PODIJELI DOŽIVLJAJ.

KOMPANIJSKA DIREKTIVA

Crnogorski Telekom a.d. Podgorica

ID broj :	163
Vrsta propisa (skraćenica):	CD
Broj verzije:	1.0
Dokument OID:	1.3.6.1.4.1.56393.1.1.2.1
Odgovorni sektor:	Sektor za razvoj servisa i digitalnu transformaciju
Datum donošenja/usvajanja:	
Datum stupanja na snagu:	20/11/2020
Validnost:	Neodređeno
Broj aneksa/priloga:	1

Praktična pravila rada za pružanje elektronske usluge povjerenja izdavanja certifikata CTrust GP CA Crnogorskog Telekoma A.D. Podgorica (CTrust GP CA Certificate Practice Statement - CTrust GP CA CPS)

	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

Eksterne reference:

OSNOVNI ZAKON

[1] Zakon o elektronskoj identifikaciji i elektronskom potpisu

PRAVILNICI

[2] Pravilnik o bližim uslovima koje mora da ispunjava kvalifikovani davalac elektronskih usluga povjerenja

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

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

[5] Pravilnik o tehničkim i operativnim zahtjevima koji se odnose na čvor - mjesto priključenja sistema elektronske identifikacije i procesu uspostavljanja okvira za interoperabilnost sistema elektronske identifikacije

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

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

[8] Pravilnik o načinu sprovođenja verifikacije i načinu vršenja usluge čuvanja kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata

OSTALI ZAKONI

[9] Zakon o zaštiti podataka o ličnosti

STANDARDI

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

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

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

[13] 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

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

[15] ETSI EN 319 412-1 V1.1.1. (2016-02) – Electronic Signatures and Infrastructures

(ESI);Certificate Profiles; Part 1: Overview and common data structures
[16] 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
[17] 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
[18] ETSI EN 319 412-5 V2.2.1. (2017-11) – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
[19] 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
[20] ETSI TS 119 312 V1.3.1. (2019-02) – Electronic Signatures and Infrastructures (ESI); Cryptographic Suites
[21] ETSI TS 119 495 V1.3.1. (2019-03) – Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366
[22] ETSI TS 119 412-1 V1.2.1 (2018-05) - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
[23] EN 419 211-1:2014 – Protection profiles for secure signature creation device – Part 1: Overview (EN 419211-1:2014)
[24] EN 419 211-2:2013 – Protection profiles for secure signature creation device – Part 2: Device with key generation (EN 419211-2:2013)
[25] 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)
[26] 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)
[27] NIST FIPS PUB 140-2 (2001) – Security Requirements for Cryptographic Modules
[28] IETF RFC 3647 – Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework
[29] IETF RFC 5280 (2008) – Internet X.509 Public Key Infrastructure; Certificate and Certificate Revocation List (CRL) Profile
[30] 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

SADRŽAJ:

1. UVOD

Crnogorski Telekom A.D. Podgorica (u daljem tekstu: CT) registrovan je kao kvalifikovani davalac elektronskih usluga povjerenja u skladu sa Zakonom o elektronskoj identifikaciji i elektronskom potpisu. 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 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-a 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 (subordinate CA): CTrust GP CA

CT ostavlja mogućnost uspostave 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.

CTrust GP CA je CTrust Root CA podređeno certifikaciono tijelo (u daljem tekstu: podređeni CA) koji izdaje certifikate:

- za napredni elektronski pečat krajnjim korisnicima,
- za napredni elektronski pečat CTrust sistemu za izradu kvalifikovanih elektronskih vremenskih pečata,
- za napredni elektronski pečat CTrust sistemu za kvalifikovanu elektronsku preporučenu dostavu,
- za OCSP servis za provjeru statusa certifikata koje izdaje podređeno certifikaciono tijelo.

Ovim dokumetnom opisani su postupci izdavanja certifikata i praktična pravila rada podređenog certifikacionog tijela CTrust GP CA.

1.1.1. OPSEG I NAMJENA

Ovaj dokument „Praktična pravila rada za pružanje elektronske usluge povjerenja izdavanja certifikata CTrust GP CA Crnogorskog Telekoma A.D. Podgorica (CTrust GP CA Certificate Practice Statement - CTrust GP CA CPS)" (engl. *Certification Practice Statement for issuing Certificates for Electronic Signatures and Electronic identification*, u daljem tekstu: CPS) opisuje postupke i procedure koje primjenjuje CTrust GP CA za izdavanje i upravljanje životnim vijekom produkcionih certifikata (u daljem tekstu: certifikati).
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.
Certifikaciono tijelo utvrđuje i interna pravila rada davaoca elektronskih usluga povjerenja (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 usluga povjerenja.

1.1.2. TIPOVI CERTIFIKATA

U poslednjoj verziji dokumenta „Pregled profila certifkata CTrust GP CA sistema" navedeni su grupe, tipovi certifikata i profil certifikata koje izdaje CTrust GP CA.
Konkretno izdaju se sledeci tipovi certifikata:

- Napredni elektronski pečat krajnjim korisnicima
- Napredni elektronski pečat sistemu za izradu kvalifikovanih elektronskih vremenskih pečata (eng. Time Stamp Authority)
- Napredni elektronski pečat sistemu za preporučenu elektronsku dostavu (eng. eDelivery)
- CTrust GP CA OCSP servis certifikat

1.2. NAZIV DOKUMENTA I IDENTIFIKACIONI PODACI

CT-u je dodijeljen od strane IANA organizacije (Internet Assigned Number Authority) sledeći OID: 1.3.6.1.4.1.56393.
Na osnovu tog OID-a CT je za potrebe pružanja elektronskih usluga povjerenja dodijelio sledeći OID: 1.3.6.1.4.1.56393.1.
U nastavku je naveden naziv ovog dokumenta i njegovi identifikacioni podaci.
Naziv: Praktična pravila rada za pružanje elektronske usluge povjerenja izdavanja certifikata CTrust GP CA Crnogorskog Telekoma A.D. Podgorica (CTrust GP CA Certificate Practice Statement - CTrust GP CA CPS)
Verzija: 1.0
Datum stupanja na snagu: 20.11.2020
Internet adrese na kojoj je objavljen ovaj 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)

Osnovna funkcija certifikacionog tijela je da izdaje certifikate korisnicima, i internim servisima za podršku infrastrukturi CTrust-a.
U opsegu ovog dokumenta i certifikacionog tijela CT-a Ctrust GP CA je izdavanje certifikata čiji su tipovi definisani u tački 1.2., stoga se mjere, postupci i politike opisane u ovom dokumentu primjenjuju na proces izdavanja certifikata korisnicima istih.
Hijerarhijska struktura certifkacionih tijela opisana je u tački 1.1.
Da bi se trećim licima omogućila provjera vjerodostojnosti i validnosti izdatih certifikta CTrust GP CA sistem organizuje objavljivanje liste opozvanih certifikata. CRL lista se periodično objavljuje na repozitorijumu namijenjenom u tu svrhu.
CTrust GP CA certifikaciono tijelo takođe u svrhu provjere statusa certifikata organizuje OCSP servis. Na OCSP servisu informacije o statusu certifikata dostupne su u realnom vremenu.

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

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 korisničkih certifikata na osnovu zahtjeva korisnika ili na svoju inicijativu;
- Izdavanje i objavljivanje liste opozvanih certifikata;
- Rješavanje sporova između 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. Zaposleni CT-a koji rade u poslovnicama u smislu ovog dokumenta predstavljaju službenike za registraciju.

Službenici za registraciju za potrebe izdavanja certifikata u ime certifikacionog tijela CT-a obavljaju sljedeće aktivnosti:

- Vrše identifikaciju korisnika po važećim zakonskim procedurama i pravilima rada CT-a, a za potrebe pružanja elektronske usluge povjerenja;
- Primjenjuju interne procedure za provjeru službenih i ovjerenih dokumenata u cilju provjere identiteta korisnika i valjanosti njihovog zahtjeva, i preuzimaju službena i ovjerena dokumenta;
- Dostavljaju korisniku popunjen zahtjev za elektronsku uslugu povjerenja, da provjeri validnost podataka;
- Registruju fizičko, pravno lice ili preduzetnika za korišćenje elektronskih usluga povjerenja koje pruža certifikaciono tijelo u sklopu procedure podnošenja zahtjeva za elektronsku uslugu povjerenja;

- Uručuje korisniku elektronske usluge povjerenja ugovor o korišćenju elektronskih usluga povjerenja kvalifikovanog davaoca elektronskih usluga povjerenja CT-a, u skladu sa internim procedurama CT-a;
- Dostavljaju sve neophodne i potrebne podatke validnih zahtjeva za uslugom povjerenja CTrust GP CA u cilju izdavanja certifikata krajnjim korisnicima;
- Učestvuju u procesu ponovnog dostavljanja aktivacionih podataka neophodnih za preuzimanje izdatih certifikata na zahtjev korisnika certifikata;
- Učestvuju u procesu opoziva certifikata na zahtjev korisnika certifikata ili nadležnog organa;
- Obavljaju i druge potrebne poslove u skladu sa internim procedurama CT-a.

CTrust registraciona tijela djeluju u skladu sa praksom, procedurama i osnovnim dokumentima rada CTrust-a. Ne postoji ograničenje na broj registracionih tijela koja mogu biti pridružena CTrust infrastrukturi.

Registraciona tijela centralizovano vode evidenciju svih aktivnosti koje izvršavaju za potrebe certifikacionog tijela. Registraciona tijela vrše prijem, verifikaciju i prosljeđivanje zahtjeva za opozivom, i ponovno dostavljanje aktivacionih podataka neophodnih za preuzimanje izdatih certifikata krajnjih korisnika prema procedurama propisanim od strane certifikacionog tijela i u skladu sa ovim dokumentom.

Registraciona tijela odgovorna su za izvršavanje gore navedenih aktivnosti shodno tački 9.6.2. ovog dokumenta.

1.3.2.2. CENTRALNO REGISTRACIONO TIJELO CTRUST-A

Centralno registraciono tijelo CT-a dio je certifikacionog tijela koje je namijenjeno da primi zahtjeve za elektronske usluge povjerenja od CTrust RA, operativnog tima ili PMA i pokrene proces realizacije usluge. Članovi CTrust operativnog tima obavljaju aktivnosti u Centralnom registracionom tijelu, i to sljedeće:

- Učestvuju u procesu izdavanja certifikata krajnjih korisnika, i pomažu kod detektovanja i otklanjanja problema nastalih u procesu izdavanja ovog tipa certifikata;
- Realizuju izdavanje certifikata za napredni elektronski pečat sistemu za izradu kvalifikovanih elektronskih vremenskih pečata (eng. *Time Stamp Authority*) i certifikata za napredni elektronski pečat sistemu za kvalifikovanu elektronsku preporučenu dostavu (eng. *eDelivery*) prema formalnoj proceduri uspostave ovih usluga;
- Realizuju izdavanje certifikata za CTrust GP CA OCSP servis prema formalnoj proceduri izdavanja ovog tipa certifikata.

1.3.3. NARUČIOCI I KORISNICI

Fizička lica, preduzetnici i pravna lica u Crnoj Gori predstavljaju korisnike elektronskih usluga povjerenja koje pruža CTrust. Naručioc *(subscriber)* moze biti fizičko lice, pravno lice ili preduzetnik. Uslugu povjerenja upotrebljava korisnik (*subject*) čije se ime ili funkcija registruju kod prijave za korišćenje elektronske usluge povjerenja.
Za elektronske usluge povjerenja definisane ovim dokumentom naručilac je istovremeno i korisnik.
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.
U cilju provjere validnosti primijenjenog certifikata, treća lica moraju uvijek da provjere status opozvanosti predmetnog certifikata u okviru liste opozvanih certifikata izdate od strane certifikacionih tijela CT-a ili putem OCSP servisa prije nego što prihvate informacije koje su navedene u certifikatu kao tačne i da provjere period važenja i ispravnost certifikata prije nego se pouzdaju u certifikat.

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

Korisnici certifikata iste upotrebljavaju u skladu sa Zakonom o elektronskoj identifikaciji i eletkronskom potpisu i u skladu sa ovim dokumentom.

1.4.1. DOZVOLJENA UPOTREBA CERTIFIKATA

Certifikati koje izdaje CTrust GP CA se mogu koristiti za različite namjene u zavisnosti od politike certifikata. Politika certifikata je u svakom izdatom certifikatu označena u ekstenziji *certificatePolicies* u skladu sa specifikacijom u RFC-u (*Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*).
Certifikate izdate od strane CTrust GP CA je dozvoljeno koristiti za verifikaciju elektronskog potpisa, verifikaciju elektronskog pečata, verifikaciju elektronskog vremenskog pečata, verifikaciju elektronske preporučene dostave. Dozvoljena namjena upotrebe pojedinog tipa certifikata koje izdaje CTrust GP CA je definisana u tački 1.1.2. Tipovi certifikata.

1.4.2. ZABRANJENA UPOTREBA CERTIFIKATA

Zabranjena je svaka upotreba certifikata izdatih od strane CTrust GP CA koja nije u skladu sa namjenom certifikata, Zakonom o elektronskoj identifikaciji i elektronskom potpisu i ovim dokumentom.

1.5. ADMINISTRACIJA CPS DOKUMENTA

1.5.1. ORGANIZACIJA KOJA UPRAVLJA CPS DOKUMENTOM

CTrust PMA u ime CT-a periodično pregleda i ažurira ovaj dokument u skladu sa promjenama odredbi u zakonskoj regulativi, prilikom promjene tehničkih karakteristika primijenjenih kriptografskih algoritama ili dužina kriptografskih ključeva, definisanja novih tipova certifikata koje izdaje CTrust GP CA, ili drugim relevatnim situacijama.

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.

1.5.4. PROCEDURA ODOBRAVANJA CPS DOKUMENTA

CPS dokument CT-a periodično se pregleda i ažurira po potrebi. Period pregleda i ažuriranja ovog dokumenta je minimalno jednom u dvije godine ili prilikom pripreme provjere usklađenosti.
Dokument se može pregledati i po potrebi ažurirati i češće ukoliko dođe do promjena u zakonskoj regulativi ili se javi potreba za promjenu primijenjenih kriptografskih algoritama ili dužina kriptografskih ključeva.
Na osnovu predloga CTrust PMA CPS 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.
Akreditacija	Formalna deklaracija od strane potvrdnog autoriteta da izvjesne funkcije/entiteti zadovoljavaju specifične formalne zahtjeve.
Aplikacija za certifikat	Zahtjev poslat od strane korisnika koji zahtijeva certifikat (aplikant) ka Certifikacionom tijelu u cilju izdavanja certifikata.
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.
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.
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 (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.
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 subordinate/intermediate entitete, kao što su certifikati drugih CA i korisnici.
Identifikacija	Utvrđivanje da dato ime pojedinca odgovara realnom identitetu pojedinca.

Identifikator objekta (Object identifier)	Sekvenca brojčanih komponenti koja može biti pridružena nekom registrovanom objektu i koja ima karakteristiku da je jedinstvena u svim identifikatorima objekata u okviru specifičnog domena.
Javni ključ	Matematički podatak koji može biti javno objavljen (najčešće se objavljuje u formi X.509v3 elektronskog certifikata) i koji se koristi za verifikaciju elektronskog potpisa, kreiranog pomoću odgovarajućeg privatnog ključa koji je matematički par sa datim javnim ključem, kao i za šifrovanje podataka za korisnika koji posjeduje odgovarajući privatni ključ.
Korisnički ugovor	Ugovor između korisnika i CT-a u cilju pružanja elektronskih usluga povjerenja.
Korisnik	Fizičko ili pravno lice koje se oslanja na elektronsku identifikaciju ili elektronsku uslugu povjerenja.
Kriptografija	Nauka o zaštiti tajnosti informacija.
Kriptografski algoritmi	Algoritmi po kojima se vrši transformacija originalne informacije u šifrovanu informaciju (šifrat) i obratno, iz šifrata u originalnu infomaciju, korišćenjem odgovarajućeg kriptografskog ključa.
Kriptografski ključ	Tajna i slučajna informacija odgovarajuće dužine u bitovima (na primjer 128 ili 256 bita) koja se koristi u kriptografskim algoritmima, u procedurama šifrovanja i dešifrovanja.
Kvalifikator politike	Informacija koja zavisi od politike certifikacije i koja je pridružena identifikatoru politike certifikacije u okviru X.509 certifikata. Može da uključi i URL na kome se nalazi publikovan CPS datog certifikacionog tijela.
Kvalifikovani certifikat za elektronski potpis	Kvalifikovani certifikat za elektronski potpis je certifikat koji ispunjava uslove propisane članom 16 Zakona o elektronskoj identifikaciji i elektronskom potpisu.
Kvalifikovani elektronski potpis	Kvalifikovani elektronski potpis je napredni elektronski potpis koji je izrađen pomoću kvalifikovanog sredstva za izradu elektronskog potpisa i zasniva se na kvalifikovanom certifikatu za elektronski potpis.
Lanac (put) certifikata	Uređena sekvenca certifikata koja se, zajedno sa javnim ključem inicijalnog objekta u lancu (putu), procesira u cilju provjere istog u 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.
Opoziv certifikata	Permanentno ukidanje validnosti datog certifikata i njegovo smještanje na CRL listu.
Organ vlasti	Državni organ, organ državne uprave, organ lokalne samouprave, odnosno lokalne uprave i pravno lice koje vrši javna ovlašćenja.
Podaci za izradu elektronskog potpisa	Jedinstveni podaci (kodovi ili privatni kriptografski ključevi), koje potpisnik koristi za izradu elektronskog potpisa.
Podaci za verifikaciju	Podaci koji se koriste za verifikaciju elektronskog potpisa.
Politika certifikacije	Imenovan skup pravila koji indicira primjenljivost certifikata na određeno okruženje i/ili na klasu aplikacija sa zajedničkim bezbjednosnim zahtjevima.

Potpisnik	Fizičko lice koje 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 korisnika primjenom asimetričnog kriptografskog algoritma.
Registraciono tijelo (RA)	Tijelo odgovorno za identifikaciju i autentifikaciju korisnika/vlasnika certifikata, kao i kreiranje zahtjeva za izdavanje certifikata, ali koji ne izdaje i ne potpisuje certifikat (tj. RA vrši odgovarajuće poslove (identifikaciju korisnika) i u tom smislu je delegirano od CA). Često se i termin LRA (Local Registration Authority) koristi u istom kontekstu.
Repozitorijum	Web stranica i/ili direktorijum na kome su javno dostupni osnovni dokumenti rada CA, kao i eventualne druge informacije koje se odnose na pružanje 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.
Kvalifikovano sredstvo za izradu elektronskog potpisa	Kvalifikovano sredstvo za izradu elektronskog potpisa je sredstvo za izradu kvalifikovanog elektronskog potpisa koje ispunjava posebne uslove propisane članom 19 Zakona o elektronskoj identifikaciji i elektronskom potpisu.
Sredstva za provjeru elektronskog potpisa	Odgovarajuća tehnička sredstva (softver i hardver) koja služe za provjeru elektronskog potpisa, uz korišćenje podataka za provjeru elektronskog potpisa.
Sredstva za provjeru kvalifikovanog elektronskog potpisa	Sredstva za provjeru elektronskog potpisa koja ispunjavaju dodatne uslove utvrđene Zakonom o elektronskom potpisu.
Šifrovanje	Transformacija koja primjenom odgovarajućeg kriptografskog algoritma i odgovarajućeg kriptografskog ključa, pretvara originalnu informaciju u oblik u kojem sadržaj te informacije postaje nedostupan neovlašćenim licima (šifrat).
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 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.
eng. Policy Managment Authority	Upravljačko tijelo CTrust-a

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
JMB	Jedinstveni Matični Broj
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) kvalifikovanog davaoca elektronskih usluga povjerenja Crnogorskog Telekoma A.D. Podgorica"
- 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, suspenziju, reaktivaciju 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 korisnicima i trećim licima u vezi s davanjem elektronskih usluga povjerenja;
- Ostale informacije vezane za rad CTrust-a.

Certifikati izdati od CTrust GP CA sistema se ne objavljuju u repozitorijumu.
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 s 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 GP CA tijelo je: http://ocsp.ctrust.telekom.me/CTrustGPCAOCSP.

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 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 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 infastrukture.
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 KORISNIKA

Procedure identifikacije i autentifikacije navedene u ovom dokumentu se odnose na certifikate koje izdaje CTrust GP CA.

3.1. DODJELJIVANJE IMENA

3.1.1. VRSTE IMENA

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

CTrust GP CA

Atribut po X.520	Vrijednost	Objašnjenje
serialNumber	Jedinstveni serijski broj u tekstualnom obliku ili numeričkom obliku	Jedinstveni serijski broj u okviru CTrust sistema
commonName (CN)	Puni ili skraćeni naziv pravnog lica	Puni ili skraćeni naziv pravnog lica
organizationIdentifier	Registrovani poreski identifikacioni broj (PIB) pravnog lica u formatu „VATME-PIB"	Identifikator pravnog lica
OrganizationName	Registrovani puni ili skraćeni naziv pravnog lica	Naziv pravnog lica
organizationlUnit	Naziv organizacione jedinice u okviru pravnog lica	Naziv organizaciona jedinica u okviru pravnog lica - opciono
organizationlUnit	Pravno lice	Oznaka da se certifikati izdaju pravnim licima
countryName	ME	Dvoslovni ISO kod države, ME za Crnu Goru

Tabela 3.1 Sadržaj imena

3.1.2. POTREBA DA IMENA BUDU SA REALNIM ZNAČENJEM

Imena koja se upisuju u certifikate koje korisnicima izdaje certifikaciono tijelo CTrust GP CA moraju odgovarati podacima iz centralnog registra privrednih subjekata (u daljem tekstu: CRPS) i drugih evidencija državnih organa Crne Gore.

3.1.3. ANONIMNOST 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 GP CA vrši se po tabeli 3.1 u tačkii 3.1.1. koja je usklađena sa zakonom i odgovarajućim standardima.

3.1.5. JEDINSTVENOST IMENA

Certifikaciono tijelo CTrust GP CA garantuje jedinstvenost imena pridruženog korisnicima certifikata izdatim različitim korisnicima, pošto se imena uvijek koriste zajedno sa atributom *SerialNumber*, tj. jedinstvenost *Subject* polja garantuje se atributima *CommonName* i *serialNumber*.

3.1.6. UPOTREBA ROBNIH MARKI („TRADEMARKS") U CERTIFIKATIMA

Certifikaciona tijela ne koriste robne marke u svojim certifikatima.

3.2. INICIJALNA PROVJERA IDENTITETA

Službenik za registraciju registracionog tijela dužan je da od podnosioca zahtjeva pribavi sva potrebna dokumenta za utvrđivanje identiteta podnosioca zahtjeva u skladu sa internim procedurama CT-a i odgovarajućim zakonima.

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

Ne postoji potreba za dokazivanjem posjedovanja privatnog ključa od strane krajnjeg korisnika jer se par asimetričnih ključeva generiše u okviru samog certifikacionog tijela u procesu izdavanja certifikata.
Prilikom generisanja para asimetričnih ključeva certifikaciono tijelo pridržava se najbolje prakse i postupaka iz standarda kojim je regulisana ova oblast.

Metoda dokazivanja posjedovanja privatnog ključa za generisanje certifikata za sistem za izradu kvalifikovanog elektronskog vremenskog pečata i sistem za preporučenu elektronsku dostavu obezbijeđena je sprovođenjem procedure uspostave sistema koji realizuju konkretne usluge i generisanja para asimetričnih ključeva.
Certifikaciono tijelo izdaje certifikate prema tački 1.1.2.

3.2.2. PROVJERA IDENTITETA PRAVNOG LICA

Pravno lice koje zahtijeva izdavanje certifikata mora da obezbijedi dovoljno dokaza o svom identitetu. Provjera identiteta pravnog lica može se vršiti koristeći jedan od sljedećih načina:

- Original ili ovjerena kopija zvaničnih dokumenata koji pružaju dokaz o identitetu pravnog lica – rješenje, odnosno izvod o registraciji iz CRPS-a, ne starije od šest mjeseci, odnosno za javne ustanove i nevladine organizacije i druge pravne subjekte, dokaz o registraciji od ovlašćenog nadležnog organa;
- Sačuvane informacije ako je bila provjera identiteta pravnog lica prethodno utvrđivana od strane CT-a.

Pravno lice podnosi zahtjev preko fizičkog lica koje mora imati važeće ovlašćenje da djeluje u ime pravnog lica. CTrust RA će provjeriti identitet ovlašćenog lica kao što je definisano u tački 3.2.3., i njegovo ovlašćenje da djeluje u ime pravnog lica kao što je definisano u tački 3.2.5.
Predaju dokumentacije za izdavanje/obnovu certifikata može predati fizičko lice koje mora imati važeće ovlašćenje formirano na osnovu propisanog obrasca ovlašćenja CT-a, ovjereno pečatom i potpisano.

3.2.3. PROVJERA IDENTITETA FIZIČKOG LICA

Fizičko lice koje je ovlašćeno da djeluje u ime pravnog lica, će biti identifikovana licem u lice. Pojedinci moraju da se identifikuju koristeći jedan od sljedećih važećih identifikacionih dokumenata, izdatih od strane odgovarajućeg državnog organa:

- Lična karta
- Pasoš

3.2.4. PODACI O KORISNIKU KOJI SE NE PROVJERAVAJU

CTrust ne provjerava podatke koji se ne nalaze na identifikacionom dokumentu (npr. e-mail adresa, broj telefona,...). Korisnik je odgovoran za tačnost podataka unesenih na Zahtjevu i Ovlašćenju, a koji se ne nalaze na identifikacionom dokumentu.

3.2.5. PROVJERA OVLAŠĆENJA

Pojedinac koji zahtijeva certifikat u ime pravnog lica mora da obezbijedi validnu dokumentaciju na ime pravnog lica koje će biti upisano u certifikate, u skladu sa tačkom 3.2.2. Provjera identiteta pravnog lica. Naziv pravnog lica koje će biti uključeno u certifikat mora biti identično Registrovanom punom ili skraćenom nazivu pravnog lica kako je u prezentiranim dokumentima.

CTrust RA službenik provjerava identičnost podataka o ovlašćenom fizičkom licu sa ovlašćenja i iz zahtjeva za izdavanje certifikata, ovlašćenje mora biti formirano na osnovu propisanog obrasca ovlašćenja CT-a, ovjereno pečatom i potpisom.

3.2.6. KRITERIJUMI ZA INTEROPERABILNOST

Procedure i prakse povezanih certifikacioni 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

3.3.1. PROVJERA IDENTITETA KOD RUTINSKE OBNOVE CERTIFIKATA

Rutinska obnova se odvija kad se valjanost certifikata ili privatnog ključa približava kraju. Za certifikate krajnjih korisnika identifikacija korisnika koji zahtijevaju obnovu certifikata se provjerava kao što je definisano u tačkama 3.2.2. Provjera identiteta pravnog lica i 3.2.3. Provjera identiteta fizičkog lica.

3.3.2. PROVJERA IDENTITETA KOD ZAHTJEVA ZA OBNOVU CERTIFIKATA POSLIJE OPOZIVA

Identifikacija korisnika koji zahtijevaju obnovu certifikata poslije opoziva se provjerava kao što je definisano u tačkama 3.2.2. i 3.2.3.

3.4. PROVJERA IDENTITETA KOD ZAHTJEVA ZA OPOZIV CERTIFIKATA

Identifikacija korisnika koji zahtijevaju opoziv certifikata se provjerava kao što je definisano u tačkama 3.2.2. Provjera identiteta pravnog lica i 3.2.3. Provjera identiteta fizičkog lica.

4. UPRAVLJANJE CERTIFIKATIMA

Procedure upravljanja certifikatima navedene u ovom dokumentu se odnose na certifikate koje izdaje CTrust GP CA.

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

Zahtjev za izdavanje certifikata mogu podnijeti pravna lica, preduzetnici ili fizička lica registrovana kod nadležnih organa u Crnoj Gori.

4.1.2. PROCES OBRADE ZAHTJEVA ZA IZDAVANJEM CERTIFIKATA I ODGOVORNOSTI

CTrust izdaje certifikate tek nakon provjere identiteta korisnika i uspješnog završetka procesa registracije. Glavni koraci u procesu obrade zahtjeva za izdavanje certifikata su:

- Korisnik podnosi potpisan obrazac za prijavu i prilaže valjan dokument za identifikaciju kao što je opisano u 3.2.;
- Korisnik prihvata CTrust CP i CPS uslove potpisivanjem korisničkog ugovora (*End-User Agreement*);
- Zahtjev za izdavanje certifikata je prihvaćen i odobren od strane CTrust RA službenika završetkom procesa registracije, unosom svih neophodnih podataka u odgovarajuću aplikaciju i pokretanjem automatizovanog procesa generisanja odgovarajućeg certifikata;
- Procedura generisanja certifikata započinje kreiranjem ili izmjenom podataka o korisniku (ukoliko već postoji) u CA aplikaciji. Za takvog korisnika se generiše par asimetričnih ključeva, lozinka i certifikat. Par asimetričnih ključeva i lozinka čuvaju se u KMS modulu zaštićeni odgovarajućim KEK i ZMK ključevima. Na zahtjev RA operatera aplikacija certifikacionog tijela kreira fajl u p12 formatu (pfx) koji sadrži par asimetričnih ključeva i zaštićen je lozinkom. Za ove operacije koriste se KMS modul i HSM.
- Personalizovani link i PIN za preuzimanje fajla generiše se u RA aplikaciji.
- Personalizovani link, PIN za preuzimanje fajla sa certifikatom u odgovarajućem formatu i lozinku je potrebno poslati korisniku koji je tražio izdavanje certifikata:

- personalizovani link sa kojeg se preuzima fajl sa certifikatom se elektronskim putem šalje na e-mail adresu koju je korisnik naveo na obrascu zahtjeva za izdavanje certifikata;
- PIN za preuzimanje fajla i lozinka za otključavanje certifikata se šalju putem SMS-a na broj telefona koji je korisnik naveo na obrascu zahtjeva za izdavanje certifikata.

Korisnik koristi personalizovani link i PIN za preuzimanje fajla sa certifikatom u odgovarajućem formatu putem internet pretraživača. Korisnik otključava certifikat koristeći lozinku.
Obaveza korisnika je:

- Da u periodu od 15 dana preuzme fajl sa certifikatom u odgovarajućem formatu, i isti otključa;
- Da provjeri e-mail, uljučujući neželjenu poštu, i SMS poruke na telefonu. Ukoliko nakon provjere ustanovi da nije primio neophodni personalizovani link i/ili lozinku i PIN o tome obavijesti CTrust RA.

CTrust RA službenik na osnovu prijave o neuspješnom prijemu personalizovanog linka i/ili lozinke i PIN-a pokreće proces ponovnog slanja istih ukoliko period od 15 dana nije istekao.

4.2. PROCESUIRANJE ZAHTJEVA ZA IZDAVANJE CERTIFIKATA

4.2.1. POSTUPAK IDENTIFIKACIJE I AUTENTIFIKACIJE KORISNIKA

CTrust vrši identifikaciju i autentifikaciju kao što je definisano u tačkama 3.2.2. Provjera identiteta pravnog lica i 3.2.3. Provjera identiteta fizičkog lica.

4.2.2. ODOBRAVANJE ILI ODBIJANJE ZAHTJEVA ZA IZDAVANJE CERTIFIKATA

Zahtjev za CTrust GP CA certifikat će biti odobren ako su ispunjeni svi sljedeći uslovi:

- Podnosilac zahtjeva je predao popunjen obrazac zahtjeva za izdavanje i priložio važeće dokumente za identifikaciju u skladu sa tačkama 3.2.2. Provjera identiteta pravnog lica i 3.2.3. Provjera identiteta fizičkog lica;
- Podnosilac zahtjeva ima odgovarajuće ovlašćenje;
- Podaci na obrascu zahtjeva za izdavanje su potpuni;
- Identifikacija identiteta korisnika i provjera ovlašćenja je uspješna;
- Podnosilac zahtjeva potpisom korisničkog ugovora potvrđuje da je upoznat sa uslovima CTrust CP/CPS i da ih prihvata.

U slučaju da bilo koji od navedenih kriterijuma nije ispunjen ili ako postoji opravdana sumnja da podnosilac zahtjeva ne ispunjava uslove ovog dokumenta, korisničkog ugovora ili propisane važećim zakonima Crne Gore CTrust Registraciono tijelo će odbiti zahtjev.

4.2.3. VRIJEME ZA OBRADU ZAHTJEVA

Inicijalna obrada zahtjeva za izdavanje certifikata počinje u toku prisustva podnosioca zahtjeva u poslovnicama CT-a, tj. obavezno se u dijelu inicijalne obrade mora obaviti provjera identiteta podnosioca zahtjeva.
Vrijeme kompletne obrade zahtjeva je do 7 dana od prijema zahtjeva, pod uslovom da su svi podaci u zahtjevu tačni i u skladu sa ovim dokumentom.

4.3. IZDAVANJE CERTIFIKATA

4.3.1. AKTIVNOSTI TOKOM PROCESA IZDAVANJA CERTIFIKATA

Izdavanje certifikata za OCSP, TSA ili eDelivery sprovodi se prema formalnoj proceduri uspostave ovih sistema i generisanja para asimetričnih ključeva. Ovu proceduru sprovode lica sa povjerljivim ulogama u zaštićenom prostoru Ctrust-a uz primjenu propisanih mjera bezbjednosti.

Nakon prijema validnog zahtjeva za izdavanjem certifikata za krajnje korisnike certifikaciono tijelo sprovodi proces izdavanja odgovarajućih certifikata na sljedeći način:

- Službenik CTrust Registracionog tijela unosi podatke sa zahtjeva u odgovarajuću aplikaciju, i nakon toga pokreće proces generisanja certifikata;
- CTrust RA aplikacija koristeći web servise CA aplikacije preko zaštićenog kanala podnosi zahtjeve za izdavanje certifikata i preuzima p12 fajlove;
- CTrust RA aplikacija kreira ili po potrebi ažurira podatke o krajnjem korisniku na CA aplikaciji i pokreće proces kreiranja tokena koji je povezan sa odgovarajućim profilima certifikata na CA tijelu. Token čine par asimetričnih ključeva, lozinka i certifikat;
- Proces kreiranja tokena u Certifikacionom tijelu podrazumijeva generisanje para asimetričnih ključeva i lozinke u KMS modulu, a zatim i kreiranje odgovarajućeg certifikata, a u skladu sa definisanim profilom konkretnog certifikata koji se izdaje. Izrada certifikata se realizuje generisanjem naprednog elektronskog potpisa koristeći privatni ključ certifikacionog tijela, čime se sprečava falsifikovanje certifikata.
- Na zahtjev CTrust RA aplikacije par asimetričnih ključeva zajedno sa certifikatom se smješta u odgovarajuću strukturu p12 formata zaštićenu lozinkom i dostavlja CTrust RA aplikaciji kroz odgovor na web servis. CTrust RA aplikacija generiše personalizovani link, PIN i isti distribuira zajedno sa lozinkom krajnjem korisniku i omogućava preuzimanje p12 fajla sa konkretnog personalizovanog linka i za konkretni PIN. Personalizovani link se dostavlja na e-mail adresu krajnjeg korisnika, a PIN i lozinka se dostavljaju putam SMS-a.
- Personalizovani link, PIN i lozinku krajnji korisnik koristi u procesu pruzimanja i otključavanja fajla u odgovarajućem formatu.

4.3.2. OBAVJEŠTENJE KORISNIKA OD STRANE CERTIFIKACIONOG TIJELA O IZDAVANJU CERTIFIKATA

Dostavljanjem personalizovanog link-a na e-mail adresu krajnjeg korisnika, i PIN-a i lozinke na mobilni uređaj krajnjeg korisnika putam SMS-a, smatra se da je korisnik obaviješten od strane certifikacionog tijela da je certifikat izdat i spreman za preuzimanje.

4.4. PRIHVATANJE CERTIFIKATA

4.4.1. SPROVOĐENJE PROCESA PRIHVATANJA CERTIFIKATA

Izdati certifikati smatraju se prihvaćenim od strane korisnika ukoliko se ispuni bilo koji od dolje navedenih uslova:

- Korisnik je putem internet pretraživača pristupio personalizovanom linku i koristeći PIN potvrdio uspješno preuzimanje fajla u odgovarajućem formatu;
- Ukoliko korisnik ne javi da postoje bilo kakvi problemi u izdatom certifikatu u periodu od petnaest (15) dana nakon dostavljanja personalizovanog linka, PIN-a i lozinke.

Korisnik je dužan da se obrati CTrust RA u slučaju bilo kakvih problema vezanih za proces prihvatanja certifikata.

4.4.2. OBJAVLJIVANJE CERTIFIKATA

Izdati certifikati se javno ne objavljuju.

4.4.3. OBAVJEŠTAVANJE OSTALIH UČESNIKA O IZDAVANJU CERTIFIKATA

Ne obavještavaju se drugi učesnici.

4.5. KORIŠĆENJE CERTIFIKATA I PRIPADAJUĆIH ASIMETRIČNIH PAROVA KLJUČEVA

4.5.1. KORIŠĆENJE PRIVATNIH KLJUČEVA I CERTIFIKATA OD STRANE KORISNIKA

Korisnik se obavezuje da će koristiti privatne ključeve i pripadajuće certifikate izdate od strane certifikacionog tijela prema definisanom načinu korišćenja ključa u samom certifikatu (*Key Usage* i *Extended Key Usage* ekstenzije definisane RFC 5280 standardom) i politikama certifikacije definisanim u ovom dokumentu.
Korišćenje privatnih ključeva i pripadajućih certifikata predstavlja dio korisnikovog ugovora sa certifikacionim tijelom. U tom smislu, korisnik može koristiti svoje privatne ključeve samo nakon prihvatanja odgovarajućih certifikata.
Takođe, korisnik mora prestati da koristi svoje privatne ključeve nakon isticanja perioda validnosti ili opoziva izdatih certifikata.
Korisnik mora čuvati privatni ključ, te preduzeti mjere opreza kako bi se spriječilo otkrivanje i neovlašćenog korišćenje njegovog privatnog ključa.

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 korišćenjem izdatih certifikata 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;
- Odmah obavijeste CA u slučaju sumnje ili poznate zloupotrebe bilo kojeg certifikata kojeg je izdao CTrust (vidi kontakt informacije u tački 1.5.2. Kontakt osoba).

4.6. OBNAVLJANJE CERTIFIKATA BEZ PROMJENE KLJUČA

Obnova certifikata bez promjene ključa je proces u kojem certifikaciono tijelo izdaje certifikat za isti javni ključ. Certifikaciono tijelo CTrust GP CA ne vrši obnovu certifikata bez promjene ključa.

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

Obnova certifikata sa novim ključem (*re-key*) je proces u kojem certifikaciono tijelo izdaje korisniku novi certifikat. Novi certifikat sadrži iste identifikacione podatke o korisniku kao stari certifikat i korisnikov novi javni ključ.

4.7.1. OKOLNOSTI POD KOJIMA SE MOŽE OBNOVITI CERTIFIKAT

Obnova certifikata se vrši:

- nakon opoziva certifikata ili
- prije isteka vremenskog perioda važnosti certifikata ili privatnog ključa, a na osnovu zahtjeva korisnika ili
- nakon što je istekao vremenski period važnosti certifikata ili privatnog ključa.

4.7.2. KO MOŽE DA ZAHTIJEVA OBNOVU CERTIFIKATA

Obnovu certifikata mogu tražiti korisnik ili ovlašćeni predstavnik pravnog lica koje je zatražilo izdavanje prvog certifikata.

4.7.3. PROCES OBRADE ZAHTJEVA ZA OBNOVU CERTIFIKATA

Obnova certifikata izvodi se na isti način kao početni zahtjev za izdavanje certifikata.

4.7.4. OBAVJEŠTAVANJE KORISNIKA O IZDAVANJU OBNOVLJENOG CERTIFIKATA

Kao što je opisano u tački 4.3.2.

4.7.5. POSTUPAK POTVRDE PRIHVATANJA OBNOVLJENOG CERTIFIKATA

Kao što je opisano u tački 4.4.1.

4.7.6. OBJAVA OBNOVLJENOG CERTIFIKATA

Kao što je opisano u tački 4.4.2.

4.7.7. OBAVJEŠTAVANJE OSTALIH UČESNIKA O IZDAVANJU OBNOVLJENOG CERTIFIKATA

Ne obavještavaju se drugi učesnici.

4.8. PROMJENA CERTIFIKATA KORISNIKA

Promjena certifikata je postupak koji omogućava korisnicima da zahtijevaju promjenu podataka sadržanih u certifikatu. Promjena certifikata traži obnovu certifikata i obrađuje se kao početni zahtjev za izdavanje certifikata.

4.8.1. OKOLNOSTI POD KOJIMA SE MOŽE PROMIJENITI CERTIFIKAT

Korisnik može zahtijevati promjenu certifikata kada se promijeni bilo koji od identifikacionih podataka (npr. Naziv pravnog lica, ili PIB).

4.8.2. KO MOŽE DA ZAHTIJEVA PROMJENU CERTIFIKATA

Promjenu certifikata mogu tražiti korisnik ili ovlašćeni predstavnik pravnog lica koje je zatražilo izdavanje prvog certifikata.

4.8.3. PROCES OBRADE ZAHTJEVA ZA PROMJENU CERTIFIKATA

Promjena certifikata izvodi se na isti način kao početni zahtjev za izdavanje certifikata.

4.8.4. OBAVJEŠTAVANJE KORISNIKA O IZDAVANJU PROMIJENJENOG CERTIFIKATA

Kao što je opisano u tački 4.3.2.

4.8.5. POSTUPAK POTVRDE PRIHVATANJA PROMIJENJENOG CERTIFIKATA

Kao što je opisano u tački 4.4.1

4.8.6. OBJAVA PROMIJENJENOG CERTIFIKATA

Kao što je opisano u tački 4.4.2

4.8.7. OBAVJEŠTAVANJE OSTALIH UČESNIKA O IZDAVANJU PROMIJENJENOG CERTIFIKATA

Ne obavještavaju se drugi učesnici.

4.9. OPOZIV I SUSPENZIJA CERTIFIKATA

4.9.1. OKOLNOSTI ZA OPOZIV CERTIFIKATA

Po zahtjevu službenika za registraciju CTrust RA tijela, nadležnog državnog organa ili samog korisnika certifikaciono tijelo vrši opoziv izdatog certifikata u sljedećim slučajevima:

- opoziv certifikata zahtijeva potpisnik, autor elektronskog pečata ili njegov ovlašćeni zastupnik;
- ako certifikaciono tijelo utvrdi da je podatak u certifikatu pogrešan ili je certifikat izdat na osnovu pogrešnih podataka;
- ako certifikaciono tijelo primi obavještenje da je potpisnik ili pravno, odnosno fizičko lice u čije ime potpisuje izgubilo poslovnu sposobnost, umrlo ili je prestalo da postoji, odnosno istekao rok važenja ovlašćenja za potpisivanje ili su se promijenile činjenice koje utiču na važenje certifikata;

- ako certifikaciono tijelo utvrdi da su podaci za izradu elektronskog potpisa ili informacioni sistem potpisnika ugroženi na način koji utiče na pouzdanost i bezbjednost izrade elektronskog potpisa ili kad treće lice te podatke koristi na neprimjeren način;
- ako certifikaciono tijelo utvrdi da su podaci za provjeru elektronskog potpisa ili informacioni sistem davaoca usluga povjerenja za izdavanje certifikata ugroženi na način koji utiče na bezbjednost i pouzdanost certifikata;
- ako certifikaciono tijelo prestaje sa radom ili mu je rad zabranjen, a izdatim certifikatima nije istekao rok važenja, osim ako elektronske usluge povjerenja izdavanja certifikata ne prenese na drugog davaoca tih usluga;
- istekne rok važenja certifikata;
- ako certifikaciono tijelo primi sudsku odluku ill upravni akt koji se odnose na važenje certifikata;
- postoje drugi pravni razlozi predviđeni internim aktima iz člana 37 stav 4 Zakona o elektronskoj identifikaciji i elektronskom potpisu, i drugim propisima koji regulišu ovu oblast;
- ako certifikaciono tijelo utvrdi da korisnik krši odredbe ovog dokumenta.

4.9.2. KO MOŽE ZAHTIJEVATI OPOZIV CERTIFIKATA

Opoziv certifikata može biti zatražen od:

- korisnika certifikata u poslovnici CT-a uz neposrednu provjeru identiteta na osnovu fizičke prisutnosti;
- službenika za registraciju CTrust RA tijela uz odgovarajući dokaz da je ispunjen jedan od uslova za opoziv iz tačke 4.9.1.;
- suda ili nadležnog organa državne uprave.

4.9.3. PROCEDURA OPOZIVA CERTIFIKATA

U slučaju da je potrebno izršiti opoziv certifikata usljed ispunjenja uslova za opoziv iz ovog poglavlja korisnik certifikata dužan je da u najkraćem mogućem roku kontaktira službenika za registraciju certifikacionog tijela radi dostavljanja zahtjeva za opoziv. Korisnik mora lično doći u poslovnicu CT-a da podnese zahtjev za opoziv certifikata.
Identifikacija podnosioca zahtjeva za opoziv se radi kao što je definisano u tački 3.4. Provjera identiteta kod zahtjeva za opoziv.
Opozivom certifikata njegov serijski broj pojavljuje se u listi opozvanih certifikata, a njegov status putem OCSP servisa postaje opozvan.
Opoziv certifikata obavezno sadrži datum i vrijeme opoziva, a proizvodi dejstvo od trenutka unošenja u evidenciju opozvanih certifikata.
Certifikaciono tijelo će da obavijesti potpisnika, odnosno autora elektronskog pečata o opozivu certifikata, u roku od 24 časa od primljenog zahtjeva ili obavještenja, odnosno nastanka okolnosti zbog koje se certifikat opoziva.

4.9.4. VRIJEME ZA PREDAJU ZAHTJEVA ZA OPOZIV CERTIFIKATA

Subjekt koji je postao svjestan okolnosti koje zahtijevaju opoziv certifikata mora zatražiti opoziv što je prije moguće i bez nepotrebnog odgađanja.

4.9.5. PERIOD VREMENA U KOJEM CERTIFIKACIONO TIJELO MORA DA OBRADI ZAHTJEV ZA OPOZIVOM CERTIFIKATA

Registraciono tijelo će odmah i bez odlaganja sprovesti postupak za opoziv certifikata, a najkasnije 24 časa po prijemu validnog zahtjeva.

4.9.6. ZAHTJEVI ZA PROVJEROM OPOZVANOSTI CERTIFIKATA OD 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 salgasnosti sa politikom certifikacije i svojim obavezama propisanim ovim dokumentom.

4.9.7. FREKVENCIJA IZDAVANJA LISTE OPOZVANIH CERTIFIKATA

Certifikaciono tijelo objavljuje listu opozvanih certifikata (CRL) svakih sat vremena, sa periodom važenja CRL liste od 24 sata.

4.9.8. MAKSIMALNO KAŠNJENJE OBJAVLJIVANJA LISTE OPOZVANIH CERTIFIKATA

U regularnim okolnostim kašnjenje u objavi liste opozvanih certifikata 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

Certifikaciono tijelo CT-a daje informacije o statusu certifikata putem OCSP servisa i objave CRL.
Informacija o statusu opozvanosti elektronskog certifikata dostupna je putem OCSP servisa i CRL i nakon isteka certifikata.
Preporuka trećim licima je da za provjeru statusa certifikata koriste OCSP servis i da se provjera statusa pristupom CRL koristi kao alternativna metoda provjere u slučaju nedostupnosti OCSP servisa ili u slučaju da aplikacija trećih lica podržava provjeru statusa certifikata samo putem CRL.

Adresa OCSP servisa zavisi od certifikacionog tijela za koje OCSP odgovara o statusu certifikata, a upisuje se u ekstenziji *Authority Information Access* svih certifikata koje izdaje pripadajuće certifikaciono tijelo.
Objedinjena CRL za certifikate koje izdaju certifikaciona tijela objavljuju se na repozitorijumu certifikacionog tijela.
Adrese objave CRL sadržane su u ekstenziji *CRLDistributionPoints* u svakom izdatom certifikatu.

4.10.1.1. ADRESE ZA PRISTUP CRL ZA CTRUST GP CA CERTIFIKATE

Adrese objedinjene CRL za CTrust GP CA certifikate na internet serverima su:
http://ca.ctrust.telekom.me/crl/CTrustGPCA.crl
http://www.telekom.me/ctrust/crl/CTrustGPCA.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

Prestanak korišćenja certifikata može se ostvariti zbog prestanka pružanja elektronskih usluga povjerenja od strane certifikacionog tijela.

4.12. ČUVANJE I REKONSTRUKCIJA PRIVATNOG KLJUČA

CTrust ne nudi ovu uslugu.

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 certifikacionog tijela, korisničkim kriptografskim ključevima i korisničkim certifikatima.

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 nisu potrebni za rad certifikacionog tijela i predstavljaju otpad, prije odlaganja u smeće se fizički uništavaju odgovarajućom metodom. Papirni otpad se propušta kroz mašine za 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 lokaciji 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 certifikaciono 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 korisnika;
  - Prijem, obradu i registraciju zahtjeva za potrebe izdavanja certifikata;
  - Prijem, obradu i registruju zahtjeve 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 elektrosnkih 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 autentifikovani korisnik 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 usluga od 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 Korisnika;
- Uobičajene prijetnje u procesu provjere informacija;
- Rad u aplikacijama koje se koriste u registracionim tijelima;
- Svjesnost o sigurnosti;
- Zaštita ličnih podataka;
- Informacije s kojima je potrebno upoznati Korisnike.

5.3.4. FREKVENCIJA I ZAHTJEVI ZA PONOVNU OBUKU

Obuka lica u certifikacionom tijelu i registracionim tijelima vrši se periodično i po potrebi radi održavanja potrebnog nivoa znanja zaposlenih za izvršavanje radnih zadataka.
Plan obrazovanja osoba se redovno revidira i u periodima koji 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 primjenjeno.

5.3.6. SANKCIJE ZA NEOVLAŠĆENE AKTIVNOSTI

U slučaju neovlašćenih aktivnosti zaposleni podliježe odgovornosti za povrednu 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 PROUZROKOVAO DOGAĐAJ

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

5.4.8. PROCJENA RANJIVOSTI SISTEMA

Certifikaciono tijelo periodično organizuje procjenu ranjivosti sistema.

5.5. ARHIVIRANJE ZAPISA/LOGOVA

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

5.5.1. TIPOVI ARHIVIRANIH ZAPISA

Zapisi koji se čuvaju:

- Zapisi o izdatim certifikatima;
- Informacije o podnešenim zahtjevima za izdavanje certifikata;
- 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 korisnicima, dokumentaciju 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 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 CTrust PMA donosi odluku o opozivu pripadajućeg certifikata certifikacionog tijela i svih certifikata koje je izdalo to certifikaciono tijelo.
O opozivu certifikata CT će obavestiti 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 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 korisnike 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 kljlučeva i aktivacionih podataka. Kripotografski ključevi koji se štite mjerama i postupcima opisanim u ovom poglavlju mogu pripadati samom certifikacionom tijelu, servisima ili krajnjim korisnicima. 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, servisa ili krajnjih korisnika.
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 upravljaja 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;
- U procesu izdavanja certifikata za naprednu elektronski pečat krajnjim korisnicima certifikaciono tijelo generiše par asimetričnih ključeva koji se smještaju na odgovarajućem tokenu u okviru certifkacionog tijela. Token čine par asimetričnih ključeva, lozinka i certifikat. Proces kreiranja tokena u Certifikacionom tijelu podrazumijeva generisanje para asimetričnih ključeva i lozinke u KMS modulu, a zatim i kreiranje i odgovarajućieg certifikata, a u skladu sa definisanim profilom konkretnog certifikata koji se izdaje. Izrada certifikat se realizuje generisanjem naprednog elektronskog potpisa koristeći privatni ključ certifikacionog tijela, čime se sprečava falsifikovanje certifikata.

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 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.
Proces isporuke privatnog ključa krajnjih korisnika za napredni elektronski pečat se realizuje na sljedeći način:

- Na zahtjev CTrust RA aplikacije par asimetričnih ključeva zajedno sa certifikatom se smješta u odgovarajuću strukturu p12 formata zaštićenu lozinkom i dostavlja CTrust RA aplikaciji kroz odgovor na web servis. CTrust RA aplikacija generiše personalizovani link, PIN i isti distribuira zajedno sa lozinkom krajnjem korisniku i na taj način omogućava preuzimanje p12 fajla krajnjem korisniku koji posjeduje odgovarajući personalizovani link i PIN. Perosnalizovani link se dostavlja na e-mail adresu krajnjeg korisnika, a lozinka i PIN se dostavljaju putam SMS-a.
- Krajnji korisnik koristi personalizovani link i PIN za preuzimanje p12 fajla, sa odgovarajuće web adrese, na svom računaru, a lozinku koristi u procesu otključavanja fajla. Nakon otključavanja fajla korisnik ima pristup paru asimetričnih ključeva, i certifikatu, i odgovoran je za čuvanje istih.

6.1.3. DOSTAVLJANJE JAVNOG KLJUČA DO CERTIFIKACIONOG TIJELA

Dostava javnog ključa podređenog certifikacionog tijela vrši se u okviru procedure uspostavljanja certifikacionog tijela.
Dostava javnog ključa OCSP servisa, sistema za izradu elektronskog vremenskog pečata, i sistema za izradu elektronske preporučene dostave vrši se u okviru formalne procedure uspostavljanja ovih sistema.
Dostava javnog kluča krajnjih korisnika nije primjenjiva.

6.1.4. DOSTAVLJANJE JAVNOG KLJUČA CERTIFIKACIONOG TIJELA TREĆIM LICIMA

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

6.1.5. DUŽINE KLJUČEVA

Za potrebe korijenskog certifikacionog tijela CTrust Root CA koristi se RSA asimetrični par ključeva dužine 3072 bita i periodom validnosti certifikata od 30 godina i 3 mjeseca. Za formiranje digitalnog potisa koristi se SHA256/RSA kombinacija hash i algoritma za potpisivanje u PKCS#1 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 i periodom validnosti certifikata od 3 mjeseca.
Za potrebe podređenog certifikacionog tijela Ctrust GP CA koristi se RSA asimetrični par ključeva dužine 3072 bita i periodom validnosti certifikata od 20 godina i 3 mjeseca. Za formiranje digitalnog potpisa koristi se SHA256/RSA kombinacija hash i algoritma za potpisivanje u PKCS#1 verzija 1.5 formatu digitalnog potpisa.
Za potrebe OCSP servisa podređenih certifikacionih tijela koristi se RSA asimetrični par ključeva dužine 2048 bita i periodom validnosti certifikata od 3 mjeseca
Za kvalifikovane certifikate za napredni elektronski pečat krajnjim korisnicima, za kvalifikovane certifikate za uslugu izrade kvalifikovanog elektronskog vremenskog pečata, za kvalifikovane certifikate za usluge preporučene elektronske dostave i certifikate za OCSP servise koristi se RSA asimetrični par ključeva dužine 2048 bita.
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), ili pomoću softverskih generatora slučajnih brojeva koji su realizovani u KMS modulu.
Kvalitet načina generisanja pomenutih kriptografskih parametara isključivo zavisi od kvaliteta hardverskog generatora slučajnih brojeva na HSM uređajima, ili kvaliteta softverskih generatora slučajnih brojeva koji su realizovani u KMS modulu.
HSM uređaj certifikovani su po standardima propisanim Zakonom o elektronskoj identifikaciji i elektronskom potpisu.

6.1.7. NAMJENA UPOTREBE KLJUČEVA (X.509 KEYUSAGE)

Certifikati koje izdaju korijensko i podređena certifikaciona tijela CT-a 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			X			X	
Certifikata za uslugu elektronskog vremenskog pečata			X				X
Certifikata za uslugu elektronske preporučene dostave			X				
certifikat za napredni elektronski pečat				X			

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

6.2. ZAŠTITA PRIVATNOG KLJUČA I KONTROLA KRIPTOGRAFSKOG HARDVERSKOG MODULA

Certifikaciono tijelo CT-a koristi odgovarajuće kriptografske uređaje za upravljanje životnim vijekom kriptografskih ključeva certifikaciongo tijela. Certifikaciono tijelo koristi Hardverski bezbjednosni modul – HSM koji u skladu sa svim relevantnim standardima zaštite kriptografskih uređaja.
Certifikaciono tijelo CT-a ne vrši zaštitu privatnih ključeva krajnjih korisnika, već su krajnji korisnici odgovorni za zaštitu istih.

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 istovremeno detektovan.
HSM uređaji ne smiju da napuštaju bezbjednu zonu certifikacionog tijela izuzev rijetkih prilika unaprijed definisanih premeštanja 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 poverljivim 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
uređaju, on se čuva u šifrovanom obliku u memoriji HSM uređaja.

6.2.8. METODA AKTIVACIJE PRIVATNOG KLJUČA

Nosioci dijeljenih tajni (staraoci) 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.

Certifikat	Rok
Certifikat korijenskog certifikacionog tijela: CTrust Root CA	30 godina i 3 mjeseca
Certifikat podređenog certifkacionog tijela: Ctrust GP CA	20 godina i 3 mjeseca
Certifikat za napredni elektronski pečat	Do 3 godine
Certifikat za uslugu izrade kvalifikovanog elektronskog vremenskog pečata	Do 5 godine
Certifikat za uslugu preporučene elektronske dostave	Do 5 godine
Certifikat za OCSP servis	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, nakon opoziva certifikata ili za vrijeme dok je certifikat suspendovan.

6.4. AKTIVACIONI PODACI

6.4.1. GENERISANJE I INSTALACIJA AKTIVACIONIH PODATAKA

Aktivacijski podaci za privatni ključ korijenskog certifikacionog tijela, podređenih cetifikacionih tijela, OCSP servisa, kvalifikovanog certifikata za uslugu izrade kvalifikovanih elektronskih vremenskih pečata i kvalifikovanog certifikata za uslugu preporučene elektronske dostave generišu se prilikom sprovođenja formalne procedure uspostavljanja ovih sistema. Aktivacijski podaci instaliraju se na pripadajuće upravljačke kartice HSM modula koje se korite 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.
Aktivacijske podatke za kvalifikovani certifikat za napredni elektronski pečat čine personalizovani link, PIN i lozinka.
Generisanje i instalacija aktivacijskih podataka za ove certifkate opisana je u tački 6.1.2.

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.
Lozinka koja služi za otključavanje p12 fajla od strane krajnjeg korisnika, a koja čini dio aktivacijskih podataka za kvaifikovani certifikat za napredni elektronski pečat, čuva se u KMS modulu certifkacionog tijela i zaštićena je sigurnim metodama koje primjenjuje certifikaciono tijelo. Personalizovani link i PIN služe za preuzimanje p12 fajla i nije neophodno da se dodatno štiti u okviru certifikacionog tijela.

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 obezbjeđena u prostorijama certifkacionog tijela.
Certifikaciono tijelo koristi i mehanizme logičke kontrole pristupa putem firewall uređaja.
Neautorizovan pristup opremi nije dozvoljen. Kritične softverske i hardverske komponente certifikacionog tijela mogu startovati samo dvije ili više ovlašćenih osoba koja poseduju odgovarajuće smart kartice i koja znaju njihove PIN-ove ili odgovarajuće lozinke.

6.5.2. RANGIRANJE BEZBJEDNOSTI RAČUNARA

HSM moduli certifikacionog tijela ima 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 potiču 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 testiranje 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 javnom internet stranicama certifikaciongo tijela. Samo ovlašćeno osoblje sa povjerljivim ulogama certifikacionog tijela ima administratorska ovlašćenja za podešavanje i upravljanje opremom za zaštitu računarske mreže. Udaljeno podešavanje opreme za zaštitu računarske mreže 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 Korisnika i trećih lica.
Svi kritični sistemi za pružanje elektronskih usluga od povjerenja smešteni 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).

Uslovi pružanja elektronske usluge povjerenja izrade kvalifikovanih vremenskih pečata biće definisana CPS dokumentom predmetne usluge.

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 cedrtifikaciono 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 s standardima ETSI EN 319 411-1, ETSI EN 319 411-2 i ETSI EN 319 412-1, ETSI EN 319 412-2, ETSI EN 319 412-3 i ETSI EN 319 412-4.
Podređena certifikaciona tijela izdaje certifikate prema profilima koji su određeni ovim 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 slijedeća X.509 osnovna polja:

X509 ekstenzija	Opis
signature	Napredni elektronski potpis kvalifikovanog 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 kvalifikovanog elektronskog certifikata
Valid To	Datum i vrijeme prestanka važenja kvalifikacionog elektronskog certifikata
subject	Jedinstveno ime korisnika certifikata
subjectPublicKeyInformation	Javni kriptografski ključ korisnika certifikata, 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 slijedeće 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 korisnika certifikata koji se računa kao hash polja *Subject Public Key Info* kvalifikovanog elektronskog certifikata korisnika.
Key Usage	Namjena (keyUsage) javnog kriptografskog ključa korisnika kvalifikovanog elektronskog certifikata kao što je navedeno u **Error! Reference source not found.** Polje je u svim certifikatima označeno kao kritično.
Extended Key Usage	Proširena namjena (ExtendedKeyUsage) javnog kriptografskog ključa korisnika kvalifikovanog elektronskog certifikata kao što je navedeno u 6.1.7. Polje je u certifikatima za uslugu elektronskog vremenskog pečata označeno kao kritično.
Certificate Policies	Identifikacija politike certifikacije i adrese Web strane na kojoj se nalazi ova praktična pravila.
Issuer Alternative Name	Alternativno ime certifikacionog tijela koji sadrži naziv, poreski identifikacioni broj i oznaku države u kojoj je davalac usluga registrovan.
Subject Alternative Name	Alternativno ime korisnika kvalifikovanog elektronskog certifikata. U ovom polju može da se navede adresa elektronske pošte korisnika certifikata, ako je adresa elektronske pošte navedena u zahtijevu za izdavanje certifikata
CRL Distribution Points	Lokacija na kojoj se nalaze registri opozvanih certifikata.
Qualified Certificate Statements	Oznaka da je certifikat izdat kao kvalifikovani elektronski certifikat (*OID.* 1.3.6.1.5.5.7.1.3), koja sadrži oznake u skladu sa tehničkim standardom ETSI EN 319 412-5. Sadržaj oznaka pojedinog tipa certifikata naveden je u 7.1.2.1.
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*).

7.1.2.1. POLJE QUALIFIED CERTIFICATE STATEMENTS (QCSTATEMENTS)

Za certifikate koje krajnjim korisnicima izdaje CTrust GP CA tijelo,polje *qCStatements* (1.3.6.1.5.5.7.1.3) sadrži oznake u skladu sa tehničkim standardom ETSI EN 319 412-5 .

Kvalifikovani certifikati za elektronske pečate

Polje *qCStatements* u Kvalifikovanom certifikatu za napredni elektronski pečat sadrži oznake:

- id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)
- QCstatement QcType (0.4.0.1862.1.6)
  - id-etsi-qct-eseal (0.4.0.1862.1.6.2)
- id-etsi-qcs-QcPDS (0.4.0.1862.1.5)

Kvalifikovani certifikati za uslugu elektronskog vremenskog pečata

Polje qCStatements u kvalifikovanom certifikatu za napredni elektronski pečat koji se koristi za uslugu kvalifikovanog elektronskog vremenskog pečata sadrži oznake:

- id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)
- QCstatement QcType (0.4.0.1862.1.6)
  - id-etsi-qct-eseal (0.4.0.1862.1.6.2)
- id-etsi-qcs-QcPDS (0.4.0.1862.1.5)

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 korisnika certifikata u slijedećim 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 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 CT-a kao kvalifikovanog davaoca elektronskih usluga povjerenja regulisana je Zakonom o elektronskoj identifikaciji i elektronskom potpisu [1], a sprovodi ga nadležni organ državne uprave.

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

Provjeru saglasnosti rada certifikacionog tijela vrši nadležni državni organ u skladu sa Zakonom o elektronskoj identifikaciji i elektronskom potpisu i odgovarajućim podzakonskim aktima.
Certifikaciono tijelo takođe vrši redovne interne provjere usklađenosti svog rada pri čemu provjeru 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 IZDAVANJA CERTIFIKATA

CT naplaćuje usluge izdavanja certifikata u skladu sa cjenovnikom. Cijene ovih usluga biće objavljene na javnim internet stranicama rezitorijuma 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 izdatih certifikata 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

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

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

Korisnik izdatih certifikata i treća lica isključivo su odgovorni da obezbijede adekvatno osiguranje ili garanciju pokrivenosti osiguranjem za korišćenje certifikata u okviru njihovih servisa ili aplikacija.

9.3. POVERLJIVOST 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 korisnika izdatih certifikata u skladu sa odgovarajućim zakonima.

9.4.2. INFORMACIJE KOJE SE TRETIRAJU KAO PRIVATNE

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

9.4.3. INFORMACIJE KOJE SE NE SMATRAJU PRIVATNIM

Certifikaciono tijelo ne smatra privatnim samo one informacije na koje je korisnik dao saglasnost da se javno objave ili informacije koji su sastavni dio izdatih certifikata.

9.4.4. ODGOVORNOST ZA ZAŠTITU PRIVATNIH INFORMACIJA

CT je odgovoran za zaštitu privatnih informacija 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 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 CERTIFIKACIONOG TIJELA

CT garantuje da pruža elektronske usluge povjerenja izdavanja certifikata, izvršava ostale procedure vezane za upravljanje certifikatima i upravlja infrastrukturom certifikacionog tijela u skladu sa ovim dokumentom i propisima iz ove oblasti. Ctrust CA odgovara za usklađenost sa procedurama opisanim u ovom dokumentu i propisama iz ove oblasti, čak i u slučaju kada pojedinu funkciju certifikacionog tijela preuzmu podugovarači.
CT se obavezuje da će:

- izdavati certifikate korisnicima u skladu sa Zakonom o elektronskoj identifikaciji i elektronskom potpisu i procedurama i profilima definisanim ovim dokumentom,
- obezbjediti sav potreban softver i hardver za za uspostavu neophodne infrastrukture za pružanje usluga izdavanja certifikata
- obezbjediti 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 obezbjediti sigurne mehanizme koji uključuju mehanizam generisanja korisničkih ključeva i ključeva CA tijela i adekvatnu kriptografsku zaštitu pomenutih ključeva,
- uspostaviti proceduru dijeljenja tajni za sve povjerljive role u skladu sa svojom PKI infrastrukturom,
- u najkraćem mogućem roku obavijestiti korisnike i treća lica o kompromitaciji sopstvenog privatnog ključa, po mogućnosti po više komunikacionih kanala,
- ispunjavati sopstveno preuzete obaveze,
- obavijestiti podnosioce zahtjeva za izdavanjem certifikata po njihovom generisanju, kao i da će obavijestiti korisnike ako ne bude u mogućnosti da im izda tražene certifikate,
- nakon prijema validnog zahtjeva za opozivom ili suspenzijom certifikata opozvati ili suspendovati certifikat,
- obezbijediti podršku 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 zahtijevima 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 obuhvaćena ovim dokumentom.
CT je odgovoran za izvršavanje navedenih obaveza u obimu koji propisuje zakonska regulativa Crne Gore.
CT nije odgovorno za neodgovarajuću provjeru validnosti certifikata od strane koja se pouzdaje u certifikate izdate od strane certifikacionog tijela.

9.6.2. GARANCIJE I ODGOVORNOSTI REGISTRACIONOG TIJELA (RA)

RA garantuje za tačnost i potpunost informacija koje provjeravaju njeni službenici. Detaljne obaveze RA definisane su u relevantnim poglavljima ovog dokumenta.

9.6.3. GARANCIJE I ODGOVORNOSTI KRAJNJIH KORISNIKA

U procesu korišćenja certifikata, krajnji korisnici se obavezuju da na pouzdan i propisan način koriste izdate certifikate. U domenu ličnih garancija krajnjih korisnika je:

- Da posjeduju odgovarajuća znanja za upotrebu izdatih certifikata,
- Da se upoznaju sa i poštuju politike pružanja elektronskih usluga povjerenja i praktična pravila rada publikovana od strane certifikacionoh tijela,
- Da prilikom podnošenja zahtjeva za izdavanjem certifikata registracionom tijelu dostave sve neophodne podatke za ovaj proces,
- Da koriste izdate certifikate samo za legalne i autorizovane svrhe u skadu sa ovim dokumentom i Zakonom o elektronskoj identifikaciji i elektronskom potpisu i pravilnicima koji proizilaze iz zakona,
- U najkraćem roku obavijeste certifikaciono tijelo ili registraciono tijelo o promjenama bilo kojih podataka koji su ranije dostavljeni,
- Da prekinu korišćenje izdatog ili izdatih certifikata ukoliko bilo koji podatak u certifikatu postane nevalidan,
- Da prekinu korišćenje izdatog ili izdatih certifikata ukoliko sam certifikat postane nevalidan,
- Da preduzmu odgovarajuće mjere zaštite koje bi onemogućile kompromitaciju, gubljenje, objavljivanje, modifikaciju ili bilo koje drugo nevalidno korišćenje svojih privatnih ključeva.
- Da svoje privatne ključeve upotrebljavaju samo za propisane namjene ovim dokumentom i Zakonom o elektronskoj identifikaciji i elektronsko potpisu,
- Da podnesu zahtjev za opozivom certifikata ako dođe do nekog događaja koji utiče na integritet izdatog certifikata,
- Odmah obavijeste certifikaciono tijelo, ako je kompromitovan privatni ključ povezan s certifikatom ili se sumnja da je bio kompromitovan,
- Da odmah obavijeste certifikaciono tijelo o bilo kojoj sumnjivoj ili poznatoj zloupotrebi bilo kojeg certifikata koji je izdat od strane certifikacionog tijela.

9.6.4. GARANCIJE I ODGOVORNOSTI TREĆIH LICA

U domenu garancija trećih lica koja se pouzdaju u izdate certifikate je:

- Da posjeduju odgovarajuća znanja za upotrebu certifikata,
- Da se upoznaju sa i poštuju politike certifikacije i praktična pravila rada publikovana od strane certifikacionog tijela,
- Budu svjesna ograničenja certifikata i odgovornosti certifikacionog tijela 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 certifikaciono tijelo o 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 takav certifikat.

9.6.5. GARANCIJE OSTALIH UČESNIKA

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

9.7. IZUZEĆA GARANCIJA I ODGOVORNOSTI

CT daje garancije i odgovorno 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 CERTIFIKACIONOG TIJELA

CT je dužno da na propisan način izdaje certifikate i odgovorno je isključivo za štetu namjerno pričinjenu licu koje se pouzdalo u taj certifikat, a u skladu sa ovim dokumentom i propisima iz ove oblasti kao i ugovorom zaključenim između certifikacionog tijela i korisnika. CT neće biti odgovoran za indirektnu, nematerijalnu, stvarnu štetu i izmaklu dobit koju 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 KORISNIKA KVALIFIKOVANOG CERTIFIKATA

Korisnik je odgovoran za štetu koja je nastala njegovom krivicom.
Korisnik nije odgovoran za štetu ako dokaže da je postupao u skladu sa ovim dokumentom i propisima iz ove oblasti kao i ugovorom zaključenim između certifikacionog tijela i 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 certifikata ili nepostupanja u skladu sa ovim dokumentom 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 dokumenta, kao rezultata objavljivanja nove verzije dokumenta, certifikat će se koristiti u skladu sa verzijom dokumeta koja je bila validna na dan izdavanja certifikata. U slučaju promjena okolnosti do nivoa kada ovo nije moguće, CT će obavijestiti 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/dokumenate preko njegove javne insternet stranice repozitorijuma.
Pogledati takođe tačku 9.12.2.

9.12. IZMJENE I DOPUNE

9.12.1. PROCEDURA ZA IZMJENU

Ovaj dokument mijenja se po potrebi. CTrust PMA može bez obavještavanja unositi tipografske ispravke, promjene kontakt podataka te druge manje ispravke koje bitno ne utiču na 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 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 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 korisnike o promjenama koje imaju materijalnog uticaja na njih, putem e-maila i na javnim internet stranicama definisanim u pogavlju 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 REŠAVANJA 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 rješavati kod nadležnog suda u Crnoj Gori.

9.14. PRIMJENA ZAKONA

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

9.15. USAGLAŠENOST SA PRIMJENLJIVIM ZAKONOM

Ovaj dokument usaglašen je sa:

- Zakonom o elektronskoj identifikaciji i elektronskom potpisu;
- Zakonom o zaštiti podataka o 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 certifikacionog tijela i korisnika.

9.16.2. PRENOS PRAVA

Korisnicima certifikata 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 (povjerenje u certifikat i upotrebu certifikata).

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, 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 izdavanje i korišćenje testnih certifikata.

Dzina Tsybulskaja
Izvršni direktor

Prilog 1

CTrust GP CA - Pregled profila certifikata

Verzija. 1.0

Podgorica, novembar 2020. godine.

CTrust GP CA - Pregled profila certifikata

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

SADRŽAJ:

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 dodeljena organizacionoj jedinici nadležnoj za pružanje usluga povjerenja - CTrust	OJCA = CT-PEN.1
Certificate Authority	OID grana koja označava konkretno CA tijelo	CAs = CPs.x
Certificate Policy	OID koji označava da li se certifikat izdaje krajnjim korisnicima ili servisnim aplikacijama y=0 – servisna aplikacija y=1 – krajnji korisnik	CP = CAs.y
Certificate Policy	OID koji iznačava redni broj tipa certifikata koji se izdaje	CP=CAs.y.N

Tipovi certifikata koje izdaje CTrust GP CA		
NAZIV GRUPE	NAZIV TIPA CERTIFIKATA	CTrust CP OID
Kvalifikovani certifikat za napredni elektronski pečat	Napredni elektronski pečat krajnjim korisnicima	1.3.6.1.4.1.56393.1.2.1.1
	Napredni elektronski pečat sistemu za izradu kvalifikovanih elektronskih vremenskih pečata (eng. Time Stamp Authority)	1.3.6.1.4.1.56393.1.2.0.2
	Napredni elektronski pečat sistemu za preporučenu elektronsku dostavu (eng. eDelivery)	1.3.6.1.4.1.56393.1.2.0.3
Certifikati za servisne aplikacije	CTrust GP CA OCSP servis certifikat	1.3.6.1.4.1.56393.1.2.0.1

Područje primjene, sredstvo zaštite privatnog ključa certifikata, tip certifkata i tip nosioca certifikata koje izdaje CTrust GP CA tijelo			
NAZIV TIPA CERTIFIKATA	PODRUČJE PRIMJENE CERTIFIKATA	SREDSTVO ZAŠTITE PRIVATNOG KLJUČA	Tip certifkata i tip nosioca certifikata
Napredni elektronski pečat krajnjim korisnicima	Izdaje se krajnjim korisnicima (pravnim licima) Koristi se za izradu naprednog elektronskog pečata koji je definisan u Zakonu o elektronskoj identifikaciji i elektronskom potpisu član 25 i u skladu sa eIDAS regulativom.	Privatni korisnički ključ je pod zaštitom KMS modula, upotrebom KEK ključa i ZMK ključa sa odgovarajućeg tokena HSM modula u CT u. Lozinka predstavlja ključ pod zaštitom KMS modula i odgovarajućih KEK i ZMK ključeva. Njome se štiti p12 fajl koji se zajedno sa lozinkom dostavlja krajnjim korisnicima.	Certifikat sa pripadajućim parom ključeva u fajlu odgovarajućeg formata

Napredni elektronski pečat sistemu za izradu kvalifikovanih elektronskih vremenskih pečata (eng. Time Stamp Authority)	Izdaje se sistemima za izradu kvalifikovanih elektronskih vremenskih pečata (eng. Time Stamp Authority). Koristi se za izradu kvalifikovanog elektronskog vremenskog pečata koji je definisan u Zakonu o elektronskoj identifikaciji i elektronskom potpisu član 26 i u skladu sa eIDAS regulativom.	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
Napredni elektronski pečat sistemu za preporučenu elektronsku dostavu (eng. eDelivery)	Izdaje se sistemima za preporučenu elektronsku dostavu (eng. eDelivery). Koristi se za za izradu naprednog elektronskog pečata koji je definisan u Zakonu o elektronskoj identifikaciji i elektronskom potpisu član 25 i u skladu sa eIDAS regulativom, a za potrebe realizacije usluge preporučene elektronske dostave definisane u Zakonu o elektronskoj identifikaciji i elektronskom potpisu član 31 i u skladu sa eIDAS regulativom.	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
CTrust GP CA OCSP servis certifikat	Izdaje se OCSP servisu za potpis OCSP odgovora za status certifikata koje izdaje CTrust GP 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 kvalifikovanog certifikata za napredni elektronski pečat krajnjim korisnicima

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 GP CA
	organizationName (O)	Crnogorski Telekom A.D. Podgorica
	organizationalIdentifer	VATME-02289377
	countryName (C)	ME
Validity	notBefore	Vrijeme izdavanja certifikata
	notAfter	Vrijeme izdavanja certifikata + 3 godine
Subject	Serial Number (serialNumber =)	Jedinstveni serijski broj – u okviru konkretnog pravnog lica i opcioni podatak u formatu **CA:ME-13315213**

	Common Name (CN=)		Puni ili skraćeni naziv pravnog lica
	organizationIdentifier		Registrovani poreski identifikacioni broj (PIB) pravnog lica u formatu „VATME-PIB" (VATME-103376982)
	OrganizationName (O =)		Registrovani puni ili skraćeni naziv pravnog lica
	Organizational Unit (OU =)		Pravno lice
	countryName (C)		ME
subjectPublic KeyInfo	AlgorithmIdentifier		RSA
	subjectPublicKey		2048-bit RSA public key
Ekstenzije			
Polje	**Kritično**	**Atribut**	**Vrijednost**
KeyUsage	DA	nonRepudiation	Uključen nonRepudiation bit
certificatePolicies	NE	policyIdentifier	CTrust GP CP OID: 1.3.6.1.4.1.56393.1.2.1.1
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } cPSuri: http://ca.ctrust.telekom.me/cpcps/
		policyIdentifier	eIDAS OID: qcp-legal, OID: 0.4.0.194112.1.1
qCStatements	NE	esi4-qcStatement-1	id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)
		esi4-qcStatement-5	id-etsi-qcs-QcPDS (0.4.0.1862.1.5) [1] URI: http://ca.ctrust.telekom.me/cpcps/CTrustGPCA_pds_en.pdf [2] URI: http://ca.ctrust.telekom.me/cpcps/CTrustGPCA_pds_sr.pdf
		esi4-qcStatement-6	QCstatement QcType (0.4.0.1862.1.6) – id-etsi-qct-eseal (0.4.0.1862.1.6.2)
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://ca.ctrust.telekom.me/crl/CTrustGPCA.crl [2] URI: http://www.telekom.me/ctrust/crl/CTrustGPCA.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 Path Length Constraint=None
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://ocsp.ctrust.telekom.me/CTrustGPCAOCSP
		id-ad-calssuers	Access Method=Certification Authority Issuer accessLocation: http://ca.ctrust.telekom.me/cacert/CTrustGPCA.cer

Navedeni atributi sadrže punu identifikaciju subjekta. Jedinstveno ime može da sadrži i dodatne atribute na primjer dodatni "Organizational Unit (OU =)" za potrebe pojedinog subjekta.

Profil kvalifikovanog certifikata za napredni elektronski pečat sistemu za izradu kvalifikovanih elektronskih vremenskih pečata (eng. Time Stamp Authority)

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 GP CA
	organizationName (O)	Crnogorski Telekom A.D. Podgorica
	organizationalIdentifer	VATME-02289377
	countryName (C)	ME
Certificate Validity	notBefore	Vrijeme izdavanja certifikata
	notAfter	Vrijeme izdavanja certifikata + 5 godine

CTrust GP CA - Pregled profila certifikata

Privatekey Validity	notBefore	Vrijeme izdavanja certifikata
	notAfter	Vrijeme izdavanja certifikata + 2 godine
Subject	Serial Number (serialNumber =)	Jedinstveni serijski broj – u okviru konkretnog pravnog lica i opcioni podatak
	Common Name (CN=)	Puni ili skraćeni naziv pravnog lica + „TSA Servis"
	organizationIdentifier	Registrovani poreski identifikacioni broj (PIB) pravnog lica u formatu „VATME-PIB"
	OrganizationName (O =)	Registrovani puni ili skraćeni naziv pravnog lica
	Organizational Unit (OU =)	Pravno lice
	countryName (C)	ME
subjectPublic KeyInfo	AlgorithmIdentifier	RSA
	subjectPublicKey	2048-bit RSA public key

Ekstenzije			
Polje	**Kritično**	**Atribut**	**Vrijednost**
KeyUsage	DA	nonRepudiation	Uključen nonRepudiation bit
extKeyUsage	DA	timeStamping	OID: 1.3.6.1.5.5.7.3.8
certificatePolicies	NE	policyIdentifier	CTrust GP CP OID: 1.3.6.1.4.1.56393.1.2.0.2
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } cPSuri: http://ca.ctrust.telekom.me/cpcps/
		policyIdentifier	eIDAS OID: qcp-legal, OID: 0.4.0.194112.1.1
qCStatements	NE	esi4-qcStatement-1	id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)
		esi4-qcStatement-5	id-etsi-qcs-QcPDS (0.4.0.1862.1.5) [1] URI: http://ca.ctrust.telekom.me/cpcps/CTrustGPCA_pds_en.pdf [2] URI: http://ca.ctrust.telekom.me/cpcps/CTrustGPCA_pds_sr.pdf
		esi4-qcStatement-6	QCstatement QcType (0.4.0.1862.1.6) – id-etsi-qct-eseal (0.4.0.1862.1.6.2)
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://ca.ctrust.telekom.me/crl/CTrustGPCA.crl [2] URI: http://www.telekom.me/ctrust/crl/CTrustGPCA.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 Path Length Constraint=None
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://ocsp.ctrust.telekom.me/CTrustGPCAOCSP
		id-ad-calssuers	Access Method=Certification Authority Issuer accessLocation: http://ca.ctrust.telekom.me/cacert/CTrustGPCA.cer

Navedeni atributi sadrže punu identifikaciju subjekta. Jedinstveno ime može da sadrži i dodatne atribute na primjer dodatni "Organizational Unit (OU =)" za potrebe pojedinog subjekta.

Profil kvalifikovanog certifikata za napredni elektronski pečat sistemu za preporučenu elektronsku dostavu (eng. eDelivery)

Biće definisan naknadno

Profil certifikata za CTrust GP 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 GP CA
	organizationName (O)		Crnogorski Telekom A.D. Podgorica
	OrganizationalIdentifier		VATME-02289377
	countryName (C)		ME
Validity	notBefore		Vrijeme izdavanja certifikata
	notAfter		Vrijeme izdavanja certifikata + 3 mjeseca
Subject	commonName (CN)		CTrust GP CA OCSP Servis
	organizationName (O)		Crnogorski Telekom A.D. Podgorica
	organizationIdentifier		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 CP OID: 1.3.6.1.4.1.56393.1.2.0.1
		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/CTrustGPCA.crl [1] URI: http://www.telekom.me/ctrust/crl/CTrustGPCA.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/CTrustGPCAOCSP
		id-ad-calssuers	Access Method=Certification Authority Issuer accessLocation: http://ca.ctrust.telekom.me/cacert/CTrustGPCA.cer

Profil CRL liste koju izdaje CTrust GP CA podčinjeno CA tijelo

Osnovna polja			
Polje	**Atribut**		**Vrijednost**
Version	Version		X.509 V2
signatureAlgorithm	AlgorithmIdentifier		SHA256withRSA
signatureValue			Potpis izdavača CRL liste
Issuer	commonName (CN)		CTrust GP CA
	organizationName (O)		Crnogorski Telekom A.D. Podgorica
	OrganizationalIdentifier		VATME-02289377
	countryName (C)		ME
	thisUpdate		Vrijeme izdavanja CRL liste
	nextUpdate		Vrijeme izdavanja CRL liste + 25 hr
Ekstenzije			
Polje	**Kritično**	**Atribut**	**Vrijednost**

CTrust GP CA - Pregled profila certifikata

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