikacija senzora kretanja**

UIA\_201  
VU mora moći utvrditi, za svaku interakciju, identitet senzora kretanja na koji je priključena.

UIA\_202  
Identitet senzora kretanja čini broj odobrenja senzora i serijski broj senzora.

UIA\_203  
VU mora autentifikovati senzor kretanja na koji je priključena:

— prilikom priključenja na senzor kretanja,

— prilikom svake kalibracije tahografa,

— prilikom uspostave napajanja.

Autentifikacija mora biti uzajamna i aktivirana od strane VU.

UIA\_204  
VU mora periodično (period određuje proizvođač i iz učestalost veću od jednom u sat vremena) ponovo identifikujeti i ponovo autentifikovati senzor kretanja na koji je priključena i osigurati da senzor kretanja koji je identifikujen tokom posljednje kalibracije tahografa nije promijenjen.

UIA\_205  
VU mora ustanoviti i spriječiti korištenje podataka za autentifikaciju koji su kopirani i reprodukovani.

UIA\_206  
Nakon što su utvrđeni uzastopni neuspješni pokušaji autentifikacije (broj određuje proizvođač, ali ne smije biti veći od 20) i/ili nakon utvrđivanja da je identitet senzora kretanja promijenjen kada to nije dopušteno (tj. van vremena kalibracije tahografa), SEF mora:

— generisati revizijski zapis događaja,

— upozoriti korisnika,

— nastaviti prihvaćati i koristiti neosigurane podatke o kretanju koje dostavlja senzor kretanja.

**4.1.2.   Identifikacija i autentifikacija korisnika**

UIA\_207  
VU mora stalno i selektivno pratiti identitet dva korisnika tahografa, praćenjem umetnutih kartica tahografa u otvoru vozača odnosno suvozača.

UIA\_208  
Identitet korisnika se sastoji od:

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| — | skupina korisnika:   |  |  | | --- | --- | | — | VOZAČ (kartica vozača), |  |  |  | | --- | --- | | — | KONTROLOR (kontrolna kartica), |  |  |  | | --- | --- | | — | RADIONICA (kartica radionice), |  |  |  | | --- | --- | | — | PREDUZEĆE (kartica prevoznika), |  |  |  | | --- | --- | | — | NEPOZNAT (kartica nije umetnuta), | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| — | ID korisnika koji se sastoji od:   |  |  | | --- | --- | | — | šifre države članice koja izdaje karticu i broja kartice, |  |  |  | | --- | --- | | — | NEPOZNAT ako je korisnička skupina NEPOZNATA. | |

NEPOZNATI identiteti mogu biti poznati implicitno ili eksplicitno.

UIA\_209  
VU mora autentifikovati svoje korisnike prilikom ubacivanja kartice.

UIA\_210  
VU mora ponovo autentifikovati svoje korisnike:

|  |  |
| --- | --- |
| — | prilikom ponovne uspostave napajanja, |

|  |  |
| --- | --- |
| — | periodično ili nakon nastuba posebnih događaja (određuju proizvođači i učestalije nego jednom dnevno). |

UIA\_211  
Autentifikacija se obavlja tako da se dokaže da je umetnuta kartica valjana kartica tahografa koja posjeduje sigurnosne podatke koje je mogao samo sistem dodijeliti. Autentifikacija mora biti uzajamna i aktivirana od strane VU.

UIA\_212  
Pored gore navedenog, od radionice se zahtjeva da se uspješno autentificiraju putem provjere PIN-a. PIN mora imati najmanje četiri znaka.

Napomena: Kada se PIN prenosi u VU iz vanjske opreme koja se nalazi u blizini VU, pouzdanost PIN-a nije potrebno štititi tokom prenosa.

UIA\_213  
VU mora prepoznati i spriječiti korištenje autentifikacijskih podataka koji su kopirani i reprodukovani.

UIA\_214  
Nakon otkrivanja pet uzastopnih neuspješnih pokušaja autentifikacije, SEF mora:

|  |  |
| --- | --- |
| — | generisati revizijski zapis o događaju, |

|  |  |
| --- | --- |
| — | upozoriti korisnika, |

|  |  |
| --- | --- |
| — | smatrati korisnika NEPOZNATIM, a karticu nevažećom (opis pod (z) i zahtjev 007). |

**4.1.3.   Daljinska identifikacija i autentifikacija preduzeća**

Mogućnost daljinskog priključka preduzeća je neobvezna. Ovaj stavak stoga vrijedi samo ako je takva mogućnost ugrađena.

UIA\_215  
Svaku interakciju s daljinski priključenom tvrkom, VU mora moći utvrditi identitet preduzeća.

UIA\_216  
Daljinski priključen identitet preduzeća se sastoji od šifre države članice koja izdaje karticu preduzeća i broja njezine kartice preduzeća.

UIA\_217  
VU mora uspješno autentifikovati daljinski priključenu firmu prije nego dopusti bilo kakvu isporuku podataka u istu.

UIA\_218  
Autentifikacija se izvodi dokazivanjem da preduzeće posjeduje valjanu karticu preduzeća koja ima sigurnosne podatke koje je samo sistem mogao dodijeliti.

UIA\_219  
VU mora prepoznati i spriječiti korištenje podataka za autentifikaciju koji su kopirani i reprodukovani.

UIA\_220  
Nakon pet uzastopnih neuspješnih pokušaja autentifikacije, VU mora:

|  |  |
| --- | --- |
| — | upozoriti daljinski priključenu firmu. |

**4.1.4.   Identifikacija i autentifikacija upravljačke naprave**

Proizvođači VU mogu predvidjeti namjenske uređaje za dodatne funkcije upravljanja VU (npr. nadograđivanje programa, ponovno unošenje sigurnosnih podataka, …). Ovaj stavak stoga vrijedi samo ako je ugrađena ovakva mogućnost.

UIA\_221  
Za svaku interakciju s upravljačkim uređajem, VU mora moći utvrditi identitet uređaja.

UIA\_222  
Prije omogućavanja svake dalje interakcije, VU mora uspješno autentifikovati upravljački uređaj.

UIA\_223  
VU mora ustanoviti i spriječiti korištenje podataka za autentifikaciju koji su kopirani i reprodukovani.

**4.2.    Upravljanje pristubom**

Upravljački uređaji za pristub osiguravaju da podatke učitavaju iz, upisuju u ili mijenjaju u TOE samo oni koji su za to ovlašćeni.

Potrebno je napomenuti da korisnički podaci koje zapisuje VU, iako iskazuju privatnost ili obelježja komercijalne osjetljivosti, nisu povjerljive naravi. Stoga funkcionalni zahtjev koji se odnosi na prava pristupa učitavanju podataka (zahtjev 011) ne podliježe funkciji sprovođenje sigurnosti.

**4.2.1.   Politika upravljanja pristubom**

ACC\_201  
VU mora upravljati i provjeriti prava upravljanja pristubom funkcijama i podacima.

**4.2.2.   Prava pristupa funkcijama**

ACC\_202  
VU mora sprovoditi pravila izbora načina rada (zahtjevi 006 do 009).

ACC\_203  
VU mora koristiti način rada za provedbu pravila upravljanja pristubom funkcijama (zahtjev 010).

**4.2.3.   Prava na pristub podacima**

ACC\_204  
VU mora sprovoditi pravila pristupa upisu identifikacijskih podataka VU (zahtjev 076).

ACC\_205  
VU mora izvršavati pravila o pristubu upisu identifikacijskih podataka uparenog senzora kretanja (zahtjevi 079 i 155).

ACC\_206  
Nakon aktivacije VU, VU osigurava da se podaci o kalibraciji mogu unositi u VU i sačuvati u njezinu memoriju podataka (zahtjevi 154 i 156) samo u režimu kalibracije.

ACC\_207  
Nakon aktivacije VU, VU sprovodi pravila pristupa upisivanju i brisanju podataka o kalibraciji (zahtjev 097).

ACC\_208  
Nakon aktivacije VU, VU mora osigurati da je samo u kalibracijskom načinu rada moguć unos podataka o podešavanju vremena i čuvanje u njenu memoriju podataka (Ovaj zahtjev ne vrijedi za mala vremenska poravnanja omogućena zahtjevima 157 i 158).

ACC\_209  
Nakon aktivacije VU, VU sprovodi pravila pristupa upisivanju i brisanju podataka o podešavanju vremena (zahtjev 100).

ACC\_210  
VU mora sprovoditi odgovarajuća prava pristupa čitanju i brisanju sigurnosnih podataka (zahtjev 080).

**4.2.4.   Struktura datoteke i uslovi pristupa**

ACC\_211  
Struktura aplikacija i podakovnih datoteka i uslovi pristupa se moraju oblikovati tokom proizvodnog postubka i potom blokirati u odnosu na sve buduće promjene ili brisanja.

**4.3.    Odgovornost**

ACT\_201  
VU mora osigurati da vozači budu odgovorni za svoje aktivnosti (zahtjevi 081, 084, 087, 105a, 105b, 109 i 109a).

ACT\_202  
VU mora trajno čuvati identifikacijske podatke (zahtjev 075).

ACT\_203  
VU mora osigurati da radionice budu odgovorne za svoje aktivnosti (zahtjevi 098, 101 i 109).

ACT\_204  
VU mora osigurati da kontrolori budu odgovorni za svoje aktivnosti (zahtjevi 102, 103 i 109).

ACT\_205  
VU mora evidentirati podatke iz brojača pređenih kilometara (zahtjev 090) i podrobne podatke o brzini (zahtjev 093).

ACT\_206  
VU mora osigurati da se korisnički podaci koji se odnose na zahtjeve 081, 093 i 102 do uključivo 105b ne mijenjaju jednom kada se upišu, osim kada postanu najstariji arhivirani podaci koje treba zamijeniti novim podacima.

ACT\_207  
VU mora voditi računa da ne izmijeni podatke koji su već sačuvani na karticu tahografa (zahtjevi 109 i 109a) osim zamjene najstarijih podataka novim podacima (zahtjev 110) ili u slučaju opisanom u bilješci tačke 2.1 Dodatka 1.

**4.4.    Revizija**

Mogućnosti revizije su obvezne samo za slučajeve koji mogu ukazivati na manipulaciju ili pokušaj ugrožavanja sigurnosti. Ovo se ne traži kod redovnog izvršavanja prava čak i ako se tiče sigurnosti.

AUD\_201  
VU mora, za događaje koji ugrožavaju sigurnost VU, zapisati takve slučajeve sa pridruženim podacima (zahtjevi 094, 096 i 109).

AUD\_202  
Događaji koji utiču na sigurnost VU su sljedeći:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| — | pokušaji ugrožavanja sigurnosti,   |  |  | | --- | --- | | — | neuspjela autentifikacija senzora kretanja, |  |  |  | | --- | --- | | — | neuspjela autentifikacija kartice tahografa, |  |  |  | | --- | --- | | — | neovlaštena promjena senzora kretanja, |  |  |  | | --- | --- | | — | greška potpunosti unosa podataka na karticu, |  |  |  | | --- | --- | | — | greška potpunosti arhiviranih korisničkih podataka, |  |  |  | | --- | --- | | — | greška unutrašnjeg prenosa podataka, |  |  |  | | --- | --- | | — | neovlašteno otvaranje kućišta. |  |  |  | | --- | --- | | — | preinake hardvera, | |

|  |  |
| --- | --- |
| — | posljednja razmjena podataka s karticom koja nije ispravno zatvorena, |

|  |  |
| --- | --- |
| — | slučaj greške podataka o kretanju, |

|  |  |
| --- | --- |
| — | slučaj prekida napajanja, |

|  |  |
| --- | --- |
| — | interna greška VU. |

AUD\_203  
VU mora izvršavati pravila pohranjivanja revizijskih zapisa (zahtjev 094 i 096).

AUD\_204  
VU mora u svojoj memoriji pohranjivati revizijske zapise koje generiše senzor kretanja.

AUD\_205  
Mora postojati mogućnost ispisa, prikaza i preuzimanja revizijskih zapisa.

**4.5.    Ponovno korištenje predmeta**

REU\_201  
VU mora osigurati da se predmeti za privremeno pohranjivanje mogu ponovo koristiti bez da to za posljedicu ima neprihvatljiv protok informacija.

**4.6.    Tačnost**

**4.6.1.   Politika upravljanja tokom informacija**

ACR\_201  
VU mora osigurati da se mogu obrađivati korisnički podaci koji se odnose na zahtjeve 081, 084, 087, 090, 093, 102, 104, 105, 105a i 109 samo iz prikladnih izvora unosa:

|  |  |
| --- | --- |
| — | podaci o kretanju vozila, |

|  |  |
| --- | --- |
| — | sat VU u realnom vremenu, |

|  |  |
| --- | --- |
| — | parametri kalibracije tahografa, |

|  |  |
| --- | --- |
| — | kartice tahografa, |

|  |  |
| --- | --- |
| — | korisnički unosi. |

ACR\_201a  
VU mora osigurati da se korisnički podaci koji se odnose na zahtjev 109a mogu unositi samo u razdoblju između posljednjeg izvlačenja kartice i trenutačog ubacivanja (zahtjev 050a).

**4.6.2.   Unutarnji prenos podataka**

Zahtjevi iz ovog stava vrijede samo ako VU koristi fizički odvojene dijelove.

ACR\_202  
Ako se prenose podaci između fizički odvojenih dijelova VU, podaci se moraju zaštititi od izmjena.

ACR\_203  
Po uočavanju greške u prenosu podataka tokom unutrašnjeg prenosa, prenos se mora ponoviti i SEF mora generisati revizijski zapis događaja.

**4.6.3.   Potpunost arhiviranih podataka**

ACR\_204  
VU mora provjeriti korisničke podatke spremljene u podakovnoj memoriji u pogledu grešaka potpunosti.

ACR\_205  
Po uočavanju greške potpunosti arhiviranih korisničkih podataka, SEF mora generisati revizijski zapis.

**4.7.    Pouzdanost servisa**

**4.7.1.   Ispitivanja**

RLB\_201  
Sve naredbe, radnje ili mjesta ispitivanja koja specifična za ispitivanja u fazi izrade VU moraju biti stavljene van pogona ili uklonjene prije aktivacije VU. Ne smije biti moguća njihova uspostava za kasnije korištenje.

RLB\_202  
VU mora provesti samoispitivanja tokom početnog puštanja u pogon i tokom normalnog rada za provjeru ispravnosti svog rada. Samoispitivanja VU moraju obuhvaćati provjeru potpunosti sigurnosnih podataka i provjeru potpunosti pohranjenog izvršnog koda (ako nije u stalnoj memoriji).

RLB\_203  
Po otkrivanju unutarnje greške tokom samoispitivanja, SEF mora:

|  |  |
| --- | --- |
| — | generisati revizijski zapis (osim u kalibracijskom načinu rada) (interna greška VU), |

|  |  |
| --- | --- |
| — | očuvati potpunost arhiviranih podataka. |

**4.7.2.   Softver**

RLB\_204  
Ne smije biti moguće analizirati ili ispravljati greške programa na terenu nakon aktivacije VU.

RLB\_205  
Ulazni podaci iz spoljnih izvora ne smiju biti prihvaćeni kao izvršni kod.

**4.7.3.   Fizička zaštita**

RLB\_206  
Ako je VU projektovana tako da se može otvoriti, VU mora detektirati svako otvaranje kućišta, osim u kalibracijskom načinu rada, čak i bez vanjskog napajanja, u trajanju od najmanje šest mjeseci. U takvom slučaju, SEF mora generisati revizijski zapis (Prihvatljivo je da se revizijski zapis generiše i pohrani nakon ponovnog priključenja napajanja).

Ako je VU projektovana tako da se ne može otvoriti, ona se projektira tako da se pokušaji neovlaštene fizičke intervencije mogu jednostavno utvrditi (npr. putem vizualnog nadzora).

RLB\_207  
Nakon aktivacije, VU mora ustanoviti unaprijed određenu (određuje proizvođač) hardversku izmjenu.

RLB\_208  
U gore opisanom slučaju, SEF mora generisati revizijski zapis i VU mora: (određuje proizvođač).

**4.7.4.   Prekidi napajanja**

RLB\_209  
VU mora ustanoviti odstupanja od propisanih vrijednosti napajanja, uključujući prekid napajanja.

RLB\_210  
U gore opisanom slučaju, SEF mora:

— generisati revizijski zapis (osim u kalibracijskom načinu rada),

— očuvati sigurno stanje VU,

— održavati sigurnosne funkcije koje se odnose na sastavne dijelove ili postubke koji su još uvijek u funkciji,

— očuvati potpunost arhiviranih podataka.

**4.7.5.   Uslovi povrata u početno stanje**

RLB\_211  
Prilikom prekida napajanja, ili ako je neka aktivnost zaustavljena prije završetka, ili u bilo kojim drugim uslovima povrata u početno stanje, VU se mora propisno vratiti u početno stanje.

**4.7.6.   Dostubnost podataka**

RLB\_212  
VU mora osigurati da se pristub izvorima dobije kada se to zatraži i da se izvori bez potrebe ne traže i ne zadržavaju.

RLB\_213  
VU mora osigurati da se kartice ne mogu izvaditi prije nego se relevantni podaci ne pohrane na kartice (zahtjevi 015 i 016).

RLB\_214  
U gore opisanom slučaju, SEF mora generisati revizijski zapis događaja.

**4.7.7.   Višestruke aplikacije**

RLB\_215  
Ako VU osigurava podatke i za druge aplikacije od tahografske aplikacije, sve aplikacije se moraju fizički i/ili logički odvojiti jedna od druge. Ove aplikacije međusobno ne dijele sigurnosne podatke. U određenom trenutku smije biti aktivan samo jedan posao.

**4.8.    Razmjena podataka**

Ovaj stavak se odnosi na razmjenu podataka između VU i priključenih uređaja.

**4.8.1.   Razmjena podataka sa senzorom kretanja**

DEX\_201  
VU mora provjeriti potpunost i autentičnost podataka o kretanju preuzetih sa senzora kretanja.

DEX\_202  
Po otkrivanju greške potpunosti ili autentičnosti podataka o kretanju, SEF mora:

— generisati revizijski zapis,

— nastaviti koristiti preuzete podatke.

**4.8.2.   Razmjena podataka sa karticama tahografa**

DEX\_203  
VU mora provjeriti potpunost i autentičnost podataka koji se preuzimaju s kartica tahografa.

DEX\_204  
Po otkrivanju greške potpunosti i autentičnosti podataka na kartici, VU mora:

— generisati revizijski zapis,

— ne koristiti podatke.

DEX\_205  
VU mora u pametne kartice tahografa isporučiti podatke s odgovarajućim sigurnosnim obilježjima tako da kartica može provjeriti njihovu potpunost i autentičnost.

**4.8.3.   Razmjena podataka s spoljnim medijima za čuvanje podataka (funkcija preuzimanja podataka)**

DEX\_206  
VU mora generisati dokaz o podrijetlu za podatke koje preuzimaju spoljni mediji.

DEX\_207  
VU mora osigurati mogućnost provjere dokaza o podrijetlu podataka preuzetih s primatelja.

DEX\_208  
VU mora predati podatke na vanjske medije za čuvanje podataka s odgovarajućim sigurnosnim obilježjima tako da se može provjeriti potpunost i autentičnost preuzetih podataka.

**4.9.    Kriptografska podrška**

Zahtjevi iz ovog stava su primjenjivi samo ako su potrebni, zavisno o korišćenim sigurnosnim mehanizmima i o rješenjima proizvođača.

CSP\_201  
Svaka kriptografska radnja koju obavlja VU mora biti u skladu s propisanim algoritmom i utvrđenom veličinom ključa.

CSP\_202  
Ako VU generiše kriptografske ključeve, to će biti u skladu s propisanim algoritmima generisanja kriptografskih ključeva i propisanim veličinama kriptografskog ključa.

CSP\_203  
Ako VU raspodjeljuje kriptografske ključeve, to mora biti u skladu s propisanim metodama raspodjele ključeva.

CSP\_204  
Ako VU pristupa kriptografskih ključevima, to će biti u skladu s propisanim metodama pristupa kriptografskim ključevima.

CSP\_205  
Ako VU uništi kriptografske ključeve, to će biti u skladu s propisanim metodama uništenja kriptografskih ključeva.

**5.   Određivanje sigurnosnih mehanizama**

Zahtijevani sigurnosni mehanizmi su propisani u Dodatku 11.

Sve druge sigurnosne mehanizme moraju odrediti proizvođači.

**6.   Minimalna otpornost sigurnosnih mehanizama**

Minimalna otpornost sigurnosnih mehanizama jedince u vozilu je ‚visoka’, kako je određeno u (ITSEC).

**7.   Nivo sigurnosti**

Ciljna nivo osiguranja jedinice u vozilu je nivo ITSEC E3, kako je određeno u (ITSEC).

**8.   Obrazloženje**

Sljedeće matrice logički obrazlažu SEF pomoću prikaza:

— koji SEF ili sredstva suzbijaju koje opasnosti,

— koji SEF ispunjavaju sigurnosni ciljevi IT.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  | **Opasnosti** | | | | | | | | | | | | | | | | | | | **Ciljevi IT** | | | | | | | | | |
| **Dostubnost** | **Identifikacija** | **Greške** | **Ispitivanja** | **Konstrukcija** | **Calibration\_Parameters** | **Card\_Data\_Exchange** | **Sat** | **Okruženje** | **Fake\_Devices** | **Hardver** | **Motion\_Data** | **Non\_Activated** | **Outpot\_DAta** | **Power\_Supply (namjerno ostavljeno prazno)** |  | **Security\_Data** | **Sofver** | **Stored\_Data** | | **Dostubnost** | **Odgovornost** | **Revizija** | **Autentifikacija** | **Potpunost** | **Izlaz** | **Obrada** | **Pouzdanost** | **Secured\_Data\_Exchange** | |
| Fizička sredstva, osoblje i načini postepena | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Razvoj | | |  |  | x | x | x |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  | |
| Proizvodnja | | |  |  |  | x | x |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  | |
| Isporuka | | |  |  |  |  |  |  |  |  |  |  |  |  | x |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  | |
| Aktivacija | | | x |  |  |  |  |  |  |  |  |  |  |  | x |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  | |
| Generisanje sigurnosnih podataka | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | x |  |  | |  |  |  |  |  |  |  |  |  | |
| Prenos sigurnosnih podataka | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | x |  |  | |  |  |  |  |  |  |  |  |  | |
| Raspoloživost kartice | | |  | x |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  | |
| Jedna kartica vozača | | |  | x |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  | |
| Mogućnost sljedivosti kartice | | |  | x |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  | |
| Ovlaštene radionice | | |  |  |  |  |  | x |  | x |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  | |
| Redovna kontrolna kalibracija | | |  |  |  |  |  | x |  | x |  |  |  | x | x |  |  | x |  |  |  | |  |  |  |  |  |  |  |  |  | |
| Pouzdane radionice | | |  |  |  |  |  | x |  | x |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  | |
| Pouzdani vozači | | |  | x |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  | |
| Nadzor nad sprovođenjem zakona | | |  | x |  |  |  | x |  | x | x |  | x |  | x |  | x |  |  | x | x | |  |  |  |  |  |  |  |  |  | |
| Nadogradnja programa | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | x | |  |  |  |  |  |  |  |  |  | |
| Funkcije sprovođenje sigurnosti | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Identifikacija i autentifikacija | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| UIA\_201 Identifikacija senzora | | |  |  |  |  |  |  |  |  |  | x |  | x |  |  |  |  |  |  |  | |  |  |  | x |  |  |  |  | x | |
| UIA\_202 Identitet senzora | | |  |  |  |  |  |  |  |  |  | x |  | x |  |  |  |  |  |  |  | |  |  |  | x |  |  |  |  | x | |
| UIA\_203 Autentifikacija senzora | | |  |  |  |  |  |  |  |  |  | x |  | x |  |  |  |  |  |  |  | |  |  |  | x |  |  |  |  | x | |
| UIA\_204 Ponovna identifikacija i ponovna autentifikacija senzora | | |  |  |  |  |  |  |  |  |  | x |  | x |  |  |  |  |  |  |  | |  |  |  | x |  |  |  |  | x | |
| UIA\_205 Trajna autentifikacija | | |  |  |  |  |  |  |  |  |  | x |  | x |  |  |  |  |  |  |  | |  |  |  | x |  |  |  |  |  | |
| UIA\_206 Neuspjela autentifikacija | | |  |  |  |  |  |  |  |  |  | x |  | x |  |  |  |  |  |  |  | |  |  | x |  |  |  |  | x |  | |
| UIA\_207 Identifikacija korisnika | | | x | x |  |  |  |  |  |  |  | x |  |  |  |  |  |  |  |  |  | | x |  |  | x |  |  |  |  | x | |
| UIA\_208 Identitet korisnika | | | x | x |  |  |  |  |  |  |  | x |  |  |  |  |  |  |  |  |  | | x |  |  | x |  |  |  |  | x | |
| UIA\_209 Autentifikacija korisnika | | | x | x |  |  |  |  |  |  |  | x |  |  |  |  |  |  |  |  |  | | x |  |  | x |  |  |  |  | x | |
| UIA\_210 Ponovna autentifikacija korisnika | | | x | x |  |  |  |  |  |  |  | x |  |  |  |  |  |  |  |  |  | | x |  |  | x |  |  |  |  | x | |
| UIA\_211 Sredstva autentifikacije | | | x | x |  |  |  |  |  |  |  | x |  |  |  |  |  |  |  |  |  | | x |  |  | x |  |  |  |  |  | |
| UIA\_212 Provjere PIN | | | x | x |  |  |  | x |  | x |  |  |  |  |  |  |  |  |  |  |  | | x |  |  | x |  |  |  |  |  | |
| UIA\_213 Trajna autentifikacija | | | x | x |  |  |  |  |  |  |  | x |  |  |  |  |  |  |  |  |  | | x |  |  | x |  |  |  |  |  | |
| UIA\_214 Neuspjela autentifikacija | | | x | x |  |  |  |  |  |  |  | x |  |  |  |  |  |  |  |  |  | |  |  | x |  |  |  |  |  |  | |
| UIA\_215 Daljinska identifikacija korisnika | | | x | x |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | x |  |  | x |  |  |  |  | x | |
| UIA\_216 Daljinski identitet korisnika | | | x | x |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | x |  |  | x |  |  |  |  |  | |
| UIA\_217 Daljinska autentifikacija korisnika | | | x | x |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | x |  |  | x |  |  |  |  | x | |
| UIA\_218 Sredstva autentifikacije | | | x | x |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | x |  |  | x |  |  |  |  |  | |
| UIA\_219 Trajna autentifikacija | | | x | x |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | x |  |  | x |  |  |  |  |  | |
| UIA\_220 Neuspjela autentifikacija | | | x | x |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  | |
| UIA\_221 Identifikacija upravljačkog uređaja | | | x | x |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | x |  |  | x |  |  |  |  |  | |
| UIA\_222 Autentifikacija upravljačkog uređaja | | | x | x |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | x |  |  | x |  |  |  |  |  | |
| UIA\_223 Trajna autentifikacija | | | x | x |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | x |  |  | x |  |  |  |  |  | |
| Upravljanje pristubom | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ACC\_201 Politika upravljanja pristubom | | | x |  |  |  |  | x |  | x |  |  |  |  |  |  |  |  | x |  | x | | x |  |  |  |  |  |  |  |  | |
| ACC\_202 Prava pristupa funkcijama | | | x |  |  |  |  | x |  | x |  |  |  |  |  |  |  |  |  |  |  | | x |  |  |  |  |  |  |  |  | |
| ACC\_203 Prava pristupa funkcijama | | | x |  |  |  |  | x |  | x |  |  |  |  |  |  |  |  |  |  |  | | x |  |  |  |  |  |  |  |  | |
| ACC\_204 VU ID | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | x | | x |  |  |  |  |  |  |  |  | |
| ACC\_205 ID priključenog senzora | | |  |  |  |  |  |  |  |  |  | x |  |  |  |  |  |  |  |  | x | | x |  |  |  |  |  |  |  |  | |
| ACC\_206 Podaci o kalibraciji | | | x |  |  |  |  | x |  |  |  |  |  |  |  |  |  |  |  |  | x | | x |  |  |  |  |  |  |  |  | |
| ACC\_207 Podaci o kalibraciji | | |  |  |  |  |  | x |  |  |  |  |  |  |  |  |  |  |  |  | x | | x |  |  |  |  |  |  |  |  | |
| ACC\_208 Podaci o podešavanju vremena | | |  |  |  |  |  |  |  | x |  |  |  |  |  |  |  |  |  |  | x | | x |  |  |  |  |  |  |  |  | |
| ACC\_209 Podaci o podešavanju vremena | | |  |  |  |  |  |  |  | x |  |  |  |  |  |  |  |  |  |  | x | | x |  |  |  |  |  |  |  |  | |
| ACC\_210 Sigurnosni podaci | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | x |  | x | | x |  |  |  |  |  |  |  |  | |
| ACC\_211 Struktura datoteke i uslovi pristupa | | | x |  |  |  |  | x |  |  |  |  |  |  |  |  |  |  | x |  | x | | x |  |  |  |  |  |  |  |  | |
| Odgovornost | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ACT\_201 Odgovornost vozača | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  | x |  |  |  |  |  |  |  | |
| ACT\_202 ID podaci o VU | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  | x | x |  |  |  |  |  |  | |
| ACT\_203 Odgovornost radionice | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  | x |  |  |  |  |  |  |  | |
| ACT\_204 Odgovornost kontrolora | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  | x |  |  |  |  |  |  |  | |
| ACT\_205 Odgovornost za kretanja vozila: | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  | x |  |  |  |  |  |  |  | |
| ACT\_206 Izmjena podataka o odgovornosti | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | x | |  |  |  |  | x |  |  | x |  | |
| ACT\_207 Izmjena podataka o odgovornosti | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | x | |  |  |  |  | x |  |  | x |  | |
| Revizija | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| AUD\_201 Revizijski zapisi | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  | x |  |  |  |  |  |  | |
| AUD\_202 Popis revizijskih slučajeva | | | x |  |  |  |  |  | x |  |  |  | x | x |  | x | x |  |  |  | x | |  |  | x |  |  |  |  |  |  | |
| AUD\_203 Pravila pohranjivanja revizijskih zapisa | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  | x |  |  |  |  |  |  | |
| AUD\_204 Revizijski zapisi senzora | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  | x |  |  |  |  |  |  | |
| AUD\_205 Sredstva za reviziju | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  | x |  |  |  |  |  |  | |
| Ponovno korištenje | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| REU\_201 Ponovno korištenje | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | x |  |  | |  |  |  |  |  |  | x | x |  | |
| Tačnost | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ACR\_201 Politika upravljanja tokom informacija | | |  |  |  |  |  | x |  |  | x |  | x |  |  |  |  |  |  |  |  | |  |  |  |  |  |  | x | x |  | |
| ACR\_202 Unutarnji prenos | | |  |  |  |  |  |  |  |  |  |  |  |  |  | x |  |  |  |  |  | |  |  |  |  |  | x | x | x |  | |
| ACR\_203 Unutarnji prenos | | |  |  |  |  |  |  |  |  |  |  |  |  |  | x |  |  |  |  |  | |  |  | x |  |  |  |  |  |  | |
| ACR\_204 Potpunost arhiviranih podataka | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | x | |  |  |  |  | x |  |  | x |  | |
| ACR\_205 Potpunost arhiviranih podataka | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | x | |  |  | x |  |  |  |  |  |  | |
| Pouzdanost | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| RLB\_201 Ispitivanja u proizvodnji | | |  |  |  | x | x |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  | x |  | |
| RLB\_202 Samoispitivanja | | |  |  | x |  |  |  |  |  |  |  | x |  |  |  | x |  |  | x |  | |  |  |  |  |  |  |  | x |  | |
| RLB\_203 Samoispitivanja | | |  |  |  |  |  |  |  |  |  |  | x |  |  |  | x |  |  | x |  | |  |  | x |  |  |  |  |  |  | |
| RLB\_204 Analiza programa | | |  |  |  |  | x |  |  |  |  |  |  |  |  |  |  |  |  | x |  | |  |  |  |  |  |  |  | x |  | |
| RLB\_205 Unos programa | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | x |  | |  |  |  |  |  | x | x | x |  | |
| RLB\_206 Otvaranje kućišta | | |  |  |  |  | x |  |  |  | x |  | x |  |  | x |  |  | x | x | x | |  |  |  |  |  | x |  | x |  | |
| RLB\_207 Preinake hardvera | | |  |  |  |  |  |  |  |  |  |  | x |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  | x |  | |
| RLB\_208 Preinake hardvera | | |  |  |  |  |  |  |  |  |  |  | x |  |  |  |  |  |  |  |  | |  |  | x |  |  |  |  |  |  | |
| RLB\_209 Prekidi napajanja | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  | x |  |  |  |  | |  |  |  |  |  |  |  | x |  | |
| RLB\_210 Prekidi napajanja | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  | x |  |  |  |  | |  |  | x |  |  |  |  |  |  | |
| RLB\_211 Vraćanje u početno stanje | | |  |  | x |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  | x |  | |
| RLB\_212 Dostubnost podataka | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  | x | x |  | |
| RLB\_213 Izvlačenje kartice | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  | x |  | |
| RLB\_214 Razmjena podataka s karticom nije ispravno završeno | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  | x |  |  |  |  |  | |
| RLB\_215 Višestruke aplikacije | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  | x |  | |
| Razmjena podataka | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DEX\_201 Osiguran unos podataka o kretanju | | |  |  |  |  |  |  |  |  |  |  |  | x |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  | x | |
| DEX\_202 Osiguran unos podataka o kretanju | | |  |  |  |  |  |  |  |  |  |  |  | x |  |  |  |  |  |  | x | |  |  |  |  |  |  |  |  |  | |
| DEX\_203 Osiguran unos podataka s kartice | | |  |  |  |  |  |  | x |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  | x | |
| DEX\_204 Osiguran unos podataka s kartice | | |  |  |  |  |  |  | x |  |  |  |  |  |  |  |  |  |  |  |  | |  |  | x |  |  |  |  |  |  | |
| DEX\_205 Osigurana isporuka podataka na kartice | | |  |  |  |  |  |  | x |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  | x | |
| DEX\_206 Dokaz o podrijetlu | | |  |  |  |  |  |  |  |  |  |  |  |  |  | x |  |  |  |  |  | |  |  |  |  |  | x |  |  |  | |
| DEX\_207 Dokaz o podrijetlu | | |  |  |  |  |  |  |  |  |  |  |  |  |  | x |  |  |  |  |  | |  |  |  |  |  | x |  |  |  | |
| DEX\_208 Osigurana isporuka na vanjske medije | | |  |  |  |  |  |  |  |  |  |  |  |  |  | x |  |  |  |  |  | |  |  |  |  |  | x |  |  |  | |
| Kriptografska podrška | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| CSP\_201 Algoritmi | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  | x | x | |
| CSP\_202 Generisanje ključa | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  | x | x | |
| CSP\_203 Raspodjela ključa | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  | x | x | |
| CSP\_204 Dostubnost ključa | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  | x | x | |
| CSP\_205 Unošenje ključa | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  | x | x | |

**GENERIČKI SIGURNOSNI CILJ KARTICE TAHOGRAFA**

**1.   Uvod**

Ovaj dokument sadrži opis kartice tahografa, opasnosti koje mora prevladati i sigurnosne ciljeve koje mora postići, propisuje tražene funkcije sprovođenje sigurnosti, te navodi zahtijevanu najmanju otpornost sigurnosnih mehanizama i zahtijevanu razinu sigurnosti za razvoj i ocjenjivanje.

Zahtjevi iz ovog dokumenta su oni iz teksta Priloga I.B. U svrhu jasnoće čitanja ponekad dolazi do ponavljanja zahtjeva u tekstu Priloga I.B i zahtjeva u vezi sigurnosnih ciljeva. Ako postoje dvojbe između zahtjeva u vezi sigurnosnog cilja i zahtjeva iz Priloga I.B na koji se poziva ovaj zahtjev u vezi sigurnosnog cilja, vrijedi zahtjev iz teksta Priloga I.B.

Zahtjevi iz teksta Priloga I.B na koje se ne pozivaju sigurnosni ciljevi ne podliježu funkcijama sprovođenje sigurnosti.

Kartica tahografa je standardna pametna kartica koja sadrži namjensku tahografsku aplikaciju i mora zadovoljiti najnovijim funkcionalnim i sigurnosnim zahtjevima koji vrijede za pametne kartice. Ovaj sigurnosni cilj stoga utjelovljuje samo dodatne sigurnosne zahtjeve potrebne za tahografsku aplikaciju.

Jednoznačne oznake su pripisane opasnostima, ciljevima, načinima postepena i specifikacijama SEF u svrhu pronalaženja dokumentacije za razvoj i ocjenu.

**2.   Kratice, definicije i literatura**

**2.1.    Kratice**

|  |  |
| --- | --- |
| IC | integirsani krug (elektronski sastavni dio namijenjen funkcijama obrade podataka i/ili memorije) |
| OS | operativni sistem |
| PIN | osobni identifikacijski broj |
| ROM | stalna memorija |
| SFP | politika sigurnosnih funkcija |
| TBD | odredit će se |
| TOE | predmet ocjenjivanja |
| TSF | sigurnosna funkcija TOE |
| VU | jedinica u vozilu. |

**2.2.    Definicije**

|  |  |
| --- | --- |
| Digitalni tahograf | Uređaj za belježenje |
| Osjetljivi podaci | Podaci koje arhivira kartica tahografa koje treba zaštititi u smislu potpunosti, neovlaštene izmjene i pouzdanosti (ako vrijedi za sigurnosne podatke). Osjetljivi podaci obuhvaćaju sigurnosne podatke i korisničke podatke. |
| Sigurnosni podaci | Posebni podaci potrebni za podržavanje funkcija sprovođenje sigurnosti (npr. kriptografski ključevi). |
| Sistem | Oprema, osoblje ili organizacije koje su na bilo koji način povezane s tahografom. |
| Korisnik | Svaka jedinica (čovjek korisnik ili spoljna jedinica IT) van TOE koja je u međudjelovanju s TOE (kada se ne koristi u izrazu ‚korisnički podaci’). |
| Korisnički podaci | Osjetljivi podaci koji se spašavaju na karticu tahografa, drugačiji od sigurnosnih podataka. Korisnički podaci obuhvaćaju identifikacijske podatke i podatke o aktivnosti. |
| Identifikacijski podaci | Identifikacijski podaci obuhvaćaju identifikacijske podatke za karticu i identifikacijske podatke nosioca kartice. |
| Identifikacijski podaci kartice | Korisnički podaci koji se odnose na identifikaciju kartice određenu zahtjevima 190, 191, 192, 194, 215, 231 i 235. |
| Identifikacijski podaci nosioca kartice | Korisnički podaci koji se odnose na identifikaciju nosioca kartice određenu zahtjevima 195, 196, 216, 232 i 236. |
| Podaci o aktivnosti | Podaci o aktivnosti obuhvaćaju podatke o aktivnostima nosioca kartice, podatke o događajima i greškama i podatke o aktivnostima nadzora. |
| Podaci o aktivnostima nosioca kartice | Korisnički podaci koji se odnose na aktivnosti nosioca kartice određene zahtjevima 197, 199, 202, 212, 212a, 217, 219, 221, 226, 227, 229, 230a, 233 i 237. |
| Podaci o događajima i greškama | Korisnički podaci koji se odnose na događaje ili greške određene u zahtjevima 204, 205, 207, 208 i 223. |
| Podaci o aktivnostima nadzora | Korisnički podaci koji se odnose na kontrolu sprovođenje zakona propisanu u zahtjevima 210 i 225. |

**2.3.    Literatura**

|  |  |
| --- | --- |
| ITSEC | Kriterijum vrednovanja sigurnosti informacijske tehnologije ITSEC 1991. |
| IC PP | Profil zaštite integriranog kruga pametne kartice – verzija 2.0 – izdanje rujan 1998. Registrovano pri francuskom certifikacijskom tijelu pod brojem PP/9806 |
| ES PP | Integirsani krug pametne kartice sa ugrađenim profilom zaštite programa – verzija 2.0 – izdanje lipanj 1999. Registrovano pri francuskom certifikacijskom tijelu pod brojem PP/9911 |

**3.   Obrazloženje proizvoda**

**3.1.    Opis kartice tahografa i način korištenja**

Kartica tahografa je pametna kartica, opisana u (IC PP) i (ES PP), koja sadrži program namijenjen njenom korištenju s tahografom.

Osnovne funkcije kartice tahografa su:

|  |  |
| --- | --- |
| — | pohranjivati identifikacijske podatke kartice i nosioca kartice. Ove podatke koristi jedinica u vozilu za identifikaciju nosioca kartice, pružanje odgovarajućih funkcija i prava na pristub podacima, te jamčenje odgovornosti nosioca kartice za svoje aktivnosti, |

|  |  |
| --- | --- |
| — | pohranjivati podatke o aktivnostima nosioca kartice, podatke o događajima i greškama i podatke o nadzornim aktivnostima, koji se odnose na vlasnike podataka. |

Kartica tahografa je stoga namijenjena korištenju od strane uređaja za kartično sučelje jedinice u vozilu. Može je takođe koristiti svaki čitač kartica (npr. osobno računalo) koje ima puno pravo na pristub čitanju svakog korisničkog podatka.

Tokom konačnog fazaa korištenja u životnom vijeku kartice tahografa (faza 7 životnog vijeka prema (ES PP), samo jedinice u vozilu mogu upisivati korisničke podatke u karticu.

Funkcionalni zahtjevi za karticu tahografa su propisani u tekstu Prilogu I.B i Dodatku 2.

**3.2.    Životni vijek kartice tahografa**

Životni vijek kartice tahografa odgovara životnom vijeku pametne kartice opisane u (ES PP).

**3.3.    Opasnosti**

Pored opštih opasnosti za pametnu karticu koji su navedeni u (ES PP) i (IC PP), kartica tahografa može se suočiti sa sljedećim opasnostima:

**3.3.1.   Krajnji ciljevi**

Krajnji cilj napadača je izmjena korisničkih podataka arhiviranih unutar TOE.

|  |  |
| --- | --- |
| T.Ident\_Data | Uspješna izmjena identifikacijskih podataka koje nosi TOE (npr. vrsta kartice ili datum isteka važnosti kartice ili identifikacijski podaci nosioca kartice) bi mogla omogućiti prijevarno korištenje TOE i mogla bi predstavljati veću opasnost za sveopšti sigurnosni cilj sistema. |
| T.Activity\_Data | Uspješna izmjena podataka o aktivnostima arhiviranih u TOE bi predstavljala opasnost za sigurnost TOE. |
| T.Data\_Exchange | Uspješna izmjena podataka o aktivnostima (dodavanje, brisanje, izmjena) tokom unosa ili isporuke podataka bi mogla predstavljati opasnost za sigurnost TOE. |

**3.3.2.   Putovi napada**

Stavke TOE se može napasti:

|  |  |
| --- | --- |
| — | pokušajem nezakonitog stjecanja saznanja o hardverskom i softverskom projektu opreme TOE i posebno o njezinim sigurnosnim funkcijama ili sigurnosnim podacima. Nedopušteno saznanje se može steći putem napada na materijal projektanta ili proizvođača materijala (krađa, mito, …) ili putem direktnog pregleda TOE (fizički uzorci, analiza zaključaka, …), |

|  |  |
| --- | --- |
| — | korištenjem slabosti u osmišljanju ili ostvarenju TOE (iskorištavanje grešaka hardvera, grešaka u softveru, propusta prenosa, grešaka koje izaziva TOE opterećenjem iz okruženja, iskorištavanje slabosti sigurnosnih funkcija kao što su postubci autentifikacije, upravljanje pristubu podacima, kriptografske radnje, …), |

|  |  |
| --- | --- |
| — | izmjenom TOE ili njezinih sigurnosnih funkcija putem fizičkih, električnih ili logičkih napada ili kombinacija istih. |

**3.4.    Sigurnosni ciljevi**

Glavni sigurnosni cilj cjelokupnog sistema digitalnog tahografa je sljedeći:

|  |  |
| --- | --- |
| O.Main | Podaci koje provjeravaju kontrolna tijela moraju biti dostubni i u potpunosti i točno odražavati aktivnost nadziranih vozača i vozila u pogledu vožnje, rada, perioda pripravnosti i odmora, te u pogledu brzine vozila. |

Stoga su glavni sigurnosni ciljevi TOE koji doprinose sveopštim sigurnosnom cilju sljedeći:

|  |  |
| --- | --- |
| O.Card\_Identification\_Data | TOE mora očuvati identifikacijske podatke o kartici i nosiocu kartice sačuvane u postubku personalizacije kartice, |
| O.Card\_Activity\_Storage | TOE mora očuvati korisničke podatke koji su arhivirani na karticu od strane jedinica u vozilu. |

**3.5.    Sigurnosni ciljevi informatičke tehnologije**

Pored opštih sigurnosnih ciljeva pametne kartice navedenih u (ES PP) i (IC PP), posebni sigurnosni ciljevi IT TOE koji doprinose njegovim glavnim sigurnosnim ciljevima tokom faze njegovog konačnog životnog vijeka korištenja su sljedeći:

|  |  |
| --- | --- |
| O.Data\_Access | TOE mora ograničiti pravo pristupa upisivanju korisničkih podataka na autentificirane jedinice u vozilu, |
| O.Secure\_Communications | TOE mora biti u stanju podržavati sigurne komunikacijske protokole i postubke između kartice i uređaja kartičnog sučelja kada to nalaže program. |

**3.6.    Fizička sredstva, osoblje ili načini postepena**

Fizička sredstva, osoblje ili načini postepena koji doprinose sigurnosti TOE su navedeni u (ES PP) i (IC PP) (poglavlja o sigurnosnim ciljevima za okruženje).

**4.   Funkcije sprovođenje sigurnosti**

Ovaj stavak podrobnije opisuje neke od dopuštenih radnji kao što su dodjela ili odabir (ES PP) i osigurava dodatne funkcionalne zahtjeve za SEF.

**4.1.    Udovoljavanje profilu zaštite**

CPP\_301  
TOE mora biti usklađen s (IC PP).

CPP\_302  
TOE mora biti usklađen s (ES PP), kako je podrobnije opisano u nastavu.

**4.2.    Identifikacija i autentifikacija korisnika**

Kartica mora identifikujeti jedinicu u koju je umetnuta i znati je li to autentificirana jedinica u vozilu ili nije. Kartica može isporučivati sve korisničke podatke bez obzira na jedinicu na koju je povezana, osim kontrolne kartice koja može isporučiti identifikacijske podatke nosioca kartice samo autentificiranim jedinicama u vozilu (tako da kontrolor bude siguran da jedinica u vozilu nije lažna uočavanjem svojeg imena na prikazu ili ispisu).

**4.2.1.   Identifikacija korisnika**

**Zadatak** (FIA\_UID.1.1) Popis aktivnosti uz posredovanje TSF: niti jedna.

**Zadatak** (FIA\_ATD.1.1) Popis sigurnosnih obelježja:

USER\_GROUP: VEHICLE\_UNIT, NON\_VEHICLE\_UNIT,

USER\_ID: registracijski broj vozila (VRN) i šifra države članice registracije (USER\_ID je poznat samo za USER\_GROUP = VEHICLE\_UNIT).

**4.2.2.   Autentifikacija korisnika**

**Zadatak** (FIA\_UAU.1.1) Popis aktivnosti uz posredovanje TSF:

|  |  |
| --- | --- |
| — | kartice vozača i radionice: isporuka korisničkih podataka sa sigurnosnim obilježjima (funkcija preuzimanja podataka sa kartice), |

|  |  |
| --- | --- |
| — | kontrolna kartica: isporuka korisničkih podataka bez sigurnosnih obelježja osim za identifikacijske podatke vozača. |

UIA\_301  
Autentifikacija jedinice u vozilu se obavlja putem dokazivanja da posjeduje sigurnosne podatke koje može raspoređivati samo sistem.

**Odabir** (FIA\_UAU.3.1 i FIA\_UAU.3.2): spriječiti.

**Zadatak** (FIA\_UAU.4.1) Identifikujeni autentifikacijski mehanizam/mehanizmi: svaki autentifikacijski mehanizam.

UIA\_302  
Kartica radionice mora osigurati dodatni autentifikacijski mehanizam provjerom šifre PIN (Svrha ovog mehanizma je da jedinica u vozilu osigura identitet nosioca kartice, a nije namijenjen zaštiti sadržaja kartice radionice).

**4.2.3.   Neuspjela autentifikacija**

Sljedeći zadaci opisuju reakciju kartice za svaki pojedini propust autentifikacije korisnika.

**Zadatak** (FIA\_AFL.1.1) Broj: 1, popis autentifikacijskih slučajeva: autentifikacija uređaja kartičnog sučelja.

**Zadatak** (FIA\_AFL.1.2) Popis radnji:

— upozoriti priključenu jedinicu,

— smatrati korisnika kao NON\_VEHICLE\_UNIT.

Sljedeći zadaci opisuju reakciju kartice kod propusta dodatnog autentifikacijskog mehanizma prema zahtjevu UIA\_302.

**Zadatak** (FIA\_AFL.1.1) Broj: 5, popis autentifikacijskih slučajeva: provjere PIN (kartica radionice).

**Zadatak** (FIA\_AFL.1.2) Popis radnji:

— upozoriti priključenu jedinicu,

— blokirati postupak provjere PIN-a tako da svaki sljedeći pokušaj provjere PIN-a bude neuspješan,

— biti u stanju naznačiti narednim korisnicima razlog blokiranja.

**4.3.    Upravljanje pristubom**

**4.3.1.   Politika upravljanja pristubom**

Na kraju svog životnog vijeka, kartica tahografa podliježe politici jedne jedine sigurnosne funkcije upravljanja pristubom (SFP) koja se naziva AC\_SFP.

Zadatak (FDP\_ACC.2.1) SFP upravljanje pristubom: AC\_SFP.

**4.3.2.   Funkcije upravljanja pristubom**

**Zadatak** (FDP\_ACF.1.1) SFP upravljanje pristubom: AC\_SFP.

**Zadatak** (FDP\_ACF.1.1) Imenovana skupina sigurnosnih obelježja: USER\_GROUP.

**Zadatak** (FDP\_ACF.1.2) Pravila koja uređuju pristub kod nadziranih subjekata i nadziranih objekata koji koriste nadzirane radnje na nadziranim objektima:

|  |  |  |
| --- | --- | --- |
| GENERAL\_READ | : | Korisnički podatak može učitati iz TOE svaki korisnik, osim identifikacijskih podataka korisnika kartice koje s kontrolnih kartica može učitati samo VEHICLE\_UNIT. |
| IDENTIF\_WRITE | : | Identifikacijski podaci se mogu upisati samo jednom i prije kraja faze 6 životnog vijeka kartice. Niti jedan korisnik ne može upisivati ili mijenjati identifikacijske podatke tokom životnog vijeka kartice. |
| ACTIVITY\_WRITE | : | Podatke o aktivnostima može na TOE upisivati samo VEHICLE\_UNIT. |
| SOFT\_UPGRADE | : | Niti jedan korisnik ne može nadograđivati softver TOE. |
| FILE\_STRUCTURE | : | Struktrura datoteka i uslovi pristupa stvaraju se prije kraja faze 6 životnog vijeka TOE i potom se blokiraju protiv svake dalje izmjene ili brisanja od strane bilo kojeg korisnika. |

**4.4.    Odgovornost**

ACT\_301  
TOE mora sadržavate trajne identifikacijske podatke.

ACT\_302  
Moraju biti naznačeni vrijeme i datum personalizacije TOE. Takva oznaka mora ostati neizmjenjiva.

**4.5.    Revizija**

TOE mora pratiti slučajeve koji označivaju potencijalnu ugrozu njegove sigurnosti.

**Zadatak** (FAU\_SAA.1.2) Podskup propisanih revizijskih događaja.

— neuspjeh u autentifikaciji nosioca kartice (5 uzastopnih neuspješnih provjera PIN),

— greška samoispitivanja,

— greška potpunosti arhiviranih podataka,

— greška potpunosti unosa podataka o aktivnosti.

**4.6.    Tačnost**

**4.6.1.   Potpunost arhiviranih podataka**

**Zadatak** (FDP\_SDI.2.2) Radnje koje treba poduzeti: upozoriti priključenu jedinicu,

**4.6.2.   Temeljna autentifikacija podataka**

**Zadatak** (FDP\_DAU.1.1) Popis objekata ili tipovi informacija: podaci o aktivnosti.

**Zadatak** (FDP\_DAU.1.2) Popis subjekata: bilo koji.

**4.7.    Pouzdanost servisa**

**4.7.1.   Ispitivanja**

**Odabir** (FPT\_TST.1.1): tokom početnog pokretanja, periodično tokom redovnog rada.

Napomena: tokom početnog pokretanja znači prije nego što se izvrši kod programa (i ne nužno tokom postubka odziva na povrat u početno stanje).

RLB\_301  
Samoispitivanja TOE moraju obuhvatiti provjeru potpunosti svakog programskog koda softvera koji nije pohranjen u ROM.

RLB\_302  
Po otkrivanju greške samoispitivanja, TSF mora upozoriti priključenu jedinicu.

RLB\_303  
Nakon provedenog ispitivanja OS, sve naredbe i radnje svojstvene ispitivanju se moraju staviti van funkcije ili ukloniti. Ne smije biti moguće premostiti ove kontrolne uređaje i vratiti ih u uporabno stanje. Naredbi koja je pridružena isključivo jednoj fazi životnog vijeka nikada se ne smije pristubiti tokom nekog druge faze.

**4.7.2.   Softver**

RLB\_304  
Ne smije biti moguće analizirati, ispravljati greške ili izmijeniti program TOE na terenu.

RLB\_305  
Unos podataka iz spoljnih izvora se ne smije prihvatiti kao izvršni kod.

**4.7.3.   Napajanje**

RLB\_306  
TOE mora održavati sigurno stanje tokom prekida ili kolebanja napajanja.

**4.7.4.   Uslovi povrata u početno stanje**

RLB\_307  
Ako se prekine napajanje TOE (ili ako dođe do kolebanja napajanja) ili ako se postupak prekine prije okončanja ili u svim drugim uslovima vraćanja u početno stanje, TOE se mora uredno vratiti u početno stanje.

**4.8.    Razmjena podataka**

**4.8.1.   Razmjena podataka s jedinicom u vozilu**

DEX\_301  
TOE mora provjeriti potpunost i autentičnost podataka koji se unose sa jedince u vozilu.

DEX\_302  
Po otkrivanju greške potpunosti unesenih podataka, TOE mora:

— upozoriti jedinicu koja šalje podatke,

— ne koristiti podatke.

DEX\_303  
TOE mora isporučivati korisničke podatke jedinici u vozilu s odgovarajućim sigurnosnim značajkama, tako da jedinica u vozilu može provjeriti potpunost i autentičnost primljenih podataka.

**4.8.2.   Isporučivanje podataka jedinici van vozila (funkcija preuzimanja podataka)**

DEX\_304  
TOE mora biti u stanju generisati dokaz o podrijetlu za podatke preuzete na vanjske medije.

DEX\_305  
TOE mora moći osigurati mogućnost provjere dokaza o podrijetlu podataka preuzetih na primatelja.

DEX\_306  
TOE mora biti u stanju preuzeti podatke na vanjske medije za čuvanje podataka s odgovarajućim sigurnosnim obilježjima tako da se može provjeriti potpunost preuzetih podataka.

**4.9.    Kriptografska podrška**

CSP\_301  
Ako TSF generiše kriptografske ključeve, to će biti u skladu s propisanim algoritmima generisanja kriptografskih ključeva i propisanim dužinama kriptografskih ključeva. Generišeni ključevi kriptografske faze moraju imati ograničen broj mogućih uporaba (koje određuje proizvođač i ne više od 240).

CSP\_302  
Ako TSF raspodjeljuje kriptografske ključeve, to mora biti u skladu sa specifičnim metodama raspodjele kriptografskih ključeva.

**5.   Određivanje sigurnosnih mehanizama**

Zahtijevani sigurnosni mehanizmi su navedeni u Dodatku 11.

Sve ostale sigurnosne mehanizme mora definirati proizvođač TOE.

**6.   Tražena najmanja otpornost mehanizama**

Najmanja otpornost mehanizama za karticu tahografa je ‚visoka’ u skladu sa (ITSEC).

**7.   Nivo sigurnosti**

Ciljna nivo sigurnosti za karticu tahografa je nivo ITSEC E3 prema definiciji u (ITSEC).

**8.   Obrazloženje**

Sljedeće matrice daju obrazloženje SEF pomoću prikaza:

— koji SEF sprečava koje opasnosti,

— koji SEF ispunjava koje sigurnosne ciljeve IT.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Opasnosti** | | | | | | | | | | | | **Ciljevi IT** | | | | | | | | |
| **T.CLON\*** | **T.DIS\_ES2** | **T.T\_ES** | **T.T\_CMD** | **T.MOD\_SOFT\*** | **T.MOD\_LOAD** | **T.MOD\_EXE** | **T.MOD\_SHARE** | **Ident\_Data** | **Activity\_Data** | | **Data\_Exchange** | **O.TAMPER\_ES** | **O.CLON\*** | **O.OPERATE\*** | **O.FLAW\*** | **O.DIS\_MECJANISM2** | **O.DIS\_MEMORY\*** | **O.MOD\_MEMORY\*** | **Data\_Access** | **Secured\_Communications** |
| UIA\_301 Značenje autentifikacije |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  | x |  |
| UIA\_302 Provjere PIN |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  | x |  |
| ACT\_301 Identifikacijski podaci |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |
| ACT\_302 Datum personalizacije |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |
| RLB\_301 Potpunost softvera |  |  |  |  |  |  |  |  |  |  |  | | x |  | x |  |  |  |  |  |  |
| RLB\_302 Samoispitivanja |  |  |  |  |  |  |  |  |  |  |  | | x |  | x |  |  |  |  |  |  |
| RLB\_303 Ispitivanja u proizvodnji |  |  |  |  | x | x |  |  |  |  |  | | x |  | x |  |  |  |  |  |  |
| RLB\_304 Analiza softvera |  |  |  |  | x |  | x | x |  |  |  | | x |  | x |  |  |  |  |  |  |
| RLB\_305 Instalacija softvera |  |  |  |  | x | x |  | x |  |  |  | | x |  | x |  |  |  |  |  |  |
| RLB\_306 Napajanje |  |  |  |  |  |  |  |  | x | x |  | | x |  | x |  |  |  |  |  |  |
| RLB\_307 Vraćanje u početno stanje |  |  |  |  |  |  |  |  |  |  |  | | x |  | x |  |  |  |  |  |  |
| DEX\_301 Siguran unos podataka |  |  |  |  |  |  |  |  |  |  | x | |  |  |  |  |  |  |  |  | x |
| DEX\_302 Siguran unos podataka |  |  |  |  |  |  |  |  |  |  | x | |  |  |  |  |  |  |  |  | x |
| DEX\_303 Sigurna isporuka podataka u VU |  |  |  |  |  |  |  |  |  |  | x | |  |  |  |  |  |  |  |  | x |
| DEX\_304 Dokaz o podrijetlu |  |  |  |  |  |  |  |  |  |  | x | |  |  |  |  |  |  |  |  | x |
| DEX\_305 Dokaz o podrijetlu |  |  |  |  |  |  |  |  |  |  | x | |  |  |  |  |  |  |  |  | x |
| DEX\_306 Sigurna isporuka spoljnim medijima |  |  |  |  |  |  |  |  |  |  | x | |  |  |  |  |  |  |  |  | x |
| CSP\_301 Generisanje ključeva |  |  |  |  |  |  |  |  |  |  |  | | x |  |  |  |  |  |  |  | x |
| CSP\_302 Raspodjela ključeva |  |  |  |  |  |  |  |  |  |  |  | | x |  |  |  |  |  |  |  | x |

**Dodatak 11.**

**ZAJEDNIČKI SIGURNOSNI MEHANIZMI**

SADRŽAJ

1. Uopšteno…

1.1. Literatura…

1.2. Označivanje i skraćenice…

2. Kriptografski sistemi i algoritmi…

2.1. Kriptografski sistemi…

2.2. Kriptografski algoritmi…

2.2.1. Algoritam RSA…

2.2.2. Algoritam kompresije…

2.2.3. Algoritam šifriranja podataka…

3. Ključevi i certifikati…

3.1. Generisanje i raspodjela ključeva…

3.1.1. Generisanje i raspodjela ključeva RSA…

3.1.2. Ispitni ključevi RSA…

3.1.3. Ključevi senzora kretanja…

3.1.4. Generisanje i raspodjela ključeva postubka T-DES…

3.2. Ključevi…

3.3. Certifikati…

3.3.1. Sadržaj certifikata…

3.3.2. Izdani certifikati…

3.3.3. Provjera i otvaranje certifikata…

4. Mehanizam uzajamne autentifikacije…

5. Mehanizam povjerljivosti prenosa, potpunosti i autentifikacije prenosa podataka između kartica i jedinice u vozilu…

5.1. Sigurne poruke…

5.2. Postepene s greškama kod sigurnog upućivanja poruka…

5.3. Algoritmi proračuna kriptografskih kontrolnih zbireva…

5.4. Algoritam proračuna kriptograma za pouzdanost DO…

6. Mehanizmi digitalnog potpisa kod preuzimanja podataka…

6.1. Generisanje potpisa…

6.2. Provjera potpisa…

**1.   UOPŠTENO**

Ovaj Dodatak propisuje sigurnosne mehanizme koji osiguravaju:

|  |  |
| --- | --- |
| — | uzajamnu autentifikaciju između jedinice vozila i kartica tahografa, uključujući dogovaranje ključa razmjene podataka, |

|  |  |
| --- | --- |
| — | povjerljivost, potpunost i autentifikaciju podataka koji se prenose između jedinice vozila i kartica tahografa, |

|  |  |
| --- | --- |
| — | potpunost i autentifikaciju podataka preuzetih s jedinice vozila na vanjske medije za pohranjivanje, |

|  |  |
| --- | --- |
| — | potpunost i autentifikaciju podataka preuzetih sa kartica tahografa na vanjske medije za pohranjivanje. |

**1.1.   Literatura**

U ovom su Dodatku korišteni sljedeći izvori:

|  |  |
| --- | --- |
| SHA-1 | Nacionalni institut za norme i tehnologiju (NIST): Publikacija FIPS 180-1: Norma sigurnosne kompresije. Travanj 1995. |
| PKCS1 | Laboratoriji RSA. PKCS # 1: Norme šifriranja RSA. Verzija 2.0. listopad 1998. |
| TDES | Nacionalni institut za norme i tehnologiju (NIST): Publikacija FIPS 46-3: Norma šifriranja podataka. Nacrt 1999. |
| TDES-OP | ANSI X9.52, Načini rada algoritma za trostruko šifriranje podataka. 1998. |
| ISO/IEC 7816-4 | Informacijska tehnologija – Identifikacijske kartice – Kontaktne kartice s integirsanim krugom/krugovima – Dio 4.: Međugranske naredbe za razmjenu: Prvo izdanje 1995. + Izmjena 1.: 1997. |
| ISO/IEC 7816-6 | Informacijska tehnologija - Identifikacijske kartice - Kontaktne kartice s integirsanim krugom/krugovima - Dio 6.: Međugranski podakovni elementi. Prvi izdanje: 1996 + ispravak. 1: 1998. |
| ISO/IEC 7816-8 | Informacijska tehnologija - Identifikacijske kartice - Kontaktne kartice s integirsanim krugom/krugovima - Dio 8.: Međugranske naredbe u vezi sigurnosti. Prvo izdanje 1999. |
| ISO/IEC 9796-2 | Informacijska tehnologija – Sigurnosne tehnike – Sistemi digitalnog potpisa za obnavljanje poruka – Dio 2.: Mehanizmi koji koriste funkciju kompresije podataka. Prvo izdanje: 1997. |
| ISO/IEC 9798-3 | Informacijska tehnologija – Sigurnosne tehnike – Mehanizmi autentifikacije jedinice – Dio 3.: Identifikacija jedinice korištenjem algoritma javnog ključa. Drugo izdanje 1998. |
| ISO 16844-3 | Drumska vozila – Tahografski sistemi Dio 3.: Sučelje senzora kretanja. |

**1.2.   Označivanje i skraćenice**

U ovom se Dodatku koriste sljedeće oznake i skraćenice:

|  |  |
| --- | --- |
| (Ka, Kb, CZK) | Snop ključeva kojega koristi algoritam za trostruko šifriranje podataka |
| CA | Certifikacijsko tijelo |
| CAR | Upućivanje na certifikacijsko tijelo |
| CC | Kriptografski kontrolni zbir |
| CG | Kriptogram |
| CH | Glava naredbe |
| CHA | Ovlaštenje nosioca certifikata |
| CHR | Upućivanje na nosioca certifikata |
| D() | Dešifriranje pomoću DES |
| DE | Podakovni element |
| DO | Podakovni objekt |
| d | Privatni ključ RSA, privatni eksponent |
| e | Javni ključ RSA, javni eksponent |
| E() | Šifriranje pomoću DES |
| EQT | Oprema |
| Hash() | vrijednost komprimirane poruke, izlazni podatak funkcije komprimiranja |
| Hash | funkcija komprimiranja |
| KID | identifikator ključa |
| Km | Ključ TDES. Glavni ključ određen u ISO 16844-3 |
| Kmvu | Ključ TDES unesen u jedinice u vozilu |
| Kmwc | Ključ TDES unesen u kartice radionice |
| m | Predstavnik poruke, cjelobrojne brojeve između 0 i n-1 |
| n | Ključevi RSA, modul |
| PB | Bajtovi za popunjenje |
| PI | Bajt indikatora popunjenja (za kriptograme povjerljivih DO) |
| PV | Nešifrirana vrijednost |
| s | Predstavnik potpisa, cijelobrojni broj između 0 i n-1 |
| SSC | Brojač redoslijeda slanja |
| SM | Sigurno upućivanje poruka |
| TCBC | Način rada ulančavanjem šifarskih blokova TDEA |
| TDEA | Algoritam trostrukog šifriranja podataka |
| TLV | Vrijednost dužine oznake |
| VU | Jedinica u vozilu |
| X.C | certifikat korisnika X koji izdaje certifikacijsko tijelo |
| X.CA | certifikacijsko tijelo korisnika X |
| X.CA.PK0X.C | radnja razvijanja certifikata za izdvajanje javnog ključa. To je infiksni operator čiji je lijevi operand javni ključ certifikacionog tijela, a desni operand je certifikat koju izdaje navedeno certifikacijsko tijelo. Ishod je javni ključ korisnika X čiji certifikat je desni operand, |
| X.PK | javni ključ korisnika X |
| X.PK[I] | šifra RSA nekog podatka I, korištenjem javnog ključa korisnika X |
| X.SK | privatni ključ RSA korisnika X |
| X.SK[I] | šifra RSA nekog podatka I, korištenjem privatnog ključa korisnika X |
| ‚xx’ | heksadecimalna vrijednost |
| || | operator ulančavanja. |

**2.   KRIPTOGRAFSKI SISTEMI I ALGORITMI**

**2.1.   Kriptografski sistemi**

CSM\_001  
Jedinice u vozilu i kartice tahografa moraju koristiti klasičan kriptografski sistem javnog ključa RSA koji osigurava sljedeće sigurnosne mehanizme:

|  |  |
| --- | --- |
| — | autentifikaciju između jedinica u vozilu i kartica, |

|  |  |
| --- | --- |
| — | prenos ključeva trostruke-DES faze između jedinica u vozilu i kartica tahografa, |

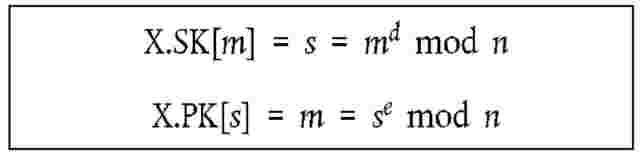
|  |  |
| --- | --- |
| — | digitalni potpis podataka preuzetih sa jedinica u vozilima ili kartica tahografa na vanjske medije. |

CSM\_002  
Jedinice u vozilu i kartice tahografa moraju koristiti trostruki simetričan kriptografski sistem DES za osiguranje mehanizma potpunosti podataka tokom razmjene korisničkih podataka između jedinica u vozilu i kartica tahografa i za osiguranje, ako je primjereno, pouzdanosti razmjene podataka između jedinica u vozilu i kartica tahografa.

**2.2.   Kriptografski algoritmi**

**2.2.1.    Algoritam RSA**

CSM\_003  
Algoritam RSA je u potpunosti definiran sljedećim odnosima:



Potpuniji opis funkcije RSA se može naći u izvoru (PKCS1).

Javni izlagač, e, za RSA izračune je cijeli broj između 3 i n-1 koji udovoljava gcd(e, lcm(p-1, q-1)) = 1.

**2.2.2.    Algoritam kompresije**

CSM\_004  
Mehanizmi digitalnog potpisa moraju koristiti algoritam kompresije SHA-1 definiran u izvoru (SHA-1).

**2.2.3.    Algoritam šifriranja podataka**

CSM\_005  
Algoritmi utemeljeni na DES se moraju koristiti u načinu ulančavanja šifriranih blokova.

**3.   KLJUČEVI I CERTIFIKATI**

**3.1.   Generisanje i raspodjela ključeva**

**3.1.1.    Generisanje i raspodjela ključeva RSA**

CSM\_006  
Ključevi RSA se moraju generisati preko tri funkcionalne hijerarhijske razine:

— europska nivo,

— nivo države članice,

— nivo opreme.

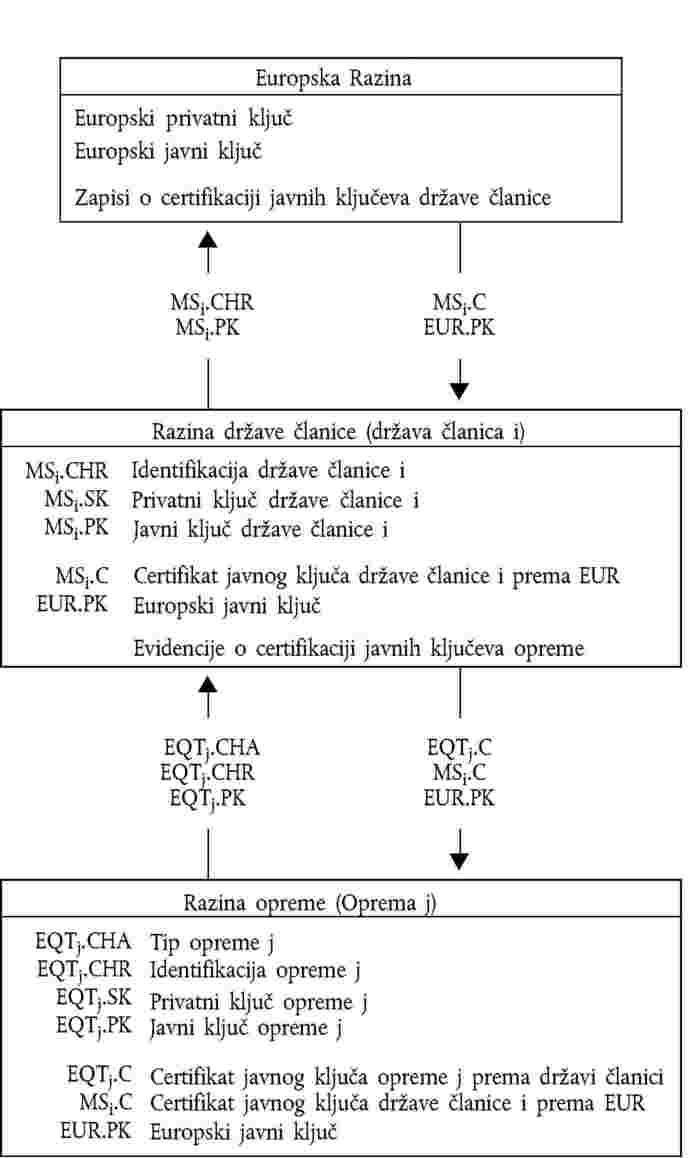
CSM\_007  
Na europskoj razini se mora generisati jedinstveni evropski par ključeva (EUR.SK i EUR.PK). Evropski privatni ključ se mora koristiti za certifikaciju javnih ključeva država članica. Moraju se voditi zapisi o svim potvrđenim ključevima. Ove poslove mora voditi Europsko certifikacijsko tijelo, pod nadležnošću i odgovornosti Evropske komisije.

CSM\_008  
Na razini države članice se mora generisati par ključeva države članice (MS.SK i MS.PK). Javni ključevi država članica moraju biti certificirani od strane Evropskog certifikacionog tijela. Privatni ključ države članice mora se koristiti za certificiranje javnih ključeva koji se unose u opremu (jedinica u vozilu ili kartica tahografa). Zapisi svih potvrđenih javnih ključeva moraju se čuvati s identifikacijom opreme za koju su namijenjeni. Ove poslove mora voditi certifikacijsko tijelo države članice. Država članica može redovito mijenjati svoj par ključeva.

CSM\_009  
Na razini opreme, generiše se i ubacuje u svaku napravu jedan jedini par ključeva (EQT.SK i EQT.PK). Javne ključeve opreme mora certificirati certifikacijsko tijelo države članice. Ove poslove mogu voditi proizvođači opreme, izvođači personalizacije opreme ili vlasti države članice. Ovaj par ključeva se koristi za službe autentifikacije, digitalnog potpisa i šifriranje

CSM\_010  
Povjerljivost privatnih ključeva mora se održavati tokom generisanja, prenosa (ako postoji) i čuvanja.

Sljedeća slika sažima protok podataka u ovom postubku:



**3.1.2.    Ispitni ključevi RSA**

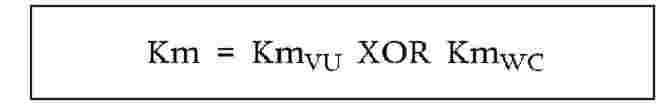
CSM\_011  
U svrhu ispitivanja opreme (uključujući ispitivanje interoperabilnosti) Europsko certifikacijsko tijelo izrađuje različit jedinstveni evropski par ispitnih ključeva i najmanje dva para ispitnih ključeva države članice, čiji se javni ključevi certificiraju evropskim privatnim ispitnim ključem. U opremu koja podliježe tipskom odobrenju proizvođači moraju unijeti ispitne ključeve certificirane jednim od ovih ispitnih ključeva države članice.

**3.1.3.    Ključevi senzora kretanja**

Povjerljivost tri ključa TDES koji su opisani u nastavu se mora odgovarajuće održavati tokom generisanja, prenosa (ako postoji) i čuvanja.

Za podršku tahografa koji zadovoljava ISO 16844, Europsko certifikacijsko tijelo i certifikacijska tijela države članice moraju, pored toga, osigurati sljedeće:

CSM\_036  
Europsko certifikacijsko tijelo mora generisati KmVU i KmWC, dva neovisna i jedinstvena trojna ključa DES, te generisati Km kao:



Europsko certifikacijsko tijelo dostavlja navedene ključeve certifikacijskim tijelu država članica u odgovarajuće osiguranim postubcima, na njihov zahtjev.

CSM\_037  
Certifikacijska tijela država članica moraju:

|  |  |
| --- | --- |
| — | koristiti Km za šifriranje podataka osjetila kretanja koje traže proizvođači senzora kretanja (podaci koji se šifriraju s Km su određeni u ISO 16844-3), |

|  |  |
| --- | --- |
| — | dostaviti KmVU proizvođačima jedinica u vozilu, u odgovarajuće osiguranim postubcima, za unošenje u jedinice u vozilu, |

|  |  |
| --- | --- |
| — | osigurati da KmWC bude umetnut u sve kartice radionica (Image u elementarnoj datoteciImage) tokom personalizacije kartice. |

**3.1.4.    Generisanje i raspodjela ključeva postubka T-DES**

CSM\_012  
Jedinice u vozilu i kartice tahografa moraju, kao dio postubka uzajamne autentifikacije, generisati i razmjenjivati podatke potrebne za izradu zajedničkog kripto ključa trojnog procesa DES. Povjerljivost ove razmjene podataka mora biti zaštićena putem kripto mehanizma šifriranja RSA.

CSM\_013  
Ovaj ključ se mora koristiti za sve naredne kriptografske radnje koje koriste sigurne poruke. Njegova valjanost mora isteći na kraju postubka (povlačenje kartice ili vraćanje kartice u početno stanje) i/ili nakon 240 upotreba (jedna upotreba ključa = jedna naredba koja koristi sigurne poruke upućene kartici i odgovarajući odgovor).

**3.2.   Ključevi**

CSM\_014  
Ključevi RSA moraju imati (bez obzira na razinu) sljedeće dužine: modul n 1024 bitova, javni eksponent e najviše 64 bitova, privatni eksponent d 1024 bitova.

CSM\_015  
Trojni ključevi DES moraju imati oblik (Ka, Kb, Ka), pri čemu su Ka i Kb nezavisni ključevi dužine 64 bita. Ne smiju biti namješteni bitovi koji ustanovljuju paritetnu grešku.

**3.3.   Certifikati**

CSM\_016  
Certifikati javnih ključeva moraju biti ‚nesamoopisni’‚karticom provjerljivi’ certifikati (izvor: ISO/IEC 7816-8)

**3.3.1.    Sadržaj certifikata**

CSM\_017  
Certifikati javnih ključeva RSA su ugrađeni u sljedeće podatke sljedećim redom:

|  |  |  |  |
| --- | --- | --- | --- |
| **Podaci** | **Oblik** | **Bajtova** | **Opis** |
| CPI | CIJELI BROJ | 1 | Identifikator profila certifikata (u ovoj verziji ‚01’) |
| CAR | OKTETNI NIZ | 8 | Upućivanje na certifikacijsku vlast |
| CHA | OKTETNI NIZ | 7 | Ovlaštenje nosioca certifikata |
| EOV | TimeReal | 4 | Kraj važnosti certifikata. Nije obvezno, dopunjen sa ‚FF’ ako se ne koristi |
| 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 točnu strukturu autentifikacijskog certifikata. Može se koristiti kao unutarnji identifikator opreme iz zaglavlja odgovarajućeg popisa koji opisuje ulančavanje podakovnih elemenata unutar certifikata.  Zaglavlje popisa pridružen sadržaju ovog certifikata je sljedeći:  Image |

|  |  |
| --- | --- |
| 2. | ‚Upućivanje na certifikacijsko tijelo’ (CAR) ima za svrhu identifikujenje CA koji izdaje certifikat tako da se podakovni element može istovremeno koristiti kao identifikator ključa vlasti za upućivanje na javni ključ certikacijske vlasti (za šifriranje, vidjeti identifikator ključa u nastavu). |

|  |  |
| --- | --- |
| 3. | ‚Ovlaštenje nosioca certifikata’ (CHA) se koristi za identifikaciju prava nosioca certifikata. Ono se sastoji od ID primjene tahografa i vrste opreme za koju je certifikat namijenjen (prema podakovnom elementu EquipmentType, ‚00’ za državu članicu). |

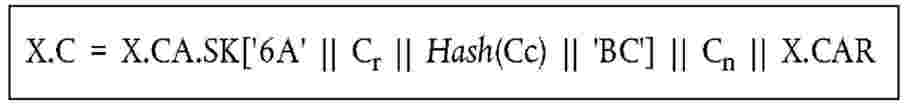
|  |  |
| --- | --- |
| 4. | ‚Upućivanje na nosioca certifikata’ (CHR) ima za cilj jedinstvenu identifikaciju nosioca certifikata tako da se podakovni element može istovremeno koristiti kao identifikator ključa predmeta za upućivanje na javni ključ nosioca certifikata. |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 5. | Identifikatori ključa na jedinstven način identifikujeju nosioca certifikata ili certifikacijske vlasti. Oni su šifrirani 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 šifriranje mm gg | Svojstveno proizvođaču | Šifra proizvođača |   Kod VU, proizvođač, prilikom traženja certifikata, može ili ne mora znati identifikaciju opreme u koju se unose ključevi.  U prvom slučaju, proizvođač će poslati na certifikaciju identifikaciju opreme s javnim ključem tijelu svoje države članice. Certifikat će potom sadržati identifikaciju opreme, a proizvođač mora osigurati da se ključevi i certifikat unesu u opremu za koju su namijenjeni. Identifikator ključa ima gore prikazan oblik.  U poslednjem slučaju, proizvođač mora na jedinstven način identifikujeti svaki zahtjev za certifikat i poslati takvu identifikaciju s javnim ključem tijelu svoje države članice na certifikaciju. Certifikat će sadržavati identifikaciju zahtjeva. Proizvođač mora povratno obavijestiti 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 | Raspon | BCD šifriranje mm gg | ‚FF’ | Šifra proizvođača | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | 5.2. | Certifikacijska vlast:   |  |  |  |  |  | | --- | --- | --- | --- | --- | | Podaci | Identifikacija vlast | Serijski broj ključa | Dodatne informacije | Identifikator | | Dužina | 4 bajta | 1 bajt | 2 bajta | 1 bajt | | Vrijednost | 1-bajtna numerička šifra države | cijeli broj | dodatno šifriranje (svojstveno CA) | ‚01’ | | 3-bajtna alfanumerička šifra države | ‚FF FF’, ako nije iskorišteno |   Serijski broj ključa se koristi 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 službe povjerljivosti (certifikat ne sadrži identifikator objekta koji bi to navodio). |

**3.3.2.    Izdani certifikati**

CSM\_018  
Izdani certifikat je digitalni potpis s djelomičnim obnavljanjem sadržaja certifikata u skladu s ISO/IEC 9796-2 osim njegovog Priloga A.4., s priloženim upućivanjem na certifikacijsku vlast.



sa sadržajem certifikata

Napomene:

|  |  |
| --- | --- |
| 1. | Dužina ovog certifikata je 194 bajta. |

|  |  |
| --- | --- |
| 2. | CAR, koji se skriven potpisom, je takođe priložen potpisu tako da može biti odabran javni ključ certifikacionog tijela za provjeru certifikata. |

|  |  |
| --- | --- |
| 3. | Osoba koja provjerava certifikat mora implicitno poznavati kod kojeg koristi certifikacijska vlast za potpisivanje certifikata. |

|  |  |
| --- | --- |
| 4. | Zaglavlje pridruženo navedenom izdanom certifikatu je sljedeće:  Image |

**3.3.3.    Provjera i otvaranje certifikata**

Provjera i otvaranje certifikata se sastoji od provjere potpisa prema ISO/IEC 9796-2, pronalaženja sadržaja certifikata i sadržanog javnog ključa: X.PK = X.CA.PK0X.C, te provjere važnosti certifikata.

CSM\_019  
Obuhvaća sljedeće korake:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | provjeriti potpis i pronaći sadržaj:   |  |  | | --- | --- | | — | u X.C pronaći Sign, Cn’ i CAR’:Image |  |  |  | | --- | --- | | — | odabrati iz CAR’ odgovarajući javni ključ certifikacijske vlasti (ako to nije učinjeno ranije drugim putem) |  |  |  | | --- | --- | | — | otvoriti Sign s javnim ključem CA: Sr’ = X.CA.PK [Znak], |  |  |  | | --- | --- | | — | provjeriti da Sr’ započinje sa ‚6A’ i završava s ‚BC’ |  |  |  | | --- | --- | | — | proračunati Cr’ i H’ iz:Image |  |  |  | | --- | --- | | — | ponovno učitati sadržaj certifikata C’ = Cr’ || Cn’, |  |  |  | | --- | --- | | — | provjeriti kompresiju poruke (C’) = H’ | |

|  |  |
| --- | --- |
|  | Ako su provjere u redu, certifikat je autentičan, njegov sadržaj je C’. |

|  |  |  |  |
| --- | --- | --- | --- |
|  | Provjeriti valjanost. Iz C’:   |  |  | | --- | --- | | — | prema potrebi, provjeriti datum isteka važnosti, | |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Pronaći i sačuvati javni ključ, identifikator ključa, aotvorizaciju 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**

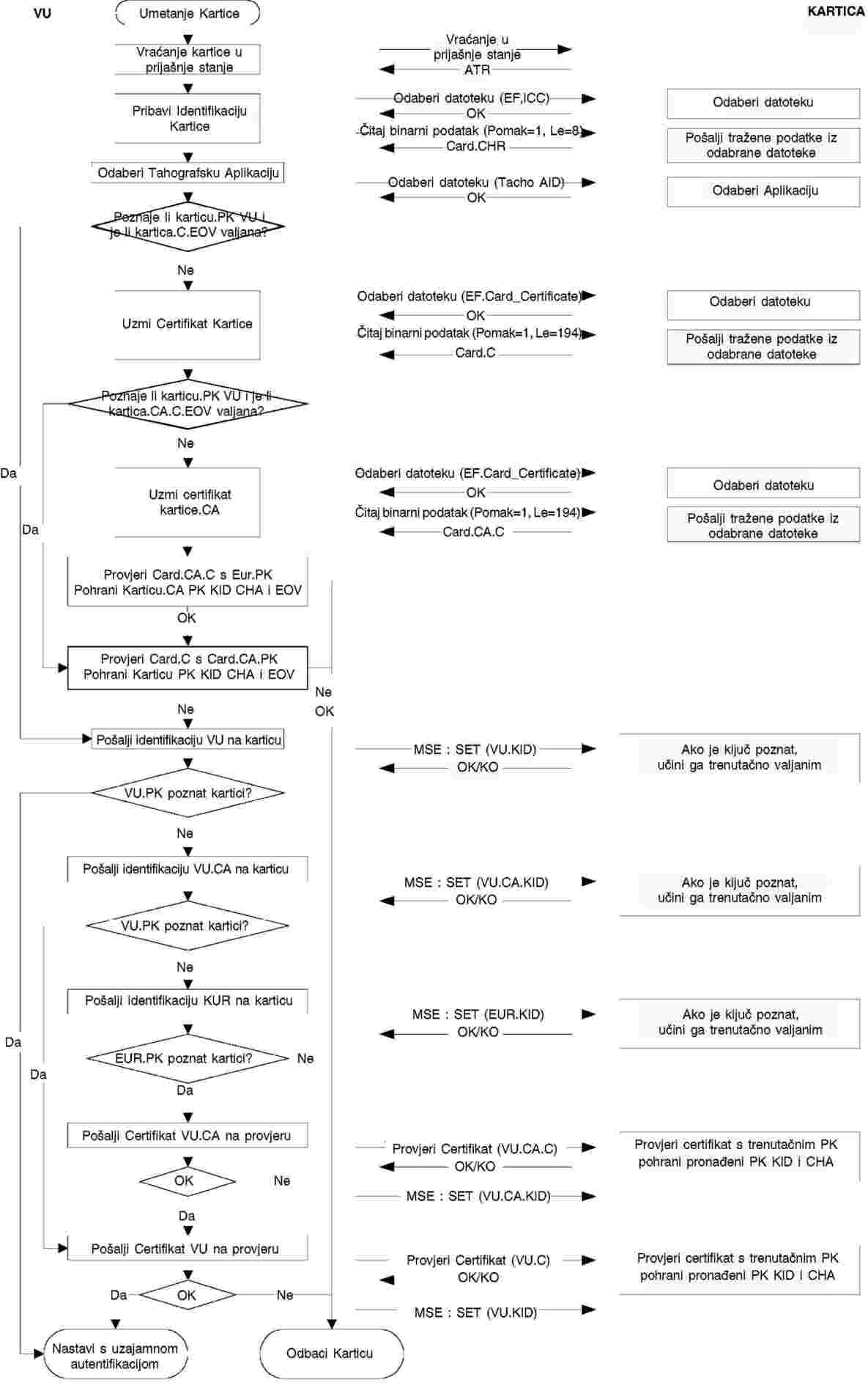
Uzajamna autentifikacija među karticama i VU se temelji na sljedećim načelu:

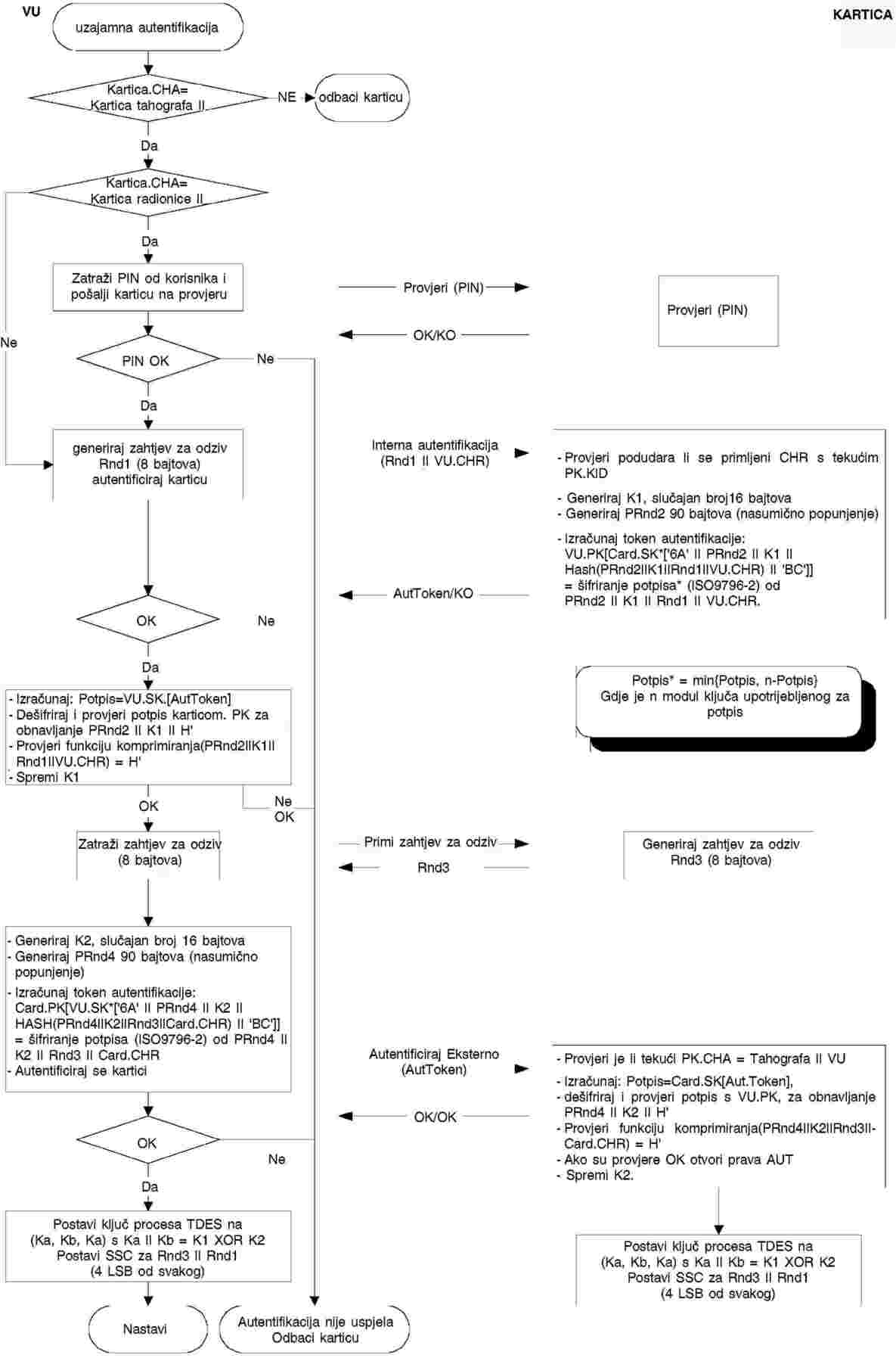
Svaka strana mora dokazati drugoj da posjeduje valjan par ključeva, javni ključ kojih je certificiran od strane certifikacijske vlasti države članice koja je i sama certificirana od strane Evropskog certifikacionog tijela.

Dokazivanje se obavlja potpisivanjem privatnim ključem slučajnog broja kojega je poslala druga strana koja mora obnoviti slučajan broj upućen prilikom provjere potpisa.

Mehanizam aktivira jedinica u vozilu prilikom ubacivanja kartice. On započinje razmjenom certifikata i razvijanjem javnih ključeva, te završava postavljanjem ključa razmjene podataka.

CSM\_020  
Mora se koristiti sljedeći protokol (strelice prikazuju naredbe i razmijenjene podatke (vidjeti Dodatak 2.))





**5. MEHANIZAM POVJERLJIVOSTI PRENOSA, POTPUNOSTI I AUTENTIFIKACIJE PRENOSA PODATAKA IZMEĐU KARTICA I JEDINICE U VOZILU**

**5.1.   Sigurne poruke**

CSM\_021  
Potpunost prenosa podataka između jedinice u vozilu i kartice se mora zaštititi putem sigurnih poruka shodno izvorima (ISO/IEC 7816-4) i (ISO/IEC 7816-8).

CSM\_022  
Kada podaci moraju biti zaštićeni tokom prenosa, podakovni objekt kriptografskog kontrolnog zbira se pridodaje podakovnim objektima koji se šalju u okviru naredbe ili odgovora. Kriptografski kontrolni zbir mora provjeriti primatelj.

CSM\_023  
Kriptografski kontrolni zbir podataka koji se šalju naredbom moraju objediniti zaglavljem naredbe, a svi poslani podakovni objekti (= > CLA = ‚0C’, i svi podakovni objekti moraju biti sažeti s oznakama u kojima je b1 = 1).

CSM\_024  
Status odziva-bajti informacije moraju biti zaštićeni kriptografskim ispitnim zbirem kada odgovor ne sadrži podakovno polje.

CSM\_025  
Kriptografski kontrolni zbir mora imati dužinu od četiri bajta.

Struktura naredbi i odgovora prilikom korištenja sigurnih poruka je stoga sljedeća:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Korišteni DO su parcijalni skup DO za sigurne poruke opisan u ISO/IEC 7816-4:   |  |  |  | | --- | --- | --- | | **Oznaka** | **Mnemonik** | **Značenje** | | ‚81’ | Tpv | Obična vrijednost ne BER-TLV šifrirani podaci (koju mora štititi CC) | | ‚97’ | TLE | Vrijednost Le u nezaštićenoj naredbi (koju mora štititi CC) | | ‚99’ | Tsw | Statusne informacije (koje mora štititi CC) | | ‚8E’ | Tcc | Kriptografski kontrolni zbir | | ‚87’ | TPI CG | Bajt koji označava popunjenje || kriptogram (obična vrijednost koja nije šifrirana u BER-TLV) | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Pod pretpostavkom nezaštićenog para odziva naredbe:   |  |  | | --- | --- | | **Zaglavlje naredbe** | **Sadržaj naredbe** | | CLA INS P1 P2 | (Lc-field) (Data field) (Le-field) | | 4 bajta | Bajtovi L, označeni kao B1 do BL |  |  |  |  | | --- | --- | --- | | **Sadržaj odziva** | **Nastavak odgovora** | | | (Podakovno polje) | SW1 | SW2 | | Lr podakovnih bajtova | dva bajta | | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Odgovarajući par zaštićenog odziva naredbe je:   |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | |  | Zaštićena naredba:   |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | **Zaglavlje naredbe (CH)** | **Sadržaj naredbe** | | | | | | | | | | | | CLA INS P1 P2 | (Novo polje Lc) | (Novo podakovno polje) | | | | | | | | | (Novo polje Le) | | ‚OC’ | Dužina novog podakovnog polja | TPV | Lpv | PV | Tle | Lle | Le | Tcc | Lcc | CC | ‚00’ | | ‚81’ | Lc | Podakovno polje | ‚97’ | ‚01’ | Le | ‚8E’ | ‚04’ | CC |   Podaci koje treba integrirati u kontrolni zbir = CH || PB || TPV || LPV || PV || TLE || LLE || Le || PB  PB = bajti za popunjenje (80..00) u skladu s ISO-IEC 7816-4 i metodom 2 po ISO 9797.  DO PV i LE su prisutni samo kada postoje neki odgovarajući podaci u nezaštićenoj naredbi. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | |  | Zaštićeni odgovor:   |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | 1. | Slučaj kada podakovno polje odziva nije prazno i ne treba ga zaštititi u pogledu povjerljivosti:   |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | **Sadržaj odgovora** | | | | | | **Nastavak odgovora** | | **(Novo podakovno polje)** | | | | | | **novi SW1 SW2** | | TPV | LPV | PV | TCC | Lcc | CC |  | | ‚81’ | Lr | Podakovno polje | ‚8E’ | ‚04’ | CC |  |   Podaci koje treba objediniti u kontrolni zbir = TPV || LPV || PV || PB |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | 2. | Slučaj kada podakovno polje odziva nije prazno i treba ga zaštititi u smislu povjerljivosti:   |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | **Sadržaj odgovora** | | | | | | **Nastavak odgovora** | | **(Novo podakovno polje)** | | | | | | **nova SW1 SW2** | | Tpi cg | Lpi cg | PI CG | TCC | Lcc | CC |  | | ‚87’ |  | PI || CG | ‚8E’ | ‚04’ | CC |  |   Podaci koje prenosi CG: podaci koji nisu šifrirani prema BER-TLV i bajtovi popunjenja.  Podaci koje treba objediniti u kontrolni zbir = TPI CG || LPI CG || PI CG || PB |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | 3. | Slučaj kada je podakovno polje odziva prazno:   |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | **Sadržaj odgovora** | | | | | | **Nastavak odgovora** | | **(Novo podakovno polje)** | | | | | | **nova SW1 SW2** | | Tsw | Lsw | SW | TCC | Lcc | CC |  | | ‚99’ | ‚02’ | Nova SW1-SW2 | ‚8E’ | ‚04’ | CC |  |   Podaci koje treba objediniti u kontrolni zbir = Tsw || Lsw || SW || PB | | |

**5.2.   Postepene s greškama kod sigurnog upućivanja poruka**

CSM\_026  
Kada kartica tahografa prepozna grešku SM prilikom tumačenja naredbe, tada se statusni bajtovi moraju vratiti bez SM. U skladu s ISO/IEC 7816-4, definirani su sljedeći statusni bajtovi za označivanje grešaka SM:

|  |  |
| --- | --- |
| ‚66 88’ | neuspješna provjera kriptografskog kontrolnog zbira, |
| ‚69 87’ | nedostaju očekivani podakovni objekti SM, |
| ‚69 88’ | neispravni podakovni objekti SM. |

CSM\_027  
Kada kartica tahografa vrati statusne bajte bez SM DO ili s pogrešnim SM DO, jedinica vozila mora prekinuti proces.

**5.3.   Algoritmi proračuna kriptografskih kontrolnih zbireva**

CSM\_028  
Kriptografski kontrolni zbirevi su sačinjeni korištenjem detaljnih MAC prema ANSI X9.19 s DES:

—početni faza: početni ispitni blok y0 je E(Ka, SSC).

—naredni faza: ispitni blokovi y1, …, yn se računaju pomoću Ka.

—konačni faza: kriptografski kontrolni zbir se računa od posljednjeg ispitnog bloka yn kako slijedi: E(Ka, D(Kb, yn)).

pri čemu E() označava šifriranje pomoću DES, a D() označava dešifriranje pomoću DES.

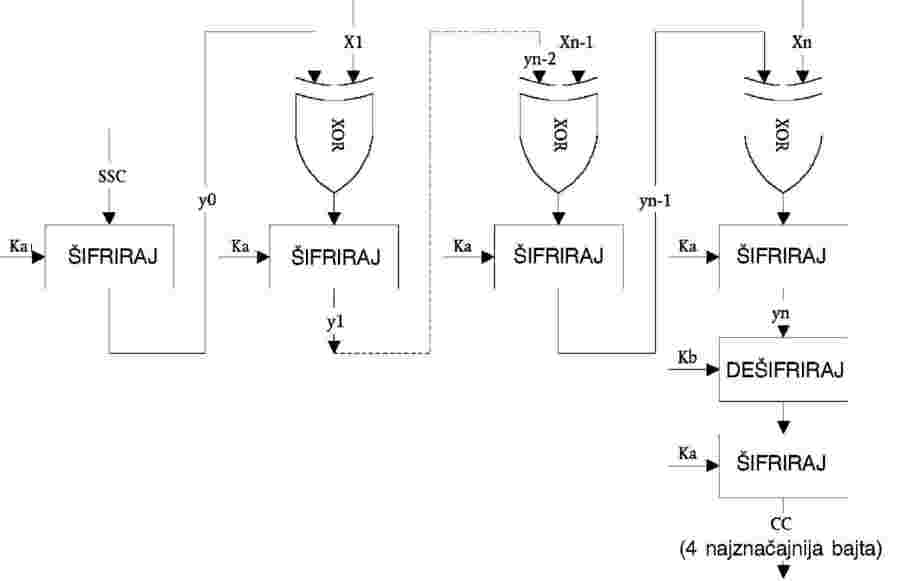
Četiri najznačajnija bajta kriptografskog kontrolnog zbira se prenose.

CSM\_029  
Brojač toka slanja (SSC) se aktivira u postubku dogovaranja ključa na:

Početni SCC: Rnd3 (4 najmanje značajna bajta) || Rnd1 (4 najmanje značajna bajta).

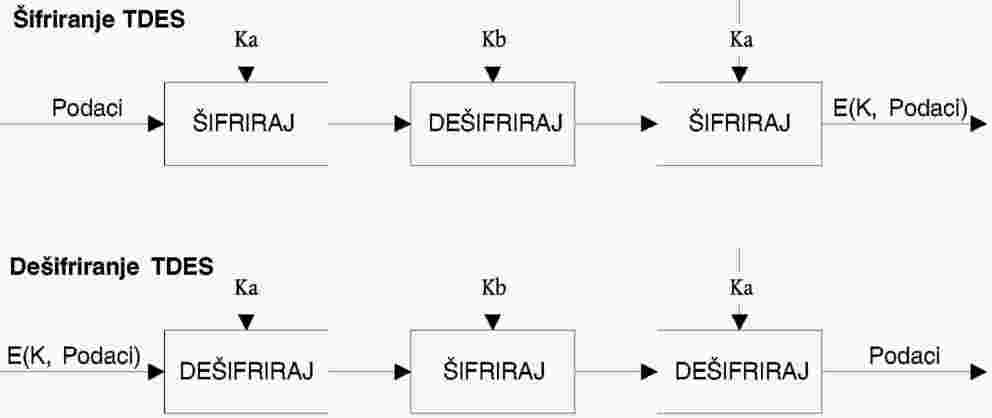
CSM\_030  
Brojač toka slanja se povećava za 1 svaki put prije proračuna MAC (tj. SSC za prvu naredbu je početni SCC + 1, SCC za prvi odgovor je početni SCC + 2).

Sljedeća slika prikazuje proračun podrobnog MAC:



**5.4.   Algoritam proračuna kriptograma za pouzdanost DO**

CSM\_031  
Kriptogrami se proračunavaju korištenjem TDEA u načinu rada TCBC u skladu s izvorima (TDES) i (TDES-OP) i s nultim vektorom kao blokom početne vrijednosti.

Sljedeća slika prikazuje korištenje ključeva u TDES:

**6.   MEHANIZMI DIGITALNOG POTPISA KOD PREUZIMANJA PODATAKA**

CSM\_032  
Inteligentna namjenska oprema (IDE) arhivira podatke primljene s opreme (VU ili kartica) tokom jednog procesa preuzimanja unutar jedne fizičke podakovne datoteke. Ova datoteka mora sadržavati certifikate MSi.C i EQT.C. Datoteka sadrži digitalne potpise podakovnih blokova opisanih u Dodatku 7. ‚Protokoli preuzimanja podataka’.

CSM\_033  
Digitalni potpisi preuzetih podataka moraju koristiti shemu digitalnog potpisa s takvim dodakom da se preuzeti podaci mogu čitati bez dešifriranja, ako se to želi.

**6.1.   Generisanje potpisa**

CSM\_034  
Generisanje podakovnog potpisa od strane opreme mora slijediti shemu potpisa s prilogom koji je definiran u izvoru (PKCS1) s funkcijom komprimiranja SHA-1.

|  |  |
| --- | --- |
|  | Potpis = EQT.SK[‚00’ || ‚01’ || PS || ‚00’ || DER(SHA-l(Podaci))] |

PS Niz okteta za popunjenje s takvom vrijednosti ‚FF’ da dužina bude 128.

DER(SHA-1(M)) je šifriranje algoritma ID za funkciju komprimiranja i vrijednost komprimiranja u vrijednosti ASN.1 tipa Digestinfo (poznata pravila šifriranja).

|  |  |
| --- | --- |
|  | ‚30’||’21’||’30’||’09’||’06’||’05’||’2B’||’0E’||03’||’02’||’lA’||’05’||’00’||’04’||’14’||vrijednost komprimiranja. |

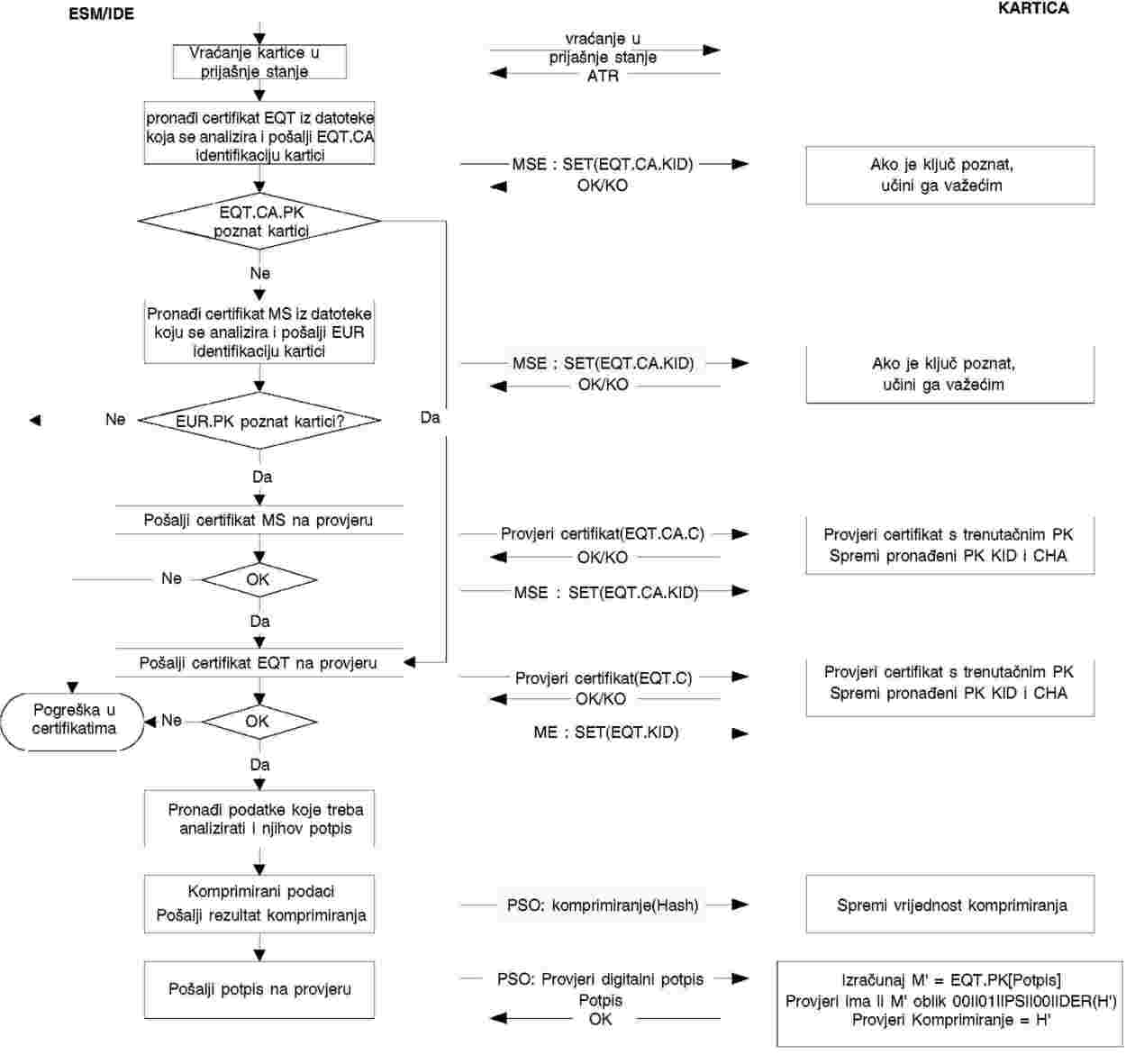
**6.2.   Provjera potpisa**

CSM\_035  
Provjera potpisa na preuzetim podacima mora slijediti shemu potpisa s dodakom koji je opisan u izvoru (PKCS1) s funkcijom komprimiranja SHA-1.

Verifikator mora nezavisno poznavati evropski javni ključ EUR.PK (i u njega imati povjerenja).

Sljedeća tabela prikazuje protokol kojega IDE koji nosi nadzornu karticu može slijediti za provjeru potpunosti podataka preuzetih i arhiviranih na ESM (spoljni medij za čuvanje). Kontrolna kartica se koristi za dešifriranje digitalnih potpisa. U ovom slučaju takva funkcija može bitno nije ugrađena u IDE.

Oprema koja je preuzela i potpisala podatke koji se analiziraju je označena s EQT.



**Dodatak 12.**

**ADAPTER ZA VOZILA KATEGORIJE M1 I N1**

**SADRŽAJ**

1. Kratice i referentni dokumenti

1.1. Kratice

1.2. Referentni standardi

2. Opšti karakteristike i funkcije adaptera

2.1. Opšti opis adaptera

2.2. Funkcije

2.3. Sigurnost

3. Zahtjevi za tahograf u slučaju ugrađenog adaptera

4. Zahtjevi za izradu i funkcionalnost adaptera

4.1. Povezivanje i prilagođavanje ulaznih impulsa brzine

4.2. Orientarea impulsurilor de intrare către senzorul de mișcare integrat

4.3. Ugrađeni senzor kretanja

4.4. Sigurnosni zahtjevi

4.5. Karakteristike izvedbe

4.6. Materijali

4.7. Oznake

5. Ugradnja tahografa u slučaju upotrebe adaptera

5.1. Ugradnja

5.2. Plombiranje

6. Provjere, inspekcijski pregledi i popravke

6.1. Periodični pregledi

7. Tipsko odobrenje tahografa kad je adapter u upotrebi

7.1. Opšte tačke

7.2. Certifikat o funkcionalnosti

**1.   KRATICE I REFERENTNI DOKUMENTI**

**1.1.   Kratice**

|  |  |
| --- | --- |
| TD | treba definirati |
| JV | jedinica u vozilu |

**1.2.   Referentni standardi**

ISO 16844-3 Drumska vozila - Sistemi tahografa - Dio 3.: Sučelje senzora kretanja

**2.   OPŠTI KARAKTERISTIKE I FUNKCIJE ADAPTERA**

**2.1.   Opšti opis adaptera**

|  |  |
| --- | --- |
| ADA\_001 | Adapter osigurava priključenoj JV sigurne podatke o kretanju vozila koji stalno prikazuju brzinu vozila i pređenu udaljenost.  Adapter je namijenjen samo onim vozilima za koja se zahtijeva da su opremljena tahografom u skladu s ovim Pravilnikom.  Ugrađuje se i upotrebljava samo u tipovima vozila utvrđenima u tački (rr), kada nije mehanički moguće ugraditi bilo koji drugi tip postojećih senzora kretanja koji su inače u skladu s odredbama ovog Priloga i njegovih dodataka 1. do 11.  Adapter nije mehanički povezan s pomičnim dijelom vozila, kako zahtijeva Dodatak 10. ovom Prilogu (odjeljak 3.1.), već je povezan s impulsima brzine/udaljenosti koje proizvode integirsani senzori ili alternativna sučelja. |
| ADA\_002 | Tipski odobren senzor kretanja (u skladu s odredbama ovog Priloga, odjeljka VIII. - Odobrenje tipa tahografa i tahografskih kartica) ugrađuje se u kućište adaptera. U kućište adaptera ugrađen je uređaj za pretvaranje ulaznih impulsa u ugrađeni senzor kretanja. Ugrađeni senzor kretanja povezan je s JV-om, tako da je sučelje između JV-a i adaptera u skladu sa zahtjevima standarda ISO 16844-3. |

**2.2.   Funkcije**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ADA\_003 | Adapter uključuje sljedeće funkcije:   |  |  | | --- | --- | | — | povezivanje i prilagođavanje ulaznih impulsa brzine, |  |  |  | | --- | --- | | — | induciranje ulaznih impulsa u ugrađeni senzor kretanja, |  |  |  | | --- | --- | | — | sve funkcije ugrađenog senzora kretanja, koje JV-u osiguravaju sigurne podatke o kretanju. | |

**2.3.   Sigurnost**

|  |  |
| --- | --- |
| ADA\_004 | Adapter nije sigurnosno certificiran u skladu s generičkim ciljem sigurnosti senzora kretanja utvrđenom u Dodatku 10. ovom Prilogu. Umjesto toga primjenjuju se sigurnosni zahtjevi utvrđeni u odjeljku 4.4. ovog Dodatka. |

**3.   ZAHTJEVI ZA TAHOGRAF U SLUČAJU UGRAĐENOG ADAPTERA**

Zahtjevi u ovom i sljedećim poglavljima navode kako se tumače zahtjevi ovog Priloga u slučaju upotrebe adaptera. Odgovarajući brojevi zahtjeva navedeni su u zagradama.

|  |  |
| --- | --- |
| ADA\_005 | Tahograf mora u svakom vozilu koje je opremljeno adapterom ispunjavati sve odredbe ovog Priloga, osim ako nije drukčije navedeno u ovom Dodatku. |
| ADA\_006 | Pri ugradnji adaptera, tahograf je sastavljen od kabla, adaptera (umjesto senzora kretanja) i JV-a (001.). |
| ADA\_007 | Otkrivanje događaja i/ili kvarova funkcije tahografa mijenja se kako slijedi:   |  |  | | --- | --- | | — | događaj „prekid napajanja” pokreće JV, kad nije u režimu kalibrisanja, u slučaju svakog prekida napajanja ugrađenog senzora kretanja dužeg od 200 milisekundi (066.), |  |  |  | | --- | --- | | — | svaki prekid napajanja adaptera duži od 200 ms (milisekundi) izaziva prekid napajanja ugrađenog senzora kretanja jednake dužine. Proizvođač adaptera utvrđuje granicu prekida adaptera, |  |  |  | | --- | --- | | — | događaj „pogreška podataka o kretanju” pokreće JV u slučaju prekida uobičajenog toka podataka između ugrađenog senzora kretanja i JV-a i/ili u slučaju pogreške vezane uz cjelovitost podataka ili pri provjeri autentičnosti tokom razmjene podataka između ugrađenog senzora kretanja i JV-a (067.), |  |  |  | | --- | --- | | — | događaj „pokušaj ugrožavanja sigurnosti” pokreće JV za bilo koji događaj koji utiče na sigurnost ugrađenog senzora kretanja, kad nije u režimu kalibrisanja (068.), |  |  |  | | --- | --- | | — | greška „tahograf” pokreće JV za svaki kvar ugrađenog senzora kretanja, kad nije u režimu kalibrisanja (070.). | |
| ADA\_008 | Kvarovi adaptera koje otkrivaju tahografi povezani su s ugrađenim senzorom kretanja (071.). |
| ADA\_009 | Kalibracijska funkcija JV dopušta automatsko sparivanje ugrađenog senzora kretanja s JV-om (154., 155.). |
| ADA\_010 | Izrazi „senzor kretanja” ili „senzor” s ciljem sigurnosti JV-a u Dodatku 10. ovom Prilogu odnose se na ugrađeni senzor kretanja. |

**4.   ZAHTJEVI ZA IZRADU I FUNKCIONALNOST ADAPTERA**

**4.1.   Povezivanje i prilagođavanje ulaznih impulsa brzine**

|  |  |
| --- | --- |
| ADA\_011 | Ulazno sučelje adaptera prihvaća impulse frekvencije koji iskazuju brzinu i pređenu udaljenost vozila. Električne karakteristike ulaznih impulsa su: TD proizvođač. Dostubnost prilagođavanja poznata je samo proizvođaču adaptera i ovlaštenoj radionici koja obavlja ugradnju i ispravno povezivanje ulaza adaptera na vozilo. |
| ADA\_012 | Ulazno sučelje adaptera može, prema potrebi, pomnožiti ili podijeliti impulse frekvencije ulaznih impulsa brzine fiksnim faktorom, kako bi se signal prilagodio vrijednosti faktora u rasponu k, utvrđenim ovim Prilogom (4 000 do 25 000 impulsa/km). Ovaj fiksni faktor može programirati samo proizvođač adaptera i ovlaštena radionica koja obavlja ugradnju adaptera. |

**4.2.   Induciranje ulaznih impulsa u ugrađeni senzor kretanja**

|  |  |
| --- | --- |
| ADA\_013 | Ulazni impulsi, koji mogu biti prilagođeni kako je gore navedeno, induciraju se u ugrađeni senzor kretanja, tako da senzor kretanja detektira svaki ulazni impuls. |

**4.3.   Ugrađeni senzor kretanja**

|  |  |
| --- | --- |
| ADA\_014 | Ugrađeni senzor kretanja stimuliraju inducirani impulsi, čime se omogućava dobivanje podataka o točnom kretanju vozila, kao da je mehanički povezano s pomičnim dijelom vozila. |
| ADA\_015 | JV koristi identifikacijske podatke ugrađenog senzora kretanja kako bi identifikujela adapter (077.). |
| ADA\_016 | Podaci o ugradnji koji su arhivirani u ugrađenom senzoru kretanja, smatraju se podacima o ugradnji adaptera (099.). |

**4.4.   Sigurnosni zahtjevi**

|  |  |
| --- | --- |
| ADA\_017 | Kućište adaptera oblikovano je tako da ga nije moguće otvoriti. Plombirano je, tako da se pokušaji fizičke manipulacije mogu jednostavno otkriti (npr. putem vizualnog pregleda, vidjeti ADA\_035). |
| ADA\_018 | Nije moguće ukloniti ugrađeni senzor kretanja iz adaptera bez lomljenja plombe (plombi) kućišta adaptera ili lomljenja plombe između senzora i kućišta adaptera (vidjeti ADA\_035). |
| ADA\_019 | Adapter osigurava da se podaci o kretanju mogu obraditi i dobiti samo preko ulaza adaptera. |

**4.5.   Karakteristike izvedbe**

|  |  |
| --- | --- |
| ADA\_020 | Adapter u potpunosti radi u rasponu temperature (TD proizvođač, ovisno o položaju ugradnje) (159.). |
| ADA\_021 | Adapter u potpunosti radi u rasponu vlažnosti od 10 % do 90 % (160.). |
| ADA\_022 | Adapter je zaštićen od previsokog napona, zamjene polariteta napajanja i kratkih spojeva (161.). |
| ADA\_023 | Elektromagnetska kompatibilnost adaptera mora biti u skladu s Direktivom Komisije 2006/28/EZ[(1)](https://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=CELEX:32009R0068&from=HR#ntr1-L_2009021HR.01000502-E0001) o prilagodbi tehničkom napretku Direktive Vijeća 72/245/EEZ te je zaštićena od elektrostatičkih pražnjenja i prelaznih pojava (162.). |

**4.6.   Materijali**

|  |  |
| --- | --- |
| ADA\_024 | Adapter mora imati stepen zaštite (TD proizvođač, ovisno o položaju ugradnje) (164.,165.). |
| ADA\_025 | Kućište adaptera je žute boje. |

**4.7.   Oznake**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ADA\_026 | Na adapter mora biti pričvršćena opisna pločica na kojoj se nalaze sljedeći podaci (169.):   |  |  | | --- | --- | | — | ime i adresa proizvođača adaptera, |  |  |  | | --- | --- | | — | kataloški broj proizvođača i godina proizvodnje adaptera, |  |  |  | | --- | --- | | — | oznaka tipskog odobrenja adaptera ili tahografa uključujući adapter, |  |  |  | | --- | --- | | — | datum ugradnje adaptera, |  |  |  | | --- | --- | | — | VIN oznaka vozila u koji je ugrađen adapter. | |
| ADA\_027 | Na opisnoj pločici navode se i sljedeći podaci (ako nije izravno čitljivo izvana na ugrađenom senzoru kretanja):   |  |  | | --- | --- | | — | ime proizvođača ugrađenog senzora kretanja, |  |  |  | | --- | --- | | — | kataloški broj proizvođača i godina proizvodnje ugrađenog senzora kretanja, |  |  |  | | --- | --- | | — | oznaka tipskog odobrenja ugrađenog senzora kretanja. | |

**5.   UGRADNJA TAHOGRAFA U SLUČAJU UPOTREBE ADAPTERA**

**5.1.   Ugradnja**

|  |  |
| --- | --- |
| ADA\_028 | Adapteri koji se trebaju ugraditi u vozila dostavljaju se samo proizvođačima vozila ili radionicama koje su odobrile nadležne vlasti država članica i koje su ovlaštene za ugradnju, aktivaciju i kalibraciju digitalnih tahografa. |
| ADA\_029 | Ovlaštena radionica koja ugrađuje adapter prilagođava ulazno sučelje i odabire omjer za izračun ulaznog signala (prema potrebi). |
| ADA\_030 | Ovlaštena radionica koja ugrađuje adapter plombira kućište adaptera. |
| ADA\_031 | Adapter se pričvrišćuje što je bliže moguće onom dijelu vozila koje daje ulazne impulse. |
| ADA\_032 | Kablovi, preko kojih se napaja adapter, crvene su boje (pozitivno napajanje) i crne (uzemljenje). |

**5.2.   Plombiranje**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ADA\_033 | Primjenjuju se sljedeći zahtjevi za plombiranje:   |  |  | | --- | --- | | — | plombira se kućište adaptera (vidjeti ADA\_017), |  |  |  | | --- | --- | | — | kućište ugrađenog senzora kretanja plombirano je za kućište adaptera, osim ako ugrađeni senzor kretanja nije moguće ukloniti bez lomljenja plombe (plombi) kućišta adaptera (vidjeti ADA\_018), |  |  |  | | --- | --- | | — | kućište adaptera plombira se za vozilo, |  |  |  | | --- | --- | | — | veza između adaptera i opreme koja osigurava ulazne impulse plombira se na oba kraja (koliko je moguće). | |

**6.   PROVJERE, INSPEKCIJSKI PREGLEDI I POPRAVKE**

**6.1.   Periodični pregledi**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ADA\_034 | Pri upotrebi adaptera, svaki periodički pregled (periodički pregled u skladu sa zahtjevima 256. do 258. poglavlja VI. Priloga 1.B) tahografa uključuje sljedeće provjere (257.):   |  |  | | --- | --- | | — | ima li adapter odgovarajuće oznake o tipskom odobrenju, |  |  |  | | --- | --- | | — | jesu li plombe na adapteru i njegovim spojevima netaknute, |  |  |  | | --- | --- | | — | je li adapter ugrađen kako je navedeno na ugrađenoj pločici, |  |  |  | | --- | --- | | — | je li adapter ugrađen kako je naveo proizvođač adaptera i/ili vozila, |  |  |  | | --- | --- | | — | je li postavljanje adaptera dopušteno za pregledavano vozilo. | |

**7.   TIPSKO ODOBRENJE TAHOGRAFA KAD JE ADAPTER U UPOTREBI**

**7.1.   Opšti tačke**

|  |  |
| --- | --- |
| ADA\_035 | Za tipsko odobrenje tahograf treba predati zajedno s adapterom (269.). |
| ADA\_036 | Svaki adapter može se predati za tipsko odobrenje kao samostalni uređaj ili kao sastavni dio tahografa. |
| ADA\_037 | Svako tipsko odobrenje uključuje funkcionalna ispitivanja adaptera. Pozitivni rezultati svakog od tih ispitivanja iskazani su odgovarajućim certifikatom (270.). |

**7.2.   Certifikat o funkcionalnosti**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ADA\_038 | Certifikat o funkcionalnosti adaptera ili tahografa koji uključuje adapter dostavlja se proizvođaču adaptera nakon što su uspješno obavljena sva sljedeća minimalna funkcionalna ispitivanja.   |  |  |  |  | | --- | --- | --- | --- | | **Br.** | **Ispitivanje** | **Opis** | **Povezani zahtjevi** | | 1. | **Upravni pregled** | | | | 1.1. | Dokumentacija | Ispravnost dokumentacije o adapteru |  | | 2. | **Vizualni pregled** | | | | 2.1. | Usklađenost adaptera s dokumentacijom | |  | | 2.2. | Identifikacija/oznake adaptera | | ADA\_026, ADA\_027 | | 2.3. | Materijali adaptera | | 163. do 167.  ADA\_025 | | 2.4. | Plombiranje | | ADA\_017, ADA\_018, ADA\_035 | | 3. | **Funkcionalna ispitivanja** | | | | 3.1. | Induciranje impulsa brzine u ugrađeni senzor kretanja | | ADA\_013 | | 3.2. | Povezivanje i prilagođavanje ulaznih impulsa brzine | | ADA\_011, ADA\_012 | | 3.3. | Provjeriti da je adapter neosjetljiv na magnetska polja. Alternativno, provjeriti da adapter reagira na magnetska polja koja ometaju detekciju kretanja vozila tako da povezana JV može detektirati, zabilježiti i pohraniti pogreške senzora | | 161a. | | 4. | **Ekološka ispitivanja** | | | | 4.1. | Rezultati ispitivanja proizvođača | Rezultati ekoloških ispitivanja proizvođača | ADA\_020, ADA\_021, ADA\_022, ADA\_023, ADA\_024 | | 5. | **Elektromagnetska kompatibilnost** | | | | 5.1. | Emisije zračenja i osjetljivosti | Provjeriti usklađenost s Direktivom 2006/28/EZ | ADA\_023 | | 5.2. | Rezultati ispitivanja proizvođača | Rezultati ekoloških ispitivanja proizvođača | ADA\_023 | |