Crne Gore

Ministarstvo unutrašnjih poslova

Na osnovu člana 2 stav 2 Pravilnika o bližim uslovima koje mora da ispunjava kvalifikovani davalac usluga certifikovanja (“Službeni list CG”, broj 53/18) Ministarstvo unutrašnjih poslova donosi

POLITIKA CERTIFIKACIJE

DAVAOCA USLUGA POVJERENJA TrustME

(TrustME CP– Politika certifikacije)

Verzija. 1.0

Podgorica, mart 2020. godine.

Sadržaj

1 Uvod i pregled osnovnih pretpostavki

Na osnovu Zakona o ličnoj karti i Zakona o elektronskoj identifikaciji i elektronskom potpisu Centar za informacione komunikacione tehnologije, informacionu bezbjednost i sisteme tehničkog nadzora, Ministarstva unutrašnjih poslova (u daljem tekstu MUP) kao kvalifikovani davalac usluga povjerenja organizuje kvalifikovano certifikaciono tijelo radi pružanja elektronskih kvalifikovanih usluga povjerenja (u daljem tekstu usluge povjerenja ili kraće TrustME).

TrustME pruža usluge izdavanja digitalnih certifikata za kvalifikovani elektronski potpis i digitalnih certifikata kao sredstva za elektronsku identifikaciju, shodno Zakonu o elektronskoj identifikaciji i elektronskom potpisu.

U skladu sa Zakonom o ličnoj karti TrustME izdaje navedene certifikate fizičkim licima – građanima (u daljem tekstu građani) Crne Gore na elektronskoj javnoj ispravi – ličnoj karti.

TrustME izdaje certifikate za građane tako što elektronski potpiše podatke koji se smještaju u certifikate na osnovu svog privatnog ključa i asimetričnog kriptografskog algoritma.

U tako formiranim certifikatima, certifikaciono tijelo se identifikuje kao kvalifikovani davalac usluga povjerenja za kvalifikovani elektronski potpis i certifikata za elektronsku identifikaciju u skladu sa Zakonom o elektronskoj identifikaciji i elektronskom potpisu i pratećim podzakonskim aktima.

MUP je izgradio infrastrukturu javnih kriptografskih ključeva (Public Key Infrastructure - PKI) i prisutan je kao davalac usluga povjerenja koji pruža usluge izdavanja elektronskih certifikata za fizička lica - građane, pod imenom TrustME. MUP Crne Gore kao kvalifikovani davalac usluga povjerenja omogućava stvaranje odnosa povjerenja potrebnog za stvaranje osnova za razvijanje elektronskog poslovanja, elektronske javne uprave odnosno elektronskog društva.

MUP ima nacionalnu pokrivenost područnim jedinicama i filijalama za građanska stanja i lične isprave (u daljem tekstu poslovnice MUP-a), a njihova informatička povezanost garantuje brzinu i pouzdatost izvršenja zahtjeva koju koristi i registraciono tijelo certifikacionog tijela MUP-a.

Usluge povjerenja koje pruža MUP usklađene su sa zakonskom regulativom [1] – [3], i mjerodavnim međunarodnim normama iz djelokruga pružanja usluga povjerenja. MUP neprekidno prati potrebe korisnika, razvoj tehnologije i promjene u normama iz područja pružanja usluga povjerenja te u skladu s tim unapređuje i usklađuje svoj rad.

1.1 Pregled osnovnih pretpostavki

MUP je uspostavio PKI infrastrukturu kojom pruža usluge povjerenja, a koje se odnose na izdavanje i upravljanje certifikatima.

Hijerarhijska struktura certifikacionog tijela zasnovana je na MNE eID Root CA kao korijenskog certifikacionog tijela, a na osnovu dvoslojne arhitekture certifikacionih tijela (engl.: Certification Authorities, u daljem tekstu: CA tijela).

Dvoslojnu arhitekturu certifikacionih tijela TrustME čine:

- Korijensko certifikaciono tijelo (root CA): MNE eID Root CA
- Podređeno certifikaciono tijelo (subordinate CA): MNE eID CA1

MUP Crne Gore ostavlja mogućnost uspostave drugih podređenih certifikacionih tijela u hijerarhijskoj strukturi za potrebe izdavanja drugih tipova elektronskih certifikata.

MNE eID Root CA je izdao samopotpisani MNE eID Root CA certifikat. Svojim samopotpisanim certifikatom MNE eID Root CA izdao je certifikate njemu podređenim certifikacionim tijelima i OCSP servisu za provjeru statusa certifikata koje izdaje MNE eID Root CA, u ovom slučaju provjerava se status podređenih certifikacionih tijela.

MNE eID CA1 je MNE eID Root CA podređeno certifikaciono tijelo (u daljem tekstu podređeni CA) koji izdaje certifikate za krajnje korisnike – građane Crne Gore (u daljem tekstu: korisnički certifikati) i OCSP servisu za provjeru statusa certifikata koje izdaje podređeno certifikaciono tijelo. U dokumentu pod nazivom „Praktična pravila rada za izdavanje certifikata za kvalifikovani elektronski potpis i elektronsku identifikaciju“ u daljem tekstu CPS, opisani su postupci certifikacije i praktična pravila rada podređenog certifikacionog tijela MUP-a MNE eID CA1.

1.1.1 Opseg i namjena

Politika certifikacije davaoca usluga povjerenja TrustME (u daljem tekstu: CP) opisuje usluge povjerenja koje pruža. Ovaj CP predstavlja i praktična pravila rada za korijensko certifikaciono tijelo MNE eID Root CA za postupke i procedure koje primjenjuje za izdavanje i upravljanje certifikata za podređena certifikaciona tijela i OCSP servis korijenskog certifikacionog tijela.

Namjena ovog dokumenta je propisivanje postupaka iz područja usluga povjerenja, a koje sprovode učesnici TrustME navedeni u tački 1.3. ovog dokumenta.

Struktura ovog dokumenta zasniva se na standardizovanom dokumentu IETF RFC 3647.

Certifikaciono tijelo utvrđuje i Interna pravila rada davaoca usluga povjerenja (u daljem tekstu: Interna pravila) u kojima su sadržani i detaljno opisani postupci i mjere koji se primjenjuju prilikom prijema zahtjeva za izdavanje certifikata, izdavanja certifikata, upravljanja životnim vijekom certifikata, upravljanja IT infrastrukturom i njenom zaštitom. Interna pravila su privatni dokumenti i predstavljaju poslovnu tajnu davaoca usluga povjerenja.

1.1.2 Tipovi certifikata

U ovom poglavlju opisani su tipovi certifikata koje izdaje korijensko certifikaciono tijelo MUP-a. U tabeli su za svaki tip digitalnog certifikata navedeni pripadajući OID-ovi politika certifikovanja (u daljem tekstu: CP OID).

Tabela 1.1. prikazuje grupe i tipove elektronskih certifikata koje izdaje MNE eID Root CA.

Certifikati koje izdaje MNE eID Root CA			
Naziv grupe certifikata	**Naziv tipa certifikata**	**TrustME i CP OID**	**Tip certifkata i tip nosioca certifikata**
Certifikati za certifikaciona tijela	Certifikat korijenskog certifikacionog tijela	TrustME CP OID: nema ETSI CP OID: nema	Certifikat sa pripadajućim parom ključeva na HSM uređaju u FIPS 140-2 Level 3 režimu rada
	Certifikat za podređeno certifikaciono tijelo	TrustME CP OID: nema CP OID: 2.5.29.32.0	Certifikat sa pripadajućim parom ključeva na HSM uređaju u FIPS 140-2 Level 3 režimu rada
Certifikati za OCSP servise	Certifikat za OCSP servis korijenskog CA tijela	TrustME CP OID: 1.3.6.1.4.1.54748.1.1.1.1	Certifikat sa pripadajućim parom ključeva u KMS aplikaciji zaštićen HSM uređajem u FIPS 140-2 Level 3 režimu rada

Tabela 1.1. Grupe i tipovi certifikata koje izdaje MNE eID Root CA

Certifikaciono tijelo izdaje tri (3) tipa certifikata:

- Certifikat korijenskog certifikacionog tijela čiji se pripadajući par asimetričnih ključeva generiše u formalnoj proceduri uspostave certifkacionog tijela i generisanja para asimetričnih ključeva koju sprovode lica s povjerljivim ulogama na HSM uređaju koji je u FIPS 140-2 Level 3 režimu rada,
- Certifikat za podređeno certifikaciono tijelo čiji se pirpadajući par asimetričnih ključeva generiše u formalnoj proceduri uspostave certifkacionog tijela i generisanja para asimetričnih ključeva koju sprovode lica s povjerljivim ulogama na HSM uređaju koji je u FIPS 140-2 Level 3 režimu rada,

- Certifikat za OCSP servis korijenskog certifikacionog tijela čiji pripadajući par ključeva generiše lice s povjerljivom ulogom gdje se par asimetričnih ključeva čuva u KMS aplikativnoj komponenti primjenom HSM uređaja u FIPS 140-2 Level 3 režimu rada.

1.1.2.1 Certifikati korijenskog certifikacionog tijela

Certifikat korijenskog certifikaciong tijela MNE eID Root CA certifikaciono tijelo izdaje sebi u vidu samopotpisanog certifikata. Ovaj certifikat koristi se za verifikaciju certifikata izdatih podređenim certifikacionim tijelima, OCSP servisu korijenskog certifikacionog tijela i verifikaciju liste opozvanih certifikata korijenskog certifikacionog tijela.

1.1.2.2 Certifikat za podređeno certifikaciono tijelo

Certifikat za podređeno certifikaciono tijelo MNE eID Root CA izdaje samo podređenim certifikacionim tijelima u okviru davaoca usluga povjerenja. Ovaj certifikat koristi se za verifikaciju certifikata koje podređeno certifikaciono tijelo izdaje korisnicima, OCSP servisu podređenog certifikacionog tijela i verifikaciju liste opozvanih certifikata podređenog certifikacionog tijela.

1.1.2.3 Certifikati za OCSP servise

MNE eID Root CA certifikat za OCSP servis je certifikat namijenjen za verifikaciju OCSP odgovora za provjeru statusa certifikata koje izdaje MNE eID Root CA, odnosno za provjeru statusa certifikata izdatih podređenim certifkacionim tijelima.

1.2 Naziv dokumenta i identifikacioni podaci

Za MUP Crne Gore dodijeljen je od strane IANA organizacije (Internet Assigned Number Authority) sledeći OID: 1.3.6.1.4.1.54748.

Na osnovu tog OID-a MUP je za potrebe pružanja usluga povjerenja certifikacionom tijelu MUP-a dodijelio sledeći OID: 1.3.6.1.4.1.54748.1.

U nastavku je naveden naziv ovog dokumenta i njegovi identifikacioni podaci.

Naziv: Politika certifikacije davaoca usluga povjerenja TrustME

Verzija: 1.0

Datum stupanja na snagu: 10.03.2020. godine.

Internet adresa na kojoj je objavljen ovaj CP dokument je: https://ca.elk.gov.me/cpcps

1.3 Učesnici u sistemu davaoca usluga povjerenja MUP-a

U ovom poglavlju opisana je arhitektura PKI sistema koji se bazira na certifikacionim tijelima u okviru MUP-a radi izdavanja certifikata za elektronsku identifikaciju i certifikata za kvalifikovani elektronski potpis u okviru usluga povjerenja koje pruža MUP.

Učesnici PKI sistema MUP-a su:

- Certifikaciona tijela MUP-a
- Registraciona tijela MUP-a
- Centralno registraciono tijelo MUP-a
- Korisnici
- Treća lica

1.3.1 Certifikaciona tijela MUP-a

Certifikaciona tijela MUP-a na koja se odnosi ovaj dokument su:

- Korijensko certifikaciono tijelo namijenjeno za izdavanje certifikata podređenim certifikacionim tijelima: MNE eID Root CA,
- Podređeno certifikaciono tijelo za izdavanje certifikata za kvalifikovani elektronski potpis i certifikata za elektronsku identifikaciju na elektronskim ličnim kartama građanima Crne Gore: MNE eID CA1,

Certifikaciona tijela MUP-a organizuju se u za to specijalno namijenjenim prostorijama MUP-a u sastavu Centra za informacione komunikacione tehnologije, informacionu bezbjednost i sisteme tehničkog nadzora MUP-a.

1.3.1.1 Policy Managment Authority

Certifikaciono tijelo MUP-a organizuje Policy Managment Authority (u daljem teksu TrustME PMA) tijelo koje je namijenjeno da obavlja sledeće aktivnosti:

- Izradu i održavanje ovog dokumenta,
- Izradu i održavanje ostalih javnih dokumenata koji su namijenjeni korisnicima, kao što su Ugovor sa krajnjim korisnikom (End-User Agreement) ili izjava o davanju usluga certifikovanja (PKI Disclosure Statement – PDS),
- Podnošenje dokumenata CP i CPS na usvajanje nadležnoj jedinici Ministarstva unutrašnjih poslova ili ministru MUP-a,
- Predlaže imenovanje osoblja na dužnosti u okviru certifikacionog tijela
- Vrši nadzor i reviziju usklađenosti davanja usluga povjerenja sa ovim dokumentom,

- Rješava potencijalne sporove nastale u domenu rada certifikacionog tijela MUP-a,
- Druge poslove upravljanja neophodne za funkcionisanje certifikacionog tijela MUP-a.

1.3.1.2 Tijelo za operativne poslova

Tijelo za operativne poslove obavlja sledeće aktivnosti:

- Instalacija, konfiguracija i održavanje IT sistema,
- Instalacija, konfiguracija i održavanje komunikacione mreže,
- Instalacija, konfiguracija i održavanje aplikacija CA tijela,
- Instalacija, konfiguracija i održavanje HSM uređaja,
- Nadzor nad radom infrastrukture CA tijela
- Ostale operativne i tehničke poslove potrebne za funkcionisanje kompletne infrastrukture davaoca usluga povjerenja.

1.3.2 Registraciona tijela

Sve poslove registracionog tijela MNE eID Root CA vrši TrustME PMA.

Poslove registracionog tijela za izdavanje certifikata krajnjim korisnicima vrše Registraciona tijela MUP-a i Centralno registraciono tijelo MUP-a opisni u nastavku dokumenta.

1.3.2.1 Registraciona tijela MUP-a

Poslovnice MUP-a predstavljaju registraciona tijela za podnošenje zahtjeva za izdavanje certifikata na elektronskoj ličnoj karti građanima Crne Gore. Uloga registracionog tijela u procesu izdavanja certifikata na elektronskoj ličnoj karti opisana je u CPS dokumentu.

1.3.2.2 Centralno registraciono tijelo MUP-a

Centralno registraciono tijelo MUP-a dio je certifikacionog tijela koje je namijenjeno da primi zahtjeve za izdavanje lične karte ujedno i zahtjeve za izdavanje certifikata za elektronsku identifikaciju i certifikata za kvalifikovani elektronski potpis posle odobrenja zahtjeva od strane registracionih tijela MUP-a i pokrene proces izdavanja lične karte i pripadajućih certifikata. Uloga centralnog registracionog tijela u procesu izdavanja certifikata na elektronskoj ličnoj karti opisana je u CPS dokumentu.

1.3.3 Korisnici

Građani Crne Gore predstavljaju korisnike usluga povjerenja koje pruža certifikaciono tijelo MUP-a. To su svi građani Crne Gore koji po Zakonu o ličnoj karti mogu posjedovati elektronsku ličnu kartu.

Obzirom da je Zakonom o ličnoj karti predviđena mogućnost da maloljetni građani mogu posjedovati ličnu kartu certifikati koji se izdaju na ličnoj karti počinju da važe:

- za punoljetna lica u trenutku izdavanja lične karte
    - kvalifikovani certifikat za elektronski potpis počinje da važi datumom početka važenja lične karte,
    - certifikat za elektronsku identifikaciju počinje da važi datumom početka važenja lične karte;
- za maloljetna lica u trenutku izdavanja lične karte
    - kvalifikovani certifikat za elektronski potpis počinje da važi datumom sticanja punoljetstva maloljetnog lica,
    - certifikat za elektronsku identifikaciju počinje da važi datumom početka važenja lične karte.

1.3.4 Treća lica (Relying parties)

Treće lica su fizička lica i poslovni subjekti (kompanije, korporacije, ustanove, tijela državne uprave i dr.) koja prihvataju izdate certifikate na ličnim kartama za potrebe elektronske identifikacije (autentifikacije) fizičkih lica i verifikacije kvalifikovanog elektronskog potpisa na bazi izdatog certifikata za kvalifikovani elektronski potpis na ličnoj karti određenih elektronskih transakcija i elektronskih dokumenata i koja vrše validaciju lanca certifikata izdatih certifikata na ličnoj karti građana Crne Gore.

U cilju provjere validnosti primijenjenog digitalnog certifikata, treće strane moraju uvijek da provjere status opozvanosti datog certifikata u okviru liste opozvanih certifikata izdate od strane certifikacionog tijela MUP-a ili putem OCSP servisa prije nego što prihvate informacije koje su navedene u certifikatu kao tačne i da provjere period važenja certifikata prije nego se pouzdaju u certifikat.

1.3.5 Ostali učesnici

Nije primjenjivo u ovom dokumentu.

1.4 Upotreba certifikata

1.4.1 Dozvoljena upotreba certifikata

Certifikaciono tijelo MNE eID Root CA koristi svoj certifikat i pripadajući par asimetričnih ključeva za izdavanje sledećih certifikata:

- Certifikat za podređno certifikaciono tijelo MNE eID CA1
- Certifikat za OCSP servis korijenskog certifikacionog tijela

Certifikat korijenskog certifikacionodg tijela i pripadajući par asimetričnih ključeva koriste se i za izdavanje liste opozvanih certifikata korijenskog certifikacionog tijela.

1.4.2 Zabranjena upotreba certifikata

Zabranjena je svaka upotreba certifikata korijenskog certifikacionog tijela za druge namjene osim dozvoljenih ovim dokumentom.

1.5 Administracija Politika certifikacije davaoca usluga povjerenja TrustME

1.5.1 Organizacija koja upravlja dokumentom Politika certifikacije davaoca usluga povjerenja TrustME

TrustME PMA u ime MUP-a Crne Gore periodično pregleda i ažurira ovaj dokument u skladu sa promjenama odredbi u zakonskoj regulativi ili prilikom promjene tehničkih karakteristika primijenjenih kriptografskih algoritama ili dužina kriptografskih ključeva.

1.5.2 Kontakt osoba

Kontakt podaci za administraciju i sadržaj ovog dokumenta dati su u nastavku.

Poštanska adresa:

> TrustME PMA: Centar za informacione komunikacione tehnologije, informacionu bezbjednost i sisteme tehničkog nadzora MUP-a
>
> Adresa: Podgorica, bulevar Svetog Petra Cetinjskog br. 22.
>
> E-mail: pma@mup.gov.me

1.5.3 Subjekt koji utvrđuje usaglašenost dokumenta sa zakonom

Nadležni organ shodno zakonu i propisima iz ove oblasti.

1.5.4 Procedura odobravanja CP dokumenta

Dokument "Politika certifikacije davaoca usluga povjerenja TrustME" certifikacionog tijela MUP-a periodično se pregleda i ažurira po potrebi. Period pregleda i ažuriranja ovog dokumenta je minimalno jednom u dvije godine ili prilikom pripreme provjere usklađenosti.

Dokument se može pregledati i po potrebi ažurirati i češće ukoliko dođe do promjena u zakonskoj regulativi ili se javi potreba za promjenu primijenjenih kriptografskih algoritama ili dužina kriptografskih ključeva.

Na osnovu predloga TrustME PMA dokument „Politika certifikacije davaoca usluga povjerenja TrustME" odobrava ministar MUP-a Crne Gore.

1.6 Definicije i skraćenice

U ovom dokumentu pojedini izrazi imaju sledeće značenje:

Pojam	Opis
Autentifikacija	Elektronski postupak koji omogućava potvrđivanje elektronske identifikacije fizičkog ili pravnog lica ili porijekla i integriteta podataka u elektronskom obliku
Akreditacija	Formalna deklaracija od strane potvrdnog autoriteta da izvjesne funkcije/entiteti zadovoljavaju specifične formalne zahtjeve.
Aplikacija za certifikat	Zahtjev poslat od strane korisnika koji zahtjeva certifikat (aplikant) ka Certifikacionom tijelu u cilju izdavanja elektronskog certifikata.
Arhiva	Specifična baza podataka za čuvanje zapisa za određeni period vremena u cilju bezbjednosti, backup-a ili audit-a.
Asimetrični kriptografski algoritmi	Kriptografski algoritmi koji se koriste za realizaciju tehnologije digitalnog potpisa kojom se obezbjeđuje: autentičnost, integritet i neporecivost transakcija. Algoritmi se nazivaju asimetričnim zato što se različiti kriptografski ključevi koriste za šifrovanje i za dešifrovanje. Asimetrični kriptografski algoritam koristi par ključeva, javni i privatni i to javni u postupku šifrovanja i privatni u postupku dešifrovanja.
Asimetrični par ključeva (key pair)	Privatni ključ i javni ključ, kao matematički par koji se koriste za potrebe rada asimetričnog kriptografskog algoritma, kao što je na primjer RSA algoritam.
Autorizacija	Procedura utvrđivanja prava koje neki autentikovani korisnik ima za korišćenje odgovarajuće aplikacije ili servisa.

CA certifikat	Certifikat za dato CA izdat (digitalno potpisan) od strane drugog CA ili samopotpisan (ukoliko se radi o MNE eID Root CA).
Certificate Practice Statement (CPS)	Javna Praktična pravila i procedure koje certifikaciono tijelo primjenjuje u proceduri izdavanja certifikata.
Certifikat za elektronski potpis	Certifikat za elektronski potpis je dokument u elektronskom obliku potpisan od davaoca usluga certifikovanja za elektronske transakcije koji povezuje podatke za provjeru elektronskog potpisa sa nekim licem i potvrđuje identitet tog lica.
Dijeljena tajna	Dio kriptografske tajne koja je podijeljena na unaprijed definisan broj smart kartica.
Dešifrovanje	Transformacija kojom se iz šifrata dobija originalna informacija primjenom odgovarajućeg kriptografskog algoritma i odgovarajućeg kriptografskog ključa.
Domen	Sistem u kome se internet adrese vezuju za određene lokacije na internetu
Ekstenzije u certifikatu	Dodatna polja u certifikatu, pored osnovnih, koja daju bliže informacije o vlasniku (korisniku) i izdavaču (CA) certifikata, kao i o procesu certifikacije.
Elektronski dokument	Skup podataka koji su elektronski oblikovani, poslati, primljeni ili skladišteni na elektronskom, magnetnom, optičkom ili drugom mediju, i koji sadrži svojstva pomoću kojih se identifikuje stvaralac, utvrđuje vjerodostojnost sadržaja i dokazuje nepromjenjivost sadržaja u vremenu, a uključuje sve oblike pisanog teksta, podatke, slike, crteže, karte, zvuk, muziku, govor i slično
Elektronski potpis	Elektronski potpis je skup podataka u elektronskom obliku koji su pridruženi ili su logički povezani sa elektronskim dokumentom i služe za potpis i elektronsku identifikaciju potpisnika. Elektronski potpis se izrađuje pomoću sredstva za izradu elektronskog potpisa i zasniva se na certifikatu za izradu elektronskog potpisa.
Elektronski certifikat	Elektronski dokument kojim se potvrđuje veza između podataka za provjeru elektronskog potpisa i identiteta potpisnika.
Hash algoritmi	Jednosmjerni kriptografski algoritmi pomoću kojih se vrši kriptografska transformacija informacije proizvoljne veličine u hash vrijednost fiksne veličine (160, 224, 256, 384, 512 bitova (ili više)).

Hijerarhija certifikata	Sekvenca certifikata bazirana na nivoima koja ima jedan Root CA certifikat i subordinate/intermediate entitete, kao što su certifikati drugih CA i korisnici.
Identifikacija	Utvrđivanje da dato ime pojedinca odgovara realnom identitetu pojedinca.
Identifikator objekta (Object identifier)	Sekvenca brojčanih komponenti koja može biti pridružena nekom registrovanom objektu i koja ima karakteristiku da je jedinstvena u svim identifikatorima objekata u okviru specifičnog domena.
Javni ključ	Matematički podatak koji može biti javno objavljen (najčešće se objavljuje u formi X.509v3 elektronskog certifikata) i koji se koristi za verifikaciju elektronskog potpisa, kreiranog pomoću odgovarajućeg privatnog ključa koji je matematički par sa datim javnim ključem, kao i za šifrovanje podataka za korisnika koji posjeduje odgovarajući privatni ključ.
Korisnički ugovor	Ugovor između korisnika i CA u cilju obezbjeđenja certifikacionih usluga.
Korisnik	Fizičko ili pravno lice koje se oslanja na elektronsku identifikaciju ili uslugu certifikovanja za elektronske transakcije
Kriptografija	Nauka o zaštiti tajnosti informacija.
Kriptografski algoritmi	Algoritmi po kojima se vrši transformacija originalne informacije u šifrovanu informaciju (šifrat) i obratno, iz šifrata u originalnu infomaciju, korišćenjem odgovarajućeg kriptografskog ključa.
Kriptografski ključ	Tajna i slučajna informacija odgovarajuće dužine u bitovima (na primjer 128 ili 256 bita) koja se koristi u kriptografskim algoritmima, u procedurama šifrovanja i dešifrovanja.
Kvalifikator politike	Informacija koja zavisi od politike certifikacije i koja je pridružena identifikatoru politike certifikacije u okviru X.509 certifikata. Može da uključi i URL na kome se nalazi publikovan CPS datog certifikacionog tijela.
Kvalifikovani certifikat za elektronski potpis	Kvalifikovani certifikat za elektronski potpis je certifikat koji ispunjava uslove propisane članom 16 Zakona o elektronskoj identifikaciji i elektronskom potpisu.
Kvalifikovani elektronski potpis	Kvalifikovani elektronski potpis je napredni elektronski potpis koji je izrađen pomoću kvalifikovanog sredstva za izradu elektronskog potpisa i zasniva se na kvalifikovanom certifikatu za elektronski potpis.

Lanac (put) certifikata	Uređena sekvenca certifikata koja se, zajedno sa javnim ključem inicijalnog objekta u lancu (putu), procesira u cilju provjere istog u poslednjem objektu na putu.
Lični identifikacioni podaci	Skup podataka u elektronskom obliku koji omogućavaju da se utvrdi identitet fizičkog ili pravnog lica
Lista opozvanih certifikata (CRL)	(Certificate Revocation List) – Lista izdata i elektronski potpisana od strane CA koja uključuje opozvane certifikate, kao i razloge njihovog opoziva. Takva lista se mora koristiti od strane trećih lica uvijek kada treba provjeriti validnost certifikata i/ili verifikaciju elektronskog potpisa.
Napredni elektronski potpis	Napredni elektronski potpis je elektronski potpis kojim se pouzdano garantuje identitet potpisnika i integritet elektronskog dokumenta. Napredni elektronski potpis mora da: 1) bude isključivo povezan sa potpisnikom; 2) nedvosmisleno identifikuje potpisnika; 3) nastaje korišćenjem sredstva za izradu elektronskog potpisa kojim potpisnik može samostalno da upravlja i koje je isključivo pod njegovim nadzorom; 4) sadrži direktnu povezanost sa podacima na koje se odnosi, i to na način koji nedvosmisleno omogućava uvid u bilo koju izmjenu izvornih podataka.
Opoziv certifikata	Permanentno ukidanje validnosti datog certifikata i njegovo smještanje na CRL listu.
Organ vlasti	Državni organ, organ državne uprave, organ lokalne samouprave, odnosno lokalne uprave i pravno lice koje vrši javna ovlašćenja
Podaci za izradu elektronskog potpisa	Jedinstveni podaci (kodovi ili privatni kriptografski ključevi), koje potpisnik koristi za izradu elektronskog potpisa
Podaci za verifikaciju	Podaci koji se koriste za verifikaciju elektronskog potpisa
Politika certifikacije	Imenovan skup pravila koji indicira primjenljivost certifikata na određeno okruženje i/ili na klasu aplikacija sa zajedničkim bezbjednosnim zahtjevima.
Potpisnik	Fizičko lice koje posjeduje sredstvo za izradu elektronskog potpisa kojim se potpisuje u svoje ime
Privatni ključ	Matematički podatak koji se koristi kao ključ za kreiranje elektronskog potpisa i za raspakivanje digitalne envelope - dešifrovanje simetričnog ključa kojim je šifrovan dokument za datog korisnika primjenom asimetričnog kriptografskog algoritma.

Registraciono tijelo (RA)	Entitet koji je odgovoran za identifikaciju i autentikaciju korisnika/vlasnika certifikata, kao i kreiranje zahtjeva za izdavanje certifikata, ali koji ne izdaje i ne potpisuje certifikat (tj. RA vrši odgovarajuće poslove (identifikaciju korisnika) i u tom smislu je delegirano od CA). Često se i termin LRA (Local Registration Authority) koristi u istom kontekstu.
Repozitorijum	Web stranica i/ili direktorijum na kome su javno dostupni osnovni dokumenti rada CA, kao i eventualne druge informacije koje se odnose na pružanje certifikacionih usluga od strane datog CA (kao na primjer objavljivanje svih izdatih certifikata, itd.).
Serijski broj certifikata	Sekvencijalni broj koji jedinstveno identifikuje certifikat u domenu datog CA.
Certifikacija	Proces izdavanja elektronskog certifikata.
Certifikaciono tijelo izdavač certifikata (issuing CA)	U kontekstu određenog certifikata, certifikaciono tijelo – izdavalac certifikata je ono CA koje je izdalo (digitalno potpisalo) certifikat.
Certifikaciono tijelo	Pravno lice koje izdaje elektronske certifikate u skladu sa odredbama Zakona o elektronskoj identifikaciji i elektronskom potpisu.
Simetrični kriptografski algoritmi	Kriptografski algoritmi koji se koriste za realizaciju šifrovanja u cilju zaštite tajnosti informacija. Algoritmi se nazivaju simetričnim zato što se isti kriptografski ključ koristi za šifrovanje i za dešifrovanje.
Smart kartica	Hardverski token koji sadrži čip na kome može da se izvrše odgovarajuće kriptografske funkcije, kao što su: elektronski potpis, šifrovanje, generisanje para asimetričnih ključeva, itd.
Sredstvo za izradu elektronskog potpisa	Sredstvo za izradu elektronskog potpisa je odgovarajuća računarska oprema ili računarski program koji se koristi prilikom izrade elektronskog potpisa uz korišćenje podataka za izradu elektronskog potpisa.
Kvalifikovano sredstvo za izradu elektronskog potpisa	Kvalifikovano sredstvo za izradu elektronskog potpisa je sredstvo za izradu kvalifikovanog elektronskog potpisa koje ispunjava posebne uslove propisane članom 19 Zakona o elektronskoj identifikaciji i elektronskom potpisu.
Sredstva za provjeru elektronskog potpisa	Odgovarajuća tehnička sredstva (softver i hardver) koja služe za provjeru elektronskog potpisa, uz korišćenje podataka za provjeru elektronskog potpisa.

Sredstva za provjeru kvalifikovanog elektronskog potpisa	Sredstva za provjeru elektronskog potpisa koja ispunjavaju dodatne uslove utvrđene Zakonom o elektronskoj identifikaciji i elektronskom potpisu.
Šifrovanje	Transformacija koja primjenom odgovarajućeg kriptografskog algoritma i odgovarajućeg kriptografskog ključa, pretvara originalnu informaciju u oblik u kojem sadržaj te informacije postaje nedostupan neovlašćenim licima (šifrat).
Treća lica	Primalac certifikata koji provjerava dati certifikat i/ili provjerava digitalni potpis dobijenog elektronskog dokumenta primjenom javnog ključa potpisnika iz certifikata. Takođe, treća lica provjeravaju validnost certifikata u istom procesu. Treća lica mogu biti takođe korisnik certifikata izdatog od strane istog certifikacionog tijela, ali i ne mora.
Upravljanje certifikatima	Aktivnosti pridružene upravljanju certifikatima uključuju čuvanje, isporuku, objavljivanje i opoziv certifikata.
Verifikacija	Postupak kojim se potvrđuje da su elektronski potpis ili elektronski pečat validni
Zahtjev za dobijanje certifikata (CSR Certificate Service Request)	Standardna forma (po PKCS#10 preporuci) koja se koristi za slanje zahtjeva za dobijanjem certifikata.

Tabela 1.2. Indeks pojmova

Skraćenice koje se koriste u ovom dokumentu:

Skraćenica	Objašnjenje
CA	Certification Authority
RA	Registration Authority
ID	Identification document
PKI	Public Key Infrastructure
OID	Object IDentifier
TSA	Time Stamping Authority
CRL	Certificate Revocation List
CSR	Certificate Service Request
CDP	CRL Distribution Point

AIA	Authority Information Access
AKI	Authority Key Identifier
SKI	Subject Key Identifier
RFC	Request For Comments
ETSI	European Telecommunication Standardization Institute
CP	Certificate Policy
CPS	Certificate Practise Statement
URL	Uniform Resource Locator
JMB	Jedinstveni Matični Broj

Tabela 1.3. Skraćenice

2 Objavljivanje i odgovornosti za repozitorijum

2.1 Repozitorijum

Repozitorijum cerifikacionog tijela MUP-a vodi Centar za informacione komunikacione tehnologije, informacionu bezbjednost i sisteme tehničkog nadzora u ime MUP-a kao kvalifikovanog davaoca usluga povjerenja. Certifikaciono tijelo je odgovorno za rad repozitorijuma, objavu dokumenata i informacija na repozitorijumu i objavu certifikata certifikacionih tijela i liste opozvanih certifikata na repozitorijumu.

U okviru normalnog funkcionisanja repozitorijuma, on je dostupan za upotrebu 24 sata na dan, 7 dana u nedelji.

U slučaju nedostupnosti repozitorijuma cetifikaciono tijelo će preduzeti sve potrebne mjere i postupke da repozitorijum učini dostupnim u najkraćem mogućem roku.

2.2 Objava informacija o pružanu usluga povjerenja

Na TrustME repozitorijumu javno su objavljeni dokumenti i informacije o pružanju usluga povjerenja.

Repozitorijum se sastoji od dijela dostupnog na internet stranicama i dijela dostupnog preko javnog LDAP imenika.

2.2.1 Sadržaji repozitorijuma

Na internet stranicama TrustME repozitorijuma objavljuju se:

- Dokument “Politike certifikacije davaoca usluga povjerenja TrustME”

- Dokument „Praktična pravila rada za izdavanje certifikata za kvalifikovani elektronski potpis i elektronsku identifikaciju”
- Prethodne verzije dokumenata: CP i CPS,
- Uslovi i izjave o pružanju usluga izdavanja certifikata (engl. *Terms and conditions* i *PKI disclosure statement*),
- Opis važećih profila certifikata,
- Obrasci ugovora o obavljanju usluga certifikovanja,
- Obrasci zahtjeva za opoziv, suspenziju, reaktivaciju certifikata,
- Certifikat korijenskog CA tijela: MNE eID Root CA
- Certifikat podređenog CA tijela: MNE eID CA1
- Objedinjene liste opozvanih certifikata za CA tijela iz PKI hijerarhije MUP-a,
- Informacije o zakonskoj regulativi iz područja elektronskog potpisa i pružanja usluga povjerenja,
- Informacije o postojanju dokumenata važnih za poslovanje koji ne mogu biti u cjelosti ili uopšte objavljeni zbog osjetljivosti ili povjerljivosti sadržaja,
- Aktuelne lokacije poslovnica MUP-a, koje predstavljaju lokacije registracionih tijela u smislu ovog dokumenta,
- Korisnička uputstva,
- Uputstva i potreban aplikativni softver za korišćenje elektronske lične karte,
- Certifikati namijenjeni za provjeru i testiranje,
- Obavještenja korisnicima i trećim licima u vezi s davanjem usluga povjerenja,
- Ostale informacije vezane za rad certifikacionog tijela MUP-a.

Korisnički certifikati izdati na ličnoj karti se ne objavljuju.

Preko internet stranice repozitorijuma moguće je pretraživanje javnog imenika i preuzimanje certifikata CA tijela i liste opozvanih certifikata certifikacionih tijela.

Objavljeni sadržaj na internet stranicama dostupan je s adrese https://ca.elk.gov.me na crnogorskom jeziku. TrustME može pojedina dokumenta objaviti i na engleskom jeziku, ako za to ima potrebe.

U strukturi javnog imenika javno se objavljuje:

- objedinjena CRL za root (MNE eID Root CA) i njegov podređeni CA (MNE eID CA1).

Adresa javnog LDAP imenika je ldap://ldap.elk.gov.me.

Putem OCSP servisa dostupne su informacije o statusu izdatih certifikata koje izdaju TrustME CA tijela. Adrese OCSP servisa za pojedina CA tijela su:

- za MNE eID Root CA: http://ocsp.elk.gov.me/MNEeIDRootCA
- za MNE eID CA1: http://ocsp.elk.gov.me/MNEeIDCA1

U repozitorijumu ne objavljuju se povjerljivi podaci.

2.2.2 Postupci objave sadržaja i upravljanja repozitorijumom

Objavu dokumenata na repozitorijumu po odobrenju obavlja ovlašćeno lice zaduženo za upravljanje sadržajem internet dijela repozitorijuma.

Obavještenja Korisnicima, informacije o zakonskim aktima objavljuju se nakon početka primjene zakonskih akata u TrustME.

Certifikati certifikacionih tijela i pripadajuće informacije objavljuju se nakon njihovog izdavanja.

Objavu dokumenata uslova pružanja usluga, korisničkih uputstava, obrazaca zahtjeva, ugovora i punomoćja odobrava TrustME PMA. Objava ovih dokumenata se obavlja bez prethodne najave, a starije verzije dokumenata brišu se iz repozitorijuma.

Obavještenja i informacije mogu se objaviti na internet stranicama repozitorijuma i bez odobrenja TrustME PMA, ali TrustME PMA mora biti pravovremeno obaviješten o svakoj objavi obavještenja i informacija.

TrustME CA tijela automatski objavljuju pripadajuće CRL na javnom imeniku i na internet stranicama repozitorijuma nakon njihovog izdavanja.

2.3 Učestalost objavljivanja podataka o uslugama od povjerenja

TrustME na godišnjem nivou održava i ažurira ovaj dokument i odobrava ga, objavljuje i primjenjuje. Prethodne verzije ovih dokumenata ostaju objavljene na repozitorijumu najmanje 10 godina posle isteka certifikata izdatih u skladu s tim dokumentima.

Drugi TrustME dokumenti i ostale relevantne informacije objavljuju se po potrebi, nakon odobrenja TrustME PMA.

Učestalost objave CRL za certifikate koje izdaju CA tijela definisana je tačkom 4.9.7 ovog dokumenta.

Online informacije o statusu izdatih certifikata dostupne su putem OCSP servisa u realnom vremenu.

2.4 Kontrola pristupa repozitorijumu

Dokumenti i informacije objavljene na TrustME repozitorijumu su besplatne i javno dostupne svim učesnicima uspostavljene PKI infastrukture.

TrustME na repozitorijumu ima uspostavljene kontrole pristupa u cilju sprečavanja neautorizovanog dodavanja, promjene ili brisanja informacija, zaštitu njihovog integriteta i autentičnosti. Pristup objavljenim dokumentima i informacijama na repozitorijumu omogućen je samo za čitanje.

Pravo dodavanja, promjene ili brisanja informacija na TrustME repozitorijumu imaju ovlašćena lica TrustME.

3 Identifikacija i autentifikacija korisnika

Procedure identifikacije i autentifikacije navedene u ovom dokumentu se odnose na certifikate koje izdaje korijensko certifikaciono tijelo.

Procedure identifikacije i autentifikacije krajnjih korisnika su opisane u CPS dokumentu.

3.1. Dodjeljivanje imena

3.1.1 Vrste imena

Certifikaciona tijela MUP-a organizovana su u TrustME hijerarhiju certifikacionih tijela. Ova hijerarhija sastoji se od dva certifikaciona tijela:

- korijensko certifikaciono tijelo pod nazivom MNE eID Root CA
- podređeno certifikaciono tijelo pod nazivom MNE eID CA1

Atributi koji čine jedinstvena imena MNE eID Root CA, MNE eID CA1 certifikacionih tijela dati su u tabelama 3.1 i 3.2 respektivno.

Korijensko certifikaciono tijelo MNE eID Root CA		
Atribut po X.520	**Vrijednost**	**Objašnjenje**
commonName (CN)	MNE eID Root CA	Naziv certifkacionog tijela
OrganizationName	Ministarstvo unutrašnjih poslova	Naziv organizacione jedinice
organizationIdentifier	VATME-02016010	Identifikator organizacione jedinice različit od naziva organizacione jedinice

countryName	ME	Dvoslovni ISO kod države, ME za Crnu Goru

Tabela 3.1 Sadržaj imena korijenskog certifikacionog tijela MNE eID Root CA

Certifikaciono tijelo MNE eID CA1		
Atribut po X.520	**Vrijednost**	**Objašnjenje**
commonName (CN)	MNE eID CA1	Naziv certifkacionog tijela
OrganizationName	Ministarstvo unutrašnjih poslova	Naziv organizacione jedinice
organizationIdentifier	VATME-02016010	Identifikator organizacione jedinice različit od naziva organizacione jedinice
countryName	ME	Dvoslovni ISO kod države, ME za Crnu Goru

Tabela 3.2 Sadržaj imena certifikacionog tijela MNE eID CA1

3.1.2 Potreba da imena budu sa realnim značenjem

Imena koja se upisuju u certifikate certifikacionih tijela imaju realno značenje i odgovaraju nazivima koji se koriste za certifikaciona tijela u okviru TrustME hijerarhije MUP-a.

Pravila imena koja se upisuju u certifikate koji se izdaju korisnicima opisana su u CPS dokumentu.

3.1.3 Anonimnost korisnika, pseudonimi i nadimci

Nije primjenjivo.

3.1.4 Pravila za interpretaciju različitih vrsta imena

Interpretacija oblika imena u polju Subject certifikata koji se izdaju certifikacionim tijelima radi se po tabelama 3.1 i 3.2 u sekciji 3.1.1 koja je usklađena sa zakonom i odgovarajućim standardima.

3.1.5 Jedinstvenost imena

Jedinstvenost imena u certifikatima certifikacionih tijela garantuje se atributom commonName. Svako novo korijensko ili podređeno certifikaciono tijelo MUP-a mora imati jedinstveno ime u okviru hijerarhije TrustME koje se upisuje u atribut commonName.

MUP vodi evidenciju o iskorisćenim imenima za certifikaciona tijela radi očuvanja jedinstvenosti imena.

3.1.6 Upotreba robnih marki („trademarks“) u certifikatima

Certifikaciona tijela ne koriste robne marke u svojim certifikatima.

3.2 Inicijalna provjera identiteta

Provjera identiteta lica sa povjerljivim ulogama zaposlenih u certifikacionom tijelu sporovodi se prema internim pravilima za zaposlene MUP-a i obavlja ih nadležna jedinica MUP-a.

3.2.1 Metoda dokazivanja posjedovanja privatnog ključa

Metoda dokazivanja posjedovanja privatnog ključa za korijensko certifikaciono tijelo i njemu podređenih certifikacionih tijela MUP-a obezbjeđena je sporovođenjem procedure uspostave certifikacionih tijela i generisanja para asimetričnih ključeva.

Certifikaciono tijelo izdaje certifikate prema poglavlju 1.1.2.

3.2.2 Provjera identiteta pravnog lica

Nije primjenjivo.

3.2.3 Provjera identiteta fizičkog lica

Nije primjenjivo.

3.2.4 Podaci o korisniku koji se ne provjeravaju

Nije primjenjivo.

3.2.5 Provjera ovlašćenja

Nije primjenjivo.

3.2.6 Kriterijumi za interoperabilnost

Procedure i prakse povezanih certifikacioni tijela moraju biti materijalno ekvivalentne procedurama i praksi TrustME kao što je definisano u ovom pravilniku. TrustME PMA je odgovorno za izradu procjena procedura i praksi certifikacionih tijela sa kojima se vrši povezivanje od slučaja do slučaja.

3.3 Provjera identiteta kod zahtjeva za obnavljanje certifikata

Nije primjenjivo.

3.4 Provjera identiteta kod zahtjeva za suspenziju/opoziv certifikata

Nije primjenjivo.

4 Upravljanje certifikatima

Procedure upravljanja certifikatima navedene u ovom dokumentu se odnose na certifikate koje izdaje korijensko certifikaciono tijelo.

Procedure upravljanja certifikatima krajnjih korisnika su opisane u dokumentu CPS.

4.1 Zahtjev za izdavanje certifikata

Izdavanje certifikata za korijensko certifikaciono tijelo „MNE eID Root CA“, za podređeno certifikaciono tijelo i OCSP servis korijenskog certifikacionog sprovodi se prema formalnoj proceduri i po odobrenju TrustME PMA.

4.1.1 Ko može da zahtijeva izdavanje certifikata

Nije primjenjivo.

4.1.2 Proces obrade zahtjeva za izdavanje certifikata i odgovornosti

Nije primjenjivo.

4.2 Procesuiranje zahtjeva za izdavaje certifikata

4.2.1 Postupak identifikacije i autentifikacije korisnika

Identifikacija i autentikacija lica s povjerljivim ulogama u okviru certifikacionog tijela vrši se po intetnim pravilima MUP-a.

4.2.2 Odobrenje ili odbijanje zahtjeva za izdavanje certifikata

TrustME PMA može vratiti proceduru za izdavanje certifikata na doradu ukoliko zaključi da podaci i procedura nisu u skladu sa ovim dokumentom. Ukoliko su svi podaci u skladu sa ovim dokumentom PMA odobrava proceduru za izdavanje certifikata.

4.2.3 Vrijeme za obradu zahtjeva

Nije primjenjivo.

4.3 Izdavanje certifikata

4.3.1 Aktivnosti tokom procesa izdavanja certifikata

Izdavanje certifikata korijenskom certifikacionom tijelu „MNE eID Root CA“ sprovodi se prema formalnoj proceduri uspostave korijenskog certifikacionog tijela i generisanja para asimetričnih ključeva.

Izdavanje certifikata podređenom certifikacionom tijelu „MNE eID CA1“ sprovodi se prema formalnoj proceduri uspostave podređenog certifikacionog tijela i generisanja para asimetričnih ključeva.

Proceduru uspostave korijenskog ili podređenog certifikacionog tijela sprovode lica sa povjerljivim ulogama u zaštićenom prostoru TrustME uz primjenu propisanih mjera bezbjednosti.

Izdavanje certifikata za OCSP servis sprovodi lice s povjerljivom ulogom upotrebom aplikacije za OCSP servis.

4.3.2 Obavještenje korisnika od strane certifikacionog tijela o izdavanju certifikata

Certifikati korijenskog certifikacionog tijela i podređenih certifikacionih tijela objavljuju se na internet stranicama TrustME repozitorijuma iz poglavlja 2.

4.4 Prihvatanje certifikata

4.4.1 Sprovođenje procesa prihvatanja certifikata

Certifikati korijenskog i podređenih certifikacionih tijela smatraju se provjerenim i prihvaćenim kao ispravni u okviru procedure generisanja ključeva i izdavanja certifikata.

4.4.2 Objavljivanje certifikata

Certifikat korijenskog certifikacionog tijela objavljuje se na internet stranicama TrustME repozitorijuma.

Certifikati podređenih certifikacionih tijela objavljuju se na internet stranicama TrustME repozitorijuma.

Certifikati za OCSP servis se ne objavljuju.

Objavljivanje korisničkih certifikata opisano je u CPS dokumentu.

4.4.3 Obavještavanje ostalih učesnika o izdavanje certifikata

Podrazumijeva se da su ostali učesnici obaviješteni o izdavanju certifikata korijenskog certifikacionog tijela i certifikata podređenih certifikacionih tijela njihovim objavljivanjem na internet stranicama TrustME repozitorijuma.

4.5 Korišćenje certifikata i pripadajućih asimetričnih parova ključeva

4.5.1 Korišćenje privatnih ključeva i certifikata od strane korisnika

Privatni ključevi korijenskog certifikacionog tijela i podređenih certifikacionih tijela koriste se isključivo za potpisivanje certifikata koje izdaje to certifikaciono tijelo i pripadajuće liste opozvanih certifikata.

Svaka druga upotreba ovih privatnih ključeva je strogo zabranjena.

Korišćenje privatnog ključa i pripadajućeg korisničkog certifikata od strane korisnika opisano je u CPS dokumentu.

4.5.2 Korišćenje javnih ključeva i certifikata od strane trećih lica

Treća lica koja namjerava koristiti usluge povjerenja koje pruža MUP i ostvariti povjerenje u korijensko certifikaciono tijelo ili u podređeno certifikaciono tijelo treba da:

- Vodi računa o dozvoljenoj upotrebi i zabranjenoj upotrebi javnog ključa i pripadajućeg certifikata u skladu sa tačkom 1.4 ovog dokumenta;
- Obavi provjeru vremena važenja svih certifikata u lancu i provjeru certifikata prema postupcima za validaciju lanca certifikata prema dokumentu RFC 5280;
- Obavi provjeru statusa certifikata upotrebom raspoloživih načina prema ovom dokumentu.

4.6 Obnavljanje certifikata bez promjene ključa

Certifikaciono tijelo ne vrši obnovu certifikata bez promjene ključa.

4.7 Obnova certifikata sa novim ključem (re-key)

Obnovu certifikata uz generisanje novog para ključeva može zatražiti lice sa povjerljivom ulogom.

Obnovu certifikata odobrava TrustME PMA.

Nakon odobrenja obnove certifikata lica s povjerljivim ulogama sprovode ceremoniju uspostave certifikacionog tijela i generisanja para asimetričnih ključeva za certifikaciono tijelo.

Novi certifikat za certifikaciono tijelo objavljuje se na internet stranicama TrustME repozitorijuma.

Zahtjev za obnovu certifikata za OCSP servis sprovodi lice s povjerljivom ulogom.

Postupak obnove certifikata za korisnike opisan je u CPS dokumentu.

4.8 Promjena certifikata korisnika

Promjena podataka u certifikatima za korijensko certifikaciono tijelo i podređena certifikaciona tijela se ne sprovode. Ukoliko se uvidi da postoji greška u korijenskom certifikatu ili certifikatu podređenog certifikacionog tijela sprovodi se nova formalna procedura uspostave certifikacionog tijela i generisanja para asimetričnih ključeva.

Postupak promjene certifikata za korisnike opisan je u dokumentu CPS.

4.9 Suspenzija i opoziv certifikata

Zahtjev za opoziv certifikata korijenskog certifikacionog tijela ili podređenog certifikacionog tijela odobrava TrustME PMA.

Suspenzija certifikata certifikacionih tijela nije dozvoljena.

Suspenzija i opoziv korisničkih certifikata opisani su u dokumentu CPS.

4.9.1 Okolnosti za opoziv certifikata

Korijensko certifikaciono tijelo vrši opoziv izdatog certifikata u sledećim slučajevima:

- Na osnovu pisanog zahtjeva za opoziv certifikata izdatog podređenom certifikacionom tijelu lica s povjerljivom ulogom u TrustME PMA;
- Ako TrustME PMA dođe do saznanja da je privatni ključ povezan sa javnim ključem u certifikatu certifikacionog tijela kompromitovan;
- Ako primijenjeni kripografski algoritam i dužina pripadajućeg asimetričnog ključa više ne zadovoljavaju kriptografske kriterijume propisane odgovarajućim standardima;
- Ako se utvrdi da su podaci u izdatom certifikatu pogrešni;
- U slučaju ako dođe do zabranjene upotrebe odnosno zloupotrebe privatnog ključa certifikacionog tijela;
- Ako certifikat svojim sadržajem, tehničkim karakteristikama i profilom ne pruža odgovarajući nivo povjerenja.

4.9.2 Ko može zahtijevati opoziv certifikata

Opoziv certifikata certifikacionih tijela se vrši na osnovu odluke TrustME PMA.

4.9.3 Procedura opoziva certifikata

Opoziv certifikata sprovode lica s povjerljivim ulogama u TrustME u bezbjednom prostoru certifikacionog tijela.

4.9.4 Vrijeme za predaju zahtjeva za opoziv certifikata

Nije primjenljivo.

4.9.5 Period vremena u kojem certifikaciono tijelo mora da obradi zahtjev za opoziv certifikata

Najkasnije 24 sata nakon prijema zahtjeva za opoziv.

4.9.6 Zahtjevi za provjeru opozvanosti certifikata sa strane trećih lica

Treća lica obavezna su da preduzimaju sve mjere i postupke propisane ovim dokumentom prilikom provjere validnosti certifikata i pouzdanosti u certifikat. Za potrebe validacije certifikata treća lica koriste sve raspoložive online resurse koje im na raspolaganje stavlja certifikaciono tijelo radi provjere statusa certifikata u koji će se pouzdati.

Treća lica moraju biti u saglasnosti sa politikom certifikacije i svojim obavezama propisanim ovim dokumentom.

4.9.7 Frekvencija izdavanja liste opozvanih certifikata

Vrijeme u kojem najkasnije mora biti izdata sledeća lista opozvanih certifikata koje je izdalo korijensko certifikaciono tijelo je najviše šest (6) mjeseci od prethodnog izdavanja liste opozvanih certifikata. Ukoliko dođe do opoziva certifikata koji je izdalo korijensko certifikaciono tijelo nova lista opozvanih certifikata biće objavljena u roku od osam (8) sati.

Vrijeme važenja izdate liste opozvanih certifikata je šest (6) mjeseci.

Frekvencija izdavanja liste opozvanih certifikata podređenih certifikacionih tijela definisana je u CPS dokumentu.

4.9.8 Maksimalno kašnjenje objavljivanja liste opozvanih certifikata

U regularnim okolnostim kašnjenje u objavi liste opozvanih certikikata nije duže od 1 minuta.

U slučaju vanrednih okolnosti certifikaciono tijelo će preduzeti sve mjere i postupke u okviru svojih mogućnosti da kumulativno kašnjenje objavljivanja liste opozvanih certifikata na godišnjem nivou bude do 10 dana.

4.9.9 Dostupnost on-line provjere statusa certifikata

Certifikaciono tijelo podržava *online* provjeru statusa opozvanosti izdatih certifikata putem OCSP servisa čiji je rad usaglašen s dokumentom IETF RFC 6960.

Informacija o statusu opozvanosti certifikata korišćenjem OCSP servisa dostupna je u realnom vremenu.

Adresa OCSP servisa zavisi od pripadajućeg CA tijela za koje OCSP servis daje odgovore o statusu, a upisuje se u ekstenziji *Authority Information Access* svakog certifikata kojeg izdaju TrustME CA tijela.

4.9.10 Zahtjevi za on-line provjeru statusa certifikata

Za korišćenje OCSP servisa treća lica treba da imaju aplikaciju koja može da koristi OCSP servis upotrebom GET ili POST HTTP metode.

4.9.11 Raspoloživost drugih formi objavljivanja statusa certifikata

Nema odredbi.

4.9.12 Specijalni zahtjevi u odnosu na kompromitaciju privatnog ključa

Nema odredbi.

4.9.13 Okolnosti za suspenziju certifikata

Korijensko certifikaciono tijelo ne vrši suspenziju certifikata podređenih certifikacionih tijela.

4.9.14 Ko može zahtijevati suspenziju certifikata

Ne primjenjuje se.

4.9.15 Procedura suspenzije certifikata

Ne primjenjuje se.

4.9.16 Maksimalno trajanje suspenzije certifikata

Ne primjenjuje se.

4.10 Servisi objavljivanja statusa certifikata

4.10.1 Operativne karakteristike

Certifikaciono tijelo MUP-a daje informacije o statusu certifikata putem OCSP servisa i objave CRL.

Informacija o statusu opozvanosti certifikata dostupna je putem OCSP servisa i CRL i nakon isteka certifikata.

Preporuka trećim licima je da za provjeru statusa certifikata koriste OCSP servis i da se provjera statusa pristupom CRL koristi kao alternativna metoda provjere u slučaju nedostupnosti OCSP servisa ili u slučaju da aplikacija trećih lica podržava provjeru statusa certifikata samo putem CRL.

Adresa OCSP servisa zavisi od certifikacionog tijela za koje OCSP odgovara o statusu certifikata, a upisuje se u ekstenziji Authority Information Access svih certifikata koje izdaje pripadajuće certifikaciono tijelo.

CRL za certifikate koje izdaju certifikaciona tijela objavljuju se na internet serveru i na javnom imeniku repozitorijuma certifikacionog tijela. Na internet serveru objavljuje se objedinjena CRL, a na javnom imeniku takođe objavljuje se objedinjena CRL.

Adrese objave CRL sadržane su u ekstenziji CRLDistributionPoints u svakom izdatom certifikatu.

4.10.1.1 Adrese za pristup CRL za MNE eID Root CA certifikate

Adresa objedinjene CRL za MNE eID Root CA certifikate na internet serveru je:

http://ca.elk.gov.me/crl/MNEeIDRootCA.crl.

Adresa objedinjene CRL za MNE eID Root CA certifikate na javnom imeniku je:

ldap://ldap.elk.gov.me/CN=MNE eID Root CA, O=Ministarstvo unutrašnjih poslova,2.5.4.97=VATME-02016010,C=ME?certificateRevocationList;binary

4.10.2 Raspoloživost servisa

Dostupnost CRL i OCSP servisa je 24 sata na dan, 7 dana u nedelji. U slučaju ispada sistema, nastanka okolnosti koje su izvan kontrole certifikacionog tijela ili usled uticaja više sile, usluga će biti dostupna u skladu s planom kontinuiteta poslovanja certifikacionog tijela MUP-a.

Vrijeme odziva na zahtjev za pristup CRL ili dobijanje OCSP odgovora u normalnim radnim uslovima je manje od 1 sekunde.

4.10.3 Dodatne funkcije

Nema odredbi.

4.11 Prestanak korišćenja certifikata

Nije primjenjivo.

4.12 Čuvanje i rekonstrukcija privatnog ključa

TrustME ne čuva i ne omogućava rekonstrukciju privatnih ključeva.

5 Upravne, operativne i fizičke bezbjednosne kontrole

U ovom poglavlju opisane su upravne, operativne i fizičke bezbjednosne kontrole koje primjenjuje certifikaciono tijelo u svom radu u cilju realizacije upravljanja kriptografskim ključevima korijenskog certifikacionog tijela i podređenih certifikacionih tijela.

5.1 Fizičke bezbjednosne kontrole

Certifikaciono tijelo u svojim prostorijama primjenjuje odgovarajuće mehanizme fizičke zaštite prostorija i kontrole pristupa prostorijama certifikacionog tijela. Prostorije certifikacionog tijela čine bezbjedni prostor koji je podijeljen na više sigurnosnih zona u koje je dozvoljen pristup samo licima koja imaju odgovarajuće povjerljive uloge.

Fizičke bezbjednosne kontrole primjenjuju se u jednakoj mjeri i na primarnoj i rezervnoj lokaciji certifikacionog tijela.

5.1.1 Lokacija i konstrukcija sajta

Certifikaciono tijelo MUP-a nalazi se na dvije lokacije u cilju implementiranja robusnosti sistema i nesmetanog rada u slučaju kvara jedne lokacije.

Primarna i rezervna lokacija certifikacionog tijela nalazi se u prostorijama MUP-a Crne Gore u Podgorici.

Prostorije certifikacionog tijela nalaze se u prostoru koji odgovara potrebama izvršenja operacija visoke bezbjednosti. Postoje označene zone sa fizičkom kontrolom pristupa i zaključane kancelarije sa odgovarajućim sefovima.

5.1.2 Fizički pristup

Pristup prostorijama certifikacionog tijela omogućen je primjenom sigurnosnih mehanizama fizičke kontrole pristupa u prostorije i iz jedne zone bezbjednosti u drugu zonu bezbjednosti, uključujući i zonu visoke bezbjednosti.

5.1.3 Električno napajanje i klimatizacija

U prostorijama certifikacionog tijela izvedeno je električno napajanje u skladu sa svim standardima propisanim za električne instalacije i sigurno i kontinuirano napajanje električnom energijom opreme koju certifikaciono tijelo koristi radi pružanja usluga povjerenja.

Sva oprema u certifikacionom tijelu priključena je na jedinice za neprekidno napajanje.

Temperatura i vlažnost vazduha se u prostorijama održava u okviru unaprijed specificiranih intervala pomoću klima uređaja, u skladu sa preporukama proizvođača računarske i druge opreme certifikacionog tijela, kao i u skladu sa principima bezbjednosti i zaštite zdravlja na radu.

Sistemi za napajanje električnom energijom i klimatizacije rade u redundantnom režimu rada.

Sve kritične komponente sistema su vezane na sistem za neprekidno napajanje (UPS) koji ima redundantne komponente. UPS sistemi su vezani na mrežno napajanje i rezervno napajanje (agregat).

5.1.4 Izloženost poplavama i vremenskim nepogodama

Prostorije certifikacionog tijela zaštićene su u razumnoj mjeri od poplava i vremenskih nepogoda.

5.1.5 Prevencija i zaštita od požara

Certifikaciono tijelo primjenjuje sve potrebne mjere i postupke na prevenciji i zaštiti od požara.

5.1.6 Medijumi za čuvanje podataka

Svi medijumi za čuvanje podataka, uključujući i medijume na kojima se nalaze rezervne kopije podataka i softvera čuvaju se na bezbjedan način i na primarnoj i na rezervnoj lokaciji fizički obezbijeđeni i zaštićeni.

5.1.7 Odlaganje nepotrebnih materijala

Svi mediji i dokumentacija koji više nisu potrebni za rad certifikacionog tijela i predstavljaju otpad, prije odlaganja u smeće se fizički uništavaju odgovarajućom metodom. Papirni otpad se propušta kroz mašine za uništavanje papira, a elektronski mediji se moraju mehanički uništiti.

5.1.8 Rezervne kopije

Za smještanje rezervnih kopija podataka i drugih materijala koristi se zaštićena bezbjedna zona na rezervnoj lokaciji koja ima uporediv nivo zaštite sa bezbjednom zonom na primarnoj lokaciji.

5.2 Proceduralne kontrole

Certifikaciono tijelo sprovodi kontrolu svojih zaposlenih radi obezbjeđivanja razumne sigurnosti i povjerljivost i kompetencije zaposlenih.

Osoblje cerifikacionog tijela potpisuje izjavu da će se pridržavati pravne regulative u vezi zaštite podataka, kao i da će zadovoljiti sve postavljene zahtjeve u vezi sa povjerljivošću i svojim zaduženjima u okviru certifikacionog tijela.

5.2.1 Povjerljive uloge

U okviru rada certifikacionog tijela osoblje certifikacionog tijela može imati sledeće povjerljive uloge:

- Rukovodilac poslova Certifikacionog tijela ima sve neophodne privilegije da:
    - Donosi odluke o radu certifikacionog tijela u skladu sa Zakonom o elektronskoj identifikaciji i elektronskom potpisu i podzakonskim aktima
    - Da dodjeljuje odgovarajuće povjerljive uloge osobama certifikacionog tijela
- HSM administrator ima sve neophodne privilegije i prava pristupa da:
    - Vrši administrativne poslove u vezi sa HSM uređajem
    - Kreira operatorske naloge
    - Kreira MBK (Master Backup Key)
- HSM operator ima sve neophodne privilegije i prava pristupa da:
    - Vrši aktivaciju HSM tokena za potrebe drugih aplikacija
    - Kreira ključeve za potrebe drugih aplikacija
    - Kreira i upotrebljava kriptografske ključeve za potrebe CA tijela
- Sistem administrator ima sve neophodne privilegije i prava pristupa da:
    - Instalira i upravlja operativnim sistemima na kojima se koriste aplikacije certifikacionog tijela
    - Upravlja korisničkim nalozima na operativnom sistemu
    - Instalira i administrira SSH servis za objavljivanje CRL liste:

  - Instalira i administrira LDAP servis za objavljivanje CRL liste

- CA Operator ima sve privilegije i prava pristupa da:
  - Kreira i mijenja profile certifikata, profile tokena, profile end entity-ja za potrebe odgovarajućeg CA tijela
  - Kreira certifikaciona tijela
  - Kreira end entity-je (korisnike certifikata)
  - Kreira i izdaje certifikate
  - Kreira i izdaje tokene
  - Izdaje CRL listu za potrebe certifikacionog tijela
  - Kreira profile ključeva
  - Kreira ključeve
  - Kreira i mijenja OCSP respondera
  - Kreira certifikat za potrebe OCSP respondera
- CA Revizor ima sve neophodne privilegije i prava da:
  - Vrši kontrolu audit logova
- Database administrator ima sve neophodne privilegije i prava pristupa da:
  - Instalira i administrira bazu podataka za potrebe CA aplikacija
- Službenik za registraciju ima sve neophodne privilegije i prava pristupa da:
  - Vrši prijem i obradu zahtjeva za potrebe izdavanja elektronskih certifikata na ličnim kartama.

Za potrebe uspostave certifikacionog tijela i sprovođenje procedure generisanja ključeva certifikacionog tijela moguće je definisati i dodatne uloge. Dodatne uloge biće definisane u dokumentu „Procedura generisanja kriptografskih ključeva certifikacionig tijela TrustME“.

5.2.2 Broj osoba koje se zahtijevaju po svakom zadatku

Sve osjetljive operacije u procesu pružanja usluga povjerenja zahtijevaju minimalno dualnu kontrolu. Sve osjetljive operacije certifikacionog tijela ne može izvesti jedan zaposleni samostalno, već je potrebno prisustvo minimalno dva zaposlena.

5.2.3 Identifikacija i autentifikacija osoba za pojedine uloge

Svaka uloga/dužnost definiše odgovarajuće zahtjeve u pogledu identifikacije i autentikacije osobe koja obavlja datu ulogu/dužnost.

Za sve osobe koje imaju povjerljivu ulogu u sistemu certifikacionog tijela MUP-a vrši se bezbjednosna provjera lica. Svaka osoba sa povjerljivom ulogom se kod prijave na aplikaciju identifikuje digitalnim certifikatom ili korisničkim imenom i lozinkom. Dijeljenje naloga i kredencijala između osoblja certifikicanog tijela je zabranjeno.

Osoblje izvršava samo one aktivnosti koje su autorizovane u okviru date uloge kroz ograničenja koje postavlja aplikacija, operativni sistem ili operativne porocedure certifikacionog tijela.

5.2.4 Uloge koje zahtijevaju razdvajanje dužnosti

U cilju razdvajanja povjerljivih uloga u certifikacionom tijelu prava prijave na sisteme certifikacionog tijela moraju biti dodijeljena u skladu sa tabelom 5.1.

PKI Uloga	Korisnički nalog na operativnom sistemu	Korisnički nalog na aplikaciji CA tijela	Korisnički nalog na HSM uređaju	Uloga na aplikaciji CA tijela
Rukovodilac poslova Certifikacionog tijela	Ne	Ne	Ne	Nema uloge
HSM administrator	Ne	Ne	Da	Nema uloge
HSM operator	Ne	Ne	Da	Nema uloge
Sistem administrator	Da	Ne	Ne	Nema uloge
CA Operator	Ne	Da	Ne	Administrator
CA Revizor	Ne	Ne	Ne	Administrator
Database administrator	Da	Ne	Ne	Nema uloge
Službenik za registraciju	Da	Ne	Ne	Nema uloge

Tabela 5.1: Prava prijave na sisteme certifikacionog tijela

U cilju razdvajanja povjerljivih uloga jednoj osobi se mogu dodijeliti uloge prema tabeli 5.2.

	Rukovodilac poslova Certifikacionog tijela	HSM administrator	HSM operator	Sistem administrator	CA Operator	CA Revizor	Database administrator	Službenik za registraciju
Rukovodilac poslova Certifikacionog tijela								
HSM administrator			Ne					
HSM operator		Ne			Ne	Ne		
Sistem administrator								
CA Operator			Ne			Ne		
CA Revizor			Ne		Ne			
Database administrator								
Službenik za registraciju								

Tabela 5.2: Pregled uloga koje se ne smiju kombinovati u sistemu certifikacionog tijela

5.3 Kadrovske bezbjednosne kontrole

5.3.1 Kvalifikacije, iskustvo i provjere

Certifikaciono tijelo izvršava neophodne aktivnosti u cilju provjere biografije, kvalifikacija, kao i neophodnog iskustva u cilju realizacije u okviru konteksta kompetencije specifičnog posla. Zaposleni u certifikacionom tijelu ne smiju biti krivično kažnjavani.

Certifikaciono tijelo sprovodi bezbjednosnu kontrolu zaposlenih u saradnji sa nadležnom jedinicom MUP-a.

Zbog specifičnosti rada na poslovima pružanja usluga povjerenja, certifikacionom tijelu su potrebni ljudi koji su tehnološki i profesionalno kompetentni i koji imaju potrebna znanja iz kriptografije, digitalnog potpisa, PKI sistema, smart kartica, HSM-ova, itd. S tim u vezi certifikaciono tijelo vrši provjeru lica da li posjeduju potrebna znanja.

5.3.2 Provjera povjerljivosti angažovanog osoblja

Nadležni organ radi provjeru povjerljivosti osoblja prema trenutno uspostavljenoj praksi u MUP-u Crne Gore, a u skladu sa zakonom i propisima iz ove oblasti.

5.3.3 Zahtjevi za obučenošću

MUP obezbjeđuje obuku za svoje zaposlene u cilju realizacije funkcija poslovanja certifikacionog tijela i registracionih tijela.

Osoblje certifikacionog tijela prije početka obavljana svojih poslova prolaze edukaciju u skladu sa poslovima koje će obavljati.

Zaposlenima s povjerljivim ulogama u radu na TrustME sistemima garantuje se edukacija i usavršavanje u skladu sa njihovim povjerljivim ulogama.

Edukacija i usavršavanje osoblja s povjerljivim ulogama u radu na TrustME sistemima obuhvata:

- Sigurnosni principi i mehanizmi,
- Svjesnost o sigurnosti,
- Obuka za korišćenje softvera na upotrebi u certifikacionom tijelu i registracionim tijelima,
- Zadaci povezani s povjerljivim ulogama koje će da obavljaju na sistemima certifikacionog tijela,
- Postupci oporavka od nezgode i nastavka poslovanja.

Edukacija Službenika za registraciju u TrustME uključuje:

- Osnovno o certifikatima,
- Tipovi certifikata koje izdaju certifikaciona tijela i područja njihove upotrebe,
- Načini registrovanja Korisnika,
- Uobičajene prijetnje u procesu provjere informacija,
- Rad u aplikacijama koje se koriste u registracionim tijelima,
- Svjesnost o sigurnosti,
- Zaštita ličnih podataka,
- Informacije s kojima je potrebno upoznati Korisnike.

5.3.4 Frekvencija i zahtjevi za ponovnu obuku

Obuka lica u certifikacionom tijelu i registracionim tijelima vrši se periodično i po potrebi radi održavanja potrebnog nivoa znanja zaposlenih za izvršavanje radnih zadataka.

Plan obrazovanja osoba se redovno revidira i u periodima koji nisu duži od godinu dana.

Sprovođenje specijalizacije zaposlenih u certifikacionom tijelu vrši se na godišnjem nivou u skladu sa planom obrazovanja.

5.3.5 Frekvencija i redosljed rotacije poslova

Zamjena lica na pojedinim poslovima definisana je internim pravilima rada.

5.3.6 Kaznene mjere za neovlašćene aktivnosti

MUP ima odgovarajuće mjere za kažnjavanje zaposlenih za neovlašćene aktivnosti, neovlašćeno korišćenje autoriteta, kao i neovlašćeno korišćenje sistema u cilju sprovođenja sankcija za određeno neposlovno i rizično ponašanje, a koje može biti različito u zavisnosti od različitih okolnosti.

Mjere protiv zaposlenih koji učine neovlašćene aktivnosti određuju se u disciplinskom postupku.

5.3.7 Zahtjevi za spoljne saradnike

Spoljni saradnici predmet su istih provjera radi zaštite privatnosti i uslova povjerljivosti kao i zaposleni u certifikacionom tijelu.

Svi koji rade na ovaj način su obavezni potpisati sporazum o tajnosti (non-disclosure agreement).

5.3.8 Dokumentacija za potrebe osoblja

Certifikaciono tijelo čini dostupnom svu dokumentaciju osoblju koja im je potrebna u obavljanju njihovih poslova u skladu sa njihovom povjerljivom ulogom i internim pravilima rada.

5.4 Procedure upravljanja revizijskih dnevnika

Procedure audit logovanja uključuju logovanje događaja i reviziju sistema i implementirane su za svrhu održavanja bezbjednog okruženja.

5.4.1 Tipovi zabilježenih događaja

Certifikaciono tijelo zapisuje događaje koji uključuju, ali nisu ograničeni na operacije vezane za životni ciklus certifikata, pokušaje pristupa sistemu, kao i zahtjeve dostavljene sistemu.

5.4.2 Frekvencija procesiranja logova

Certifikaciono tijelo čuva audit logove u realnom vremenu, koji se kasnije po potrebi procesiraju.

5.4.3 Period čuvanja audit logova

Certifikaciono tijelo procesira i arhivira audit logove na sedmičnom nivou, koji se čuvaju u periodu od najmanje deset (10) godina od trenutka nastanka audit loga.

5.4.4 Zaštita audit logova

Audit logovi se samo mogu vidjeti od strane autorizovanog osoblja. Integritet audit loga koji nastaje iz softvera certifikacionog tijela zaštićen je primjenom odgovarajućih kriptografskih metoda.

5.4.5 Procedure backup-a audit logova

Certifikaciono tijelo implementira procedure backup-a audit logova.

5.4.6 Sistem sakupljanja audit logova

Certifikaciono tijelo sakuplja i čuva audit logove u realnom vremenu.

5.4.7 Obavještavanje lica koje je prouzrokovao događaj

Lice koje je prouzrokovalo određeni audit događaj se ne obavještava o samoj audit aktivnosti.

5.4.8 Procjena ranjivosti sistema

Certifikaciono tijelo periodično organizuje procjenu ranjivosti sistema.

5.5 Arhiviranje zapisa/logova

Opšte odredbe koje se odnose na čuvanje logova različitih komponenti certifikacionog tijela definisane su ovim poglavljem.

5.5.1 Tipovi arhiviranih zapisa

Zapisi koji se čuvaju:

- Zapisi o izdatim certifikatima
- Informacije o podnešenim zahtjevima za izdavanje certifikata
- Druga potrebna dokumentacija.

5.5.2 Period čuvanja arhive

Elektronski dnevnici čuvaju se najmanje deset (10) godina.

Certifikati i statusi certifikata čuvaju se trajno.

Ugovore sa korisnicima, dokumentaciju korisnika i korespodenciju trećih lica najmanje 10 godina.

5.5.3 Zaštita arhive

Uslovi za zaštitu arhive uključuju:

- Zapise koje samo zaposleni kojima su pridružene dužnosti čuvanja podataka mogu da vide i arhiviraju.
- Zaštitu u odnosu na modifikaciju arhive, kao što je čuvanje podataka na medijumu na koga se može upisati samo jednom.
- Zaštitu u odnosu na brisanje arhive.
- Zaštitu u odnosu na kvarenje karakteristika medijuma vremenom na kojima se arhiva čuva, kao na primjer realizacija zahtjeva da se podaci periodično migriraju na svježe medijume.

5.5.4 Procedura pravljenja rezervnih kopija arhive

Certifikaciono tijelo pravi rezervne kopije arhive periodično i čuva dvije odvojene kopije arhive na primarnoj i rezervnoj lokaciji.

5.5.5 Zahtjevi za vremenski pečat arhiviranih podataka

Arhivirani podaci sadrže vrijeme dobijeno sa sistema u okviru podataka. To vrijeme nije kriptografski vremenski pečat (žig).

5.5.6 Sistem sakupljanja zapisa

Certifikaciono tijelo sakuplja zapise i logove koji se arhiviraju po interno propisanoj proceduri.

5.5.7 Procedure za dobijanje i verifikaciju informacija iz arhive

Pristup zapisima iz arhive imaju samo lica ovlašćena za pristup podacima iz arhive. Pristup podacima arhiviranim u sigurnim zonama imaju samo ovlašćena lica, uz dualnu kontrolu.

Verifikacija podataka iz arhive obavlja se provjerom njihovog integriteta.

Arhivirani podaci u elektronskom obliku se po potrebi upoređuju s pripadajućom kopijom.

5.6 Obnova CA certifikata

U slučaju isteka certifikata certifikacionog tijela ili opoziva certifkata certifikacionog tijela certifikaciono tijelo vrši generisanje novog para ključeva certifikacionog tijela i formira certifikat za novogenerisani privatni ključ.

Ceritikaciono tijelo distribuira svoj novi certifikat svim korisnicima i trećim licima, kao i u slučaju prvobitnog generisanog certifkata certifikacionog tijela putem sopstvenog repozitorijuma.

5.7 Kompromitovanje i oporavak sistema poslije nepredviđenih situacija

5.7.1 Procedure za postupanje u incidentnim i kompromitujućim situacijama

Internim pravilima rada dokumentovane su procedure koje treba izršiti pri rješavanju incidenata, kao i izvještavanje usled potencijalne kompromitacije privatnog ključa certifikacionog tijela.

5.7.2 Računarski resursi, softver ili podaci koji su oštećeni

Certifikaciono tijelo dokumentuje procedure oporavka koje se koriste ukoliko su računarski resursi, softver ili podaci neispravni ili se sumnja da su neispravni.

5.7.3 Procedure koje se sprovode kod kompromitacije privatnog ključa

U slučaju saznanja da je došlo do kompromitacije privatnog ključa korijenskog certifikacionog tijela ili podređenog certifikacionog tijela MUP će odmah po saznaju prekinuti sa upotrebom potencijalno kompromitovanog privatnog ključa.

U slučaju potvrde kompromitacije privatnog ključa MUP preko TrustME PMA donosi odluku o opozivu pripadajućeg certifikata certifikacionog tijela i svih certifikata koje je izdalo to certifikaciono tijelo.

O opozivu certifikata MUP će obavijestiti sve učesnike PKI putem izdavanja obavještenja na internet stranicama TrustME repozitorijuma.

Nakon ustanovljavanja okolnosti zbog kojih je došlo do kompromitacije privatnog ključa certifikacionog tijela MUP će preduzeti mjere na otkljanjanju tih okolnosti radi sprečavanja ponovne kompromitacije privatnog ključa.

Certifikaciono tijelo će organizovati novu formalnu cermoniju uspostave certifikacionog tijela i generisanja para asimetričnih ključeva.

5.7.4 Mogućnosti kontinuiteta poslovanja nakon katastrofe

Plan kontinuiteta poslovanja se implementira da osigura nastavak poslovanja nakon prirodne ili druge katastrofe.

5.8 Završetak rada

Certifikaciono tijelo će u slučaju prestanka rada:

- Obavijestiti sve korisnike putem internet stranica i nadležni organ državne uprave najmanje šest mjeseci prije planiranog prestanka rada,

- Korisnicima kojima je već izdao certifikate obezbijediće nastavak pružanja usluga povjerenja kod drugog davaoca usluga povjerenja i dostaviće mu svu dokumentaciju u vezi sa obavljanjem usluga povjerenja,
- U slučaju da ne obezbijedi nastavak davanja usluga povjerenja kod drugog davaoca usluga povjerenja opozvaće sve izdate certifikata i u najkraćem mogućem roku, a najkasnije u roku do 48 sati o tome obavijestiti nadležni organ državne uprave i dostaviti mu svu dokumentaciju u vezi sa obavljenim uslugama,
- Osiguraće raspoloživost liste opozvanih certifikata u periodu od godinu dana posle opoziva svih certifikata,
- Arhiviraće sve podatke u skladu sa periodom propisanim odgovarajućim zakonom od zadnjeg dana rada certifikacionog tijela.

6 Tehničke bezbjednosne kontrole

Certifikaciono tijelo MUP-a primjenjuje tehničke bezbjednosne mjere u cilju zaštite kripotografskih kljlučeva i aktivacionih podataka. Kripotografski ključevi koji se štite mjerama i postupcima opisanim u ovom poglavlju mogu pripadati samom certifikacionom tijelu. Primjena ovih mjera kritična je u smislu osiguranja da kriptografski ključevi i aktivacioni podaci budu zaštićeni i da se koriste isključivo od strane autorizovanih zaposlenih i servisa.

Ovim poglavljem definisane su sve mjere, postupci i metodi, i druge tehničke bezbjednosne kontrole koje se primjenjuju prilikom upravljanja ključevima i certifikatima. Tehničke kontrole uključuju životni ciklus bezbjednosnih kontrola kao i operativne bezbjednosne kontrole.

6.1 Generisanje i instalacija asimetričnog para ključeva

6.1.1 Generisanje asimetričnog para ključeva

Certifikaciono tijelo prilikom generisanja i upravljanja sopstvenim privatnim ključevima primjenjuje sve odredbe Zakona o elektronskoj identifikaciji i elektronskom potpisu i pravilnicima koji proizilaze iz njega i primjenjuje sve javne, internacionalne i evropske standarde u vezi bezbjednih i pouzdanih sistema.

Certifikaciono tijelo primjenjuje sve mjere, postupke i metode propisane ovim dokumentima u cilju bezbjednog i pouzdanog generisanja privatnih ključeva i u cilju sprečavanja kompromitacije ili neautorizovanog korišćenja sopstvenih privatnih ključeva.

Certifikaciono tijelo generiše sledeće parove asimetričnih ključeva:

- U formalnoj proceduri uspostave korijenskog certifikacionog tijela generiše se par asimetričnih ključeva na hardverskom bezbjednosnom modulu (HSM – Hardware Security Module) za potrebe korijenskog certifikacionog tijela,

- U formalnoj proceduri uspostave podređenog certifikacionog tijela generiše se par asimetričnih ključeva na hardverskom bezbjednosnom modulu (HSM – Hardware Security Module) za potrebe podređenog certifikacionog tijela,

Za potrebe međusobne komunikacije softverskih i hardverskih komponenti certifikacionog tijela generišu se potrebni simetrični i asimetrični ključevi radi zaštite mrežne komunikacije između komponenti sistema.

Certifikaciono tijelo koristi bezbjedan proces generisanja privatnih ključeva za korijensko i podređeno certifikaciono tijelo u skladu sa dokumentovanom procedurom. Certifikaciono tijelo distribuira dijeljene tajne za svoje privatne ključeve i vlasnik je privatnih ključeva i posjeduje autoritet da prenese odgovarajuće dijeljene tajne na autorizovane nosioce dijeljenih tajni, odnosno lica sa provjerljivim ulogama u okviru certifikacionog tijela MUP-a.

Privatni ključ korijenskog certifikacionog tijela koristi se za elektronsko potpisivanje certifkata podređenog certifikacionog tijela, odgovarajuće liste opozvanih certifikata i odgovora OCSP servisa za ovo certifikaciono tijelo i u druge svrhe se ne smije koristiti.

Privatni ključ podređenog certifikacionog tijela koristi se za elektronsko potpisivanje certifikata za elektronsku identifikaciju i certifikata za kvalifikovani elektronski potpis koji se izdaju korisnicima na elektronskoj javnoj ispravi, odgovarajuće liste opozvanih certifikata i odgovora OCSP servisa za ovo certifikaciono tijelo i u druge svrhe se ne smije koristiti.

Privatni ključevi koji se izdaju korisnicima na elektronskoj javnoj ispravi korisnici koriste u skladu sa Zakonom o elektronskoj identifikaciji i elektronskom potpisu i CP i CPS dokumentima.

6.1.2 Isporuka privatnog ključa

Privatni ključevi certifikacionih tijela (korijensko i podređeno certifikaciono tijelo) se generišu u okviru procedure uspostavljanja certifikacionog tijela.

Postupak isporuke privatnog ključa za korinike (građane Crne Gore) opisan je u CPS dokumentu.

6.1.3 Dostavljanje javnog ključa do certifikacionog tijela

Dostava javnog ključa podređenog certifikacionog tijela vrši se u okviru procedure uspostavljanja certifikacionog tijela.

Postupak dostave javnog ključa za korinike (građane Crne Gore) opisan je u CPS dokumentu.

6.1.4 Dostavljanje javnog ključa certifikacionog tijela trećim licima

Certifikaciono tijelo dostavlja svoje javne ključeve korijenskog i podređenog certifikacionog tijela, u obliku X.509v3 certifikata putem svog online repozitorijuma kome mogu da pristupaju svi korisnici i treća lica.

6.1.5 Dužine ključeva

Za potrebe korijenskog certifikacionog tijela MNE eID Root CA koristi se RSA asimetrični par ključeva dužine 3072 bita i periodom validnosti certifikata od 30 godina i 3 mjeseca. Za formiranje digitalnog potisa koristi se SHA256/RSA kombinacija hash i algoritma za potpisivanje u PKCS#1 1.5 formatu digitalnog potpisa.

Za potrebe podređenog certifikacionog tijela MNE eID CA1 koristi se RSA asimetrični par ključeva dužine 3072 bita i periodom validnosti certifikata od 20 godina i 3 mjeseca. Za formiranje digitalnog potpisa koristi se SHA256/RSA kombinacija hash i algoritma za potpisivanje u PKCS#1 1.5 formatu digitalnog potpisa.

Za potrebe elektronske identifikacije i formiranja kvalifikovanog elektronskog potpisa korisnika korisiti se RSA asimetrični par ključeva dužine 2048 bita i periodom validnosti certifikata do 10 godina.

Certifikaciono tijelo zadržava pravo na izmjenu gore navedenih kombinacija algoritama i dužina ključeva ukoliko se u kriptografskoj teoriji i praksi pokažu slabosti navedenih algoritama i svjetska kriptografska javnost preporuči druge algoritme, kao i u slučajevima definisanja novih standarda za hash i asimetrične algoritme.

6.1.6 Generisanje kriptografskih parametara i provjera kvaliteta

Parovi asimetričnih kriptografskih ključeva se generišu pomoću hardverskih generatora slučajnih brojeva koji su realizovani na kriptografskim hardverskim uređajima:

- HSM – za parove ključeva za certifikaciona tijela i potpis odgovora OCSP servisa,
- QSCD uređaj (smart kartica, elektronska javna isprava) – za korisničke ključeve za elektronsku identifikaciju i kvalifikovani elektronski potpis.

Kvalitet načina generisanja pomenutih kriptografskih parametara isključivo zavisi od kvaliteta hardverskog generatora slučajnih brojeva na HSM-ovima i QSCD uređaja.

HSM uređaj i QSCD uređaj (elektronska javna isprava) certifikovani su po standardima propisanim Zakonom o elektronskoj identifikaciji i elektronskom potpisu. QSCD uređaj nalazi se na evropskoj listi uređaja za pouzdano formiranje elektronskog potpisa.

6.1.7 Namjena upotrebe ključeva (X.509 keyUsage)

Certifikati koje izdaju korijensko i podređeno certifikaciono tijelo MUP-a mogu se naći sledeće vrijednosti u ekstenzijama „Key Usage“ i „Extended Key Usage“.

	Key Usage				Extended Key Usage	
	Certificate Signing	CRL Signing	Digital signature	Non-Repudiation	Client authentication	OCSP Signing
Certifikat korijenskog certifikacionog tijela	X	X				
Certifikat podređenog certifikacionog tijela	X	X				
Certifikat za OCSP servis			X			X
Certifikata za elektronsku identifikaciju			X		X	
Certifikat za kvalifikovani elektronski potpis				X		

Tabela 6.1. Vrijedonsti Key Usage i Extended Key Usage ekstenzija u certifikatima koje izdaje certifikaciono tijelo MUP-a

6.2 Zaštita privatnog ključa i kontrola kriptografskog hardverskog modula

Certifikaciono tijelo MUP-a koristi odgovarajuće kriptografske uređaje za upravljanje životnim vijekom kriptografskih ključeva certifikaciongo tijela. Certifikaciono tijelo koristi Hardverski bezbjednosni modul – HSM koji je u skladu sa svim relevantnim standardima zaštite kriptografskih uređaja.

6.2.1 Standardi i kontrole kriptografskog hardverskog modula

Generisanje privatnog ključa korijenskog i podređenog certifikacionog tijela se vrši u okviru bezbjednog kriptografskog uređaja koji zadovoljava odgovarajuće zahtjeve u skladu sa međunarodnim standardom FIPS 140-2 L3. Ispunjavanje ovog standarda garantuje, između ostalog, da je bilo koji pokušaj narušavanja integriteta uređaja ili kriptografske memorije istovremeno detektovan.

HSM uređaji ne smiju da napuštaju bezbjednu zonu certifikacionog tijela izuzev rijetkih prilika unaprijed definisanih premještanja i preseljenja. Certifikaciono tijelo vodi evidenciju u vezi svih tih premještanja ili preseljenja.

U slučaju da odgovarajući HSM zahtjeva održavanje ili popravku, koja se ne može izvršiti u okviru bezbjedne zone certifikacionog tijela, oni se onda bezbjedno prenose do njihovog proizvođača uz poštovanje svih neophodnih bezbjednosnih mjera.

6.2.2 *k* od *n* distribucija odgovornosti kontrole privatnog ključa

Generisanje privatnog ključa certifikacionog tijela zahtijeva kontrolu više osoba sa povjerljivim ulogama u okviru certifikacionog tijela MUP-a. S tim u vezi certifikaciono tijelo implementira politiku 2 od 3 distribucije odgovornosti kontrole privatnog ključa.

Prilikom generisanja ili upotrebe kriptografskog ključa certifikacionog tijela potrebno je da minimalno dvije osobe sa povjerljivim ulogama autorizuju generisanje ili upotrebu privatnog ključa. Autorizacija se vrši aktivacijom HSM slota na kojem se generiše i čuva privatni ključ. Kada se slot aktivira on ostaje aktiviran sve dok se eksplicitno ne deaktivira, ugasi HSM uređaj ili se ugasi aplikacija certifikacionog tijela.

Privatni ključ certifikacionog tijela se koristi pod uslovima definisanim u okviru ***k*** od ***n*** kontrole od strane više zaposlenih sa povjerljivim ulogama.

Prije nego što nosilac aktivacionih podataka prihvati podatke (upotreba PIN-a, korisničkog naloga i pripadajuće lozinke, upotreba smart kartice i pripadajućeg PIN-a) on mora lično da se upozna sa kreiranjem, zamjenom i upotrebom aktivacionih parametara.

Nosilac aktivacioni parametara može primiti aktivacione parametre na fizičkom medijumu, kao što je određeni hardverski kriptografski modul (na primjer smart kartica) koji je odobren za korišćenje od strane certifikacionog tijela. Certifikaciono tijelo čuva pisane zapise u vezi distribucije dijeljene tajne.

Certifikaciono tijelo koristi dijeljene dijeljene tajne za aktivaciju svog privatnog ključa i ima mogućnost da izmijeni način distribucije smart kartica u slučaju da nosioci smart kartice zahtijevaju da budu zamijenjeni u njihovim rolama kao nosioci smart kartica.

6.2.3 Deponovanje (key escrow) privatnog ključa

Nije dozvoljeno deponovanje privatnog ključa..

6.2.4 Rezervna kopija i čuvanje privatnog ključa

Certifikaciono tijelo čuva svoje privatne ključeve u skladu sa zahtjevima iskazanim u standardu FIPS 140-2 L3.

Procedura čuvanja privatnog ključa zahtijeva od strane autorizovanog osoblja sa povjerljivim ulogama višestruke i odgovarajuće kontrole.

Hardverski i softverski mehanizmi koji štite privatne ključeve obezbjeđuje bezbjedni kriptografsku uređaj. Mehanizmi zaštite privatnog ključa certifikacionog tijela su u najmanju ruku ekvivalentne snage kao i sami privatni ključevi koji se štite, a po specifikaciji proizvođača bezbjednog kriptografskog modula.

Certifikaciono tijelo vrši pravljenje rezervne kopije privatnog ključa u skladu sa procedurom definisanom pratećom dokumentacijom HSM proizvođača što je definisano internim pravilima rada.

Kopije privatnog ključa certifikacionog tijela se čuvaju na eksternoj memoriji (flash memorija, CD, ...) na sigurnom mjestu u šifrovanom obliku u dva primjerka. Jedan primjerak čuva se na primarnoj lokaciji, dok se drugi čuva na rezrevnoj lokaciji.

6.2.5 Arhiviranje privatnog ključa

Ne vrši se arhiviranje privatnog ključa.

6.2.6 Transfer privatnog ključa na hardverski kriptografski modul

Procedura bezbjednog eksportovanja privatnog ključa certifikacionog tijela u cilju rezervne kopije, kao i procedura bezbjednog importa arhiviranog privatnog ključa na HSM su opisane u posebnim internim pravilima rada i dokumentaciji proizvođača bezbjednog kriptografskog modula.

6.2.7 Čuvanje privatnog ključa na hardverskom kriptografskom modulu

Kada se privatni ključ certifikacionog tijela nalazi i koristi na HSM uređaju, on se čuva u šifrovanom obliku u memoriji HSM uređaja.

6.2.8 Metoda aktivacije privatnog ključa

Nosioci dijeljenih tajni certifikacionog tijela imaju zadatak da aktiviraju i deaktiviraju privatni ključ. Privatni ključ je tada aktivan sve dok se ključ ne deaktivira.

6.2.9 Metoda deaktiviranja privatnog ključa

Privatni ključe se deaktivira gašenjem ili restartom aplikacije certifikacionog tijela, gašenjem ili restartom HSM uređaja ili deaktivacijom privatnog ključa putem logoff mehanizma.

6.2.10 Metoda uništenja privatnog ključa

Privatni ključ certifikacionog tijela će biti uništen na kraju svog životnog ciklusa brisanjem sa bezbjednog kriptografskog uređaja i brisanjem svih postojećih rezervnih kopija privatnog ključa.

6.2.11 Nivo sigurnosti kriptografskih modula

Kao što je definisano u odjeljku 6.2.1.

6.3 Drugi aspekti upravljanja parom ključeva

6.3.1 Arhiviranje javnog ključa

Certifikaciono tijelo arhivira javne ključeve pojedinačnih certifikacionih tijela (korijensko i podređeno certifikaciono tijelo).

6.3.2 Periodi validnosti certifikata i privatnog ključa

Rok važenja certifikata po vrstama je definisan u Tabeli 6.1.

Certifikat	Rok
Certifikat korijenskog certifikacionog tijela: MNE eID Root CA	30 godina i 3 mjeseca
Certifikat podređenog certifkacionog tijela: MNE eID CA1	20 godina i 3 mjeseca
Certifikat za kvalifikovani elektronski potpis	do 10 godina
Certifikat za elektronsku identifikaciju	10 godina
Certifikat za OCSP servis	3 mjeseca

Tabela 6.1. Periodi važenja certifikata

Certifikat podređenog certifikacionog tijela izdaje se s vremenom važenja koje ne prelazi perioda važenja certifikata korijenskog certifikacionog tijela.

Vremenski period važenja privatnog ključa jednak je vremenskom periodu važenja pripadajućeg certifikata. Nije dozvoljena upotreba privatnih ključeva nakon isteka perioda važenja pripadajućih certifikata, nakon opoziva certifikata ili za vrijeme dok je certifikat suspendovan.

6.4 Aktivacioni podaci

6.4.1 Generisanje i instalacija aktivacionih podataka

Certifikaciono tijelo bezbjedno procesira aktivacione podatke pridružene svim privatnim ključevima u svom PKI sistemu.

6.4.2 Drugi aspekti u vezi aktivacionih podataka

Ovo poglavlje nije primjenljivo u okviru ovog dokumenta.

6.5 Bezbjednosne kontrole računara

6.5.1 Specifični zahtjevi za bezbjednost računara

Certifikaciono tijelo primjenjuje mehanizme kontrole pristupa računarskim sistemima koji se koriste u okviru certifikacionog tijela. Računarska i komunikaciona oprema koja se koristi u okviru certifikacionog tijela fizički je obezbijeđena u prostorijama certifkacionog tijela.

Certifikaciono tijelo koristi i mehanizme logičke kontrole pristupa putem firewall uređaja.

Neautorizovan pristup opremi nije dozvoljen. Kritične softverske i hardverske komponente certifikacionog tijela mogu startovati samo dvije ili više ovlašćenih osoba koja posjeduju odgovarajuće smart kartice i koja znaju njihove PIN-ove ili odgovarajuće lozinke.

6.5.2 Rangiranje bezbjednosti računara

Računari i operativni sistemi koje koristi certifikaciono tijelo su komercijalni proizvodi koji su dodatno bezbjednosno ojačani.

6.6 Životni ciklus tehničkih bezbjednosnih kontrola

6.6.1 Kontrole razvoja sistema

Certifikaciono tijelo nadgleda i kontroliše razvoj sistema za proizvodnju dokumenata i izdavanje certifikata.

6.6.2 Kontrole upravljanja bezbjednošću

Certifikaciono tijelo nadgleda i kontroliše bezbjednost i upravljanje bezbjednošću sistema za proizvodnju dokumenata i izdavanje certifikata.

6.6.3 Životni ciklus bezbjednosnih kontrola

Nije primjenljivo.

6.7 Mrežne bezbjednosne kontrole

Sigurnost računarske mreže certifikacionog tijela zasnovana je na konceptu segmentacije mreže na mrežne zone različitih nivoa. Mrežne zone razgraničavaju se firewall-ovima koji propuštaju samo neophodan mrežni saobraćaj. Na sve sisteme locirane unutar jedne mrežne zone primjenjuju se iste sigurnosne mjere.

Mrežni segment na kom se nalaze radne stanice za administraciju certifikacionog tijela firewall-om je odvojen od ostalih mrežnih segmenata i računara koji se nalaze u tim mrežnim segmentima.

Oprema za zaštitu računarske mreže evidentira tok saobraćaja i pokušaje pristupa servisima i LDAP servisu javnog imenika certifikaciongo tijela. Samo ovlašćeno osoblje sa povjerljivim ulogama certifikacionog tijela ima administratorska ovlašćenja za podešavanje i upravljanje opremom za zaštitu računarske mreže. Udaljeno podešavanje opreme za zaštitu računarske mreže nije dozvoljeno.

Nepotrebne komunikacije, nalozi, portovi, protokoli i servisi su eksplicitno zabranjeni ili deaktivirani.

Interna računarska mreža certifikacionog tijela zaštićena je od neovlašćenog pristupa, uključujući pristup korisnika i trećih lica.

Svi kritični sistemi za davanje usluga povjerenja smješteni su u sigurnoj zoni certifikacionog tijela i raspoređeni su u više različitih sigurnosnih mrežnih zona.

Mrežne komponente certifikacionog tijela čuvaju se u fizički i logički sigurnom okruženju i usaglašenost njihove konfiguracije periodično se provjerava.

6.8 Vremenski pečat

Certifikaciono tijelo ne koristi vremenski pečat, s tim u vezi ovo poglavlje nije primjenljivo u okviru ovog dokumenta.

7 Sadržaj certifikata, lista opozvanih certifikata i OCSP profili

7.1 Profil certifikata

Ovo poglavlje sadrži opis profila certifikata, listu opozvanih certifikata (CRL) i odgovora OCSP servisa koje certifikaciono tijelo kao davalac usluga povjerenja kroz MNE eID Root CA i MNE eID CA1 certifikaciona tijela izdaje u skladu sa opsegom ovog dokumenta.

Profili certifikata iz opsega ovog dokumenta koje izdaje podređeno CA tijelo usaglašeni su s standardima ETSI EN 319 411-1, ETSI EN 319 411-2 i ETSI EN 319 412-1, ETSI EN 319 412-2, ETSI EN 319 412-3 i ETSI EN 319 412-4.

Podređeno certifikaciono tijelo izdaje certifikate prema definisanim profilima. Zavisno o namjeni certifikata, nivou sigurnosti i načinu čuvanja pripadajućih privatnih ključeva, svaki tip certifikata ima definisan jedinstveni OID politike certifikacije, a pored tog OID-a sadrži i odgovarajući ETSI OID politike certifikacije, ako je takav OID primjenjiv.

7.1.1 Verzija certifikata

Certifikati su u skladu s verzijom 3 prema X.509 specifikaciji.

7.1.2 Ekstenzije certifikata

Dokument s opisom profila certifikata iz opsega ovog dokumenta i opisom profila MNE eID Root CA i podređenog MNE eID CA1 certifikata dostupan je na internet stranicama TrustME repozitorijuma i direktno putem internet adrese https://ca.elk.gov.me/cpcps.

7.1.3 Identifikator objekta (OID) algoritama

Algoritmi s pripadajućim OID identifikatorima za sve certifikate koje izdaje TrustME prikazani su u Tabeli 7.1.

Algoritam	OID
sha256WithRSAEncryption	1.2.840.113549.1.1.11
rsaEncryption	1.2.840.113549.1.1.1

Tabela 7.1. Algoritmi s pripadajućim OID identifikatorima

7.1.4 Forme imena

Oblici naziva za MNE eID Root CA i za podređeni MNE eID CA1 opisani su u tački 1.3.1. ovog dokumenta. Oblici naziva za certifikate koje izdaje podređeni MNE eID CA1 opisani su u tačkama 3.1.1. i 3.1.4. CPS dokumenta.

7.1.5 Ograničenja za ime

Specijalni znaci čije korišćenje u imenima nije dozvoljeno su: ? (upitnik), \ (backslash), / (slash), # (taraba), $ (dolar), % (procenat), = (jednako), + (plus), | (uspravna crta), ; (tačka-zarez), < (manje), > (veće) i , (zarez). Iste je potrebno izostaviti ili zamijeniti drugim znacima.

7.1.6 Identifikator objekta (OID) politika certifikacije

Ekstenzija Certificate Policies certifikata sadrži odgovarajuće TrustME i ETSI OID-ove. U tabeli 1.1. tačke 1.1.2. ovog dokumenta naveden je popis tipova certifikata i pripadajući TrustME i ETSI OID-ovi opštih pravila certifikovanja u ekstenziji Certificate Policies.

7.1.7 Upotreba ekstenzije Policy Constraints

Ekstenzija *Policy Constraints* se ne koristi.

7.1.8 Sintaksa i semantika kvalifikatora politika certifikacije

Kvalifikator politika certifikacije u ekstenziji Certificate Policies sadrži link u URI formatu koji sadrže internet adresu ovog dokumenta. Dokument se nalazi na naznačenoj lokaciji obavezno u verziji na crnogorskom jeziku, a može biti preveden na engleski jezik.

7.1.9 Procesuiranje semantike za kritičnu ekstenziju Politike Certifikovanja

Nema odredbi.

7.2 Profil CRL

Profil CRL u skladu je s dokumentom IETF RFC 5280.

7.2.1 Broj(evi) verzije

CRL su u skladu s verzijom 2 prema X.509 specifikaciji.

7.2.2 CRL i ekstenzije unosa u CRL

Ekstenzije CRL koje se koriste u CRL listama i u elementima unosa CRL lista koje izdaje podređeno certifikaciono tijelo definisane su u skladu sa standardom RFC5280.

7.3 OCSP profil

Profil odgovora OCSP servisa usaglašen je s dokumentom IETF RFC 6960.

7.3.1 Broj(evi) verzije

Profil odgovora OCSP servisa u skladu je sa verzijom 1 prema dokumentu IETF RFC 6960.

7.3.2 OCSP ekstenzije

Ekstenzije odgovora OCSP servisa prikazane su u tabeli 7.2.

Ekstenzije	Vrijednost
Nonce	Vrijednost Nonce iz zahtjeva za status certifikata.
Extended Revoked Definition	Kod razloga opoziva certifikata (*Reason code*)

Tabela 7.2. Ekstenzije odgovora OCSP servisa

8 Provjera usaglašenosti i druge procjene

Provjera rada certifikacionog tijela MUP-a kao kvalifikovanog davaoca usluga povjerenja regulisana je Zakonom o elektronskoj identifikaciji i elektronskom potpisu [2] koji implementira regulativu (EU) br. 910/2014 [1], a sprovodi ga nadležni organ državne uprave.

Provjeru rada certifikacionog tijela kvalifikovanog davaoca usluga povjerenja u području praćenja sprovođenja propisa o zaštititi ličnih podataka sprovodi nadležni državni organ.

Provjera usaglašenosti rada obavlja se u cilju potvrđivanja da certifikaciono tijelo kao kvalifikovani davalac usluga povjerenja i usluge izdavanja certifikata koje certifikaciono tijelo pruža ispunjava zahtjeve utvrđene Zakonom o elektronskoj identifikaciji i elektronskom potpisu, regulativom (EU) br. 910/2014 [1] i standardom ETSI EN 319 411-2.

8.1 Frekvencija ili okolnosti kada se vrši revizija

TrustME će u skladu sa zakonom peroidično vršiti internu provjeru usaglašenosti svojih CP i CPS. Nadležni organ za provjeru usaglašenosti periodično će vršiti reviziju.

Certifikaciono tijelo organizuje svoj rad u skladu sa najznačajnijim pravnim aktima koji regulišu rad davalaca usluga povjerenja u Crnoj Gori, prije svega Zakona o elektronskoj identifikaciji i elektronskom potpisu i Zakona o ličnoj karti i pravilnicima koji proizilaze iz njih, a odnose se na usluge povjerenja.

Izdavanje certifikata usaglašeno je i sa eIDAS regulativom (Regulativa EU br. 910/2014 Evropskog parlamenta i Savjeta).

Certifikaciono tijelo organizovaće bar jednom godišnje sopstvenu provjeru usaglašenosti ovog dokumenta i svog rada sa odgovarajućim propisima.

8.2 Identitet/kvalifikacije revizora

Provjeru usaglašenosti rada certifikacionog tijela vrši nadležni državni organ u skladu sa Zakonom o elektronskoj identifikaciji i elektronskom potpisu i odgovarajućim podzakonskim aktima.

Certifikaciono tijelo takođe vrši redovne interne provjere usklađenosti svog rada pri čemu provjeru vrše lica zaposlena u certifikaconom tijelu koja raspolažu adekvatnim znanjima i poznavanjem sledećih oblasti:

- Zakona o elektronskoj identifikaciji i elektronskom potpisu,
- Standarda EN 319 411-1 i EN 319 411-2,
- Posjeduju znanja iz PKI oblasti i informacione sigurnosti,
- Poznaju ostale propise koji regulišu ovu oblast.

Interne provjere sprovodi Odjeljenje za internu reviziju u MUP-u, ili eksterni revizor kojeg angažuje MUP na predlog TrustME PMA.

8.3 Odnos revizora prema ocjenjivanom subjektu

Nadležni organ za ocenu usaglašenosti i angažovani revizor su nezavisni od certifikacionog tijela MUP-a i sopstvenog sistema ocjenjivanja certifikacionog tijela. Angažovani revizor treba da je oslobođen konflikta interesa.

Lica angažovana na internoj provjeri usaglašenosti ne ocjenjuju usaglašenost iz sopstvene oblasti odgovornosti.

8.4 Teme pokrivene u procesu procjenjivanja

Provjera usaglašenosti rada certifikacionog tijela obuhvata, ali se ne ograničava samo na sledeće oblasti pružanja usluga povjerenja:

- Kompletnost i tačnost dokumentacije
- Organizacione procese, metode i procedure,
- Tehničke procese i procedure
- Mjere iz oblasti informacione bezbjednosti
- Mjere iz oblasti fizičke bezbjednosti
- Usluge povjerenja koje pruža certifikaciono tijelo

Na zahtjev revizora certifikaciono tijelo pružiće pristup svim prostorima u kojima certifikaciono tijelo vrši usluge povjerenja.

8.5 Aktivnosti preduzete u slučaju neusaglašenosti

Certifikaciono tijelo uskladiće svoj rad sa preporukama i nalazima internog revizora ili revizora angažovanog od strane nadležnog organa.

8.6 Objavljivanje rezultata

Rezultati interne revizije povjerljive su prirode i ne objavljuju se javno.

O izvedenoj reviziji od strane nadležnog organa certifikaciono tijelo sastaviće izvještaj i dostaviti ga nadležnom organu u zakonskom roku. Izvod iz tog izvještaja certifkaciono tijelo objaviće na internet stranicama svog repozitorijuma. Neusaglašenosti utvrđene tokom revizije smatraju se povjerljivim informacijama i one se ne objavljuju.

9 Drugi poslovni i pravni aspekti

9.1 Cijene

9.1.1 Cijene izdavanja certifikata

Certifikaciono tijelo MUP-a izdaje certifikate koji su predmet ovog dokumenta u procesu izdavanje elektronske javne isprave, pa stim u vezi certifikaciono tijelo ne naplaćuje usluge izdavanja certifikata.

9.1.2 Cijena pristupa certifikatima

Certifikaciono tijelo ne naplaćuje pristup certifikatima.

9.1.3 Cijena pristupa informacijama o statusu certifikata i naknade za opoziv cetifikata

Certifikaciono tijelo ne naplaćuje provjeru statusa certifikata bilo putem OCSP servisa bilo putem liste opozvanih certifikata.

Certifikaciono tijelo ne naplaćuje uslugu opoziva certifikata.

9.1.4 Cijene za druge servise

Ovo poglavlje nije primjenljivo u okviru ovog dokumenta.

9.1.5 Politika refundiranja

Troškovi se ne refundiraju.

9.2 Finansijska odgovornost

TrustME snosi finansijsku odgovornost za potencijalnu štetu koja može nastati korišćenjem izdatih certifikata u skladu sa zakonima koji regulišu ovu oblast.

9.2.1 Pokrivanje osiguranja

Certifikaciono tijelo nije dužno da obezbjedi najniži iznos osiguranja od rizika odgovornosti za potencijalnu štetu nastalu vršenjem usluga povjerenja u skladu sa članom 35 stav 1 Zakona o elektronskoj identifikaciji i elektronskom potpisu.

9.2.2 Ostala sredstva

Nije primjenljivo.

9.2.3 Osiguranje ili garancijsko pokrivanje za krajnje korisnike

Korisnik izdatih certifikata dužan je da nadoknadi nastalu štetu koju bi certifikaciono tijelo moglo da ima kao rezultat nedozvoljenih radnji, kao što su:

- Lažno predstavljanje prilikom registracije korisnika,
- Bilo kog propusta korisnika za koji korisnik ne može dokazati da je propust nenamjerno učinjen,
- Ako korisnik ne obezbijedi korišćenje privatnih ključeva na elektronskoj javnoj ispravi u skladu sa zakonom i ovim dokumentom,
- Ukoliko upotrebom privatnih ključeva na elektronskoj javnoj ispravi krši bilo koji zakon koji je primjenjiv (na primjer ukoliko krši zakon o žaštiti intelektualne svojine),
- U svim drugim slučajevima koji su u suprotnosti sa zakonom, ovim pravilnikom i drugim zakonskim aktima Crne Gore.

9.3 Povjerljivost poslovnih informacija

Certifikaciono tijelo ne prikuplja poslovne informacije o korisnicima.

9.4 Privatnost i zaštita ličnih podataka

9.4.1 Plan privatnosti

Cerifikaciono tijelo sprovodi mjere i postupke na zaštiti privatnosti i zaštiti ličnih podataka korisnika izdatih certifikata u skladu sa odgovarajućim zakonima.

9.4.2 Informacije koje se tretiraju kao privatne

Certifikaciono tijelo smatra privatnim sve informacije koje se odnose na korisnike certifikata, osim onih podataka koji su sastavni dio izdatih certifikata.

9.4.3 Informacije koje se ne smatraju privatnim

Certifikaciono tijelo tretira javnim samo one informacije na koje je korisnik dao saglasnost da se javno objave i podatke koji su sastavni dio izdatih certifikata.

9.4.4 Odgovornost za zaštitu privatnih informacija

Certifikaciono tijelo snosi odgovornost za zaštitu privatnosti informacija korisnika.

9.4.5 Otkrivanje informacija shodno pravnim i administrativnim procesima

Certifikaciono tijelo je ovlašćeno da koristi ili objavljuje lične podatke samo na osnovu saglasnosti korisnika ili na pravno validan zahtjev nadležnog organa.

9.4.6 Druge okolnosti za otkrivanje informacija

Certifikaciono tijelo ustupiće podatke sudu, tužilaštvu i drugim nadležnim državnim organima u slučajevima propisanim odgovarajućim zakonima.

9.5 Prava intelektualnog vlasništva

MUP ima sva prava intelektualnog vlasništva nad ovim dokumentom, certifikatima koje izdaje, repozitorijima na kojima objavljuje informacije i svim dokumentima i informacijama koje su objavljene na repozitorijumima certifikaconog tijela.

9.6 Garancije i odgovornosti

9.6.1 Garancije i odgovornosti certifikacionog tijela

TrustME se obavezuje da će sprovoditi sve mjere bezbjednosti, postupke i procedure definisane ovim dokumentom. Certifikaciono tijelo definiše korisnički ugovor i koristi ovu Politiku certifikacije radi stvaranja legalnih uslova korišćenja certifikata za elektronsku identifikaciju i elektronski potpis na ličnoj kartu u skladu sa Zakonom o ličnoj karti i Zakonom o elektronskoj identifikaciji i elektronskom potpisu od strane korisnika i trećih lica.

TrustME obavezuje se da će:

- pružiti usluge povjerenja za elektronske transakcije u skladu sa Zakonom o elektronskoj identifikaciji i elektronskom potpisu i odgovarajućim pravilnicima kojii proizilaze iz zakona,
- da će obezbjediti sav potreban softver i hardver za uspostavu certifikacionog tijela
- da će obezbjediti odgovarajuće repozitorijume za objavljivanje svih potrebnih informacija i sadržaja za podršku uslugama od povjerenja,
- da će objaviti kontakt informacije certifikacionog tijela,
- da će u skladu sa standardima koji regulišu ovu oblast i dobrom kriptografskom praksom obezbjediti sigurne mehanizme koji uključuju mehanizam generisanja korisničkih ključeva i ključeva CA tijela i adekvatnu kriptografsku zaštitu pomenutih ključeva,
- Da će uspostaviti proceduru dijeljenja tajni za sve povjerljive role u skladu sa svojom PKI infrastrukturom,
- U najkraćem mogućem roku obavijestiti korisnike i treće strane o kompromitaciji sopstvenog privatnog ključa, po mogućnosti po više komunikacionih kanala,

- Da će izdavati certifikate korisnicima u skladu sa Zakonom o elektronskoj identifikaciji i elektronskom potpisu i procedurama definisanim ovim dokumentom,
- Da će ispunjavati sopstveno preuzete obaveze,
- Da će obavjestiti podnosioce zahtjeva za izdavanje certifikata po njihovom generisanju, kao i da će obavjestiti korisnike ako ne bude u mogućnosti da im izda tražene certifikate,
- Da će nakon prijema zahtjeva za izdavanje certifikata od centralnog registracionog tijela ako je u mogućnosti izdati tražene certifikate,
- Da će nakon prijema validnog zahtjeva za opoziv ili suspenziju certifikata opozvati ili suspendovati certifikat.
- Da će obezbjediti podršku korisnicima i trećim licima u skladu sa ovim dokumentom,
- Da će redovno i periodično objavljivati informacije o statusu certifikata putem liste opozvanih certifikata, a da će isto tako informacije o statusu certifikata biti dostupne putem OCSP servisa u realnom vremenu,
- Da će na zahtjev dostaviti kopiju ovog dokumenta svim zainteresovanim stranama,
- Da će redovno ažurirati ovaj dokument.

TrustME se obavezuje da će ispuniti i sve obaveze koje su proizilaze iz Zakona o elektronskoj identifikaciji i elektronskom potpisu i odgovarajućim podzakonskim aktima, a nisu obuhvaćena ovim dokumentom.

TrustME odgovorno je za izvršavanje navedenih obaveza u obimu koji propisuje zakonska regulativa Crne Gore.

TrustME nije odgovorno za neodgovarajuću provjeru validnosti certifikata od strane koja se pouzdaje u certifikate izdate od strane CA tijela MUP-a.

TrustME izdaje certifikate za elektronsku identifikaciju i kvalifikovani elektronski potpis građanima na ličnoj karti koja je QSCD uređaj primjenjujući standarde koji regulišu ovu oblast po standardu pa nisu odgovorni za zaštitu pripadajućih privatnih ključeva.

TrustME nije odgovorno za neizvršavanje svojih obaveza kao posledice više sile.

9.6.2 Garancije i odgovornosti registracionog tijela (RA)

Registraciona tjela, odnosno poslovnice MUP-a imaju sledeće obaveze i odgovornosti:

- Sprovode postupak registracije korisnika za izdavanje certifikata na ličnoj karti,
- Sprovode identifikaciju i autentikaciju korisnika i provjeru njihovih podataka na način propisan ovim dokumentom,
- Prosleđuju tačne i provjerene podatke o korisnicima na dalju obradu u certifikaciono tijelo,
- Čuvaju, arhiviraju i štite podatke korisnika i prateće dokumentacije najmanje 10 godina od prestanka validnosti certifikata na koji se odnose,

- Čuvaju podatke korisnika od gubitka i povrede povjerljivosti,
- Obaveštavaju korisnike o javno objavljenim i dostupnim uslovima o pružanju usluga povjerenja i ovim dokumentom.

9.6.3 Obaveze i odgovornosti korisnika

U procesu korićenja izdatih elektronskih certifikata na ličnoj karti korisnici se obavezju da na pouzdan i propisan način koriste izdate certifkate. U domenu lične odgovornosti korisnika je:

- Da posjeduje odgovarajuća znanja za upotrebu izdatih certifikata,
- Da se upozna i da poštuje politike certifikacije i praktična pravila rada publikovana od strane certifikacionoh tijela,
- Da prilikom pribavljanje lične karte i ujedno podnošenja zahtjeva za izdavanje certifikata na ličnoj karti registracionom tijelu MUP-a dostavi sve podrebne podatke za ovaj proces,
- Da koristi izdate certifikata na ličnoj karti samo za legalne i autorizovane svrhe u skadu sa ovim dokumentom i Zakonom o elektronskoj identifikaciji i elektronskom potpisu i pravilnicima koji proizilaze iz zakona.
- Da na vrijeme, a u skladu sa Zakonom o ličnoj karti obavijesti certifikaciono tijelo ili registraciono tijelo o promjenama bilo kojih podataka koji su ranije dostavljeni,
- Da prekine korišćenje izdatog ili izdatih certifikata ukoliko bilo koji podatak u certifikatu postane nevalidan,
- Da prekine korišćenje izdataog ili izdatih certifikata ukoliko sam certifikat postane nevalidan,
- Da spreči kompromitaciju, gubljenje, objavljivanje, modifikaciju ili bilo koje drugo nevalidno korišćenje svojih privatnih ključeva.
- Da svoje privatne ključeve upotrebljava samo za propisane namjene ovim dokumentom i Zakonom o elektronskoj identifikaciji i elektronsko potpisu,
- Da podnese zahtjev za opoziv certifikata ako dođe do nekog događaja koji utiče na integritet izdatog certifikata (na primjer da opozove certifikate ukoliko je došlo do gubitka lične karte),
- Da prijave svaku moguću zloupotrebo svojih privatnih ključeva i da u tom slučaju podnesu zahtjev za opoziv pripadajućeg certifikata,

Iako se certifikati izdaju na elektronskoj javnoj ispravi – ličnoj karti, koja predstavlja QSCD uređaj visokog nivoa bezbjednosti u smislu zaštite kripografskog materijala na njoj, sami korisnici su odgovorni da se pridržavaju gore navedenih obaveza u cilju pravno validne i bezbjedne upotrebe izdatih certifikata.

9.6.4 Garancije i odgovornosti trećih lica

Treća lica koja se oslanja na certifikate izdate od strane certifikacionog tijela obavezuje se:

- Da posjeduje odgovarajuća znanja za upotrebu izdatih certifikata,
- Da se upozna i da poštuje politike certifikacije i praktična pravila rada publikovana od strane certifikacionoh tijela,
- Da verifikuje izdate certifikate od strane certifikacionog tijela primjenom svih raspoloživih metoda provjere certifikata: da provjeri da li je certifikat validan (da provjeri period važenja certifikata; da provjeri da li je certifikat izdat od strane certifikacionog tijela MUP-a; da provjeri da li je potpis elektronskog certifikata vjerodostojan; da provjeri status datog certifkata na važećoj listi opozvanih certifikata ili putem OCSP servisa certifikacionog tijela, a u skladu sa procedurom validacije certifikata i potpunog lanca certifkata),
- Da provjeri da li se izdati certifikat koristi za namjenu za koju je namijenjen (certifikat za elektronsku identifikaciju se koristi za elektronsku identifikaciju, a certifikat za kvalifikovani elektronski potpis za kreiranje elektronskog potpisa elektronske transakcije ili elektronskog dokumenta).
- Da vjeruje u izdati certifikat samo ukoliko se sve informacije koje se odnose na taj certifikat mogu provjeriti da su korektne i ažurne,
- Da se razumno pouzda u izdati certifikata u skladu sa odgovarajućim okolnositma.

9.6.5 Garancije ostalih učesnika

Bilo koji drugi učesnici obavezni su da koriste certifikate i ponašaju se u skladu sa ovim dokumentom i važećim propisima iz ove oblasti.

9.7 Izuzeća garancija i odgovornosti

Certifikaciono tijelo daje garancije i odgovornost samo za aktivnosti definisane zakonom i u poglavlju 9.6.1. TrustME naročito isključuje:

- Bilo koju odgovornost za štetu koja može da se pojavi od momenta kada CA tijelo MUP-a primi validan zahtjev za opoziv certifikata, do momenta objave informacije o opozivu istog na CRL, u skladu sa odjeljkom 4.9.5.
- Bilo koju odgovornost za stvari van kontrole CA tijela MUP-a uključujući raspoloživost ili rad Interneta, ili telekomunikacija ili drugih infrastruktura ili RA sistema, uključujući opremu i programe,
- Bilo koju odgovornost za štete koje su nastale kao rezultat događaja više sile kako je detaljno opisano u odjeljku 9.16.5.

9.8 Ograničenja odgovornosti

TrustME prihvata samo one odgovornosti definisane dokumentima CP i CPS, Zakonom o elektronskoj identifikaciji i elektronskom potpisu i pratećim pravilnicima.

9.9 Obeštećenja

Sve strane koje učestvuju u PKI infrastrukturi koju organizuje Minsitarstvo unutrašnjih poslova za sebe snose odgovornost za nadoknadu štete drugim stranama za pretrpljenu štetu nastalu kao rezultat neovlašćenog korišćenja certifikata ili korišćenja certifikata koje nije u skladu sa Zakonom o elektronskoj identifikaciji i elektronskom potpisu, pravilnicima koji proističu iz zakona, CP i CPS dokumentima.

9.10 Početak i kraj validnosti

Ovaj dokument stupa na snagu danom donošenja. Dokument nema vremensko ograničenje.

Dokument može biti stavljen van snage objavljivanjem nove verzije ovog dokumenta.

Nakon stavljana van snage ovog dokumenta, npr zbog objavljivanja nove verzije ovog dokumenta certifikati će se koristiti u skladu sa pravilnikom koji je bio validan na dan izdavanja certifikata.

U slučajevima kada ovo nije moguće certifikaciono tijelo će obavijestiti korisnike o tome na svojim web stranicama.

9.11 Pojedinačna obavještenja i komunikacija sa učesnicima

Ovo poglavlje nije primjenjivo u okviru ovog dokumenta.

9.12 Ispravke

Ovo poglavlje nije primjenjivo u okviru ovog dokumenta.

9.13 Procedure rešavanja sporova

Svi sporovi u vezi certifikata moraju se dostaviti na adresu iz odeljka 1.5.2.

Sve sporove treba ako je moguće rješavati sporazumno. Ukoliko se dogovor ne može postići sporazumno spor će rješavati kod nadležnog suda u Crnoj Gori.

9.14 Primjena zakona

Ovaj dokument u skladu je sa Zakonom o elektronskoj identifikaciji i elektronskom potpisu i njegovim podzakonskim aktima.

9.15 Usaglašenost sa primjenljivim zakonom

Ovaj dokument usaglašen je sa:

- Zakonom o elektronskoj identifikaciji i elektronskom potpisu

- Zakonom o zaštiti podataka o ličnosti
- Zakonom o ličnoj karti
- Drugim propisima iz ove oblasti.

9.16 Razne odredbe

9.16.1 Ugovor o pružanju usluga certifikovanja

CP i CPS dokumenti i ugovor o pružanju usluga certifikovanja sadrže sve elemente koji definišu odnos između certifikacionog tijela MUP-a i korisnika certifikata (vlasnika lične karte).

9.16.2 Prenos prava

Korisnicima certifikata nije dozvoljeno da prava i obaveze koja proističu iz CP i CPS dokumenata i ugovora prenesu na treća lica po bilo kom osnovu.

9.16.3 Klauzula o valjanosti

Nevaljanost jednog ili više djelova ovog dokumenta nemaju uticaj na valjanost ostalih odredbi ovog dokumenta ukoliko nemaju uticaj na materijalne odredbe.

9.16.4 Izvršenje (nadoknade za pravnog zastupnika i odricanje od prava)

Nije primjenjivo.

9.16.5 Viša sila

Višu silu predstavljaju vanredne okolnosti i nepredvidljive situacije kao što su prirodne katastrofe, nedostatak napajanja ili prekid telekomunikacionih veza, požar, zemljotres, nepredvidljivi IT incidenti kao napadi virusa ili napadi sa ciljem onemogućavanja servisa i slično.

Učesnici TrustME neće biti odgovorne za bilo kakvu štetu koja je nastala usled događaja kao rezultat više sile.

9.17 Ostale odredbe

Nema odredbi.

Reference

Osnovni zakoni

[1] Uredba (EU) br. 910/2014 Europskog parlamenta i Savjeta od 23. Jula.

o elektronskoj identifikovanju i uslugama povjerenja za elektronske transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ

[2] Zakon o elektronskoj identifikaciji i elektronskom potpisu

[3] Zakon o ličnoj karti

Pravilnici

[4] Pravilnik o bližim uslovima koje mora da ispunjava kvalifikovani davalac usluga certifikovanja

[5] Pravilnik o načinu ocjenjivanja usaglašenosti kvalifikovanih sredstava za izradu elektronskih potpisa i elektronskih pečata i sadržaju liste certifikovanih kvalifikovanih sredstava za izradu elektronskih potpisa i elektronskih pečata

[6] Pravilnik o mjerama i aktivnostima za zaštitu certifikata za elektronski potpis i elektronski pečat

[7] Pravilnik o okviru za interoperabilnost sistema elektronske identifikacije

[8] Pravilnik o sadržini i načinu vođenja evidencije davalaca usluga certifikovanja i registra kvalifikovanih davalaca usluga certifikovanja

[9] Pravilnik o najnižem iznosu osiguranja rizika od odgovornosti za štete koje nastanu pružanjem usluga certifikovanja

Ostali zakoni

[10] Zakon o zaštiti podataka o ličnosti

Standardi

[11] ISO/IEC 27001:2013 – Information technology – Security techinques – Information security management

[12] ISO 9001:2015 - Quality management systems - Requirements

[13] ETSI EN 319 401 V2.2.1. (2018-04) – Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

[14] ETSI EN 319 411-1 V1.2.2. (2018-04) – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements

[15] ETSI EN 319 411-2 V2.2.2. (2018-04) – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates

[16] ETSI EN 319 412-1 V1.1.1. (2016-02) – Electronic Signatures and Infrastructures (ESI);Certificate Profiles; Part 1: Overview and common data structures

[17] ETSI EN 319 412-2 V2.1.1. (2016-02) – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons

[18] ETSI EN 319 412-3 V1.1.1. (2016-02) – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons

[19] ETSI EN 319 412-5 V2.2.1. (2017-11) – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements

[20] ETSI EN 319 403 V 2.2.2 (2015-08) - Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers

[21] ETSI TS 119 312 V1.3.1. (2019-02) – Electronic Signatures and Infrastructures (ESI); Cryptographic Suites

[22] ETSI TS 119 495 V1.3.1. (2019-03) – Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366

[23] ETSI TS 119 412-1 V1.2.1 (2018-05) - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures

[24] EN 419 211-1:2014 – Protection profiles for secure signature creation device – Part 1: Overview (EN 419211-1:2014)

[25] EN 419 211-2:2013 – Protection profiles for secure signature creation device – Part 2: Device with key generation (EN 419211-2:2013)

[26] EN 419 211-4:2013 – Protection profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted channel to certificate generation application (EN 419211-4:2013)

[27] EN 419 211-5:2013 –Protection profiles for secure signature creation device – Part 5: Extension for device with key generation and trusted channel to signature creation application (EN 419211-5:2013)

[28] NIST FIPS PUB 140-2 (2001) – Security Requirements for Cryptographic Modules

[29] IETF RFC 3647 – Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework

[30] IETF RFC 5280 (2008) – Internet X.509 Public Key Infrastructure; Certificate and Certificate Revocation List (CRL) Profile

[31] IETF RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP (2013)

Ovaj dokument stupa na snagu danom potpisivanja.
Broj:
Podgorica, 10.03.2020. godine.

Ministar
Mavludin Nuhodžić