PODIJELI DOŽIVLJAJ.

# IZJAVA O USLUGAMA CTRUST PKI SISTEMA (CTRUST PKI DISCLOSURE STATEMENT – CTRUST PDS)

Version: 1.0

## REFERENCE

| | |
|---|---|
| Interne reference: | • Politika pružanja elektronskih usluga povjerenja (CTrust Certificate Policy – CTrust CP)<br>• 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: | Standardi<br>[1] 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<br>[2] IETF RFC 3647 – Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework<br>[3] American Bar Association, PKI Assessment Guidelines, v0.30, Public Draft For Comment, June 2001 |

## ISTORIJA DOKUMENTA

| Verzija | Datum stupanja na snagu propisa/izmjena | Kratak opis izmjena |
|---|---|---|
| 1.0 | 21.01.2021. | Inicijalna verzija u skladu sa internim i eksternim referencama |

## SADRŽAJ:

## 1. UVOD

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

Elektronske usluge povjerenja koje pruža CTrust usklađene su sa zakonskom regulativom i mjerodavnim međunarodnim normama iz djelokruga pružanja ovih usluga.

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

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

CT ostavlja mogućnost uspostavljanja drugih podređenih certifikacionih tijela u hijerarhijskoj strukturi za potrebe izdavanja drugih tipova certifikata.

Svrha ovog dokumenta je da sumira i prezentuje sve najvažnije tačke iz „Praktična pravila rada za izdavanje kvalifikovanih certifikata za napredni elektronski pečat i kvalifikovanih certifikata za napredni elektronski potpis (CTrust Certificate Practice Statement - CTrust CPS)" dokumenta u lakše čitljivom i razumljivom formatu na dobrobit krajnjih korisnika i trećih lica.

Ovaj dokument (CTrust PDS) nije zamjena za CTrust CPS dokument po kojem se izdaju certifikati. Svi korisnici koji se žele prijaviti za dobijanje certifikata ili se oslanjanju na certifikate moraju pročitati CTrust CPS dokument koji je objavljen na sljedećoj lokaciji: http://ca.ctrust.telekom.me/cpcps.

Struktura ovog dokumenta je usaglašena sa standardom: ETSI EN 319 411-1 V1.2.2. (2018-04), Anex A.

## 2. KONTAKT INFORMACIJE

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

Poštanska adresa: CTrust : Crnogorski Telekom A.D.
81000 Podgorica, Moskovska br. 29.

E-mail: ctrust_pma@telekom.me
Web: http://ca.ctrust.telekom.me/cpcps

## 3. TIPOVI, UPOTREBA I OPOZIV CERTIFIKATA

### Tipovi certikata

CTrust GP CA tijelo izdaje sljedeće tipove certifikata, kojima je CTrust tijelo dodijelio identifikatore objekata (OIDs):

| NAZIV GRUPE | NAZIV TIPA CERTIFIKATA | CTrust CP OID |
|---|---|---|
| Kvalifikovani certifikat za napredni elektronski pečat | Kvalifikovani certifikat za napredni elektronski pečat krajnjim korisnicima | 1.3.6.1.4.1.56393.1.2.1.1 |
| | Kvalifikovani certifikat za 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 |

| | | |
|---|---|---|
| **Kvalifikovani certifikat za napredni elektronski potpis** | Kvalifikovani certifikat za napredni elektronski potpis fizičkog lica u okviru pravnog lica | 1.3.6.1.4.1.56393.1.2.1.2 |
| **Certifikati za servisne aplikacije** | CTrust GP CA OCSP servis certifikat | 1.3.6.1.4.1.56393.1.2.0.1 |

## 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 naprednog elektronskog potpisa, verifikaciju naprednog elektronskog pečata i verifikaciju kvalifikovanog elektronskog vremenskog pečata.

| NAZIV TIPA CERTIFIKATA | PODRUČJE PRIMJENE CERTIFIKATA |
|---|---|
| Napredni elektronski pečat krajnjim korisnicima | Izdaje se krajnjim korisnicima.<br>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. |
| 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).<br>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. |
| Napredni elektronski potpis fizičkog lica u okviru pravnog lica | Izdaje se krajnjim fizičkim licima koji su ovlašćeni od strane pravnog lica.<br>Koristi se za izradu naprednog elektronskog potpisa koji je definisan u Zakonu o elektronskoj identifikaciji i elektronskom potpisu član 16 i u skladu sa eIDAS regulativom. |
| 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. |

## Opoziv certifikata

U slučaju potrebe, i u skladu sa smjernicama datim u CTrust CPS GP dokumentom moguće je izvšiti opoziv sertifikata.
Po zahtjevu službenika za registraciju CTrust RA tijela, nadležnog državnog organa ili samog krajnjeg korisnika certifikaciono tijelo vrši opoziv izdatog certifikata u sljedećim slučajevima:

- opoziv certifikata zahtijeva krajnji korisnik 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 krajnji korisnik 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 krajnjeg korisnika 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 elektronskih usluga povjerenja 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 ne prenese na drugog davaoca tih usluga;

- istekne rok važenja certifikata;
- ako certifikaciono tijelo primi sudsku odluku ili 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 krajnji korisnik krši odredbe CP/CPS dokumenta.

Opoziv certifikata može biti zatražen od:

- krajnjeg 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;
- suda ili nadležnog organa državne uprave.

**Procedura opoziva certifikata**

U slučaju da je potrebno izvršiti opoziv certifikata krajnji korisnik certifikata dužan je da u najkraćem mogućem roku kontaktira službenika za registraciju davaoca elektronskih usluga povjerenja radi dostavljanja zahtjeva za opoziv. Krajnji korisnik mora lično doći u poslovnicu CT-a da podnese zahtjev za opoziv certifikata.
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 krajnjeg korisnika o opozivu certifikata, u roku od 24 časa od primljenog zahtjeva ili obavještenja, odnosno nastanka okolnosti zbog koje se certifikat opoziva.

## 4. OBAVEZE KRAJNJIH KORISNIKA

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

- Da posjeduju odgovarajuća znanja za upotrebu izdatih certifikata;
- Da budu svjesna ograničenja certifikata i odgovornosti certifikacionog tijela kako je detaljno opisano u CTrust CPS dokumentu;
- 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 CTrust CPS 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 opisanim u CTrust CPS dokumentu 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.
- Da 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.

## 5. OBAVEZE PROVJERE STATUSA CERTIFIKATA OD STRANE TREĆIH LICA

Svako ko se oslanja na informacije koje postoje u certifikatima mora verifikovati da isti nijesu opozvani ili da validnost certifikata još postoji u trenutku potpisivanja ili pečatiranja. Za ovu potrebu u svakom certifikatu koje izdaju CTrust CA tijela postoji adresa liste opozvanih certifikata (Certificate Revocation List (CRL)) i adresa Online Certificate Status Protocol servisa.
Certifikaciono tijelo objavljuje listu opozvanih certifikata (CRL) svakih sat vremena, sa periodom važenja CRL liste od 24 sata. Informacija o statusu opozvanosti certifikata korišćenjem OCSP servisa dostupna je u realnom vremenu.

Treća lica koja se pouzdaju u certikate treba:

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

Treće lice koje ne poštuje propise, te ne postupa u skladu sa obavezama i odgovornostima, samo snosi sve rizike pouzdanja u takav certifikat.

## 6. ODGOVORNOST I OGRANIČENJE OD ODGOVORNOSTI

**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 CTrust CPS dokumentom i propisima iz ove oblasti kao i ugovorom zaključenim između certifikacionog tijela davaoca elektronske usluge povjerenja i krajnjih korisnika. CT neće biti odgovoran za indirektnu, nematerijalnu, stvarnu štetu i izmaklu dobit koju krajnji korisnik eventualno pretrpi. Maksimalna finansijska odgovornost certifikacionog tijela u ovom slučaju je do 50.000,00 EUR kumulativno na godišnjem nivou.
CTrust tijelo isključuje odgovornost za:

- 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 CTrust CPS 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;
- 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.

**Odgovornost i ograničenje od odgovornosti krajnjih korisnika kvalifikovanog certifikata**

Krajnji korisnik je odgovoran za štetu koja je nastala njegovom krivicom.

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

**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.

## 7. PRIMIJENJENE POLITIKE I OSTALI SADRŽAJ

Sve politike i sadržaji od interesa za krajnje korisnike su objavljeni na repozitorijumu CTrust tijela:
http://www.telekom.me/ctrust

## 8. 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. PRIMJENJIVI ZAKONI, ŽALBE I RJEŠAVANJE SPOROVA

Aktivnosti CTrust tijela su usaglašene sa Zakonom o elektronskoj identifikaciji i elektronskom potpisu, i njegovim podzakonskim aktima, Zakonom o zaštiti podataka o ličnosti i ostalim pozitivnim propisima u Crnoj Gori.

Svi sporovi nastali u vezi sa pružanjem elektronskih usluga povjerenja rješavaće se sporazumno.
Ukoliko se dogovor ne može postići sporazumno, spor će se rješavati kod nadležnog suda u Crnoj Gori.


Dzina Tsybulskaja
Izvršni direktor