PODIJELI DOŽIVLJAJ.

KOMPANIJSKA DIREKTIVA

Crnogorski Telekom a.d. Podgorica

ID broj:	162
Vrsta propisa (skraćenica):	CD
Broj verzije:	2.0
Dokument OID:	1.3.6.1.4.1.56393.1.1.1.1
Odgovorni sektor:	Sektor za razvoj servisa i digitalnu transformaciju
Datum donošenja/usvajanja:	
Datum stupanja na snagu:	01/12/2020
Validnost:	Neodređeno
Broj aneksa/priloga:	1

Politika pružanja elektronskih (CTrust Certificate Policy – CTrust CP)

	Ime i prezime	Sektor	Pozicija
Odgovorni podnosilac – član Menadžment komiteta / kao Podnosilac:	Dušan Banović	Sektor za razvoj servisa i digitalnu transformaciju	Direktor Sektora za razvoj servisa i digitalnu transformaciju
Pripremili Eksperti:	Tanja Bokan	Sektor za razvoj servisa i digitalnu transformaciju	Rukovodilac odjeljenja za digitalnu transformaciju
	Ivan Stanković	Sektor Tehnike	Vođa službe za IT infrastrukturu i IT/NT bezbjednost
	Jovana Novaković		Glavni specijalista za regulatorna pitanja i odnose sa Vladom
	Biljana Papović	Sektor za razvoj servisa i digitalnu transformaciju	Vođa službe za unapređenje i automatizaciju poslovnih procesa
	Jelena Đođić	Sektor za razvoj servisa i digitalnu transformaciju	Specijalista za unapređenje korisničkih procesa i parametara kvaliteta
	Dragomir Stevanović– S&T Crna Gora d.o.o.		
	Slobodan Pavićević – S&T Crna Gora d.o.o.		

Revidirano:			
Odobrenje pravne usklađenosti:	Pavle Đurović	Sektor za korporativne i pravne poslove	Direktor Sektora za korporativne i pravne poslove i Sekretar Društva

Interne reference:

- Kompanijska direktiva o pripremi i usvajanju internih propisa
- Obavezujuća korporativna pravila za zaštitu privatnosti
- Kompanijska direktiva o sigurnosti
- Kompanijska direktiva o kontrolnom setu sigurnosti
- Praktična pravila rada za izdavanje certifikata za napredni elektronski pečat i certifikata za napredni elektronski potpis (CTrust Certificate Practice Statement NQ - CTrust CPS NQ)

Eksterne reference:

OSNOVNI ZAKON

[1] Zakon o elektronskoj identifikaciji i elektronskom potpisu

PRAVILNICI

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

[3] Pravilnik o sadržini i načinu vođenja evidencije davalaca elektronskih usluga povjerenja i registra kvalifikovanih davalaca elektrosnkih usluga povjerenja

[4] Pravilnik o najnižem iznosu osiguranja rizika od odgovornosti za štete koje nastanu vršenjem elektronskih usluga povjerenja

OSTALI ZAKONI

[5] Zakon o zaštiti podataka o ličnosti

STANDARDI

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

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

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

[9] 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

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

[11] 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

[12] 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

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

[14] 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
[15] ETSI TS 119 312 V1.3.1. (2019-02) – Electronic Signatures and Infrastructures (ESI); Cryptographic Suites
[16] ETSI TS 119 412-1 V1.2.1 (2018-05) - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
[17] EN 419 211-1:2014 – Protection profiles for secure signature creation device – Part 1: Overview (EN 419211-1:2014)
[18] EN 419 211-2:2013 – Protection profiles for secure signature creation device – Part 2: Device with key generation (EN 419211-2:2013)
[19] 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)
[20] 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)
[21] NIST FIPS PUB 140-2 (2001) – Security Requirements for Cryptographic Modules
[22] IETF RFC 3647 – Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework
[23] IETF RFC 5280 (2008) – Internet X.509 Public Key Infrastructure; Certificate and Certificate Revocation List (CRL) Profile
[24] IETF RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP (2013)

ISTORIJA DOKUMENTA

Verzija	Datum stupanja na snagu propisa/izmjena	Kratak opis izmjena
1.0	20.11.2020.	Dokument sa popunjenim poglavljima 1 – 9 prema RFC 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
2.0	1.12.2020.	Ažuriranje definicija pojmova, korigovanje dijelova dokumenta u skladu sa ažuriranim definicijama i ispravka slovnih grešaka. Napravljene korekcije u poglavljima: • 1.1. PREGLED OSNOVNIH PRETPOSTAVKI • 4.9. SUSPENZIJA I OPOZIV I SUSPENZIJA CERTIFIKATA • 5.7.3. PROCEDURE KOJE SE SPROVODE KOD KOMPROMITACIJE PRIVATNOG KLJUČA • 6.1.5. DUŽINE KLJUČEVA • 6.1.7. NAMJENA UPOTREBE KLJUČEVA (X.509 KEYUSAGE) • 6.3.2. PERIODI VALIDNOSTI CERTIFIKATA I PRIVATNOG KLJUČA • 7.1.2. EKSTENZIJE CERTIFIKATA

SADRŽAJ:

1. UVOD

Crnogorski Telekom A.D. Podgorica (u daljem tekstu: CT) je uspostavio infrastrukturu i u okviru svoje organizacije oformio tijelo za pružanje elektronskih usluga povjerenja (u daljem tekstu: CTrust).

Elektronske usluge povjerenja koje pruža CTrust usklađene su sa zakonskom regulativom [1], i mjerodavnim međunarodnim normama iz djelokruga pružanja ovih usluga. CT neprekidno prati potrebe krajnjih korisnika, razvoj tehnologije i promjene u normama iz područja pružanja elektronskih usluga povjerenja te u skladu s tim unapređuje i usklađuje svoj rad.

Ovim dokumentom definiše se način na koji CTrust ispunjava tehničke, organizacione i proceduralne zahtjeve poslovanja, koji su propisani za elektronske usluge povjerenja, u skladu sa standardom ETSI EN 319 401.

1.1. PREGLED OSNOVNIH PRETPOSTAVKI

Hijerarhijska struktura CTrust sistema za pružanje elektronskih usluga povjerenja zasnovana je na dvoslojnoj arhitekturi certifikacionih tijela (engl.: *Certification Authorities*, u daljem tekstu: CA tijela) koju čine:

- Korijensko certifikaciono tijelo (root CA): CTrust Root CA
- Podređeno certifikaciono tijelo (podređeno CA): CTrust GP CA

CT ostavlja mogućnost uspostavljanja drugih podređenih certifikacionih tijela u hijerarhijskoj strukturi za potrebe izdavanja drugih tipova certifikata.
CTrust Root CA je izdao samopotpisani certifikat za CTrust Root CA. Svojim samopotpisanim certifikatom CTrust Root CA izdao je certifikate njemu podređenim certifikacionim tijelima i OCSP servisu za provjeru statusa certifikata koje izdaje CTrust Root CA, u ovom slučaju provjerava se status podređenih certifikacionih tijela.

Postupci koji se primjenjuju u izdavanju certifikata krajnjim korisnicima opisani su u dokumentu Praktična pravila rada za izdavanje certifikata za napredni elektronski pečat i certifikata za napredni elektronski potpis (CTrust Certificate Practice Statement NQ - CTrust CPS NQ).

1.1.1. OPSEG I NAMJENA

Politika pružanja elektronskih usluga povjerenja opisuje pravila, procedure i postupke koji se primjenjuju prilikom pružanja elektronskih usluga povjerenja kao i praktična pravila rada za korijensko certifikaciono tijelo CTrust Root CA za postupke i procedure koje primjenjuje za izdavanje i upravljanje certifikata za podređena certifikaciona tijela i OCSP servis korijenskog certifikacionog tijela (u daljem tekstu: CTrust CP).
Namjena ovog dokumenta je propisivanje postupaka iz područja elektronskih usluga povjerenja, a koje sprovode učesnici navedeni u tački 1.3. ovog dokumenta.
Struktura ovog dokumenta zasniva se na standardizovanom dokumentu IETF RFC 3647.
Davalac elektronskih usluga povjerenja utvrđuje i interna pravila (u daljem tekstu: interna pravila) u kojima su sadržani i detaljno opisani postupci i mjere koji se primjenjuju prilikom prijema zahtjeva za izdavanjem certifikata, izdavanja certifikata, upravljanja životnim vijekom certifikata, upravljanja IT infrastrukturom i njenom zaštitom. Interna pravila su privatni dokumenti i predstavljaju poslovnu tajnu davaoca elektronskih usluga povjerenja.

1.1.2. TIPOVI CERTIFIKATA

U posljednjoj verziji dokumenta „Pregled profila certifkata CTrust Root CA" navedeni su grupe, tipovi certifikata i profil certifikata koje izdaje CTrust Root CA.

CTrust Root CA izdaje certifikate za:

- CTrust Root CA Certifikaciono tijelo
- CTrust Root CA podređeno certifikaciono tijelo

- CTrust Root CA OCSP servis

Grupe, tipovi certifikata i profil certifikata koje izdaju podređena certifikaciona tijela biće definisani u CPS dokumentu konkretne elektronske usluge povjerenja.

1.2. NAZIV DOKUMENTA I IDENTIFIKACIONI PODACI

CT-u je dodijeljen od strane IANA organizacije (Internet Assigned Number Authority) sljedeći OID: 1.3.6.1.4.1.56393.
Na osnovu tog OID-a CT je za potrebe pružanja elektronskih usluga povjerenja dodijelio sljedeći OID: 1.3.6.1.4.1.56393.1. (CTrust sistem).
U nastavku je naveden naziv ovog dokumenta i njegovi identifikacioni podaci.
Naziv: Politika pružanja elektronskih usluga povjerenja (CTrust Certificate Policy– Ctrust CP)
Verzija: 2.0
Datum stupanja na snagu: 01.12.2020.
Internet adresa na kojoj je objavljen ovaj CP/CPS dokument je: http://ca.CTrust.telekom.me/cpcps.

1.3. UČESNICI U SISTEMU DAVAOCA ELEKTRONSKIH USLUGA POVJERENJA

Učesnici CTrust-a davaoca elektronskih usluga povjerenja CT-a su:

- Certifikaciona tijela
- Registraciona tijela
- Korisnici
- Treća lica

1.3.1. CERTIFIKACIONA TIJELA (CERTIFICATION AUTHORITY)

Certifikaciona tijela na koja se odnosi ovaj dokument su:

- Korijensko certifikaciono tijelo: CTrust Root CA
- Podređeno certifikaciono tijelo: CTrust GP CA

Tehnički djelovi certifikacionih tijela organizuju se u za to specijalno namijenjenim prostorijama CT-a, koje ispunjavaju sve zahtjeve propisane relevantnim propisima.

1.3.1.1. UPRAVLJAČKO TIJELO CTRUST-A (CTRUST PMA ILI SAMO PMA)

CT organizuje upravljačko tijelo CTrust-a (eng. *Policy Managment Authority* – u daljem tekstu: CTrust PMA ili samo PMA) koje je odgovorno za obavljanje sljedećih aktivnosti:

- Izradu i održavanje ovog dokumenta;
- Izradu i održavanje definicija profila certifikata;
- Izradu i održavanje ostalih javnih dokumenata koji su namijenjeni korisnicima, kao što su Ugovor sa krajnjim korisnikom (*End-User Agreement*) ili izjava o pružanju elektronskih usluga povjerenja (*PKI Disclosure Statement* – PDS);
- Podnošenje Politike pružanja elektronskih usluga povjerenja i praktičnih pravila rada na usvajanje izvršnom direktoru CT-a;
- Predlaže imenovanje osoblja na dužnosti u okviru certifikacionog tijela;
- Vrši nadzor i organizuje reviziju usklađenosti pružanja elektronskih usluga povjerenja sa ovim dokumentom;
- Odobrava izdavanje certifikata za korijensko i podređena certifikaciona tijela i OCSP servise korijenskog i podređenih certifikacionih tijela;
- Zahtijeva obnovu certifikata za korijensko i podređena certifikaciona tijela;
- Odgovorno je za izradu procjena, procedura i praksi drugih sistema koji pružaju elektronske usluge povjerenja, a sa kojima se vrši međusobno povezivanje;

- Rješava potencijalne sporove nastale u domenu rada CTrust-a;
- I druge poslove upravljanja neophodne za funkcionisanje CTrust-a.

1.3.1.2. TIJELO ZA OPERATIVNE POSLOVE (CTRUST OA)

Tijelo za operativne poslove obavlja sljedeće 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;
- Upravljanje i nadzor infrastrukturom certifikacionog tijela u skladu sa ovim dokumentom;
- Zahtijevanje opoziva certifikata članova operativnog osoblja certifikacionog tijela;
- Objavljivanje certifikata na javnom repozitorijumu;
- Opoziv certifikata krajnjih korisnika na osnovu zahtjeva krajnjih korisnika ili na svoju inicijativu;
- Izdavanje i objavljivanje liste opozvanih certifikata;
- Rješavanje sporova između krajnjih korisnika i registracionog tijela;
- I ostale operativne i tehničke poslove potrebne za funkcionisanje kompletne infrastrukture davaoca elektronskih usluga povjerenja.

1.3.2. REGISTRACIONA TIJELA (REGISTRATION AUTHORITIES ILI CTRUST RA)

Poslove registracionog tijela za krajnje korisnike vrše Registraciona tijela CTrust-a i Centralno registraciono tijelo CTrust-a opisani u nastavku dokumenta.

1.3.2.1. REGISTRACIONA TIJELA CTRUST-A (CTRUST RA)

Poslovnice CT-a predstavljaju registraciona tijela za podnošenje zahtjeva za elektronske usluge povjerenja. Uloga registracionog tijela u procesu podnošenja zahtjeva za elektronsku uslugu povjerenja opisana je u praktičnim pravilima rada za konkretnu elektronsku uslugu povjerenja (u daljem tekstu: CPS dokument konkretne usluge).

1.3.2.2. CENTRALNO REGISTRACIONO TIJELO CTRUST-A

Centralno registraciono tijelo CT-a ima obavezu da primi zahtjeve za elektronske usluge povjerenja od CTrust RA i pokrene proces realizacije usluge. Uloga centralnog registracionog tijela u procesu realizacije elektronske usluge povjerenja opisana je u CPS dokumentu konkretne usluge.

1.3.3. NARUČIOCI I KORISNICI

Krajnji korisnici elektronskih usluga povjerenja koje pruža CTrust su fizička lica, preduzetnici i pravna lica koja imaju prebivalište odnosno sjedište u Crnoj Gori.
Naručioc *(subscriber)* može biti fizičko lice, pravno lice ili preduzetnik. Uslugu povjerenja upotrebljava krajnji korisnik (*subject*) čije se ime ili funkcija registruju kod prijave za korišćenje elektronske usluge povjerenja.
Kada elektronsku uslugu povjerenja traži naručilac fizičko lice ili preduzetnik, tada je naručilac istovremeno i krajnji korisnik.
Kada elektronsku uslugu povjerenja traži naručilac koji je pravno lice, tada naručilac daje pravo na upotrebu usluge povjerenja krajnjem korisniku.
Punu odgovornost koja proističe iz upotrebe elektronske usluge povjerenja snosi naručilac, bez obzira da li je naručilac fizičko, pravno lice ili preduzetnik.

1.3.4. TREĆA LICA (RELYING PARTIES)

Treća lica su fizička lica i poslovni subjekti (kompanije, preduzetnici, korporacije, ustanove, tijela državne uprave i dr.) koja se pouzdaju u elektronske usluge povjerenja.

Prije nego se pouzdaju u elektronsku uslugu povjerenja, treća lica moraju uvijek da realizuju procedure provjere predmetne usluge definisane CPS dokumentom konkretne usluge povjerenja.

1.3.5. OSTALI UČESNICI

Ostali učesnici su pravna ili fizička lica koja, na neki način, doprinose ili učestvuju u obezbjeđivanju kvaliteta pružanja elektronskih usluga povjerenja.

1.4. UPOTREBA CERTIFIKATA

1.4.1. DOZVOLJENA UPOTREBA CERTIFIKATA

Certifikaciono tijelo CTrust Root CA koristi svoj certifikat i pripadajući par asimetričnih ključeva za izdavanje sljedećih certifikata:

- Certifikat za podređena certifikaciona tijela;
- Certifikat za OCSP servis korijenskog certifikacionog tijela.

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

Dozvoljena upotreba certifikata koje izdaju podređena certifikaciona tijela definisani su u CPS dokumentu konkretne usluge.

1.4.2. ZABRANJENA UPOTREBA CERTIFIKATA

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

Zabranjena upotreba certifikata koje izdaju podređena certifikaciona tijela definisana je CPS dokumentom konkretne usluge.

1.5. ADMINISTRACIJA POLITIKE PRUŽANJA ELEKTRONSKIH USLUGA POVJERENJA

1.5.1. ORGANIZACIJA KOJA UPRAVLJA DOKUMENTOM POLITIKA PRUŽANJA ELEKTRONSKIH USLUGA POVJERENJA

CTrust PMA u ime CT-a 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:

CTrust PMA: Crnogorski Telekom A.D.
Adresa: 81000 Podgorica, Moskovska br. 29.
E-mail: CTrust_pma@telekom.me

1.5.3. SUBJEKT KOJI UTVRĐUJE USAGLAŠENOST DOKUMENTA SA ZAKONOM

Nadležni organ shodno zakonu i propisima iz ove oblasti utvrđuje usaglašenost dokumenta sa zakonom. Upravni nadzor nad sprovođenjem Zakona o elektronskoj identifikaciji i elektronskom potpisu [1] vrši Ministarstvo.
Inspekcijski nadzor nad radom davalaca elektronskih usluga povjerenja i kvalifikovanih davalaca elektronskih usluga povjerenja i ispunjenošću uslova sistema elektronske identifikacije vrši inspekcija za usluge informacionogdruštva, u skladu sa zakonom kojim se uređuje inspekcijski nadzor i Zakonom o elektronskoj identifikaciji i elektronskom potpisu [1].

1.5.4. PROCEDURA ODOBRAVANJA OVOG DOKUMENTA

Ovaj dokument se periodično 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 promjenom primijenjenih kriptografskih algoritama ili dužina kriptografskih ključeva.
Na osnovu predloga CTrust PMA ovaj dokument odobrava izvršni direktor CT-a.

1.6. DEFINICIJE I SKRAĆENICE

U ovom dokumentu pojedini izrazi imaju sljedeće značenje:

Pojam	Opis
Autentifikacija	Elektronski postupak koji omogućava potvrđivanje elektronske identifikacije fizičkog ili pravnog lica ili porijekla i integriteta podataka u elektronskom obliku.
Arhiva	Specifična baza podataka za čuvanje zapisa za određeni period vremena u cilju bezbjednosti, backup-a ili revizije.
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 autentifikovani korisnik ima za korišćenje odgovarajuće aplikacije ili servisa.
Autor elektronskog pečata	Pravno lice ili organ vlasti koje upotrebljava elektronski pečat korišćenjem podataka za izradu elektronskog pečata.
CA certifikat	Certifikat za dato CA izdat (digitalno potpisan) od strane drugog CA ili samopotpisan (ukoliko se radi o CTrust Root CA).
Certificate Practice Statement (CPS)	Javna praktična pravila i procedure koje certifikaciono tijelo primjenjuje u proceduri izdavanja certifikata odnosno pružanja elektronskih usluga povjerenja.
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.
Certifikat za elektronski pečat	Certifikat za elektronski pečat je elektronska potvrda koja povezuje podatke za verifikaciju elektronskog pečata sa pravnim licem ili organom vlasti i potvrđuje naziv tog pravnog lica ili organa vlasti.
Dijeljena tajna	Dio kriptografske tajne koja je podijeljena na unaprijed definisani 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 (krajnjem 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 pečat	Elektronski pečat je skup podataka u elektronskom obliku koji su pridruženi drugim podacima u elektronskom obliku ili su logički povezani sa njima radi obezbjeđenja porijekla i integriteta tih podataka i zasniva se na certifikatu za elektronski pečat
Certifikat	Elektronski dokument kojim se potvrđuje veza između podataka za provjeru elektronskog potpisa/pečata 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 podčinjeno/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 krajnjeg korisnika koji posjeduje odgovarajući privatni ključ.
Korisnički ugovor	Ugovor između krajnjeg korisnika i CT-a u cilju pružanja elektronskih usluga povjerenja.
Korisnik	Fizičko ili pravno lice koje se oslanja na elektronsku identifikaciju ili elektronsku uslugu povjerenja.
Krajnji korisnik	Autor elektronskog pečata ili potpisnik
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.
Lanac (put) certifikata	Uređena sekvenca certifikata koja se, zajedno sa javnim ključem inicijalnog objekta u lancu (putu), procesira u cilju provjere istog u posljednjem 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.
Napredni elektronski pečat	Napredni elektronski pečat je elektronski pečat koji ispunjava sledeće zahtjeve: 1) isključivo je povezan s autorom pečata; 2) Nedvosmisleno identifikuje autora pečata; 3) nastaje korišćenjem sredstva za izradu elektroničkog pečata kojim autor pečata 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 izradu elektronskog pečata	Jedinstveni podaci koje autor elektronskog pečata koristi za izradu elektronskog pečata
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.
Verifikacija	Postupak kojim se potvrđuje da su elektronski potpis ili elektronski pečat validni
Potpisnik	Fizičko lice koje se potpisuje u svoje ime ili u ime fizičkog ili pravnog lica korišćenjem podataka za izradu elektronskog potpisa.
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 krajnjeg korisnika primjenom asimetričnog kriptografskog algoritma.
Registraciono tijelo (RA)	Tijelo odgovorno za identifikaciju i autentifikaciju krajnjeg korisnika/vlasnika certifikata, kao i kreiranje zahtjeva za izdavanje certifikata, ali koji ne izdaje i ne potpisuje certifikat (tj. RA vrši odgovarajuće poslove (identifikaciju krajnjeg 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 elektronskih usluga povjerenja 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 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 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.
Sredstvo za izradu elektronskog pečata	Odgovarajuća računarska oprema ili računarski program koji se koristi za izradu elektronskog pečata
Sredstva za provjeru elektronskog potpisa/pečata	Odgovarajuća tehnička sredstva (softver i hardver) koja služe za provjeru elektronskog potpisa/pecata, uz korišćenje podataka za provjeru elektronskog potpisa/pečata.
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).
Treće lice	Primalac certifikata koji provjerava dati certifikat i/ili provjerava digitalni potpis dobijenog elektronskog dokumenta primjenom javnog ključa potpisnika iz certifikata. Takođe, treće lice provjerava validnost certifikata u istom procesu. Treće lice može biti takođe krajnji 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.

Skraćenice koje se koriste u ovom dokumentu:

Skraćenica	Objašnjenje
CT	Crnogorski Telekom A.D. Podgorica
CTrust	Tijelo CT-a koje pruža elektronske usluge povjerenja
CA	Certification Authority – Certifikaciono tijelo
CTrust Root CA	CTrust korijensko certifikaciono tijelo
CTrust GP CA	CTrust podređeno certifikaciono tijelo
GP	General Purpose – Opšta namjena
OA	Operations Authority – Tijelo za operativne poslove
RA	Registration Authority – Registraciono tijelo
ID	Identification document – Identifikacioni dokument
PKI	Public Key Infrastructure – Infrastruktura za razmjenu javnih ključeva
OID	Object IDentifier
TSA	Time Stamping Authority – Sistem za izradu elektronskog vremenskog pečata
CRL	Certificate Revocation List – Lista opozvanih certifikata
CSR	Certificate Service Request
CDP	CRL Distribution Point
AIA	Authority Information Access
AKI	Authority Key Identifier
SKI	Subject Key Identifier
RFC	Request For Comments – Publikacije Internet društva (ISOC) i njegovih povezanih tijela, najistaknutije Radne grupe za internet inženjering (IETF), glavnih tijela za tehnički razvoj i uspostavljanje standarda za Internet.

ETSI	European Telecommunication Standardization Institute – Evropski institut za standardizaciju telekomunikacija
CP	Certificate Policy – Politika pružanja elektronskih usluga povjerenja
CPS	Certificate Practice Statement – Praktična pravila rada certifikacionog tijela
URL	Uniform Resource Locator
PMA	Policy Managment Authority – Upravljačko tijelo CTrust-a
CPAL	Cryptographically Protected Audit Log – Kriptografski zaštićen audit log
KMS	Key Management System – Komponenta koja na bezjbedan način čuva korisničke ključeve i omogućava njihovo korišćenje na HSM uređaju
KEK	Key Encryption Key – Ključ koji se čuva u KMS-u i služi za bezbjedno čuvanje korisničkih ključeva
ZMK	Zone Master Key – Ključ koji se kreira na HSM uređaju prilikom uspostave sistema. Služi za zaštitu KEK ključeva u KMS-u.
PKCS #12	Standard koji definiše fajl format koji može sadržati više kriptografskih objekata. Najčešće je enkriptovan i zaštićen lozinkom.
P12, PFX	Ekstenzija ili tip fajla definisanog PKCS #12 standardom
IM	Identity Management – Aplikacija za centralizovano upravljanje korisnicima

2. OBJAVLJIVANJE I ODGOVORNOSTI ZA REPOZITORIJUM

2.1. REPOZITORIJUM

CT je odgovoran za rad repozitorijuma, objavu dokumenata i informacija na repozitorijumu i objavu certifikata certifikacionih tijela i liste opozvanih certifikata na repozitorijumu.
U okviru redovnog funkcionisanja repozitorijuma, on je dostupan za upotrebu 24 sata na dan, 7 dana u nedjelji.
U slučaju nedostupnosti repozitorijuma CT će preduzeti sve potrebne mjere i postupke da repozitorijum učini dostupnim u najkraćem mogućem roku.

2.2. OBJAVA INFORMACIJA O PRUŽANJU ELEKTRONSKIH USLUGA POVJERENJA

Na repozitorijumu javno su objavljeni dokumenti i informacije o pružanju elektronskih usluga povjerenja.
Repozitorijum se sastoji od dijela dostupnog na internet stranicama.

2.2.1. SADRŽAJ REPOZITORIJUMA

Na internet stranicama CTrust repozitorijuma objavljuju se:

- Dokument „Politika pružanja elektronskih usluga povjerenja (CTrust Certificate Policy – CTrust CP)"
- Dokumenta Praktična pravila rada (CPS) za konkretne elektronske usluge povjerenja;
- Prethodne verzije dokumenata: CP i CPS za konkretne elektronske usluge povjerenja;
- Uslovi i izjave o pružanju elektronskih usluga povjerenja (engl. *Terms and conditions* i *PKI disclosure statement*);
- Opis važećih profila certifikata;
- Obrasci ugovora o pružanju elektronskih usluga povjerenja;
- Obrasci zahtjeva za opoziv certifikata;
- Obrasci zahtjeva za prekid/reaktivaciju korišćenja elektronske usluge povjerenja;
- Certifikati CA tijela iz hijerarhije CTrust-a;
- Objedinjene liste opozvanih certifikata za CA tijela iz hijerarhije CTrust-a;
- Informacije o zakonskoj regulativi iz područja pružanja elektronskih 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 CT-a, koje predstavljaju lokacije registracionih tijela u smislu ovog dokumenta;
- Korisnička uputstva;
- Uputstva i potreban aplikativni softver za korišćenje elektronskih usluga povjerenja;
- Certifikati namijenjeni za provjeru i testiranje;
- Cjenovnik elektronskih usluga povjerenja;
- Obavještenja krajnjim korisnicima i trećim licima u vezi s davanjem elektronskih usluga povjerenja;
- Ostale informacije vezane za rad CTrust-a.

Certifikati krajnjih korisnika se ne objavljuju.
Preko internet stranice repozitorijuma moguće je pretraživanje i preuzimanje certifikata CA tijela i liste opozvanih certifikata certifikacionih tijela.
Objavljeni sadržaj na internet stranicama dostupan je sa adrese http://www.telekom.me/CTrust na crnogorskom jeziku.
CTrust PMA može pojedina dokumenta objaviti i na engleskom jeziku, ako za to ima potrebe.

Putem OCSP servisa dostupne su informacije o statusu izdatih certifikata koje izdaju CA tijela. Adrese OCSP servisa za CTrust Root CA tijelo je: http://ocsp.CTrust.telekom.me/CTrustRootCAOCSP.

Adrese OSCP servisa za druga CA tijela iz hijerarhije CTrust-a definisane su u CPS dokumentu konkretne elektronske usluge povjerenja.
U repozitorijumu se ne objavljuju 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 krajnjim korisnicima, informacije o zakonskim aktima objavljuju se nakon početka primjene zakonskih akata u CTrust-u.
Certifikati certifikacionih tijela i pripadajuće informacije objavljuju se nakon njihovog izdavanja.
Objavu dokumenata uslova pružanja elektronskih usluga povjerenja, korisničkih uputstava, obrazaca zahtjeva, ugovora i ovlašćenja odobrava CTrust 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 CTrust PMA, ali CTrust PMA mora biti pravovremeno obaviješteno o svakoj objavi obavještenja i informacija.
CTrust CA tijela automatski objavljuju pripadajuće CRL na javnom imeniku i na internet stranicama repozitorijuma nakon njihovog izdavanja.

2.3. UČESTALOST OBJAVLJIVANJA PODATAKA O ELEKTRONSKIM USLUGAMA POVJERENJA

CTrust PMA održava, ažurira, odobrava i objavljuje periodično po potrebi CP i CPS za odgovarajuće elektronske usluge povjerenja. Prethodne verzije ovih dokumenata ostaju objavljene na repozitorijumu najmanje 10 godina posle isteka certifikata izdatih u skladu s tim dokumentima.
Drugi dokumenti i ostale relevantne informacije objavljuju se po potrebi.
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 repozitorijumu su besplatne i javno dostupne svim učesnicima uspostavljene infrastrukture.

Repozitorijum 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 repozitorijumu imaju ovlašćena lica.

3. IDENTIFIKACIJA I AUTENTIFIKACIJA KRAJNJIH KORISNIKA

Procedure identifikacije i autentifikacije navedene u ovom dokumentu se odnose na certifikate koje izdaje korijensko certifikaciono tijelo.
Procedure identifikacije i autentifikacije krajnjih korisnika definisane su CPS dokumentom konkretne elektronske usluge povjerenja.

3.1. DODJELJIVANJE IMENA

3.1.1. VRSTE IMENA

Atributi koji čine jedinstvena imena CTrust Root CA, dati su u tabeli 3.1.

Korijensko certifikaciono tijelo CTrustCTrust Root CA		
Atribut po X.520	**Vrijednost**	**Objašnjenje**
commonName (CN)	CTrust Root CA ili CTrust GP CA ili naziv drugog podređenog certifikacionog tijela	Naziv certifikacionog tijela
OrganizationName	Crnogorski Telekom A.D. Podgorica	Naziv pravnog lica
organizationIdentifier	VATME-02289377	Identifikator pravnog lica
countryName	ME	Dvoslovni ISO kod države, ME za Crnu Goru

Tabela 3.1 Sadržaj imena korijenskog certifikacionog tijela

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

3.1.3. ANONIMNOST KRAJNJIH KORISNIKA I PSEUDONIMI I NADIMCI

Nije primjenjivo.

3.1.4. PRAVILA ZA INTERPRETACIJU RAZLIČITIH VRSTA IMENA

Interpretacija oblika imena u polju *Subject* certifikata koji izdaje CTrust Root CA vrši se po tabeli 3.1 u tački 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 CT-a mora imati jedinstveno ime u okviru hijerarhije CTrust-a koje se upisuje u atribut *commonName*.
CT vodi evidenciju o iskorišćenim 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 CT-a i obavlja ih nadležna organizaciona jedinica ili ovlašćena lica CT-a.

3.2.1. METODA DOKAZIVANJA POSJEDOVANJA PRIVATNOG KLJUČA

Metoda dokazivanja posjedovanja privatnog ključa za korijensko certifikaciono tijelo i njemu podređenih certifikacionih tijela CT-a obezbijeđena je sprovođenjem procedure uspostave certifikacionih tijela i generisanja para asimetričnih ključeva. Certifikaciono tijelo izdaje certifikate prema tački 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 KRAJNJEM KORISNIKU KOJI SE NE PROVJERAVAJU

Nije primjenjivo.

3.2.5. PROVJERA OVLAŠĆENJA

Nije primjenjivo.

3.2.6. KRITERIJUMI ZA INTEROPERABILNOST

Procedure i prakse povezanih certifikacionih tijela moraju biti materijalno ekvivalentne procedurama i praksi CTrust-a kao što je definisano u ovom dokumentu. CTrust 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 CPS dokumentima konkretne elektronske usluge povjerenja.

4.1. ZAHTJEV ZA IZDAVANJEM CERTIFIKATA

Izdavanje certifikata za korijensko certifikaciono tijelo „CTrust Root CA“, za podređena certifikaciona tijela i OCSP servis korijenskog certifikacionog sprovodi se prema formalnoj proceduri i po odobrenju CTrust PMA.

4.1.1. KO MOŽE DA ZAHTIJEVA IZDAVANJE CERTIFIKATA

Nije primjenjivo.

4.1.2. PROCES OBRADE ZAHTJEVA ZA IZDAVANJEM CERTIFIKATA I ODGOVORNOSTI

Nije primjenjivo.

4.2. PROCESUIRANJE ZAHTJEVA ZA IZDAVAJE CERTIFIKATA

4.2.1. POSTUPAK IDENTIFIKACIJE I AUTENTIFIKACIJE KORISNIKA

Identifikacija i autentifikacija lica s povjerljivim ulogama u okviru certifikacionog tijela vrši se po internim pravilima CT-a.

4.2.2. ODOBRAVANJE ILI ODBIJANJE ZAHTJEVA ZA IZDAVANJE CERTIFIKATA

CTrust PMA može vratiti proceduru za izdavanje certifikata na doradu ukoliko zaključi da podaci i procedura nijesu 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 „CTrust Root CA" sprovodi se prema formalnoj proceduri uspostave korijenskog certifikacionog tijela i generisanja para asimetričnih ključeva.
Izdavanje certifikata podređenih certifikacionih tijela sprovodi se prema formalnoj proceduri uspostave konkretnog podređenog certifikacionog tijela i generisanja para asimetričnih ključeva.
Proceduru uspostave korijenskog ili podređenog certifikacionog tijela sprovode lica sa povjerljivim ulogama u zaštićenom prostoru CTrust-a uz primjenu propisanih mjera bezbjednosti.
Izdavanje certifikata za OCSP servis sprovodi lice s povjerljivom ulogom upotrebom aplikacije za OCSP servis.

4.3.2. OBAVJEŠTENJE KRAJNJIH KORISNIKA OD STRANE CERTIFIKACIONOG TIJELA O IZDAVANJU CERTIFIKATA

Certifikati korijenskog certifikacionog tijela i podređenih certifikacionih tijela objavljuju se na internet stranicama 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 CTrust repozitorijuma.
Certifikati podređenih certifikacionih tijela objavljuju se na internet stranicama CTrust repozitorijuma.
Certifikati za OCSP servis se ne objavljuju.
Objavljivanje korisničkih certifikata opisano je u CPS dokumentu konkretne elektronske usluge povjerenja.

4.4.3. OBAVJEŠTAVANJE OSTALIH UČESNIKA O IZDAVANJU CERTIFIKATA

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

4.5. KORIŠĆENJE CERTIFIKATA I PRIPADAJUĆIH ASIMETRIČNIH PAROVA KLJUČEVA

4.5.1. KORIŠĆENJE PRIVATNIH KLJUČEVA I CERTIFIKATA OD STRANE KRAJNJIH 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 certifikata krajnjeg korisnika od strane krajnih korisnika opisano je u CPS dokumentu konkretne elektronske usluge povjerenja.

4.5.2. KORIŠĆENJE JAVNIH KLJUČEVA I CERTIFIKATA OD STRANE TREĆIH LICA

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

- Vode računa o dozvoljenoj upotrebi i zabranjenoj upotrebi javnog ključa i pripadajućeg certifikata u skladu sa tačkom 1.4. ovog dokumenta;
- Obave provjeru vremena važenja svih certifikata u lancu i provjeru certifikata prema postupcima za validaciju lanca certifikata prema dokumentu RFC 5280 ili RFC 6960;
- Obave provjeru statusa certifikata upotrebom raspoloživih načina prema ovom dokumentu.

4.6. OBNAVLJANJE CERTIFIKATA BEZ PROMJENE KLJUČA

Korijensko certifikaciono tijelo i podređena certifikaciona tijela ne vrše obnovu certifikata bez promjene ključa.
Obnavljanje certifikata bez promjene ključa za usluge povjerenja definisano je CPS dokumetnom konkretne elektronske usluge povjerenja.

4.7. OBNOVA CERTIFIKATA SA NOVIM KLJUČEM (RE-KEY)

Obnovu certifikata korijenskog certifikacionog tijela i podređenih certifikacionih tijela uz generisanje novog para ključeva može zatražiti lice sa povjerljivom ulogom.
Obnovu certifikata odobrava CTrust 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 repozitorijuma.
Zahtjev za obnovu certifikata za OCSP servis sprovodi lice s povjerljivom ulogom.
Postupak obnove certifikata za krajnje korisnike opisan je u pripadajućem CPS dokumentu konkretne elektronske usluge povjerenja.

4.8. PROMJENA CERTIFIKATA KRAJNJIH KORISNIKA

Promjene 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 krajnjih korisnika opisan je u CPS dokumentu konkretne elektronske usluge povjerenja.

4.9. OPOZIV I SUSPENZIJA CERTIFIKATA

Zahtjev za opoziv certifikata koje je izdalo korijensko certifikaciono tijelo odobrava CTrust PMA.

Opoziv certifikata korijenskog certifikacionog tijela nije dozvoljena.
Suspenzija certifikata korijenskog certifikacionog tijela ili podređenog certifikacionog tijela nije dozvoljena.
Suspenzija i opoziv certifikata krajnjih korisnika opisani su u CPS dokumentu konkretne elektronske usluge povjerenja.

4.9.1. OKOLNOSTI ZA OPOZIV CERTIFIKATA

Korijensko certifikaciono tijelo vrši opoziv izdatog certifikata u sljedećim slučajevima:

- Na osnovu pisanog zahtjeva za opoziv certifikata izdatog podređenom certifikacionom tijelu lica s povjerljivom ulogom u CTrust PMA;
- Ako CTrust 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 i na osnovu posebne odluke CTrust PMA;
- 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.

Okolnosti za opoziv certifikata krajnjih korisnika opisani su u CPS dokumentu konkretne elektronske usluge povjerenja.

4.9.2. KO MOŽE ZAHTIJEVATI OPOZIV CERTIFIKATA

Opoziv certifikata certifikacionih tijela se vrši na osnovi odluke CTrust PMA.

4.9.3. PROCEDURA OPOZIVA CERTIFIKATA

Opoziv certifikata sprovode lica s povjerljivim ulogama u CT-u 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 OPOZIVOM CERTIFIKATA

Najkasnije 24 sata nakon prijema zahtjeva za opoziv.

4.9.6. ZAHTJEVI ZA PROVJEROM OPOZVANOSTI CERTIFIKATA SA STRANE TREĆIH LICA

Treća lica obavezna su da preduzimaju sve mjere i postupke propisane ovim dokumentom prilikom provjere validnosti certifikata i pouzdanja 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 pružanja elektronskih usluga povjerenja i svojim obavezama propisanim ovim dokumentom.

4.9.7. FREKVENCIJA IZDAVANJA LISTE OPOZVANIH CERTIFIKATA

Vrijeme u kojem najkasnije mora biti izdata sljedeća 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 konkretne elektronske usluge povjerenja.

4.9.8. MAKSIMALNO KAŠNJENJE OBJAVLJIVANJA LISTE OPOZVANIH CERTIFIKATA

U regularnim okolnostima 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 koje izdaju CTrust 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

Ne primjenjuje se.

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

Korijensko certifikaciono tijelo i podređena certifikaciona tijela daje informacije o statusu certifikata kroz pružanje 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 treće strane podržava provjeru statusa certifikata samo putem CRL.
CRL za certifikate koje izdaju certifikaciona tijela objavljuju se na repozitorijumu.
Adrese objave CRL sadržane su u ekstenziji *CRLDistributionPoints* u svakom izdatom certifikatu.

4.10.1.1. ADRESE ZA PRISTUP CRL ZA CTRUST ROOT CA CERTIFIKATE

Adresa objedinjene CRL za CTrust Root CA certifikate na internet serverima je:
http://ca.CTrust.telekom.me/crl/CTrustRootCA.crl
http://www.telekom.me/CTrust/crl/CTrustRootCA.crl

4.10.2. RASPOLOŽIVOST SERVISA

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

CTrust 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 koje imaju odgovarajuće povjerljive uloge. Dozvoljen je pristup i drugim licima, ali samo uz prisustvo lica operativnog osoblja koja imaju odgovarajuće povjerljive uloge.

5.1.1. LOKACIJA I KONSTRUKCIJA SAJTA

Najvažnija oprema CTrust certifikacionog tijela se nalazi u posebnoj i zaštićenoj prostoriji, lociranoj u Data centru CT-a. Prostorija certifikacionog tijela nalazi 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. KONTROLA FIZIČKOG PRISTUPA

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.
CTrust Certifikaciono tijelo koristi za kontrolu fizičkog pristupa elektronske brave sa elektronskom karticom i čitačem otiska prsta.
Prostorija u kojoj su smješteni tehnički sistemi certifikacionog tijela je nadgledana 24 sata/7 dana nedjeljno:

- Video nadzorom koji je povezan sa centralnim uređajem sistema u portirnici;

- Fizičkom zaštitom na nivou poslovne zgrade CT-a u kojoj se nalazi Data centar, koju realizuje licencirana zaštitarska kuća.

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 elektronskih 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 centralnog sistema klimatizacije Data centra CT-a, 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 na odgovarajući način od poplava i vremenskih nepogoda.
Unutar prostorija certifikacionog tijela nema vodovodnih instalacija, a oprema je smještena na povišenim podovima.
Prostorija nije smještena u prizemlju i suterenu.

5.1.5. PREVENCIJA I ZAŠTITA OD POŽARA

Certifikaciono tijelo primjenjuje sve potrebne mjere i postupke na prevenciji i zaštiti od požara.
Kompletan prostor Data centra CT-a je zaštićen sistemom za otkrivanje i automatsku dojavu požara tj. senzorima koji su povezani sa centralnim uređajem sistema u portirnici i sistemom obavještavanja na mobilni telefon rukovodioca službe za osiguranje i protivpožarnu zaštitu. U prostoriji certifikacionog tijela nalazi se i dodatni aparat za ručno gašenje požara.

5.1.6. SMJEŠTANJE MEDIJA

Svi mediji na kojima se nalaze podaci certifikacionog tijela, uključujući rezervne kopije sistema i softvera čuvaju se na bezbjedan način na dvije odvojene lokacije. Jedna lokacija je sef koji se nalazi u prostorijama CT-a. Druga lokacija je sef koji se nalazi na udaljenoj lokaciji u Podgorici.

5.1.7. ODLAGANJE NEPOTREBNIH MATERIJALA

Svi mediji i dokumentacija koji više nijesu potrebni za rad certifikacionog tijela i predstavljaju otpad, prije odlaganja u smeće se fizički uništavaju odgovarajućom metodom. Papirni otpad se propušta kroz mašine za sječenje papira, a elektronski mediji se mogu mehanički uništiti ili koristeći poseban uređaj koji zadovoljava najstrože sigurnosne standarde iz ove oblasti (*degausser*).

5.1.8. SMJEŠTANJE KOPIJA MEDIJA NA UDALJENOJ LOKACIJI

Smještanje kopija medija realizuje se na drugoj lokacija koja se nalazi u Podgorici, a koja ima uporediv nivo zaštite sa bezbjednom zonom na lokaciji CT-a.

5.2. ORGANIZACIONE MJERE ZAŠTITE

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 sljedeće povjerljive uloge:

- 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.
- CA Administrator 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 Operator ima sve privilegije i prava pristupa da:
  - Kreira end entity-je (korisnike certifikata);
  - Kreira i izdaje certifikate;
  - Kreira i izdaje tokene.
- 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 je CA Operator i dodatno ima sve neophodne privilegije i prava pristupa da vrši:
  - Provjeru identiteta krajnjih korisnika;
  - Prijem, obradu i registraciju zahtjeva za potrebe izdavanja certifikata;
  - Prijem, obradu i registraciju zahtjeva za opoziv certifikata;
  - Pokretanje procesa za izdavanje ili opoziv certifikata;
  - Po potrebi, provjeru distribucije presonalizovanog linka, PINa i lozinke, i ponovnog slanja istih krajnjem korisniku.

Za potrebe uspostave certifikacionog tijela i sprovođenje procedure generisanja ključeva certfikacionog tijela moguće je definisati i dodatne uloge. Dodatne uloge biće definisane u dokumentu „Procedura generisanja kriptografskih ključeva certifikacionih tijela CTrust sistema".

5.2.2. BROJ OSOBA KOJE SE ZAHTIJEVAJU PO SVAKOM ZADATKU

Sve osjetljive operacije u procesu pružanja elektronskih 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 CT-a vrši se bezbjednosna provjera lica. Upravljanje korisničkim nalozima i kontrola autentifikacionih i autorizacionih parametara obavlja se centralizovano i pod kontrolom je sistem administratora. Svaka osoba sa povjerljivom ulogom ima korisnički nalog na Identity serveru i identifikuje se:

- aplikacijama certifikacionog tijela – certifikatom za klijentsku autentifikaciju na odgovarajućoj smart kartici ili tokenu,
- operativnom sistemu - SSH ključem i kombinacijom korisničnog imena i lozinke.

Svaka operacija nad aplikacijama certifikacionog tijela zahtijeva da lice sa povjerljivom ulogom ima odgovarajuće privilegije za njihovo izvršavanje. Dijeljenje naloga i sredstava za autentifikaciju između osoblja je zabranjeno.
Osoblje izvršava samo one aktivnosti koje su autorizovane u okviru povjerljive uloge kroz ograničenja koje postavlja aplikacija, operativni sistem ili operativne procedure 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	Pristup operativnom sistemu	Pristup aplikaciji CA tijela	Pristup CPAL aplikaciji	Pristup HSM uređaju
HSM administrator	Ne	Ne	Ne	Da
HSM operator	Ne	Ne	Ne	Da
Sistem administrator	Da	Ne	Ne	Ne
CA Administrator	Ne	Da	Ne	Ne
CA Operator	Ne	Da	Ne	Ne
CA Revizor	Ne	Da	Da	Ne
Database administrator	Da	Ne	Ne	Ne
Službenik za registraciju	Ne	Da	Ne	Ne

Tabela 5.1: Prava prijave na sisteme certifikacionog tijela

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

	HSM administrator	HSM operator	Sistem administrator	CA Administrator	CA Operator	CA Revizor	Database administrator	Službenik za registraciju
HSM administrator		Ne				Ne		Ne
HSM operator	Ne			Ne	Ne	Ne		Ne
Sistem administrator						Ne		Ne
CA Administrator					Ne			
CA Operator		Ne				Ne		Ne

CA Revizor	Ne	Ne	Ne	Ne	Ne		Ne	Ne
Database administrator						Ne		Ne
Službenik za registraciju	Ne	Ne	Ne	Ne	Da	Ne	Ne	

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. CT vrši sigurnosnu provjeru u skladu sa internim procedurama CT-a.
Zbog specifičnosti rada na poslovima pružanja elektronskih 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 u skladu sa članom 34 Zakona o elektronskoj identifikaciji i elektronskom potpisu.

5.3.2. PROVJERA PRETHODNIH ANGAŽOVANJA

Provjera osoblja se vrši prema trenutno uspostavljenoj praksi u CT-u, a u skladu sa zakonom i propisima iz ove oblasti.

5.3.3. ZAHTJEVI ZA OBUKAMA

CT 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 CTrust sistemima garantuje se obuka i usavršavanje u skladu sa njihovim povjerljivim ulogama.
Obuka i usavršavanje osoblja s povjerljivim ulogama u radu na CTrust sistemima obuhvata:

- Sigurnosni principi i mehanizmi;
- Svjesnost o sigurnosti;
- Obuka za korišćene 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.

Obuka i usavršavanje osoblja za registraciju u radu na CTrust sistemima uključuje:

- Osnovno o certifikatima;
- Tipovi certifikata koje izdaju certifikaciona tijela i područja njihove upotrebe;
- Načini registrovanja krajnjih 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 krajnje 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 nijesu 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 ULOGA

Nije primjenjivo.

5.3.6. SANKCIJE ZA NEOVLAŠĆENE AKTIVNOSTI

U slučaju neovlašćenih aktivnosti zaposleni podliježe odgovornosti za povredu radne obaveze, a sankcije se određuju u okviru propisanog disciplinskog postupka CT-a.

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 (AUDIT LOGOVA)

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 nijesu 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 procesiraju na dnevnom nivou i arhiviraju na sedmičnom nivou.

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 PROUZROKOVALO 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;
- I druga potrebna dokumentacija.

5.5.2. PERIOD ČUVANJA ARHIVE

Elektronske dnevnike najmanje deset (10) godina.
Certifikati i statusi certifikata čuvaju se trajno.
Ugovore sa krajnjim korisnicima, dokumentaciju krajnjih korisnika i korespodenciju trećih lica najmanje 10 godina.

5.5.3. ZAŠTITA ARHIVE

Podaci za arhive se prikupljaju u bezbjednoj zoni. Pristup bezbjednoj zoni je dozvoljen samo ovlašćenim osobama, kako je to definisano internim procedurama za pristup.
Za arhive operativnog sistema se upotrebljavaju zaštite koje omogućava sam operativni sistem.
Audit logovi aplikacija certifikacionog tijela su zaštićeni tehnologijom kriptografije javnih kriptografskih ključeva.

5.5.4. PROCEDURA PRAVLJENJA REZERVNIH KOPIJA ARHIVE

Certifikaciono tijelo pravi rezervne kopije arhive periodično i čuva dvije odvojene kopije arhive. Jedna kopija arhive se čuva u sefu u CT-u, a druga u sefu na udaljenoj lokaciji koja se nalazi u Podgorici.

5.5.5. ZAHTJEVI ZA VREMENSKI PEČAT ARHIVIRANIH PODATAKA

Arhivirani podaci sadrže vrijeme dobijeno sa sistema na kojem su kreirani. To vrijeme nije elektronski vremenski pečat.

5.5.6. SISTEM SAKUPLJANJA ZAPISA

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

5.5.7. PROCEDURE ZA PRISTUP 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 po isteku 70% perioda važenja certifikata ili ranije, ili opoziva certifikata certifikacionog tijela, certifikaciono tijelo vrši generisanje novog para ključeva certifikacionog tijela i formira certifikat za novo generisani javni ključ, prema formalnoj proceduri uspostave ovih tijela i generisanja para asimetričnih ključeva.
Ceritikaciono tijelo distribuira svoj novi certifikat svim krajnjim korisnicima i trećim licima, kao i u slučaju prvobitno generisanog certifikata 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 usljed 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 certfikacionog tijela ili podređenog certifikacionog tijela CT će odmah po saznanju prekinuti sa upotrebom potencijalno kompromitovanog privatnog ključa.
U slučaju potvrde kompromitacije privatnog ključa korijenskog certifikacionog tijela CTrust PMA donosi odluku o opozivu svih certifikata koje je izdalo to certifikaciono tijelo.
U slučaju potvrde kompromitacije privatnog ključa podređenog certifikacionog tijela CTrust PMA donosi odluku o opozivu pripadajućeg certifikata podređenog certifikacionog tijela i svih certifikata koje je izdalo to certifikaciono tijelo.

O opozivu certifikata CT će obavijestiti sve učesnike CTrust-a putem izdavanja obavještenja na repozitorijumu.
Nakon ustanovljavanja okolnosti zbog kojih je došlo do kompromitacije privatnog ključa certfikacionog tijela CT će preduzeti mjere na otkljanjanju tih okolnosti radi sprečavanja ponovne kompromitacije privatnog ključa.
Certifikaciono tijelo će organizovati novu formalnu proceduru uspostave ovih tijela i generisanja para asimetričnih ključeva, i izdati sve certifikate krajnjih korisnika važeće u momentu kompromitovanja ključa certikacionog tijela koristeći novo generisani certifikat cetifikacionog tijela.

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:

- Obavjestiti sve krajnje korisnike i treća lica putem repozitorijuma i nadležni organ državne uprave najmanje šest mjeseci prije planiranog prestanka rada;
- Korisnicima kojima je već izdao certifikate obezbijediće nastavak pružanja elektronskih usluga povjerenja kod drugog davaoca elektronskih usluga povjerenja i dostaviće mu svu dokumentaciju u vezi sa obavljanjem usluga;
- U slučaju da ne obezbijedi nastavak pružanja elektronskih usluga povjerenja kod drugog davaoca 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 CT-a primjenjuje tehničke bezbjednosne mjere u cilju zaštite kripotografskih ključeva 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 ključeva i certifikata. Tehničke kontrole uključuju životni ciklus bezbjednosnih kontrola kao i operativne bezbjednosne kontrole.

6.1. GENERISANJE KLJUČEVA I INSTALACIJA

6.1.1. GENERISANJE 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 sljedeće 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 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 povjerljivim ulogama u okviru certifikacionog tijela CT-a.
Privatni ključ korijenskog certifikacionog tijela koristi se za napredno elektronsko potpisivanje certifikata podređenog certifikacionog tijela, odgovarajuće liste opozvanih certifikata i certifikata za OCSP servis za ovo certifikaciono tijelo i u druge svrhe se ne smije koristiti.
Privatni ključ podređenog certifikacionog tijela koristi se za napredno elektronsko potpisivanje certifikata koji se izdaju krajnjim korisnicima sa ovog cetifikacionog tijela, odgovarajuće liste opozvanih certifikata i cetifikata za OCSP servis za ovo certifikaciono tijelo i u druge svrhe se ne smije koristiti.

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 krajnje korisnike konkretne elektronske usluge povjerenja opisan je u odgovarajućem 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 krajnje korisnike konkretne elektronske usluge povjerenja opisan je u odgovarajućem 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 krajnji korisnici i treća lica.

6.1.5. DUŽINE KLJUČEVA

Za potrebe korijenskog certifikacionog tijela CTrust Root CA koristi se RSA asimetrični par ključeva dužine 3072 bita . Za formiranje digitalnog potpisa koristi se SHA256/RSA kombinacija hash i algoritma za potpisivanje u PKCS#1 verzija 1.5 formatu digitalnog potpisa.
Za potrebe OCSP servisa korijenskog certifikacionog tijela CTrust Root CA OCSP koristi se RSA asimetrični par ključeva dužine 2048 bita .
Za potrebe podređenih certifikacionih tijela koristi se RSA asimetrični par ključeva dužine 3072 bita . Za formiranje digitalnog potpisa koristi se SHA256/RSA kombinacija hash i algoritma za potpisivanje u PKCS#1 verzija 1.5 formatu digitalnog potpisa.
Za potrebe OCSP servisa podređenog certifikacionog tijela koristi se RSA asimetrični par ključeva dužine 2048 bita .
Za potrebe konkretne elektronske usluge povjerenja dužine ključeva će biti definisane u CPS dokumentu konkretne usluge.
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 modulima).
Kvalitet načina generisanja pomenutih kriptografskih parametara isključivo zavisi od kvaliteta hardverskog generatora slučajnih brojeva na HSM uređajima.
HSM uređaji su certifikovani po standardima propisanim Zakonom o elektronskoj identifikaciji i elektronskom potpisu.

6.1.7. NAMJENA UPOTREBE KLJUČEVA (X.509 KEYUSAGE)

U certifikatima koje izdaje korijensko certifikaciono tijelo mogu se naći sljedeće 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	timeStamping
Certifikat korijenskog certifikacionog tijela	X	X					
Certifikat podređenog certifikacionog tijela	X	X					
Certifikat za OCSP servis korijenskog certifikacionog tijela			X			X	

Tabela 6.1. Vrijednosti *Key Usage* i *Extended Key Usage* ekstenzija u certifikatima koje izdaje korijensko certifikaciono tijelo

U certifikatima koje izdaju podređena certifikaciona tijela CTrust-a vrijednosti u ekstenzijama „Key Usage" i „Extended Key Usage" biće definisane u CPS dokumentima konkretne elektronske usluge povjerenja.

6.2. ZAŠTITA PRIVATNOG KLJUČA I KONTROLA KRIPTOGRAFSKOG HARDVERSKOG MODULA

Certifikaciono tijelo CT-a koristi odgovarajuće kriptografske uređaje za upravljanje životnim vijekom kriptografskih ključeva certifikacionog 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 podređenih certifikacionih tijela se vrši u okviru bezbjednog kriptografskog uređaja koji zadovoljava odgovarajuće zahtjeve u skladu sa međunarodnim standardom FIPS 140-2 L3. Ispunjenje ovog standarda garantuje, između ostalog, da je bilo koji pokušaj narušavanja integriteta uređaja ili kriptografske memorije 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 zahtijeva 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 certifikaciont tijela zahtijeva kontrolu više osoba sa povjerljivim ulogama u okviru certifikacionog tijela CT-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 aktivacionih 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 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 udaljenoj 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 (autorizovano osoblje) certifikacionog tijela imaju zadatak da aktiviraju i deaktiviraju privatni ključ. Privatni ključ je tada aktivan sve dok se ne deaktivira.

6.2.9. METODA DEAKTIVIRANJA PRIVATNOG KLJUČA

Privatni ključ 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 tački 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 podređena certifikaciona tijela).

6.3.2. PERIODI VALIDNOSTI CERTIFIKATA I PRIVATNOG KLJUČA

Rok važenja certifikata po vrstama je definisan u Tabeli 6.1 za certifikate koje izdaje CTrust Root CA.

Certifikat	Rok
Certifikat korijenskog certifikacionog tijela: CTrust Root CA	30 godina i 3 mjeseca
Certifikat podređenog certifkacionog tijela	20 godina i 3 mjeseca
Certifikat za OCSP servis korijenskog certifikacionog tijela	3 mjeseca

Tabela 6.1. Periodi važenja certifikata

Certifikat podređenih certifikacionih tijela izdaje se s vremenom važenja koje ne prelazi perioda važenja certifikata korijenskog certifikacionog tijela.
Vremenski period važenja privatnog ključa može biti jednak vremenskom periodu važenja pripadajućeg certifikata.
Nije dozvoljena upotreba privatnih ključeva nakon isteka perioda važenja istih, nakon isteka perioda važenja pripadajućih certifikata, ili nakon opoziva certifikata.

Rok važenja certifikata po vrstama koje izdaju podređena certifikaciona tijela CTrust-a biće definisane u CPS dokumentima konkretne elektronske usluge povjerenja.

6.4. AKTIVACIONI PODACI

6.4.1. GENERISANJE I INSTALACIJA AKTIVACIONIH PODATAKA

Aktivacijski podaci za privatni ključ korijenskog certifikacionog tijela, podređenih cetifikacionih tijela i OCSP servisa generišu se prilikom sprovođenja formalne procedure uspostavljanja ovih certifikacionih tijela. Aktivacijski podaci instaliraju se na pripadajuće upravljačke kartice HSM modula koje se koriste za aktivaciju slotova na HSM modulu na koje su smješteni odgovarajući privatni ključevi, na principu K od N u skladu sa tačkom 6.2.2.
Podaci za upravljačke kartice HSM modula generišu se u bezbjednom prostoru CT-a od strane službenika operativnog tijela CTrust-a.
Generisanje i instalacija aktivacijskih podataka za druge elektronske usluge povjerenja definisano je u CPS dokumentu konkretne usluge.

6.4.2. ZAŠTITA AKTIVACIJSKIH PODATAKA

Aktivacijski podaci za privatni ključ korijenskog certifikacionog tijela, podređenih cetifikacionih tijela i OCSP servisa koji su smješteni na odgovarajuće kartice HSM modula, zaštićeni su odgovarajućim lozinkama. Lozinke se generišu u bezbjednom prostoru CT-a od strane službenika operativnog tijela CTrust-a. Upravljačke kartice HSM modula i pripadajuće lozinke dodjeljuju se ovlašćenim licima sa povjerljivim ulogama. Upravljačke kartice i pripadajuće lozinke smješaju se u zasebne koverte i čuvaju na dvije lokacije – primarna lokacija u CT-u i udaljena lokacija u Podgorici.
Generisanje i instalacija aktivacijskih podataka za druge elektronske usluge povjerenja definisano je u CPS dokumentu konkretne usluge.

6.4.3. DRUGI ASPEKTI U VEZI AKTIVACIONIH PODATAKA

Nije primjenjivo.

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 koje posjeduju odgovarajuće smart kartice i koja znaju njihove PIN-ove ili odgovarajuće lozinke.

6.5.2. RANGIRANJE BEZBJEDNOSTI RAČUNARA

HSM moduli certifikacionog tijela imaju ocjenu sigurnosti nivoa EAL4+.
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 izdavanje certifikata. Softver koji se koristi u CTrust sistemu potiče iz pouzdanog izvora. Nove verzije softvera testiraju se kod proizvođača u fazi razvoja, a nakon toga i u CTrust sistemu u okviru testnog sajta. Nakon pozitivnih testova, vrši se implementacija softvera u produkcionom okruženju, u skladu sa internom procedurom upravljanja izmjenama na IT sistemima i aplikacijama CT-a.

6.6.2. KONTROLE UPRAVLJANJA BEZBJEDNOŠĆU

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

6.6.3. ŽIVOTNI CIKLUS BEZBJEDNOSNIH KONTROLA

Certifikaciono tijelo sprovodi sva testiranja prije implementacije u okviru testnog sajta.

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 bilježi tok saobraćaja i pokušaje pristupa servisima i javnim internet stranicama certifikacionog 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 je dozvoljeno pod strogo kontrolisanim uslovima.
Nepotrebne komunikacije, nalozi, portovi, protokoli i servisi su eksplicitno zabranjeni ili deaktivirani.
Interna računarska mreža certifikacionog tijela zaštićena je od neovlašćenog pristupa, uključujući pristup krajnjih korisnika i trećih lica.
Svi kritični sistemi za pružanje elektronskih 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

Vremenski pečat se ne koristi u okviru rada korijenskog certifikacionog tijela i podređenih certifikacionih tijela.
CTrust sistemi se usklađuju sa internim servisom tačnog vremena, koji je usklađen sa vanjskim izvorom tačnog vremena (satelitska sinhronizacija tačnog vremena sa atomskim satom putem NTP protokola).

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 elektronskih usluga povjerenja kroz korijensko certifikaciono tijelo i podređena certifikaciona tijela izdaje u skladu sa opsegom ovog dokumenta.
Profili certifikata iz opsega ovog dokumenta koje izdaju podređena CA tijela usaglašeni su sa 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, ETSI EN 319 412-4, i ETSI EN 319 412-5.

Podređena certifikaciona tijela izdaje certifikate prema profilima koji su određeni odgovarajućim dokumentom. 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

CTrust certifikaciona tijela izdaju X.509 v3 certifikate u skladu sa RFC 3280. Koriste se sljedeća X.509 osnovna polja:

X509 ekstenzija	Opis
signature	Napredni elektronski potpis elektronskog certifikata privatnim kriptografskim ključem aplikacije certifikacionog tijela. Algoritam potpisa je RSA-SHA256.
issuer	Jedinstveno ime certifikacionog tijela
Valid From	Datum i vrijeme početka važenja elektronskog certifikata
Valid To	Datum i vrijeme prestanka važenja elektronskog certifikata
subject	Jedinstveno ime krajnjeg korisnika ili naziv OCSP servisa kojem je izdat certifikat
subjectPublicKeyInformation	Javni kriptografski ključ krajnjeg korisnika ili OCSP servisa kojem je izdat certifikat, dužina javnog ključa i naziv algoritma javnog ključa.
version	Verzija X.509 certifikata, verzija 3 (2)
serialNumber	Jedinstveni serijski broj certifikata

7.1.2. EKSTENZIJE CERTIFIKATA

Koriste se sljedeće ekstenzije certifikata:

Naziv polja-ekstenzije	Opis polja – ekstenzije
Authority Key Identifier	Identifikator javnog kriptografskog ključa certifikacionog tijela koji se računa kao RSA-SHA256 hash polja *Subject Public Key* Info certifikata certifikacionog tijela.
Subject Key Identifier	Identifikator javnog kriptografskog ključa krajnjeg korisnika ili OCSP servisa kojem je izdat certifikat koji se računa kao hash polja *Subject Public Key Info* elektronskog certifikata.
Key Usage	Namjena (*keyUsage*) javnog kriptografskog ključa krajnjeg korisnika ili OCSP servisa kojem je izdat certifikatkao što je navedeno u 6.1.7. Polje je u svim certifikatima označeno kao kritično.
Extended Key Usage	Proširena namjena (*ExtendedKeyUsage*) javnog kriptografskog ključa krajnjeg korisnika ili OCSP serivsa kojem je izdatcertifikat kao što je navedeno u 6.1.7.
Certificate Policies	Identifikacija politike certifikacije i adrese Web strane na kojoj se nalaze politika pružanja elektronskih usluga povjerenja i praktična pravila rada.
Issuer Alternative Name	Alternativno ime certifikacionog tijela koje sadrži naziv, poreski identifikacioni broj i oznaku države u kojoj je davalac elektronskih usluga povjerenja registrovan.

Subject Alternative Name	Alternativno ime krajnjeg korisnika ili OCSP servisa kojem je izdat certifikat. U ovom polju npr. može da se navede adresa elektronske pošte krajnjeg korisnika certifikata, ako je adresa elektronske pošte navedena u zahtjevu za izdavanje certifikata.
CRL Distribution Points	Lokacija na kojoj se nalazi lista opozvanih certifikata.
Authority Information Access (authorityInfoAccess)	Informacije o Lokaciji na kojoj je dostupan certifikat na kojem se zasniva napredni elektronski potpis certifikacionog tijela (polje *id-ad-calssuers*).

Ekstenzije certifikata koje izdaju podređena certifikaciona tijela biće definisana u CPS dokumentu konkretne elektronske usluge povjerenja.

7.1.3. IDENTIFIKATOR OBJEKTA (OID) ALGORITAMA

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

Algoritam	OID
sha256WithRSAEncryption	1.2.840.113549.1.1.11
rsaEncryption	1.2.840.113549.1.1.1
Sha1WithRSAEncryption	1.2.840.113549.1.1.5

Tabela 7.1. Algoritmi s pripadajućim OID identifikatorima

7.1.4. FORME IMENA

Certifikati izdati od strane CTRUST-a sadrže kompletno X.500 jedinstveno ime izdavača certifikata i krajnjeg korisnika ili OCSP servisa kojem je izdat certifikat u sljedećim poljima: *issuer name* (CA ime) i *subject name*. Jedinstvena imena su tekstualna polja u X.501 printable, teletex ili UTF8 formatu.

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 OID-ove CTrust-a i/ili ETSI OID-ove. U tački 1.1.2. ovog dokumenta naveden je popis tipova certifikata i pripadajući OID-ovi CTrust-a i standardni 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

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

Klijentske aplikacije moraju procesuirati ekstenzije označene kao kritične u saglasnosti sa RFC 3280.

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 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 s 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 regulisana je Zakonom o elektronskoj identifikaciji i elektronskom potpisu [1], Upravni nadzor nad sprovođenjem Zakona o elektronskoj identifikaciji i elektronskom potpisu [1] vrši Ministarstvo. Inspekcijski nadzor nad radom davalaca elektronskih usluga povjerenja i kvalifikovanih davalaca elektronskih usluga povjerenja i ispunjenošću uslova sistema elektronske identifikacije vrši inspekcija za usluge informacionog društva, u skladu sa zakonom kojim se uređuje inspekcijski nadzor i Zakonom o elektronskoj identifikaciji i elektronskom potpisu [1].

8.1. FREKVENCIJA ILI OKOLNOSTI KADA SE VRŠI REVIZIJA

CTrust PMA će u skladu sa zakonom periodično organizovati internu provjeru i druge procjene usklađenosti sistema. Certifikaciono tijelo organizuje svoj rad u skladu sa relevantnim pravnim aktima koja regulišu rad davalaca elektronskih usluga povjerenja u Crnoj Gori, prije svega Zakona o elektronskoj identifikaciji i elektronskom potpisu i pravilnicima koji proizilaze iz istog, a odnose se na elektronske usluge povjerenja.
Certifikaciono tijelo organizovaće bar jednom godišnje sopstvenu provjeru saglasnosti ovog dokumenta i svog rada sa odgovarajućim propisima, a provjeru će izvršiti interni ili eksterni revizori.

Moguće je izvršiti i više od jedne interne revizije godišnje ukoliko je to zahtijevano od strane PMA ili je to posljedica nezadovoljavajućih rezultata prethodne revizije.

8.2. IDENTITET/KVALIFIKACIJE REVIZORA

Provjera saglasnosti rada certifikacionog tijela vrši se 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 saglasnosti vrši interni revizor koji raspolaže adekvatnim revizorskim iskustvima i poznavanjem Zakona o elektronskoj identifikaciji i elektronskom potpisu.

8.3. ODNOS REVIZORA PREMA OCJENJIVANOM SUBJEKTU

Nadležni organ za ocjenu saglasnosti i angažovana lica su nezavisni od certifikacionog tijela CT-a, sistema ocjenjivanja samog certifikacionog tijela, i oslobođeni su od konflikta interesa.
Interni revizor na internoj provjeri saglasnosti ne ocjenjuje usaglašenost iz sopstvene oblasti odgovornosti, ukoliko ima neku od povjerljivih uloga u CTrust-u.

8.4. TEME POKRIVENE U PROCESU PROCJENJIVANJA

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

- Provjeru usaglašenosti ovog dokumenta i Zakona o elektronskoj identifikaciji i elektronskom potpisu;
- Kompletnost i tačnost dokumentacije;
- Organizacione procese, metode i procedure;
- Tehničke procese i procedure;
- Mjere iz oblasti informacione bezbjednosti;
- Mjere iz oblasti fizičke bezbjednosti;
- Elektronske usluge povjerenja koje pruža certifikaciono tijelo.

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

8.5. AKTIVNOSTI PREDUZETE U SLUČAJU NEUSAGLAŠENOSTI

Certifikaciono tijelo uskladiće svoj rad sa preporukama i nalazima internog revizora ili nadležnog organa za ocjenu saglasnosti.

8.6. OBJAVLJIVANJE REZULTATA

Izvještaj revizije od strane nadležnog organa dostavljaju se CTrust PMA. Izvod iz tog izvještaja certifkaciono tijelo će objaviti na internet stranicama svog repozitorijuma. Neusaglašenosti utvrđene tokom revizije od strane nadležnog organa smatraju se povjerljivim informacijama i one se ne objavljuju.
Rezultati interne revizije dostavljaju se CTrust PMA, povjerljive su prirode i ne objavljuju se javno.

9. DRUGI POSLOVNI I PRAVNI ASPEKTI

9.1. CIJENE

9.1.1. CIJENE PRUŽANJA ELEKTRONSKIH USLUGA POVJERENJA

CT naplaćuje pružanje elektronskih usluga povjerenja u skladu sa cjenovnikom. Cijene ovih usluga biće objavljene na javnim internet stranicama repozitorijuma ili web stranici CT-a www.telekom.me.

9.1.2. NADOKNADE ZA PRISTUP CERTIFIKATU

Ne naplaćuje se.

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

Pogledati tačku 9.1.1.

9.1.5. POLITIKA REFUNDIRANJA

Troškovi se ne refundiraju.

9.2. FINANSIJSKA ODGOVORNOST

CT snosi finansijsku odgovornost za potencijalnu štetu koja može nastati korišćenjem elektronskih usluga povjerenja u skladu sa zakonima koji regulišu ovu oblast.

9.2.1. POKRIVANJE OSIGURANJA

CT je osiguran od rizika odgovornosti za potencijalnu štetu nastalu vršenjem elektronskih usluga povjerenja u skladu sa zakonima i podzakonskim aktima koji regulišu ovu oblast.
CT dodatno osigurava imovinu polisom osiguranja koja pokriva osiguranje od rizika požara, vremenskih nepogoda, poplava, eksplozija, i slično.

9.2.2. OSTALA SREDSTVA

Nije primjenljivo.

9.2.3. OSIGURANJE ILI GARANCIJSKO POKRIVANJE OD STRANE KRAJNJIH KORISNIKA I TREĆIH LICA

Krajnji korisnici elektronskih usluga povjerenja i treća lica koja se pouzdaju u elektronske usluge povjerenja isključivo su odgovorni da obezbijede adekvatno osiguranje ili garanciju pokrivenosti osiguranjem za korišćenje usluga u okviru njihovih servisa ili aplikacija.
Dodatne odredbe vezane za osiguranje ili garancijsko pokrivanje od strane krajnjih korisnika i trećih lica za pojedine usluge biće definisane u CPS dokumentu konkretne elektronske usluge povjerenja.

9.3. POVJERLJIVOST POSLOVNIH INFORMACIJA

9.3.1. OBIM POVJERLJIVIH INFORMACIJA

Sve informacije koje se prikupljaju, generišu, prenose i održavaju od strane CTrust-a, smatraće se povjerljivim, osim informacija opisanih u tački 9.3.2., koje se ne smatraju povjerljivim.

9.3.2. INFORMACIJE KOJE NE ULAZE U OBIM POVJERLJIVIH INFORMACIJA

Informacije koje se objavljuju kao dio certifikata, putem OCSP servisa i CRL, ovog dokumenta ili druge informacije koje se objavljuju u javnom repozitorijumu certifikacionog tijela, neće se smatrati povjerljivim.

9.3.3. ODGOVORNOST ZA ZAŠTITU POVJERLJIVIH INFORMACIJA

CT je odgovoran za zaštitu povjerljivih informacija u skladu sa internim propisima CT-a koji regulišu ovu oblast i pozitivnim propisima Crne Gore.

9.4. PRIVATNOST I ZAŠTITA LIČNIH PODATAKA

CT posvećuje pažnju zaštiti ličnih podataka koje prikuplja, skladišti i upotrebljava u cilju pružanju elektronskih usluga povjerenja iz opsega ovog dokumenta, te sa ličnim podacima postupa u skladu sa odgovarajućim zakonima. Podnošenjem zahtjeva za registraciju za korišćenje elektronskih usluga povjerenja i sklapanjem ugovora, korisnici daju saglasnost CT-u za korišćenje i obradu njihovih ličnih podataka prikupljenih u postupku registracije u skladu sa postojećom zakonskom regulativom te čuvanje tih podataka u trajanju od najmanje 10 godina od prestanka važenja elektronskih usluga povjerenja na koje se ti podaci odnose.

9.4.1. PLAN PRIVATNOSTI

Cerifikaciono tijelo sprovodi mjere i postupke na zaštiti privatnosti i zaštiti ličnih podataka krajnjih korisnika elektronskih usluga povjerenja u skladu sa odgovarajućim zakonima.

9.4.2. INFORMACIJE KOJE SE TRETIRAJU KAO PRIVATNE

Certifikaciono tijelo smatra privatnim sve informacije koje se odnose na krajnje korisnike elektronskih usluga povjerenja, osim onih informacija koje su definisane da se ne tretiraju kao privatne u CPS dokumentu konkretne elektronske usluge povjerenja.

9.4.3. INFORMACIJE KOJE SE NE SMATRAJU PRIVATNIM

Certifikaciono tijelo ne smatra privatnim samo one informacije na koje je krajnji korisnik dao saglasnost da se javno objave ili informacije koje su definisane da se ne tretiraju kao privatne u CPS dokumentu konkretne elektronske usluge povjerenja.

9.4.4. ODGOVORNOST ZA ZAŠTITU PRIVATNIH INFORMACIJA

CT je odgovoran za zaštitu privatnih informacija krajnjih korisnika u skladu sa internim propisima CT-a koji regulišu ovu oblast i pozitivnim propisima Crne Gore.

9.4.5. OTKRIVANJE INFORMACIJA SHODNO PRAVNIM I ADMINISTRATIVNIM PROCESIMA

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

9.4.6. OTKRIVANJE INFORMACIJE U SKLADU SA SUDSKIM ILI ADMINISTRATIVNIM PROCESOM

CT će ustupiti podatke sudu, tužilaštvu i drugim nadležnim državnim organima u slučajevima propisanim odgovarajućim zakonima.

9.4.7. OSTALE OKOLNOSTI KADA SE MOGU OTKRIVATI INFORMACIJE

CT će otkriti privatnu informaciju u ostalim okolnostima samo uz pismenu saglasnost krajnjeg korisnika.

9.5. PRAVA INTELEKTUALNOG VLASNIŠTVA

Sva prava intelektualnog vlasništva nad ovim dokumentom, zaštitnim znacima, certifikatima koje izdaje, repozitorijima na kojima objavljuje informacije i svim dokumentima i informacijama koje su objavljene na repozitorijumima certifikaconog tijela ostaju isključivo vlasništvo Certifikacionog tijela.

9.6. GARANCIJE I ODGOVORNOSTI

9.6.1. GARANCIJE I ODGOVORNOSTI DAVAOCA ELEKTRONSKIH USLUGA POVJERENJA

CT garantuje da pruža elektronske usluge povjerenja, izvršava ostale procedure vezane za upravljanje elektronskim uslugama povjerenja i upravlja infrastrukturom neophodnom za pružanje navedenih usluga u skladu sa ovim dokumentom i propisima iz ove oblasti. CTrust PMA odgovara za usklađenost sa procedurama opisanim u ovom dokumentu i propisama iz ove oblasti, čak i u slučaju kada pojedinu funkciju vezanu za elektronske usluge povjerenja preuzmu podugovarači.
CT se obavezuje da će:

- Pružiti elektronske usluge povjerenja u skladu sa Zakonom o elektronskoj identifikaciji i elektronskom potpisu i odgovarajućim pravilnicima koji proizilaze iz zakona;
- Obezbijediti sav potreban softver i hardver za uspostavu neophodne infrastrukture za pružanje elektronskih usluga povjerenja;
- Obezbijediti odgovarajuće repozitorijume za objavljivanje svih potrebnih informacija i sadržaja za podršku elektronskim uslugama povjerenja;
- Objaviti kontakt informacije certifikacionog tijela;
- U skladu sa standardima koji regulišu ovu oblast i dobrom kriptografskom praksom obezbijediti sigurne mehanizme koji uključuju mehanizam generisanja ključeva krajnjih korisnika, OCSP servisa, i ključeva CA tijela i adekvatnu kriptografsku zaštitu pomenutih ključeva;
- Uspostaviti proceduru dijeljenja tajni za sve povjerljive uloge u skladu sa svojom PKI infrastrukturom;
- U najkraćem mogućem roku obavijestiti krajnje korisnike i treća lica o kompromitaciji sopstvenog privatnog ključa, po mogućnosti po više komunikacionih kanala;
- Ispunjavati sopstveno preuzete obaveze;
- Obavijestiti podnosioce zahtjeva za registraciju za elektronske usluge povjerenja po realizovanoj registraciji, kao i da će obavijestiti krajnje korisnike ako ne bude u mogućnosti da izvrši registraciju navedene usluge;
- Nakon prijema validnog zahtjeva za opozivom elektronske usluge povjerenja opozvati istu;
- Obezbijediti podršku krajnjim korisnicima i trećim licima u skladu sa ovim dokumentom;
- 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;
- Na zahtjev dostaviti kopiju ovog dokumenta svim zainteresovanim stranama;
- Redovno ažurirati ovaj dokument;
- Osigurati da službenici registracionog tijela budu svjesni odredbi koje se na njih odnose u ovom dokumentu;
- Pratiti raspoloživost kapaciteta, planirati održavanje i dalji razvoj sistema u skladu sa budućim potrebama, zahtjevima normi i razvoju tehnologije.

CT se obavezuje da će ispuniti i sve obaveze koje proizilaze iz Zakona o elektronskoj identifikaciji i elektronskom potpisu i odgovarajućim podzakonskim aktima, a nijesu obuhvaćene ovim dokumentom.
CT je odgovoran za izvršavanje navedenih obaveza u obimu koji propisuje zakonska regulativa Crne Gore.
CT nije odgovoran za neodgovarajuću provjeru validnosti certifikata korijenskog certifikacionog tijela od strane koja se pouzdaje u certifikate izdate od strane korijenskog certifikacionog tijela.

9.6.2. GARANCIJE I ODGOVORNOSTI REGISTRACIONOG TIJELA (RA)

RA garantuje za tačnost i potpunost informacija koje provjeravaju njeni službenici. Obaveze, privilegije i prava pristupa RA definisane su u tačkama 1.3.2.1. i 5.2.1. ovog dokumenta, a dodatne obaveze vezane za elektronske usluge povjerenja biće definisane u CPS dokumentu konkretne usluge.

9.6.3. GARANCIJE I ODGOVORNOSTI KRAJNJIH KORISNIKA

U procesu korišćenja elektronskih usluga povjerenja, krajnji korisnici se obavezuju da iste koriste na pouzdan i propisan način. U domenu ličnih garancija krajnjih korisnika je:

- Da posjeduju odgovarajuća znanja za upotrebu certifikata;
- Da se upoznaju sa i poštuju politike pružanja elektronske usluge povjerenja i praktična pravila rada publikovana od strane davaoca elektronske usluge povjerenja;
- Budu svjesna ograničenja certifikata i odgovornosti davaoca elektronske usluge povjerenja kako je detaljno opisano u ovom dokumentu;
- Da verifikuju izdate certifikate od strane certifikacionog tijela primjenom svih raspoloživih metoda provjere certifikata, u smislu provjere da li je certifikat validan (da provjere: period važenja certifikata; da li je certifikat izdat od strane certifikacionog tijela; da li je potpis elektronskog certifikata vjerodostojan; status datog certifikata na važećoj listi opozvanih certifikata ili putem OCSP servisa certifikacionog tijela, a u skladu sa procedurom validacije certifikata i potpunog lanca certifikata);
- Da ograniče oslanjanje na certifikate koje je izdalo certifikaciono tijelo za odgovarajuće upotrebe kako je detaljno objašnjeno u tački 1.4.,
- Da vjeruju u izdati certifikat samo ukoliko se sve informacije koje se odnose na taj certifikat mogu provjeriti da su korektne i ažurne;
- Da se razumno pouzdaju u izdati certifikata u skladu sa odgovarajućim okolnostima;
- Da odmah obavijeste davaoca elektronske usluge povjerenja o bilo kojoj sumnjivoj ili poznatoj zloupotrebi bilo kojeg certifikata koji je izdat od strane certifikacionog tijela.

Dodatne garancije i odgovornosti krajnjih korisnika za pojedine elektronske usluge povjerenja biće definisane u CPS dokumentu konkretne usluge.

9.6.4. GARANCIJE I ODGOVORNOSTI TREĆIH LICA

U procesu korišćenja elektronskih usluga povjerenja, treća lica se obavezuju da iste koriste na pouzdan i propisan način. U domenu garancija trećih lica je:

- Da posjeduju odgovarajuća znanja za upotrebu certifikata;
- Da se upoznaju sa i poštuju politike pružanja elektronske usluga povjerenja i praktična pravila rada publikovana od strane davaoca elektronske usluge povjerenja;
- Budu svjesna ograničenja certifikata i odgovornosti davaoca elektronske usluge povjerenja kako je detaljno opisano u ovom dokumentu;
- Da verifikuju izdate certifikate od strane certifikacionog tijela primjenom svih raspoloživih metoda provjere certifikata, u smislu provjere da li je certifikat validan (da provjere: period važenja certifikata; da li je certifikat izdat od strane certifikacionog tijela; da li je potpis elektronskog certifikata vjerodostojan; status datog certifikata na važećoj listi opozvanih certifikata ili putem OCSP servisa certifikacionog tijela, a u skladu sa procedurom validacije certifikata i potpunog lanca certifikata);
- Ograniče oslanjanje na certifikate koje je izdalo certifikaciono tijelo za odgovarajuće upotrebe kako je detaljno objašnjeno u tački 1.4.;
- Da vjeruju u izdati certifikat samo ukoliko se sve informacije koje se odnose na taj certifikat mogu provjeriti da su korektne i ažurne;
- Da se razumno pouzdaju u izdati certifikata u skladu sa odgovarajućim okolnostima;
- Da odmah obavijeste davaoca elektronske usluge povjerenjao bilo kojoj sumnjivoj ili poznatoj zloupotrebi bilo kojeg certifikata koji je izdat od strane certifikacionog tijela.

Treće lice koje ne poštuje propise i ovaj dokument, te ne postupa u skladu sa obavezama i odgovornostima iz ove tačke, samo snosi sve rizike pouzdanja u konkretnu elektronsku uslugu povjerenja.

Dodatne garancije i odgovornosti trećih lica za pojedine elektronske usluge povjerenja biće definisane u CPS dokumentu konkretne usluge.

9.6.5. GARANCIJE OSTALIH UČESNIKA

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

9.7. IZUZEĆA GARANCIJA I ODGOVORNOSTI

CT daje garancije i odgovorno je samo za aktivnosti definisane zakonom i u tački 9.6.1. CT naročito isključuje:

- Bilo koju odgovornost štete koja je nastala kao rezultat lažnog davanja podataka i lažnog predstavljana privrednog subjekta ili fizičkog lica, tokom procesa identifikacije i potvrde identiteta, ako je službenik RA proceduru identifikacije i verifikacije podataka sproveo u skladu sa ovim dokumentom i propisanom procedurom;
- Bilo koju odgovornost za štetu koja može da se pojavi od momenta kada certifikaciono tijelo primi validan zahtjev za opoziv certifikata, do momenta objave informacije o opozivu istog na CRL, u skladu sa tačkom 4.9.5.;
- Bilo koju odgovornost za stvari van kontrole certifikacionog tijela 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 tački 9.16.5.

9.8. OGRANIČENJA ODGOVORNOSTI

9.8.1. ODGOVORNOST I OGRANIČENJE OD ODGOVORNOSTI DAVAOCA ELEKTRONSKIH USLUGA POVJERENJA

CT je dužan da na propisan način pruža elektronske usluge povjerenja i odgovorno je isključivo za štetu namjerno pričinjenu licu koje se pouzdalo u konkretnu elektronsku uslugu povjerenja, a u skladu sa ovim dokumentom, CPS dokumetnom konkretne elektronske usluge povjerenja i propisima iz ove oblasti kao i ugovorom zaključenim između davaoca elektronske usluge povjerenja i krajnjeg korisnika. CT neće biti odgovoran za indirektnu, nematerijalnu, stvarnu štetu i izmaklu dobit koju krajnji korisnik eventualno pretrpi. Maksimalna finansijska odgovornost certifikacionog tijela u ovom slučaju je do 50.000,00 EUR kumulativno na godišnjem nivou.

9.8.2. ODGOVORNOST I OGRANIČENJE OD ODGOVORNOSTI KRAJNJIH KORISNIKA ELEKTRONSKE USLUGE POVJERENJA

Krajnji korisnik je odgovoran za štetu koja je nastala njegovom krivicom.
Krajnji korisnik nije odgovoran za štetu ako dokaže da je postupao u skladu sa ovim dokumentom, CPS dokumentom konkretne elektronske usluge povjerenja i propisima iz ove oblasti kao i ugovorom zaključenim između davaoca elektronske usluge povjerenja i krajnjeg korisnika.

9.9. OBEŠTEĆENJA

Svaka strana za sebe snosi isključivu odgovornost za nadoknađivanje štete drugim stranama za pretrpljene gubitke ili štetu koja je nastala kao rezultat neovlašćenog korišćenja elektronske usluge povjerenja ili nepostupanja u skladu sa ovim dokumentom, CPS dokumentom konkretne elektronske usluge povjerenja i propisima iz ove oblasti.

9.10. TRAJANJE I PRESTANAK VAŽENJA

9.10.1. TRAJANJE

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

9.10.2. PRESTANAK VAŽENJA

Dokument može biti stavljen van snage objavljivanjem nove verzije ovog dokumenta. U novoj verziji dokumenta biće naznačene obavljene izmjene i datum donošenja nove verzije dokumenta.

9.10.3. POSLJEDICE PRESTANKA VAŽENJA I NASTAVAK DJELOVANJA

Nakon prestanka važenja ovog dokumenta, kao rezultata objavljivanja nove verzije dokumenta, elektronske usluge povjerenja će se koristiti u skladu sa verzijom dokumenta koja je bila validna na dan realizacije zahtjeva za elektronsku uslugu povjerenja. U slučaju promjena okolnosti do nivoa kada ovo nije moguće, CT će obavijestiti krajnje korisnike na način definisan u tački 9.12.2., kao i treća lica preko javnih internet stranica, a na način definisan u tački 2.1.

9.11. POJEDINAČNA OBAVJEŠTENJA I KOMUNIKACIJA SA UČESNICIMA

CT nakon usvajanja dokumenta, distribuira isti kao i druge važeće akte/dokumente preko svoje javne internet stranice repozitorijuma.
Pogledati takođe tačku 9.12.2.

9.12. IZMJENE I DOPUNE

9.12.1. PROCEDURA ZA IZMJENU

Ovaj dokument se mijenja po potrebi. CTrust PMA može bez obavještavanja unositi tipografske ispravke, promjene kontakt podataka te druge manje ispravke koje bitno ne utiču na krajnje korisnike i treća lica. Svi učesnici mogu na kontakt adresu CTrust PMA definisanu u tački 1.5.2. ovog dokumenta poslati dopis s predlogom za ispravke grešaka, predlog dopuna ili izmjenu ovog dokumenta. U dopisu se navode kontakt podaci osobe koja je poslala predlog promjene. CTrust PMA može prihvatiti, prilagoditi ili odbiti predložene promjene nakon razmatranja istih. Izradu nove verzije ili izmjenu i dopunu postojeće verzije dokumenta odobrava i sprovodi CTrust PMA, a u skladu sa poslovnom regulativmom CT-a i relevantnom zakonskom regulativom.

9.12.2. MEHANIZMI OBAVJEŠTAVANJA I VREMENSKI PERIODI

CTrust PMA može odlučiti da ne obavještava krajnje korisnike i treća lica u slučaju izmjena sa malim ili nikakvim uticajem. CTrust PMA u potpunosti odlučuje o tome da li izmjene imaju bilo kakav uticaj na krajnje korisnike i treća lica, na sopstvenu odgovornost.
Sve izmjene u ovom dokumentu biće objavljene na način koji je definisan u poglavlju 2.
CTrust PMA će obavijestiti krajnje korisnike o promjenama koje imaju materijalnog uticaja na njih, putem e-maila i na javnim internet stranicama definisanim u poglavlju 2.

9.12.3. OKOLNOSTI POD KOJIMA SE OID MORA IZMIJENITI

Donošenjem nove verzije dokumenta stvaraju se i okolnosti za definisanje nove OID vrijednosti predmetnog dokumenta.

9.13. PROCEDURE RJEŠAVANJA SPOROVA

Svi sporovi u vezi certifikata moraju se dostaviti na adresu iz tačke 1.5.2.
Sve sporove treba ako je moguće rješavati sporazumno. Ukoliko se dogovor ne može postići sporazumno spor će se rješavati kod nadležnog suda u Crnoj Gori.

9.14. PRIMJENA ZAKONA

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

9.15. USAGLAŠENOST SA PRIMJENLJIVIM ZAKONOM

Ovaj dokument je usaglašen sa:

- Zakonom o elektronskoj identifikaciji i elektronskom potpisu;
- Zakonom o zaštiti podataka o ličnost;
- i drugim propisima iz ove oblasti.

9.16. RAZNE ODREDBE

9.16.1. UGOVOR O PRUŽANJU ELEKTRONSKIH USLUGA POVJERENJA

Ovaj dokument i ugovor o pružanju elektronskih usluga povjerenja sadrže sve elemente koji definišu odnos između davaoca elektronskih usluga povjerenja i krajnjih korisnika.

9.16.2. PRENOS PRAVA

Krajnjim korisnicima elektronskih usluga povjerenja nije dozvoljeno da prava i obaveze koja proističu iz ovog dokumenta i ugovora prenesu u cjelosti ili parcijalno na druga 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)

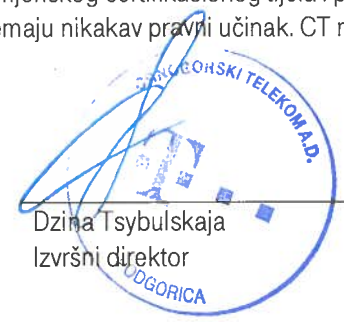
Nije primjenjivo.

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 što su napadi virusa ili napadi sa ciljem onemogućavanja servisa, greške u kriptografskim algoritmima i slično.
CT, krajnji korisnici ili treća lica neće biti odgovorni za bilo kakvu štetu koja je nastala usljed događaja kao rezultat više sile.

9.17. OSTALE ODREDBE

CTrust izdaje testne certifikate. Testni certifikati se prvenstveno izdaju za potrebe testiranja sistema, a mogu se izdati i drugom poslovnom subjektu u svrhu testiranja sistema. Svi testni certifikati označavaju se na način da desni dio vrijednosti *commonName* atributa unutar polja *Subject* završava nizom znakova „Test" ili „TEST" (bez navodnika) u certifikatima korijenskog certifikacionog tijela i podređenih certifikacionih tijela. Testni certifikati izdaju se isključivo u svrhu testiranja i nemaju nikakav pravni učinak. CT ne preuzima nikakvu odgovornost za korišćenje testnih certifikata.



Dzina Tsybulskaja
Izvršni direktor

Prilog 1

Pregled profila certifikata CTrust Root CA

Verzija. 1.1

Podgorica, decembar 2020. godine.

Pregled profila certifikata CTrust Root CA

ISTORIJA DOKUMENTA

Verzija	Datum stupanja na snagu propisa/izmjena	Kratak opis izmjena
1.0	20.11.2020	Definisan dokument sa informacijama o profilima svih certifikata
1.1	1.12.2020	Promjenjen naziv dokumenta. Napravljene promjene u zaglavlju dokumenta i ispravljene slovne greške

SADRŽAJ:

Pregled profila certifikata CTrust Root CA

Struktura OID brojeva za dodjeljivanje Certificate Policy OID brojeva

Struktura CP OID		
NAZIV GRUPE	NAZIV GRANE OID-a	OID
Crnogorski Telekom PEN	Private enterprise number Crnogorski Telekom AD	CT-PEN
Organizaciona jedinica Crnogorskog Telekoma za izdavanje certifikata	OID grana dodijeljena organizacionoj jedinici nadležnoj za izdavanje certifikata - CTrust	OJCA = CT-PEN.1
Certificate Authority	OID grana koja označava konkretno CA tijelo	CAs = OJCAs.x
Certificate Policy	OID koji označava da li se certifikat izdaje za potrebe servisnih aplikacija ili je u pitanju OID koji označava konkretni dokument davaoca elektronskih usluga povjerenja y=0 – certifikat za aplikacije y=1 – Politika pružanja elektronskih usluga povjerenja (CTrust Certificate Policy – Ctrust CP) y=3 – Praktična pravila rada za izdavanje certifikata za napredni elektronski pečat i certifikata za napredni elektronski potpis (CTrust Certificate Practice Statement NQ - CTrust CPS NQ)	CP = CAs.y
Certificate Policy	OID koji označava redni broj tipa certifikata koji se izdaje ili OID koji označava verziju dokumenta davaoca elektronskih usluga povjerenja	CP=CAs.y.N

Tipovi certifikata, oblast primjene certifikata i način čuvanja privatnih ključeva

Tipovi certifikata koje izdaje CTrustRoot CA		
NAZIV GRUPE	NAZIV TIPA CERTIFIKATA	CTrust i ETSI CP OID
Certifikat root CA tijela	CTrust Root CA Certifikat	CTrust CP OID: nema ETSI CP OID: nema
Certifikat za podčinjena CA tijela	CTrust Root CA podčinjeno tijelo certifikat	CTrust CP OID: nema ETSI CP OID: 2.5.29.32.0
Certifikati za OCSP servise	CTrust Root CA OCSP servis certifikat	CTrust CP OID: 1.3.6.1.4.1.56393.1.1.0.1

Područje primjene, sredstvo zaštite privatnog ključa certifikata, tip certifkata i tip nosioca certifikata koje izdaje CTrust Root CA tijelo			
NAZIV TIPA CERTIFIKATA	PODRUČJE PRIMJENE CERTIFIKATA	SREDSTVO ZAŠTITE PRIVATNOG KLJUČA	Tip certifkata i tip nosioca certifikata
CTrust root CA certifikat	Self-sigend root CA certifikat. Koristi se za izradu potpisa prilikom izdavanja certifikata za subordinirani CA i odgovarajući OCSP servis i za potpisivanje izdate CRL liste.	Odgovarajući token na HSM modulu u Crnogorskom Telekomu	Certifikat sa pripadajućim parom ključeva na HSM uređaju u FIPS 140-2 Level 3 režimu rada

Pregled profila certifikata CTrust Root CA

CTrust Root CA podčinjeno tijelo certifikat	Izdaje se subordiniranom CTrust Root CA tijelu. Koristi se za izradu potpisa prilikom izdavanja certifikata krajnjim korisnicima, odgovarajućim servisima i za potpisivanje CRL liste koju izdaje subordinirani CA.	Odgovarajući token na HSM modulu u Crnogorskom Telekomu	Certifikat sa pripadajućim parom ključeva na HSM uređaju u FIPS 140-2 Level 3 režimu rada
CTrust Root CA OCSP servis certfifikat	Izdaje se OCSP servisu za potpis OCSP odgovora za status certifikata koje izdaje CTrust Root CA, osim za sam certifikat OCSP servisa.	Ključ je pod zaštitom KMS modula, upotrebom KEK ključa i ZMK ključa sa odgovarajućeg tokena HSM modula u CT-u	Certifikat sa pripadajućim parom ključeva u KMS aplikaciji zaštićen HSM uređajem u FIPS 140-2 Level 3 režimu rada

Profil certifikata za root CA tijelo: CTrust Root CA

Osnovna polja		
Polje	**Atribut**	**Vrijednost**
Version	Version	X.509 V3
serialNumber	CertificateSerialNumber	9 okteta, serijski broj je uvijek pozitivna vrijednost (18 hexadecimalnih cifri)
signatureAlgorithm	AlgorithmIdentifier	SHA256withRSA
signatureValue		Self-signed digital signature
Issuer	commonName	CTrust Root CA
	organizationName	Crnogorski Telekom A.D. Podgorica
	organizationalIdentifier	VATME-02289377
	countryName	ME
Validity	notBefore	Vrijeme izdavanja certifikata
	notAfter	Vrijeme izdavanja certifikata + 30 godina i 3 meseca
Subject	commonName	CTrust Root CA
	organizationName	Crnogorski Telekom A.D. Podgorica
	organizationalIdentifier	VATME-02289377
	countryName	ME
subjectPublic KeyInfo	AlgorithmIdentifier	RSA
	subjectPublicKey	3072-bit RSA public key

Ekstenzije			
Polje	**Kritično**	**Vrijednost**	
KeyUsage	DA	KeyCertSign, cRLSign	
BasicConstraints	DA	cA=true, pathLen=None	
AuthorityKeyIdentifier	NE	160-bit SHA-1 hash as per RFC 5280	
SubjectKeyIdentifier	NE	160-bit SHA-1 hash as per RFC 5280	
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://ca.ctrust.telekom.me/crl/CTrustRootCA.crl [1] URI: http://www.telekom.me/ctrust/crl/CTrustRootCA.crl

Profil certifikata za podčinjeno CA tijelo: CTrust GP CA

Osnovna polja		
Polje	**Atribut**	**Vrijednost**

Pregled profila certifikata CTrust Root CA

Version	Version	X.509 V3
serialNumber	CertificateSerialNumber	9 okteta, serijski broj je uvijek pozitivna vrijednost (18 hexadecimalnih cifri)
signatureAlgorithm	AlgorithmIdentifier	SHA256withRSA
signatureValue		Potpis izdavača certifikata
Issuer	commonName	CTrust Root CA
	organizationName	Crnogorski Telekom A.D. Podgorica
	organizationalIdentifier	VATME-02289377
	countryName	ME
Validity	notBefore	Vrijeme izdavanja certifikata
	notAfter	Vrijeme izdavanja certifikata + 20 godina + 3 meseca
Subject	commonName	CTrust GP CA
	organizationName	Crnogorski Telekom A.D. Podgorica
	organizationalIdentifier	VATME-02289377
	countryName	ME
subjectPublic KeyInfo	AlgorithmIdentifier	RSA
	subjectPublicKey	3072-bit RSA public key

Ekstenzije			
Polje	**Kritično**	**Vrijednost**	
KeyUsage	DA	KeyCertSign, cRLSign	
BasicConstraints	DA	cA=true pathLen=0	
certificatePolicies	NE	policyIdentifier	anyPolicy: 2.5.29.32.0
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1} cPSuri: http://ca.ctrust.telekom.me/cpcps/
AuthorityKeyIdentifier	NE	160-bit SHA-1 hash as per RFC 5280	
SubjectKeyIdentifier	NE	160-bit SHA-1 hash as per RFC 5280	
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://ocsp.ctrust.telekom.me/CTrustRootCAOCSP
		id-ad-calssuers	Access Method=Certification Authority Issuer accessLocation: http://ca.ctrust.telekom.me/cacert/CTrustRootCA.cer
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://ca.ctrust.telekom.me/crl/CTrustRootCA.crl [1] URI: http://www.telekom.me/ctrust/crl/CTrustRootCA.crl

Profil certifikata za OCSP servis za CTrust Root CA tijelo: CTrust Root CA OCSP servis

Osnovna polja		
Polje	**Atribut**	**Vrijednost**
Version	Version	X.509 V3
serialNumber	CertificateSerialNumber	9 okteta, serijski broj je uvijek pozitivna vrijednost (18 hexadecimalnih cifri)
signatureAlgorithm	AlgorithmIdentifier	SHA256withRSA
signatureValue		Potpis izdavača certifikata
Issuer	commonName (CN)	CTrust Root CA

Pregled profila certifikata CTrust Root CA

	organizationName (O)	Crnogorski Telekom A.D. Podgorica
	orgazinationalIdentifier	VATME-02289377
	countryName (C)	ME
Validity	notBefore	Vrijeme izdavanja certifikata
	notAfter	Vrijeme izdavanja certifikata + 3 mjeseca
Subject	commonName (CN)	CTrust Root CA OCSP Servis
	organizationName (O)	Crnogorski Telekom A.D. Podgorica
	organizationalIdentifier	VATME-02289377
	countryName (C)	ME
subjectPublic KeyInfo	AlgorithmIdentifier	RSA
	subjectPublicKey	2048-bit RSA javni ključ

Ekstenzije			
Polje	**Kritično**	**Atribut**	**Vrijednost**
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
extKeyUsage	DA	OCSPSigning	OID: 1.3.6.1.5.5.7.3.9
ocsp-nocheck	NE		OID: 1.3.6.1.5.5.7.48.1.5
certificatePolicies	NE	policyIdentifier	CTrust Root CA OCSP CP OID: 1.3.6.1.4.1.56393.1.1.0.1
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1} cPSuri: http://ca.ctrust.telekom.me/cpcps/
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://ca.ctrust.telekom.me/crl/CTrustRootCA.crl [1] URI: http://www.telekom.me/ctrust/crl/CTrustRootCA.crl
AuthorityKeyIdentifier	NE	keyIdentifier	160-bit SHA-1 hash as per RFC 5280
SubjectKeyIdentifier	NE	keyIdentifier	160-bit SHA-1 hash as per RFC 5280
BasicConstraints	NE		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://ocsp.ctrust.telekom.me/CTrustRootCAOCSP
		id-ad-calssuers	Access Method=Certification Authority Issuer accessLocation: http://ca.ctrust.telekom.me/cacert/CTrustRootCA.cer

Profil CRL liste koju izdaje CTrust Root CA tijelo

Osnovna polja		
Polje	**Atribut**	**Vrijednost**
Version	Version	X.509 V2
signatureAlgorithm	AlgorithmIdentifier	SHA256withRSA
signatureValue		Potpis izdavača CRL liste
Issuer	commonName (CN)	CTrust Root CA
	organizationName (O)	Crnogorski Telekom A.D. Podgorica
	organizationalIdentifier	VATME-02289377
	countryName (C)	ME
	thisUpdate	Vrijeme izdavanja CRL liste
	nextUpdate	Vrijeme izdavanja CRL liste + 6 mjeseci. Period preklapanja je 5 dana

Ekstenzije			
Polje	**Kritično**	**Atribut**	**Vrijednost**
CRLNumber	NE	CRL Number	Monotono rastući pozitivan broj, početna vrijednost 1
AuthorityKeyIdentifier	NE	keyIdentifier	160-bit SHA-1 hash as per RFC 5280
ReasonCode	NE	reasonCode	Kod razloga opoziva certifikata