# KOMPANIJSKA DIREKTIVA

Crnogorski Telekom a.d. Podgorica

| | |
|---|---|
| ID broj : | 170 |
| Vrsta propisa (skraćenica): | CD |
| Broj verzije: | 1.0 |
| Dokument OID: | 1.3.6.1.4.1.56393.1.1.5.1 |
| Odgovorni sektor: | Sektor za razvoj servisa i digitalnu transformaciju |
| Datum donošenja/usvajanja: | 06/05/2021 |
| Datum stupanja na snagu: | 15/05/2021 |
| Validnost: | Neodređeno |
| Broj aneksa/priloga: | 1 |

# Praktična pravila rada za pružanje usluge izrade kvalifikovanih elektronskih vremenskih pečata (CTrust QTSA Certificate Practice Statement - CTrust QTSA 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
- Politika pružanja elektronskih usluga povjerenja (CTrust Certificate Policy – CTrust CP)
- Praktična pravila rada za izdavanje kvalifikovanih certifikata za napredni elektronski pečat i kvalifikovanih certifikata za napredni elektronski potpis (CTrust Certificate Practice Statement - CTrust CPS)

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 sadržini i načinu vođenja evidencije davalaca elektronskih usluga povjerenja i registra kvalifikovanih davalaca elektrosnkih usluga povjerenja

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

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

**OSTALI ZAKONI**

[8] Zakon o zaštiti podataka o ličnosti

**STANDARDI**

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

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

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

[12] 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

[13] 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

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

[15] 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

[16] 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

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

[18] 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

[19] ETSI EN 319 421 V1.1.1 (2016-03) - Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

[20] ETSI EN 319 422 V1.1.1 (2016-03) - Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles

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

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

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

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

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

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

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

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

[29] IETF RFC 3628 (2003) – Policy Requirements for Time-Stamping Authorities (TSAs)

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

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

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

[33] IETF RFC 3161 (2001) Internet X.509: Public Key Infrastructure: Time Stamp Protocol (TSP)

[34] IETF RFC 5816 ESSCertIDv2 Update for RFC 3161

## ISTORIJA DOKUMENTA

| Verzija | Datum stupanja na snagu propisa/izmjena | Kratak opis izmjena |
|---|---|---|
| 1.0 | 16.05.2021. | Dokument sa popunjenim poglavljima 1 – 5 prema ETSI EN 319 421 V1.1.1: Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps |

## SADRŽAJ:

# 1. OPŠTI POJMOVI

## 1.1. UVOD

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

Kvalifikovane elektronske usluge povjerenja (u daljem tekstu: elektronske usluge povjerenja) koje pruža CTrust usklađene su sa zakonskom regulativom 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 kvalifikovanu elektronsku uslugu povjerenja izrade kvalifikovanih elektronskih vremenskih pečata, u skladu sa Zakonom o elektronskoj identifikaciji i elektronskom potpisu [1], standardima ETSI EN 319 401, ETSI EN 319 421 i ETSI EN 319 422.

## 1.2. USLUGA POVJERENJA IZRADE KVALIFIKOVANIH ELEKTRONSKIH VREMENSKIH PEČATA (TSA)

Pružanje usluga izrade elektronskih vremenskih pečata u ovom dokumentu je podijeljeno na sljedeće komponente u svrhe klasifikovanja zahtjeva:

- Obezbjeđivanje izrade elektronskog vremenskog pečata: Ova komponenta usluge izrađuje elektronske vremenske pečate.
- Upravljanje elektronskim vremenskim pečatom: Ova komponenta usluge nadgleda i kontroliše rad usluge izrade elektronskog vremenskog pečata kako bi se osiguralo da pružena usluga bude u skladu sa nevednim u praktičnim pravilima rada davaoca usluge izrade elektronskih vremenskih pečata. Ova komponenta usluge ima odgovornost za instalaciju i deinstalaciju usluge izrade elektronskog vremenskog pečata.

## 1.3. DAVALAC USLUGE POVJERENJA IZRADE KVALIFIKOVANIH ELEKTRONSKIH VREMENSKIH PEČATA (TSA)

Davalac usluge povjerenja izrade elektronskih vremenskih pečata (TSA) svojim naručiocima izdaje potvrdu o vremenu neke transakcije, odnosno da je podatak u nekom momentu postojao. TSA odgovara za siguran i ispravan rad jedne ili više TSU jedinica s kojima proizvodi ili digitalno potpisuje zapise vremenskog pečata (TST). TSA ima obavezu izdavati takve zapise vremenskog pečata, koje je naknadno moguće pravilno verifikovati (u skladu sa 5.7.1.).

TSU privatni ključ koji se koristi za potpisivanje zapisa vremenskog pečata je vlasništvo davaoca usluge povjerenja. Davalac usluge povjerenja, prema ovom dokumentu, ima punu odgovornost pridržavati se svih obaveza u vezi TSU privatnog ključa. CTrust QTSA može svoje servise izvoditi sa više TSU jedinica. Svaka jedinica u tom slučaju posjeduje vlastiti privatni ključ kojim se potpisuju zapisi vremenskog pečata. Svaku jedinicu moguće je pravilno identifikovati.

## 1.4. NARUČIOCI

Naručioci su fizička ili pravna lica, koja sa CT-om zaključe Ugovor o korišćenju usluga povjerenja, a koji obuhvata i uslove korišćenja usluga izrade kvalifikovanih elektronskih vremenskih pečata .

Kada je naručilac pravno lice s jednim ili više korisnika, tada dio obaveza koje važe za naručioca, istovremeno važe i za njegove korisnike. U svakom slučaju naručilac će biti odgovoran za sve obaveze koje nastanu kada njegovi korisnici ne ispunjavaju u potpunosti svoje obaveze. Naručilac je obavezan da sam na adekvatan način obavijesti svoje korisnike o pravima i obavezama po osnovu korišćenja predmetne usluge.

Kada je naručilac fizičko lice, onda je on direktno odgovoran za sve obaveze propisane ovim Pravilnikom.

### 1.5. TREĆA LICA

Treća lica su fizička lica i poslovni subjekti (kompanije, korporacije, ustanove, tijela državne uprave i dr.) koja se pouzdaju u elektronske usluge povjerenja.
Prije nego se pouzdaju u elektronsku uslugu povjerenja, treća lica moraju uvijek da realizuju procedure provjere predmetne usluge definisane CPS dokumentom konkretne usluge povjerenja.

### 1.6. IZRADA KVALIFIKOVANIH ELEKTRONSKIH VREMENSKIH PEČATA I PRAKTIČNA PRAVILA DAVAOCA USLUGE

Hijerarhijska struktura CTrust sistema opisana je u dokumentu „Politika pružanja elektronskih usluga povjerenja (CTrust Certificate Policy – CTrust CP)" u poglavlju 1.1.

Ova Praktična pravila za pružanje usluge izrade kvalifikovanih elektronskih vremenskih pečata (CTrust QTSA Certificate Practice Statement - CTrust QTSA CPS) (u daljem tekstu: Praktična pravila ili CTrust QTSA CPS) opisuju postupke i procedure koji se primjenjuju pri pružanju usluga izdavanja kvalifikovanih elektronskih vremenskih pečata, a u skladu sa odredbama Politike pružanja elektronskih usluga povjerenja (CTrust Certificate Policy – CTrust CP).

U okviru CTrust sistema, za potrebe pružanja usluge izrade kvalifikovanih elektronskih vremenskih pečata uspostavljeno je tijelo CTrust QTSA (CTrust Qualified Time Stamp Authority). Kvalifikovani davalac usluge izrade elektronskih vremenskih pečata CTrust QTSA izrađuje kvalifikovane elektronske vremenske pečate u skladu sa Zakonom o elektronskoj identifikaciji i elektronskom potpisu [1]. Svi elektronski vremenski pečati izdati od strane CTrust QTSA su kvalifikovani elektronski vremenski pečati.

Elektronski vremenski pečati su veoma koristan alat u kontekstu elektronskih transakcija gdje datum i vrijeme igraju značajnu ulogu u procesu provjere autentičnosti različitih događaja, podataka, dokumenata, ugovora ili certifikata. To je svojevrsna potvrda vremena u elektronskoj formi koja povezuje bilo koju vrstu elektronskih podataka u određenom vremenu, dokazujući da su ti podaci postojali u to vrijeme. Kvalifikovani elektronski vremenski pečati koje izrađuju kvalifikovani davaoci usluga povjerenja obezbjeđuju korist na osnovu visokog nivoa sigurnosti i pravne sigurnosti usluga povjerenja.

Za kvalifikovani elektronski vremenski pečat podrazumijeva se tačnost datuma i vremena koji su u njima sadržani i integritet podataka sa kojima su datum i vrijeme povezani.

## 2. DEFINICIJE I SKRAĆENICE

### 2.1. DEFINICIJE

U ovom dokumentu koriste se sljedeće definicije:

| Pojam | Opis |
|---|---|
| **Elektronski vremenski pečat** | Skup podataka u elektronskom obliku koji povezuju druge podatke u elektronskom obliku sa određenim vremenom i na taj način dokazuju da su ti podaci postojali u to vrijeme. |
| **Kvalifikovani elektronski vremenski pečat** | Elektronski vremenski pečat koji ispunjava posebne zahtjeve, i to:<br>1) povezuje datum i vrijeme sa podacima tako da se sprječava svaka mogućnost promjene podataka;<br>2) zasnovan je na preciznom vremenskom izvoru koji je povezan sa koordiniranim univerzalnim vremenom (UTC) i |

| | |
|---|---|
| | 3) potpisan je naprednim elektronskim potpisom ili pečatiran pomoću naprednog elektronskog pečata kvalifikovanog davaoca usluga povjerenja. |
| **Vremenski pečat** | Sinonim za Elektronski vremenski pečat |
| **Davalac elektronskih usluga povjerenja** | Pravno ili fizičko lice koje kao davalac elektronskih usluga povjerenja pruža jednu ili više usluga u skladu sa Zakonom o elektronskoj identifikaciji i elektronskom potpisu. |
| **Kvalifikovani davalac elektronskih usluga povjerenja** | Pravno ili fizičko lice koje ispunjava zahtjeve propisane Zakonom o elektronskoj identifikaciji i elektronskom potpisu za kvalifikovanog davaoca elektronskih usluga povjerenja za jednu ili više usluga u predmetnom zakonu. |
| **Time-Stamping Authority (TSA)** | Davalac usluge povjerenja izrade elektronskih vremenskih pečata. |
| **Time-Stamping Unit (TSU)** | Jedinica za izradu zapisa vremenskog pečata - uređaj (aplikacija ili hardver) kojeg koristi davalac usluge povjerenja izrade elektronskog vremenskog pečata i ima samo jedan aktivan ključ za digitalno potpisivanje zapisa vremenskog pečata. |
| **Koordinirano svjetsko vrijeme (UTC)** | Mjerenje vremena na bazi sekunde, kako je to definisano prema ITU-R (International Telecommunications Radio Committee) preporuci (ITU-R Recommendation TF.460-5). |
| **UTC(k)** | Vremenska skala koja je dobijena u laboratoriji „k", koja zadržava tačnost svog vremena sa UTC s mogućom greškom u okviru plus minus 100ns. (više u ITU-R preporuci TF.536-I).<br>NAPOMENA: Lista UTC(k) laboratorija dostupna u sekciji I, CircularT koju objavljuje BIPM i dostupna je na BIPM stranicama (http://www.bipm.org/). |
| **Javni ključ** | Matematički podatak koji može biti javno objavljen (najčešće se objavljuje u formi X.509v3 elektronskog certifikata) i koji se koristi za verifikaciju elektronskog potpisa, kreiranog pomoću odgovarajućeg privatnog ključa koji je matematički par sa datim javnim ključem, kao i za šifrovanje podataka za krajnjeg korisnika koji posjeduje odgovarajući privatni ključ. |
| **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. |
| **Privatni ključ** | Matematički podatak koji se koristi kao ključ za kreiranje elektronskog potpisa i za raspakivanje digitalne envelope - dešifrovanje simetričnog ključa kojim je šifrovan dokument za datog krajnjeg korisnika primjenom asimetričnog kriptografskog algoritma. |
| **Certifikat/Digitalni certifikat** | Elektronski dokument kojim se potvrđuje veza između podataka za provjeru elektronskog potpisa/pečata i identiteta potpisnika ili autora pečata. |
| **Heš** (heš vrijednost ili heš kod) | Heš vrijednost u kriptografiji je broj generisan iz niski teksta. Heš vrijednost je znatno manja od samog teksta i generisana je heš algoritmom na takav način da je vjerovatnoća da neki drugi tekst ima istu heš vrijednost zanemarljiva. |
| Heš funkcija/algoritam | Heš funkcija je svaki algoritam koji podacima proizvoljne dužine dodeljuje podatke fiksne dužine. Vrednost koju vraća heš funkcija zove se heš vrijednost ili heš kod. |

## 2.2. SKRAĆENICE

U ovom dokumentu koriste se sljedeće skraćenice:

| Skraćenica | Objašnjenje |
|---|---|
| CT | Crnogorski Telekom A.D. Podgorica |

| | |
|---|---|
| **CTrust** | Sistem CT-a za pružanje elektronske usluge povjerenja / kvalifikovane elektronske usluge povjerenja |
| **CTrust QTSA** | CTrust Qualified Time Stamp Authority – Tijelo CTrust-a za usluge izrade kvalifikovanih elektronskih vremenskih pečata |
| **CA** | Certification Authority – Certifikaciono tijelo |
| **CTrust GP CA** | CTrust podređeno certifikaciono tijelo |
| **GP CA** | General Purpose CA – Certifikaciono tijelo za opšte namjene |
| **CTrust PMA** | CTrust Policy Managment Authority – Upravljačko tijelo CTrust-a |
| **TSA** | Time-Stamping Authority – Davalac usluge povjerenja izrade elektronskih vremenskih pečata |
| **TSU** | Time-Stamping Unit – Jedinica za izradu zapisa vremenskog pečata |
| **TST** | Time-Stamping Token – Zapis vremenskog pečata |
| **UTC** | Coordinated Universal Time – Koordinirano svjetsko vrijeme |
| **NTP** | Network Time Protocol – Mrežni vremenski protokol |
| **BIPM** | Bureau International des Poids et Mesures – Međunarodni biro za tegove i mjere |
| **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. |
| **OCSP** | Online Certificate Status Protocol – Protokol on-line provjere statusa certifikata |
| **Opoziv certifikata** | Permanentno ukidanje validnosti datog certifikata i njegovo smještanje na CRL listu. |
| **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 |

# 3. PRAVILA IZRADE KVALIFIKOVANIH ELEKTRONSKIH VREMENSKIH PEČATA

## 3.1. UVOD

Prema ovim Praktičnim pravilima, CTrust QTSA izrađuje zapise vremenskog pečata (TST) s tačnošću od jedne (1) sekunde ili tačnije.

Praktična pravila podrazumjevaju da su elektronski vremenski pečati zasnovani na tehnologiji infrastrukture javnih ključeva i digitalnog potpisa.

## 3.2. IDENTIFIKACIJA USLUGE IZRADE KVALIFIKOVANIH ELEKTRONSKIH VREMENSKIH PEČATA

Identifikaciona oznaka (OID) za uslugu izrade kvalifikovanih elektronskih vremenskih pečata izdate po ovim Praktičnim pravilima je: 1.3.6.1.4.1.56393.1.4.1.1

CTrust QTSA će navedeni OID koristiti u svim zapisima vremenskog pečata koje izdaje naručiocima.

## 3.3. KORISNICI I PRIMJENJIVOST

Kvalifikovani elektronski vremenski pečati izdati po ovim Praktičnim pravilima namijenjeni su za upotrebu u aplikacijama kao što su na primjer potvrda da je dokument postojao u određeno vrijeme i održavanje validnosti kvalifikovanog elektronskog potpisa ili kvalifikovanog elektronskog pečata na period koji je duži od validnosti samog certifikata kojim su izrađeni. Kvalifikovani elektronski vremenski pečat je moguće koristiti u svim drugim aplikacijama koje imaju slične ili iste zahtjeve.

# 4. POLITIKE I PRAKSE

## 4.1. ANALIZA RIZIKA

TSA će izvršiti procjenu rizika kako bi identifikovao, analizirao i procijenio rizike usluga poverenja uzimajući u obzir poslovna i tehnička pitanja. Na osnovu rezultata procjene rizika, TSA će odabrati odgovarajuće mjere tretiranja rizika. Mjere za tretiranje rizika će osigurati da nivo zaštite bude srazmjeran stepenu rizika, i utvrdiće se svi bezbjednosni zahtjevi i operativni postupci koji su neophodni za sprovođenje odabranih mjera tretiranja rizika.
Procjena rizika će se redovno pregledati i revidirati. CTrust PMA će odobriti procjenu rizika i prihvatiti utvrđeni preostali rizik.

## 4.2. PRAKTIČNA PRAVILA DAVAOCA USLUGE POVJERENJA IZRADE KVALIFIKOVANIH ELEKTRONSKIH VREMENSKIH PEČATA

### 4.2.1. NAZIV DOKUMENTA

CT-u je dodijeljen od strane IANA organizacije (Internet Assigned Number Authority) sljedeći OID: 1.3.6.1.4.1.56393.

Na osnovu tog OID-a CT je za potrebe pružanja kvalifikovanih elektronskih usluga povjerenja dodijelio sljedeći OID: 1.3.6.1.4.1.56393.1. (CTrust sistem).

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

Naziv „Praktična pravila rada za pružanje usluge izrade kvalifikovanih elektronskih vremenskih pečata (CTrust QTSA Certificate Practice Statement - CTrust QTSA CPS)" i sadrži opšta pravila i postupke pružanja usluge povjerenja izrade kvalifikovanih elektronskih vremenskih pečata i pravila i postupke o zaštiti sistema koji CTrust QTSA koristi za pružanje predmetne usluge povjerenja (u daljem tekstu: Praktična pravila).

Identifikaciona oznaka (OID) za dokument Praktična pravila je: 1.3.6.1.4.1.56393.1.1.5.1.

Internet adresa na kojoj je objavljen ovaj CP/CPS dokument je: http://ca.CTrust.telekom.me/cpcps.

Struktura dokumenta je u potpunosti usklađena sa odredbama navedenim u tehničkim standardom ETSI EN 319 421.

### 4.2.1. ORGANIZACIJA KOJA UPRAVLJA DOKUMENTOM

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

### 4.2.2. 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

### 4.2.3. SUBJEKT KOJI UTVRĐUJE USAGLAŠENOST DOKUMENTA SA ZAKONOM

Nadležni organ shodno zakonu i propisima iz ove oblasti utvrđuje usaglašenost dokumenta sa zakonom. Upravni nadzor nad sprovođenjem Zakona o elektronskoj identifikaciji i elektronskom potpisu [1] vrši nadležno Ministarstvo.
Inspekcijski nadzor nad radom davalaca elektronskih usluga povjerenja i kvalifikovanih davalaca elektronskih

usluga povjerenja i ispunjenošću uslova sistema elektronske identifikacije vrši inspekcija za usluge informacionog društva, u skladu sa zakonom kojim se uređuje inspekcijski nadzor i Zakonom o elektronskoj identifikaciji i elektronskom potpisu [1].

#### 4.2.4. PROCEDURA ODOBRAVANJA OVOG DOKUMENTA

Ovaj dokument se periodično pregleda i ažurira po potrebi. Period pregleda i ažuriranja ovog dokumenta je minimalno jednom u dvije (2) godine ili prilikom pripreme provjere usklađenosti.
Dokument se može pregledati i po potrebi ažurirati i češće ukoliko dođe do promjena u zakonskoj regulativi ili se javi potreba za promjenom primijenjenih kriptografskih algoritama ili dužina kriptografskih ključeva.
Na osnovu predloga CTrust PMA ovaj dokument odobrava izvršni direktor CT-a.

### 4.3. USLOVI KORIŠĆENJA USLUGE

CTrust QTSA objavljuje obavještenje korisnicima i trećim licima o uslovima korišćenja usluge izrade kvalifikovanih elektronskih vremenskih pečata na veb lokaciji http://www.telekom.me/CTrust koje sadrži odredbe usaglašene sa EN 319 421 [5], B.2 TSA Disclosure Statement Structure.

### 4.4. POLITIKA BEZBJEDNOSTI INFORMACIJA

CT ima usvojenu politiku bezbjednosti informacija.

### 4.5. TSA ODGOVORNOSTI

#### 4.5.1. OPŠTE

CTće ispuniti sve zahtjeve u skladu sa opisom u poglavlju 5. CT će osigurati usklađenost svojih postupaka s bilo kojim zahtjevom koji je naveden ovim Praktičnim pravilima ili posredno u nekoj od navedenih referenci.

#### 4.5.2. OBAVEZE TSA PREMA NARUČIOMA

Crnogorski Telekom je dužan da ispuni sve obaveze prema naručiocima, uključujući obaveze o dostupnosti i kvalitetu usluge.
CTrust kao davalac usluge izrade kvalifikovanih elektronskih vremenskih pečata (CTrust QTSA) obavezuje se na tačnost podataka o vremenu ugrađenom u elektronskom vremenskom pečatu. Podatak o UTC vremenu koji se ugrađuje u svaki pojedini elektronski vremenski pečat ima odstupanje manje od +/- 1 s.
CTrust, takođe ima obavezu:

- pružati uslugu izrade elektronskih vremenskih pečata u skladu sa Zakonom [1] te drugih dokumenata i preporuka na koje isti upućuju, ovim Praktičnim pravilima, te drugim aktima CTrust-a vezanim za pružanje usluge izrade elektronskh vremenskihj pečata,
- realizovati izradu elektronskih vremenskih pečata sa pouzdanim kriptografskim uređajem, HSM modulom, koji posjeduje sertifikat o usaglašenosti sa standardom FIPS 140-2 level 3 i zadovoljava EAL 4 nivo sigurnosti, u skladu sa ISO/IEC 15408 standardom,
- sprovoditi zahtijevane sigurnosne mjere za zaštitu prostora i opreme sistema za izradu elektronskih vremenskih pečata,
- osigurati nesmetan rad i maksimalnu raspoloživost usluga izrade elektronskih vremenskih pečata u skladu sa najboljom poslovnom praksom,
- objaviti akte, koji mogu biti javno dostupni, na veb lokaciji http://www.telekom.me/CTrust,
- obavljati usluge izrade elektronskih vremenskih pečata s pažnjom dobrog stručnjaka,
- primjenjivati u svom poslovanju organizacijske i tehničke mjere zaštite ličnih podataka prikupljenih od korisnika i prikupljene podatke čuvati povjerljivima te ih koristiti isključivo za potrebe usluga iz opsega ovog dokumenta i dodatnih usluga iz skupa CTrust usluga,

- primjenjivati odredbe Zakona o zaštiti podataka o ličnosti [8] i drugih propisa kojima je uređena zaštita ličnih podataka te tajnost podataka u Crnoj Gori,
- poštovati pravo intelektualne svojine vlasništvo, licencna i druga srodna prava,
- rješavati zastoje i greške u radu sistema za izradu elektronskih vremenskih pečata u najkraćem mogućem roku,
- planirati održavanje i dalji razvoj sistema za izradu elektronskih vremenskih pečata u skladu sa važećim normama i razvojem tehnologije.

#### 4.5.3. OBAVEZE NARUČILACA

Naručilac mora po preuzimanju zapisa elektronskog vremenskog pečata da provjeri elektronski potpis kvalifikovanog elektronskog vremenskog pečata, važenje TSU certifikata i da posjeduje hešHeš vrijednost podataka za koje je tražio kvalifikovani elektronski vremenski pečat. Naručilac je odgovoran za tačnu izradu hešHeš vrijednosti podataka za koje je tražio kvalifikovani elektronski vremenski pečat.

#### 4.5.4. OBAVEZE TREĆIH LICA

Treća lica (saglasno uslovima prema 4.3), prije nego što prihvate zapise elektronskog vremenskog pečata kao važeće, dužni su:

a) provjeriti da je zapis elektronskog vremenskog pečata ispravno potpisan;
b) provjeriti validnost TSU ključa s kojim je zapis potpisan;
Napomena: Provjera validnosti TSU javnog ključa vrši se provjerom liste opozvanih certifikate (CRL) ili korišćenjem OCSP servisa. Ukoliko odgovarajući certifikat nije opozvan vrši se i provjera da certifikat javnog ključa TSU nije istekao;
c) uzeti u obzir bilo koje ograničenje za upotrebu zapisa vremenskog pečata, kako je definisano ovim Praktičnim pravilima.

### 4.6. OGRANIČENJE ODGOVORNOSTI

Ovaj dokument ne definiše dodatna ograničenja odgovornosti davaoca usluge povjerenja izrade kvalifikovanih elektronskih vremenskih pečata.
Prema ovim Praktičnim pravilima CT može ograničiti svoje odgovornosti do nivoa koji nije suprotan zakonima Crne Gore.

## 5. ZAHTJEVI ZA TSA POSTUPKE

### 5.1. UVOD

Svi postupci koje realizuje CTrust QTSA opisani su u ovim Praktičnim pravilima, kao i u dokumentima „Politika pružanja elektronskih usluga povjerenja (CTrust Certificate Policy – CTrust CP)“ i „Praktična pravila rada za izdavanje kvalifikovanih certifikata za napredni elektronski pečat i kvalifikovanih certifikata za napredni elektronski potpis (CTrust Certificate Practice Statement - CTrust CPS)“.

### 5.2. INTERNA ORGANIZACIJA

#### 5.2.1. POUZDANOST ORGANIZACIJE

CT, kao kvalifikovani davalac elektronskih usluga povjerenja, čiji je sastavni dio CTrust QTSA, posjeduje stabilnost i raspolaže dovoljnim sredstvima koja osiguravaju nesmetano pružanje usluga povjerenja u skladu s ovim dokumentom.

CT, kao kvalifikovani davalac elektronskih usluga povjerenja, ima osiguran rizik od odgovornosti za štete koje nastanu obavljanjem usluga povjerenja.

CT dodatno osigurava imovinu polisom osiguranja koja pokriva osiguranje od rizika požara, vremenskih nepogoda,poplava, eksplozija, udara groma, pada ili udara letjelice, demonstracija, kao i osiguranje opreme, električne opreme, elektronskih i komunikacijskih uređaja, instalacija i slično.

### 5.2.2. RAZDVAJANJE DUŽNOSTI

CTrust QTSA, kao sastavni dio CTrust sistema, vrši razdvajanje povjerljivih uloga na način opisan u dokumentu „Politika pružanja elektronskih usluga povjerenja (CTrust Certificate Policy – CTrust CP)", poglavlje 5.2.4.

## 5.3. KONTROLA OSOBLJA

Osoblje CTrust sistema, sačinjavaju stalno zaposleni ili zaposleni na određeno vrijeme. Oni su angažovani na poslovima davaoca usluga povjerenja i adekvatno osposobljeni za izvršavanje radnih zadataka, i u tom smislu obavljaju određene radne zadatke i u okviru CTrust QTSA koji je dio CTrust sistema.

Kako bi se osiguralo adekvatno upravljanje kadrovima uspostavljene su sigurnosne mjere u skladu sa dokumentima „Politika pružanja elektronskih usluga povjerenja (CTrust Certificate Policy – CTrust CP)" poglavlje 5.3.

Osoblje CTrust QTSA se obavezuje da ne smije da objavljuje ili saopštava povjerljive informacije vezane za bezbjednost davaoca usluga povjerenja ili informacije o naručiocma.

Osoblju CTrust QTSA se ne dodjeljuju poslovi izvan djelokruga poslova za koje su angažovani kod davaoca usluga povjerenja, a koji bi mogli dovesti da sukoba interesa sa ovim poslovima.

## 5.4. UPRAVLJANJE IMOVINOM

### 5.4.1. OPŠTI ZAHTJEVI

CT, kao kvalifikovani davalac elektronskih usluga povjerenja, čiji je sastavni dio CTrust QTSA, osigurava odgovarajući nivo zaštite imovine koja se koristi za pružanje usluge izrade kvalifikovanih elektronskh vremenskih pečata. Kako bi se osiguralo adekvatno upravljanje i zaštita imovine, te spriječilo neautorizovano otkrivanje, modifikacija, premještanje ili uništavanje informacija koje su sačuvane na medijima, uspostavljene su sigurnosne mjere u skladu sa dokumentom „Politika pružanja elektronskih usluga povjerenja (CTrust Certificate Policy – CTrust CP)", poglavlje 5.1.

### 5.4.2. RUKOVANJE MEDIJIMA

Mediji na kojima se nalaze arhivske i sigurnosne kopije CTrust QTSA podataka u elektronskom obliku, kopije sadržaja nosioca podataka i sigurnosne kopije programske opreme skladište se na dvije odvojene zaštićene lokacije sa uspostavljenom protivpožarnom zaštitom i zaštitom od poplava. Ovi mediji su zaštićeni od oštećenja, krađe i neovlašćenog pristupa.

Rukovanje medijima je opisano u poglavljima 5.1.6., 5.1.7. i 5.1.8. dokumenta „Politika pružanja elektronskih usluga povjerenja (CTrust Certificate Policy – CTrust CP)".

## 5.5. KONTROLA PRISTUPA

Sistemi neopodni za pružanje usluge izrade kvalifkovanih elektronskih vremenskih pečata smješteni su u istom prostoru gdje je smještena i infrastruktura CTrust sistema. Primjenjuju se mjere kontrole pristupa kako je opisano u poglavlju 5.1. „Politike pružanja elektronskih usluga povjerenja (CTrust Certificate Policy – CTrust CP)".

## 5.6. KRIPTOGRAFSKE MJERE ZAŠTITE

### 5.6.1. OPŠTE

CTrust QTSA koristi odgovarajuće kriptografske mjere zaštite, detaljno opisane u poglavlju 6. dokumenata „Politika pružanja elektronskih usluga povjerenja (CTrust Certificate Policy – CTrust CP)" i „Praktična pravila rada za izdavanje kvalifikovanih certifikata za napredni elektronski pečat i kvalifikovanih certifikata za napredni elektronski potpis (CTrust Certificate Practice Statement - CTrust CPS)".

### 5.6.2. GENERISANJE PRIVATNOG KLJUČA TSU

Par kriptografskih ključeva za elektronsko potpisivanje kvalifikovanih elektronskih vremenskih pečata je generisan prilikom instaliranja aplikacije TSU i tokom postupka generisanja ključa (Key Generatian Ceremony) po definisanoj proceduri. U toku generisanja para kriptografskih ključeva za elektronsko potpisivanje koristi se zaštita koja važi za prostorije CTrust certifikacionog tijela, višestruka autentifikacija ovlašćenih lica i hardverski kriptografski modul (Hardware Security Module - HSM).
Generisanje TSU privatnog ključa za potpisivanje se izvodi sa pouzdanim kriptografskim uređajem, HSM modulom, koji posjeduje sertifikat o usaglašenosti sa standardom FIPS 140-2 level 3 i zadovoljava EAL 4 nivo sigurnosti, u skladu sa ISO/IEC 15408 standardom. Algoritam za kreiranje TSU ključeva, dužina ključeva i algoritam za potpisivanje TSU certifikata u potpunosti odgovaraju specifikaciji u ETSI TS 119 312 . TSU privatni ključ se isključivo čuva u HSM modulu i ne radi se import u bilo koji drugi kriptografski modul. U jednom trenutku može biti aktivan samo jedan ključ koji se koristi za kreiranje kvalifikovanih elektronskih vremenskih pečata.

### 5.6.3. ZAŠTITA PRIVATNOG KLJUČA TSU

Sve operacije za generisanje TSU kriptografskih ključeva i potpisivanja kvalifikovanih elektronskih vremenskih pečata vrše se na hardverskom kriptografskom modulu koji posjeduje sertifikat o usaglašenosti sa standardom FIPS 140-2 Level 3 i zadovoljava EAL 4 nivo sigurnosti, u skladu sa ISO/IEC 15408 standardom. Ispunjenje ovog standarda garantuje, između ostalog, da je bilo koji pokušaj narušavanja integriteta uređaja ili kriptografske memorije detektovan.

U operacijama u kojima se upravlja hardverskim kriptografskim modulom uvijek je potrebno prisustvo najmanje dva lica sa odgovarajućim punomoćjem koji se identifikuju sa pametnom karticom hardverskog kriptografskog modula i tajnom lozinkom kartice (Aktivacijski podaci).
Aktivacijski podaci za privatni ključ TSU koji su smješteni na odgovarajuće upravljačke 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.
Sigurnosne kopije privatnog ključa TSU obezbijeđene su sigurnosnim mehanizmima hardverskog kriptografskog modula.

Privatni ključevi TSU se ne arhiviraju.

### 5.6.4. CERTIFIKAT JAVNOG KLJUČA TSU

Javni ključ TSU se objavljuje u TSU digitalnom certifikatu. Korisnici mogu da dobiju TSU digitalni certifikat u bilo kom trenutku na veb stranici http://www.telekom.me/CTrust ili ga traže u okviru zahtjeva za izdavanje kvalifikovanih elektronskih vremenskih pečata, ali je njihova odgovornost da provjere identitet TSU naveden u TSU digitalnom certifikatu i integritet TSU digitalnog certifikata.

Digitalni certifikati koje koristi TSU su izdati od strane CTrust GP CA kao kvalifikovani certifikat za napredni elektronski pečat. Certifikati imaju dodatno polje (extendedKeyUsage) timestamping (OID: 1.3.6.1.5.5.7.3.8) koje je u certifikatu označeno kao kritično.

### 5.6.5. OBNAVLJANJE TSU KLJUČEVA

Rok važnosti javnih ključeva i TSU digitalnih certifikata je do 5 godina.

Privatni ključ TSU obnavlja se prije isteka perioda korišćenja privatnog ključa TSU koji nije duži od dvije (2) godine. Novi par ključeva generiše se tokom procesa obnove u skladu s odredbama poglavlja 5.6.2.

### 5.6.6. UPRAVLJANJE ŽIVOTNIM VIJEKOM HARDVERSKOG KRIPTOGRAFSKOG MODULA

Hardverski kriptografski modul dobavljač šalje na adresu CTrust QTSA u zatvorenoj pošiljci. Po prijemu pošiljke, operativno osoblje CTrust QTSA provjerava da nije oštećena ili otvorena. Nakon otvaranja pošiljke, operativno osoblje CTrust QTSA provjerava integritet hardverskog kriptografskog modula.
Hardverski kriptografski modul čuva se u sigurnim prostorijama CTrust QTSA. Instalaciju i aktiviranje hardverskog kriptografskog modula vrši operativno osoblje CTrust QTSA u sigurnim prostorijama. U procesu aktiviranja i generisanja ključeva koriste se tehničke i organizacione kontrole višestruke autorizacije (four-eyes principle).
HSM uređaji ne smiju da napuštaju bezbjednu zonu certifikacionog tijela izuzev rijetkih prilika unaprijed definisanih premještanja i preseljenja. Certifikaciono tijelo vodi evidenciju u vezi svih tih premještanja ili preseljenja.
U slučaju da odgovarajući HSM zahtijeva održavanje ili popravku, koja se ne može izvršiti u okviru bezbjedne zone certifikacionog tijela, oni se onda bezbjedno prenose do njihovog proizvođača uz poštovanje svih neophodnih bezbjednosnih mjera.

### 5.6.7. KRAJ ŽIVOTNOG VIJEKA KLJUČEVA TSU

CTrust QTSA garantuje da neće koristiti privatne ključeve TSU nakon isteka roka važnosti istih.

Svaki zahtjev za izradu kvalifikovanih elektronskih vremenskih pečata sa privatnim ključem koji je istekao biće odbijen.

Privatni ključevi se uništavaju tako da ih nije moguće vratiti. Mediji koji sadrže privatni ključ se brišu na siguran način. U toku uništavanja privatnih ključeva uništava se i sigurnosna kopija privatnih ključeva. Proces se strogo kontroliše i dokumentuje.

## 5.7. KVALIFIKOVANI ELEKTRONSKI VREMENSKI PEČAT

### 5.7.1. IZRADA KVALIFIKOVANOG ELEKTRONSKOG VREMENSKOG PEČATA

CTrust QTSA izrađuje svaki kvalifikovani elektronski vremenski pečat na siguran način i on sadrži tačno vrijeme. Bitne karakteristike svakog kvalifikovanog elektronskog vremenskog pečata su:

a) Sadrži identitikacionu oznaku (OID) u skladu sa ovim Praktičnim pravilima.
b) Svaki kvalifikovani elektronski vremenski pečat sadrži jedinstveni identifikator (serialNumber).
c) Izvor vremena kojeg koristi TSU prilikom izrade svojih zapisa, povezan je sa bar jednom od vrijednosti koje distribuira neki UTC(k) laboratorij sa liste koju objavljuje BIPM.
d) Izvor vremena sinhronizovan je sa UTC sa odstupanjem ne većim od jedne (1) sekunde.
e) Kada se ustanovi, da sat TSU nije u okviru propisane tačnosti kvalifikovani elektronski vremenski pečat se ne izdaje.
f) Zapis vremenskog pečata sadrži Heš vrijednost, koju šalje korisnik u svom zahtjevu.
g) Kvalifikovani elektronski vremenski pečat potpisan je sa TSU ključem koji se koristi isključivo za tu svrhu.
h) TSU će odbiti pokušaj izrade zapisa tačnog vremena kada period validnosti TSU privatnog ključa istekne.

#### 5.7.1.1. ZAHTJEV ZA IZRADU KVALIFIKOVANOG ELEKTRONSKOG VREMENSKOG PEČATA

Zahtjev za izradu kvalifikovanog elektronskog vremenskog pečata koji šalju korisničke aplikacije mora biti u skladu sa RFC 3161.

Zahtjev za izradu kvalifikovanog elektronskog vremenskog pečata može sadržati sljedeća polja:

- reqPolicy,
- nonce i
- certReq.

Heš podataka za koje se traži kvalifikovani elektronski vremenski pečat mora biti jedan od sljedećih algoritama:
- Sha-256 (OID: 2.16.840.1.101.3.4.2.1);
- Sha-384 (OID: 2.16.840.1.101.3.4.2.2);
- Sha-512 (OID: 2.16.840.1.101.3.4.2.3).

#### 5.7.1.2. ODGOVOR NA ZAHTJEV ZA IZRADU KVALIFIKOVANOG ELEKTRONSKOG VREMENSKOG PEČATA

Odgovor na zahtjev za izradu kvalifikovanog elektronskog vremenskog pečata koji šalje CTrust QTSA u skladu je sa RFC 3161 i RFC 5816. Prema ETSI EN 319 422 svaki odgovor sadrži sljedeća polja:
- accuracy i
- nonce (ako je bio proslijeđen u zahtjevu).

U odgovoru na zahtjev za izradu kvalifikovanog elektronskog vremenskog pečata polje nonce sadrži istu vrijednost koja je stavljena u istoimenom polju zahtjeva za izdavanje kvalifikovanog elektronskog vremenskog pečata.

Odgovor na zahtjev za izradu kvalifikovanog elektronskog vremenskog pečata potpisan je privatnim ključem TSU.

U skladu sa ETSI TS 119 312, algoritam koji se koristi za potpisivanje zapisa elektronskog vremenskog pečata je:
- sha256-with-rsa (OID: 1.2.848.113549.1.1.11).

### 5.7.2. SINHRONIZACIJA IZVORA VREMENA SA UTC

Satovi servera TSU su sa GPS prijemnikom UTC vremena i dodatno sa izvorima vremena koji distribuiraju tačno vrijeme NTP protokolom i koji su na listi UTC(k) laboratorija dostupni u sekciji 1, CircularT koju objavljuje BIPM i dostupna je na BIPM stranicama (http://wwww.bipm.org).

Serveri TSU za izdavanje kvalifikovanih elektronskih vremenskih pečata sinhronizuju svoje satove sa GPS prijemnikom vremena u skladu sa NTP mrežnim protokolom vremena.

GPS prijemnik vremena zaštićen je od neovlašćenog pristupa.

TSU sat je sinhronizovan sa UTC u okviru deklarisane tačnosti sa najmanje sljedećim pojedinačnim zahtjevima:
a) Kalibracija TSU satova se održava tako da satovi ne odlaze izvan deklarisanih tačnosti.
b) Proglašena tačnost je 1 sekunda ili bolja.
c) TSU satovi će biti zaštićeni od prijetnji koje bi mogle rezultirati neotkrivenom promjenom sata koja bi bila van kalibracije. Prijetnje mogu da uključuju npr. neovlašćeno osoblje, radio ili električne udare.
d) TSA će otkriti da li vrijeme koje bi bilo naznačeno u elektronskom vremenskom pečatu odmiče ili iskače iz sinhronizacije sa UTC.
e) Ako se otkrije da vrijejme koje bi bilo naznačeno u elektronskom vremenskom pečatu odmiče ili iskače iz sinhronizacije sa UTC, TSU će zaustaviti izradu elektronskog vremenskog pečata.
f) Sinhronizacija sata održavaće se kada nastupi prestupna sekunda, a u skldu sa obavještenjem dobijenim od nadležnog tijela. Promjena koja uzima u obzir prestupnu sekundu dogodiće se u poslednjem minutu dana kada je promjena planirana. Vodiće se evidencija tačnog vremena (u okviru deklarisane tačnosti) kada je došlo do ove promjene.

### 5.7.3. FIZIČKA SIGURNOST SISTEMA I SIGURNOST NJEGOVOG OKRUŽENJA

CTrust QTSA sistem je smješten u istom prostoru gdje je smještena i infrastruktura CTrust-a. Primjenjuju se mjere fizičke bezbjednosti kako je opisano u poglavlju 5.1. „Politike pružanja elektronskih usluga povjerenja (CTrust Certificate Policy – CTrust CP)".

### 5.7.4. SIGURNOSNO UPRAVLJANJE

CTrust QTSA Informacioni sistem dio je cjelokupne CTrust infrastrukture i primjenjuju se iste kontrole nad računarskim resursima i životnim ciklusom softvera koje su opisane u dokumentima „Politika pružanja elektronskih usluga povjerenja (CTrust Certificate Policy – CTrust CP, poglavlja 5.1. do 5.3.

CTrust QTSA sistem zasnovan je na pouzdanim hardverskim i softverskim komponentama, a sve operacije sistema podržane su redundantnim komponentama.

### 5.7.5. BEZBJEDNOST RAČUNARSKE MREŽE

Računarsku mrežu CTrust QTSA čine povezani mrežni segmenti, na kojima se nalaze serveri i radne stanice. Segmenti su međusobno povezani firewall-ovima. Računarska mreža je preko više firewall-a povezana sa Internetom. Bezbjedonosna pravila na firewall-ovima dozvoljavaju saobraćaj samo protokolima koji su neophodno potrebni za pristup servisima davaoca usluga povjerenja izrade kvalifikovanih elektronskih vremenskih pečata. Primjenjuju se mjere bezbjednosti računarske mreže kako je opisano u poglavlju 6.7. „Politike pružanja elektronskih usluga povjerenja (CTrust Certificate Policy – CTrust CP).

### 5.7.6. UPRAVLJANJE INCIDENTIMA

CTrust QTSA ima implementirane procedure reagovanja na bezbjednosne incidente i kvarove u skladu sa pozitivnim zakonskim propisima.

Internim pravilima rada definisane su procedure koje treba izvršiti pri rješavanju incidenata, kao i izvještavanje usljed potencijalne kompromitacije privatnog ključa certifikacionog tijela.

### 5.7.7. PRIKUPLJANJE DOKAZA (COLLECTION OF EVIDENCE)

Postupci vezani za prikupljanje, obradu i zaštitu revizijskih zapisa kao dokaza sprovode se na način koji je opisan u poglavlju 5.4. „Politike pružanja elektronskih usluga povjerenja (CTrust Certificate Policy – CTrust CP)".
Pored toga, bilježe se specifične aktivnosti vezane za rad CTrust QTSA što uključuje:

- aktivnosti vezane za generisanje i životni ciklus TSU ključeva i TSU certifikata,
- aktivnosti vezane za sinhronizaciju TSU sa UTC vremenom uključujući regularno kalibriranje satova, kvarove i ispade sistema uključujući gubitak sinhronizacije ili nemogućnost kalibriranja satova.

Prikupljeni revizijski dnevnici arhiviraju se minimalno deset (10) godina nakon njihovog nastanka, prema praksi koja je opisana u poglavlju 5.5. „Politike pružanja elektronskih usluga povjerenja (CTrust Certificate Policy – CTrust CP)".

CTrust QTSA 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. Arhiva je zaštićena odgovarajućim sigurnosnim mehanizmima. Pristup arhivama je dozvoljen samo ovlašćenim licima.

### 5.7.8. UPRAVLJANJE KONTINUITETOM RADA

Primjenjuju se mjere kako je opisano u poglavlju 5.7.4. „Politike pružanja elektronskih usluga povjerenja (CTrust Certificate Policy – CTrust CP).

### 5.7.9. PRESTANAK RADA CTRUST QTSA

U slučaju planiranog prestanka pružanja usluge izrade kvalifikovanog elektronskog vremenskog pečata Crnogorski Telekom će učiniti sve razumne napore kako bi se minimizirao uticaj ukidanja usluge na poslovni proces naručilaca ili trećih lica.

CT će naročito:

- Raskinuti ugovore sa naručiocima i o tome obavjestiti naručioce i treća lica putem repozitorijuma i nadležni organ državne uprave najmanje tri mjeseca prije dana predviđenog za raskid ugovora;
- Naručiocima predmetne usluge obezbijediće nastavak pružanja usluge kod drugog davaoca elektronskih usluga povjerenja i dostaviće mu svu dokumentaciju u vezi sa obavljanjem usluge;
- U slučaju da ne obezbijedi nastavak pružanja predmetne usluge kod drugog davaoca opozvaće sve izdate certifikata TSU 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 obavljenom uslugom;
- uništiti sve privatne ključeve TSU uključujući i sve kopije na način koji garantuje da se privatni ključevi više ne mogu obnoviti;
- Osiguraće raspoloživost liste opozvanih certifikata u periodu od godinu dana posle opoziva svih TSU certifikata;
- Arhiviraće sve podatke u skladu sa periodom propisanim odgovarajućim zakonom od zadnjeg dana rada davaoca usluge povjerenja.

### 5.7.10. USAGLAŠENOST SA VAŽEĆIM ZAKONIMA I RJEŠAVANJE SPOROVA

Ova Praktična pravila su usaglašena sa:

- Zakonom o elektronskoj identifikaciji i elektronskom potpisu,
- i drugim pozitivnim propisima iz ove oblasti.

Sve sporove nastale u vezi sa pružanjem usluge izrade kvalifikovanih elektronskih vremenskih pečata treba ako je moguće rješavati sporazumno. Ukoliko se dogovor ne može postići sporazumno, spor će se rješavati kod nadležnog suda u Crnoj Gori.


Dzina Tsybulskaja
Izvršni direktor

# PRILOG 1

## Struktura OID brojeva za dodjeljivanje Certificate Policy OID brojeva

| Struktura CP OID | | |
|---|---|---|
| **NAZIV GRUPE** | **NAZIV GRANE OID-a** | **OID** |
| **Crnogorski Telekom PEN** | Private enterprise number Crnogorski Telekom AD | CT-PEN |
| **Organizaciona jedinica Crnogorskog Telekoma za izdavanje certifikata** | OID grana dodijeljena organizacionoj jedinici nadležnoj za izdavanje certifikata - CTrust | OJCA = CT-PEN.1 |
| **Certificate Authority** | OID grana koja označava konkretno CA tijelo ili konkretnu uslugu<br>x=4 – CTrust usluga izrade kvalifikovanih elektronskih vremenskih pečata | CAs = OJCAs.x |
| **Certificate Policy** | OID koji označava da se kvalifikovani elektronski vremenski pečat izrađuje krajnjim korisnicima<br>y=1 – krajnji korisnik | CP = CAs.y |
| **Certificate Policy** | OID koji označava redni broj tipa elektronskog vremenskog pečata koji se izrađuje<br>N=1- kvalifikovani elektronski vremenski pečat | CP=CAs.y.N |