PODIJELI DOŽIVLJAJ.

KOMPANIJSKA DIREKTIVA

Crnogorski Telekom a.d. Podgorica

ID broj :	169
Vrsta propisa (skraćenica):	CD
Broj verzije:	1.3
Dokument OID:	1.3.6.1.4.1.56393.1.1.6.1
Odgovorni sektor:	Sektor za razvoj servisa i digitalnu transformaciju
Datum donošenja/usvajanja:	1.9.2021.
Datum stupanja na snagu:	7.9.2021.
Validnost:	Neodređeno
Broj aneksa/priloga:	0

Praktična pravila rada za pružanje kvalifikovane usluge verifikacije kvalifikovanih elektronskih potpisa i kvalifikovanih elektronskih pečata (CTrust QSVA Certificate Practice Statement - CTrust QSVA 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 TS 119 312 V1.3.1. (2019-02) – Electronic Signatures and Infrastructures (ESI); Cryptographic Suites
[20] 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
[21] ETSI TS 119 412-1 V1.2.1 (2018-05) - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
[22] ETSI TS 119 102-1 V 1.2.1 (2018-08) - Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation
[23] ETSI TS 119 172-1 V 1.1.1 (2015-07) - Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents
[24] ETSI TS 119 441 V1.1.1 (2018-08) – Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services
[25] EN 419 211-1:2014 – Protection profiles for secure signature creation device – Part 1: Overview (EN 419211-1:2014)
[26] EN 419 211-2:2013 – Protection profiles for secure signature creation device – Part 2: Device with key generation (EN 419211-2:2013)
[27] 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)
[28] 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)
[29] ETSI EN 319 122-1 V1.1.1 (2016-04) Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures
[30] ETSI EN 319 122-2 V1.1.1 (2016-04), Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures
[31] ETSI EN 319 132-1 V1.1.1 (2016-04) Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures
[32] ETSI EN 319 132-2 V1.1.1 (2016-04) Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures

[33] ETSI EN 319 142-1 V1.1.1 (2016-04) Electronic Signatures and Infrastructures (ESI);PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures
[34] ETSI EN 319 142-2 V1.1.1 (2016-04) Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles
[35] ETSI TR 101 533-2 V1.2.1 (2011-12) Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 2: Guidelines for Assessors
[36] ETSI TS 101 533-1 V1.2.1 (2011-12) Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security;vPart 2: Guidelines for Assessors
[37] NIST FIPS PUB 140-2 (2001) – Security Requirements for Cryptographic Modules
[38] IETF RFC 3647 – Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework
[39] IETF RFC 5280 (2008) – Internet X.509 Public Key Infrastructure; Certificate and Certificate Revocation List (CRL) Profile
[40] 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	02.02.2021.	Dokument sa popunjenim poglavljima 1 – 3 prema ETSI TS 119 441 V1.1.1 (2018-08) – Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation service
1.1	8.7.2021	Izmjene u tačkama 1.1.2, 1.4.3, 2.12 i 2.7
1.2	24.8.2021	Izmjene u tačkama 1.1.2, 3.3.1 i dodata tačka 3.3.1.1
1.3	01.09.2021	Izmjene u tačkama 1.1.2 i 3.1.2

SADRŽAJ:

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 naručioca, 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 verifikacije kvalifikovanih elektronskih potpisa i kvalifikovanih elektronskih pečata, u skladu sa Zakonom o elektronskoj identifikaciji i elektronskom potpisu [1], Pravilnikom o načinu sprovođenja verifikacije i načinu vršenja usluge čuvanja kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata [7], standardom ETSI EN 319 401 i tehničkim specifikacijama ETSI TS 119 441.

1.1. PREGLED

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

U okviru CTrust sistema, za potrebe kvalifikovane usluge verifikacije kvalifikovanih elektronskih potpisa i kvalifikovanih elektronskih pečata uspostavljeno je tijelo CTrust QSVA.

1.1.1. UČESNICI

1.1.1.1. DAVALAC USLUGE POVJERENJA

CT je, kao kvalifikovani davalac elektronskih usluga povjerenja, ujedno i davalac kvalifikovane usluge verifikacije kvalifikovanog elektronskog potpisa, odnosno kvalifikovanog elektronskog pečata.

1.1.1.2. NARUČIOCI

Naručioci su fizička ili pravna lica, koja sa CT-om zaključe Ugovor o korišćenju usluga povjerenja, a koji obuhvata i uslove korišćenja kvalifikovane usluge verifikacije kvalifikovanog elektronskog potpisa, odnosno kvalifikovanog elektronskog pečata

Naručilac je direktno odgovoran za sve obaveze propisane ovim dokumentom.

1.1.1.3. TREĆA LICA

Treća lica su fizička lica i poslovni subjekti (kompanije, korporacije, ustanove, tijela državne uprave i dr.) koja se pouzdaju u kvalifikovanu uslugu verifikacije kvalifikovanog elektronskog potpisa, odnosno kvalifikovanog elektronskog pečata.

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

1.1.2. 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 kvalifikovane usluge verifikacije kvalifikovanih elektronskih potpisa i kvalifikovanih elektronskih pečata („CTrust QSVA Certificate Practice Statement - CTrust QSVA CPS)". U njemu su opisana opšta pravila i postupci pružanja kvalifikovane usluge verifikacije kvalifikovanih elektronskih potpisa i kvalifikovanih elektronskih pečata (u daljem tekstu: Praktična pravila).
Verzija: 1.3
Identifikaciona oznaka (OID) za dokument Praktična pravila je: 1.3.6.1.4.1.56393.1.1.6.1
Internet adresa na kojoj je objavljen ovaj CPS dokument je: http://ca.CTrust.telekom.me/cpcps.

Struktura dokumenta je u potpunosti usklađena sa odredbama navedenim u tehničkim specifikacijama ETSI TS 119 441.

1.1.3. PODRŽANA POLITIKA PRUŽANJA KVALIFIKOVANE USLUGE VERIFIKACIJE – IDENTIFIKACIJA USLUGE

Politika kvalifikovane usluge verifikacije kvalifikovanih elektronskih potpisa, odnosno kvalifikovanih elektronskih pečata je identifikovana formalnim registrovanim identifikatorom objekta (OID) 1.3.6.1.4.1.56393.1.5.1.1

CTrust QSVA će navedeni OID koristiti u svim izvještajima verifikacije koje izdaje korisnicima.

1.2. KOMPONENTE USLUGE ZA VERIFIKACIJU

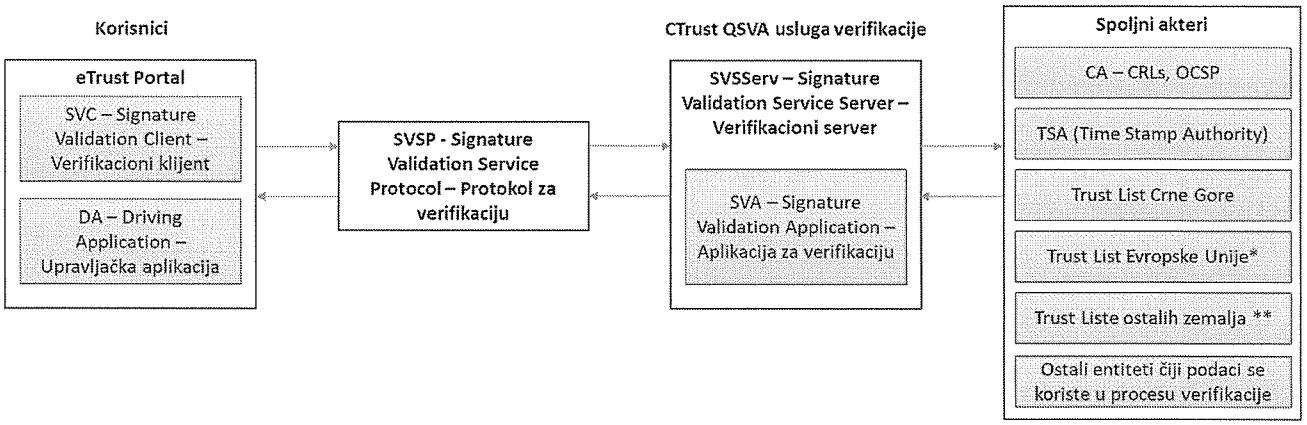
1.2.1. ULOGE U PRUŽANJU USLUGE VERIFIKACIJE

Pojedine komponente usluge verifikacije kvalifikovanih elektronskih potpisa i kvalifikovanih elektronskih pečata imaju sljedeće uloge u procesu verifikacije:

- **eTrust Portal**, kao softverska komponenta koja obezbjeđuje korisnički interfejs (Signature Validation Client – SVC) i kao upravljačka aplikacija koja koristi aplikaciju za validaciju i naručiocu obezbjeđuje funkcionalnost verifikacije (Driving Application – DA);
- **Protokol za verifikaciju**, koji predstavlja bezbjedan komunikacioni kanal za razmjenu informacija naručioca i servera za verifikaciju (Signature Validation Service Protocol – SVP);
- **Verifikacioni server**, kao komponenta koja implementira protokol verifikacije na strani davaoca usluge verifikacije (Signature Validation Service Server – SVSServ) i kao aplikacija za verifikaciju, tj. softverska komponenta koja je odgovorna za verifikaciju kvalifikovanih elektronskih potpisa i kvalifikovanih elektronskih pečata, implementira algoritam verifikacije i kreira izvještaj o verifikaciji (Signature Validation Application – SVA);
- **Spoljni akteri** – Certifikacioni tijela, tijela za izradu elektronskog vremenskog pečata, evropska i crnogorska lista povjerenja, kao i ostali entiteti čiji se podaci koriste u procesu verifikacije kvalifikovanog elektronskog potpisa/pečata.

1.2.2. ARHITEKTURA USLUGE ZA VERIFIKACIJU

Dijagram na slici 1. prikazuje pojednostavljenu arhitekturu usluge za verifikaciju kvalifikovanih elektronskih potpisa i kvalifikovanih elektronskih pečata, kao i učesnike u procesu verifikacije.



Slika 1. – Arhitektura usluge za verifikaciju

* Biće dostupna od dana pristupanja Crne Gore Evropskoj Uniji shodno Zakonu

** Trust Liste zemalja sa kojima Crna Gora ima sklopljene bilateralne sporazume, koji su implementirani u pogledu interoperabilnosti

1.3. DEFINICIJE I SKRAĆENICE

1.3.1. DEFINICIJE

U ovom dokumentu koriste se sljedeće definicije:

Pojam	Opis
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.
Izvještaj verifikacije	Sveobuhvatni izvještaj o obavljenoj verifikaciji, dostavljen od strane aplikacije za verifikaciju upravljačkoj aplikaciji, koji dozvoljava upravljačkoj aplikaciji ili trećim stranama da izvrše provjeru detalja odluka donijetih tokom verifikacionog procesa, kao i detalja koji su doveli do statusa verifikacije dobijenog od aplikacije za verifikaciju.
Kriterijum verifikacije	Tehnički kriterijum koji se provjerava tokom verifikacije kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata.
Podaci za verifikaciju	Podaci koji se koriste za verifikaciju elektronskog potpisa ili elektronskog pečata (kodovi ili javni kriptografski ključevi).
Politika verifikacije	Skup tehničkih kriterijuma za verifikaciju koji se provjeravaju od strane aplikacije za verifikaciju, na osnovu kojih se odlučuje da li je elektronski potpis/pečat ispravan i na osnovu kojih se izrađuje izvještaj o verifikaciji.
Status verifikacije	Jedna od indikacija: USPJEŠNO (TOTAL-PASSED), NEUSPJEŠNO (TOTAL-FAILED ili NEODREĐENO (INDETERMINATE)
Validacija - validation	U ovom dokumentu se engleski izraz „validation" (validacija) može smatrati sinonimom za izraz verifikacija, u skladu sa pravnom regulativom Crne Gore.
Verifikacija	Verifikacija kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata podrazumijeva korišćenje podataka za verifikaciju (kodovi ili javni kriptografski

Pojam	Opis
	ključevi), kako bi se utvrdilo da li je elektronski potpis izrađen privatnim ključem koji odgovara javnom ključu u certifikatu i da li je došlo do promjene podataka, provjeru perioda važenja kvalifikovanih certifikata za elektronski potpis i kvalifikovanih certifikata za elektronski pečat i provjeru da li su ti certifikati opozvani.
Certifikat/Digitalni certifikat	Elektronski dokument kojim se potvrđuje veza između podataka za provjeru elektronskog potpisa/pečata i identiteta potpisnika ili autora elektronskog pečata.
Kvalifikovani certifikat za elektronski potpis	Kvalifikovani certifikat za elektronski potpis je certifikat koji ispunjava uslove propisane Zakonom o elektronskoj identifikaciji i elektronskom potpisu.
Kvalifikovani certifikat za kvalifikovani elektronski potpis	Kvalifikovani certifikat za kvalifikovani elektronski potpis je certifikat koji ispunjava uslove propisane Zakonom o elektronskoj identifikaciji i elektronskom potpisu.
Kvalifikovani certifikat za elektronski pečat	Kvalifikovani certifikat za elektronski pečat je certifikat koji ispunjava uslove propisane Zakonom o elektronskoj identifikaciji i elektronskom potpisu.
Kvalifikovani certifikat za kvalifikovani elektronski pečat	Kvalifikovani certifikat za kvalifikovani elektronski pečat je certifikat koji ispunjava uslove propisane Zakonom 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.
Kvalifikovani elektronski pečat	Kvalifikovani elektronski pečat je napredni elektronski pečat koji je izrađen pomoću kvalifikovanog sredstva za izradu elektronskog pečata i zasniva se na kvalifikovanom certifikatu za elektronski pečat.
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.
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.
Opoziv certifikata	Permanentno ukidanje validnosti datog certifikata i njegovo smještanje na CRL listu.
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.
Potpisnik	Fizičko lice koje se potpisuje u svoje ime ili u ime fizičkog ili pravnog lica korišćenjem podataka za izradu elektronskog potpisa.

Pojam	Opis
Autor elektronskog pečata	Pravno lice ili organ vlasti koje upotrebljava elektronski pečat korišćenjem podataka za izradu elektronskog pečata.
Heš (heš vrednost 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.
Trust List	Lista povjerenja

1.3.2. 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
CA	Certification Authority – Certifikaciono tijelo
CTrust PMA	CTrust Policy Managment Authority – Upravljačko tijelo CTrust-a
DA	Driving Application – Upravljačka aplikacija
PoE	Proof of Existence – Dokaz postojanja
QSVSP	Qualified Signature Validation Service Provider – Kvalifikovani pružalac usluga verifikacije kvalifikovanih elektronskih potpisa i kvalifikovanih elektronskih pečata
SVC	Signature Validation Client – Verifikacioni klijent
SVP	Signature Validation Protocol – Protokol za verifikaciju
SVA	Signature Validation Application – Aplikacija za verifikaciju
SVSServ	Signature Validation Service Server – Verifikacioni server
QSVA	Qualified Signature Verification Authority – Tijelo za pružanje kvalifikovane usluge verifikacije kvalifikovanih elektronskih potpisa i kvalifikovanih elektronskih pečata
CTrust QSVA	CTrust Qualified Signature Verification Authority – Tijelo CTrust-a za pružanje kvalifikovane usluge verifikacije kvalifikovanih elektronskih potpisa i kvalifikovanih elektronskih pečata
SVU	Signature Verification Unit – Verifikaciona jedinica
SD	Signer's Document – Dokument potpisnika ili autora elektronskog pečata
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
QSCD	Qualified Signature Creation Device – kvalifikovano sredstvo za izradu kvalifikovanog elektronskog potpisa/pečata
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
OID	Object Identifier – Identifikato objekta

1.4. POLITIKE I PRAKSE (PROCEDURE)

1.4.1. ORGANIZACIJA ZADUŽENA ZA ADMINISTRIRANJE DOKUMENTA

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

1.4.2. 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

1.4.3. PRIMJENLJIVOST PRAKTIČNIH PRAVILA

CTrust QSVA je odgovoran za izradu i administraciju dokumenta Praktična pravila verifikacije i to u smislu periodične kontrole i ažuriranja, kao i vanrednih izmjena odgovarajućih odredbi koje proističu iz eventualnih promjena u zakonskoj regulativi ili tehničkim karakteristikama primijenjenih rješenja.

Praktična pravila su javno dostupna na repozitorijumu CTrust-a, koji se nalazi na internet adresi:
http://ca.CTrust.telekom.me/cpcps

Nadležni organ shodno zakonu i propisima iz ove oblasti utvrđuje usaglašenost dokumenta sa zakonom. Upravni nadzor nad sprovođenjem Zakona o elektronskoj identifikaciji i elektronskom potpisu [1] vrši Ministarstvo.

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

Ovaj dokument se periodično pregleda i ažurira po potrebi. Period pregleda i ažuriranja ovog dokumenta je minimalno jednom u dvije godine ili prilikom pripreme provjere usklađenosti.
Dokument se može pregledati i po potrebi ažurirati i češće ukoliko dođe do promjena u zakonskoj regulativi ili se javi potreba za promjenom primijenjenih kriptografskih algoritama ili dužina kriptografskih ključeva.

Na osnovu predloga CTrust PMA ovaj dokument odobrava izvršni direktor CT-a.
Sve usvojene izmjene i dopune ovog dokumenta zvanično se dostavljaju bez odlaganja državnom organu nadležnom za ocjenu ispunjenosti uslova za vršenje kvalifikovanih elektronskih usluga povjerenja

2. UPRAVLJANJE I RADNI POSTUPCI

2.1. INTERNA ORGANIZACIJA

2.1.1. POUZDANOST ORGANIZACIJE

CT, kao kvalifikovani davalac elektronskih usluga povjerenja, čiji je sastavni dio CTrust QSVA, 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.

2.1.2. RAZDVAJANJE DUŽNOSTI

CTrust QSVA, 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.

2.2. LJUDSKI RESURSI

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 QSVA koji je dio CTrust sistema.

Kadrovske bezbjednosne mjere opisane su u dokumentu „Politika pružanja elektronskih usluga povjerenja (CTrust Certificate Policy – CTrust CP)", poglavlje 5.3.

2.3. UPRAVLJANJE IMOVINOM

2.3.1. OPŠTI ZAHTJEVI

CT, kao kvalifikovani davalac elektronskih usluga povjerenja, čiji je sastavni dio CTrust QSVA, osigurava odgovarajući nivo zaštite imovine koja se koristi za pružanje kvalifikovane usluge povjerenja verifikacije kvalifikovanih elektronskih potpisa i kvalifikovanih elektronskih 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.

2.3.2. RUKOVANJE MEDIJIMA

Mediji na kojima se nalaze arhivske i sigurnosne kopije CTrust QSVA 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)".

2.4. KONTROLA PRISTUPA

Sistemi neophodni za pružanje usluge verifikacije 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)".

2.5. KRIPTOGRAFSKE MJERE ZAŠTITE

CTrust QSVA 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)".

2.6. FIZIČKA SIGURNOST SISTEMA I SIGURNOST NJEGOVOG OKRUŽENJA

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

2.7. SIGURNOSNO UPRAVLJANJE

Informacioni sistem neophodan za pružanje usluge verifikacije dio je cjelokupne CTrust infrastrukture i primjenjuju se iste bezbjednosne mjere nad računarskitn resursima i životnim ciklusom softvera koje su opisane u dokumentima „Politika pružanja elektronskih usluga povjerenja (CTrust Certificate Policy – CTrust CP)" poglavlje 6.5.
CT ima usvojenu kompanijsku direktivu za upravljanje bezbjednošću informacijama..

2.8. BEZBJEDNOST RAČUNARSKE MREŽE

Računarska mreža neophodna za pružanje usluge verifikacije je dio računarske mreže CTrust sistema i na nju su primijenjene bezbjednosne mjere opisane u dokumentu „Politika pružanja elektronskih usluga povjerenja (CTrust Certificate Policy – CTrust CP)" u poglavlju 6.7.

2.9. UPRAVLJANJE INCIDENTIMA

CTrust ima implementirane procedure reagovanja na bezbjednosne incidente i kvarove u skladu sa pozitivnim zakonskim propisima. Način na koji se upravlja incidentima opisan je u dokumentu „Politika pružanja elektronskih usluga povjerenja (CTrust Certificate Policy – CTrust CP)" u poglavlju 5.7.

2.10. PRIKUPLJANJE DOKAZA (COLLECTION OF EVIDENCE)

Postupci vezani uz 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 pružanje usluge verifikacije što uključuje:

- aktivnosti vezane za generisanje i životni ciklus SVU ključeva i SVU certifikata,
- ukoliko se uz revizijske zapise evidentira i identitet naručioca, neophodno je postupati po Zakonu o zaštiti ličnih podataka.

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)".

Arhiva se čuva na lokaciji CT-a i na udaljenoj lokaciji. Arhiva je zaštićena odgovarajućim sigurnosnim mehanizmima. Pristup arhivama je dozvoljen samo ovlašćenim licima.

2.11. PLAN KONTINUITETA POSLOVANJA

CT ima uspostavljene procedure u internim pravilima rada i Plan kontinuiteta poslovanja, koji pokrivaju oporavak poslovanja nakon kvara računarskih resursa, softvera i podataka, kao i slučajeve prirodnih i drugih katastrofa , kao što je navedeno u poglavljima 5.7.1. i 5.7.4. dokumenta „Politika pružanja elektronskih usluga povjerenja (CTrust Certificate Policy – CTrust CP)".

2.12. PREKID RADA PRUŽAOCA USLUGA POVJERENJA

U slučaju planiranog prestanka pružanja usluge verifikacije kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata, a u skladu sa Planom prekida pružanja usluga CTrust sistema poglavlje: Prestanak poslovanja kvalifikovanog davaoca elektronskih usluga povjerenja, Crnogorski Telekom će učiniti sve razumne napore kako bi se minimizirao uticaj ukidanja usluge na poslovni proces naručilaca ili trećih lica.
CT će naročito:

- Raskinuće ugovore sa korisnicima i o tome obavijestiti naručioce i treća lica putem repozitorijuma i nadležni organ državne uprave najmanje tri mjeseca prije dana predviđenog za raskid ugovora;
- Korisnicima usluge verifikacije obezbijediće nastavak pružanja usluge kod drugog davaoca elektronskih usluga povjerenja i dostaviće mu svu dokumentaciju u vezi sa obavljanjem usluga;
- U slučaju da ne obezbijedi nastavak pružanja usluge verifikacije kod drugog davaoca opozvaće sve izdate certifikate SVU 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 SVU certifikata;
- Arhiviraće sve podatke u skladu sa periodom propisanim odgovarajućim zakonom od zadnjeg dana rada davaoca usluge povjerenja.

2.13. USAGLAŠENOST SA VAŽEĆIM ZAKONIMA I RJEŠAVANJE SPOROVA

Ova Praktična pravila su usaglašena sa:

- Zakonom o elektronskoj identifikaciji i elektronskom potpisu [1],
- Pravilnikom o načinu sprovođenja verifikacije i načinu vršenja usluge čuvanja kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata [7] i
- drugim pozitivnim zakonskim propisima iz ove oblasti.

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

3. DIZAJN USLUGE ZA VERIFIKACIJU

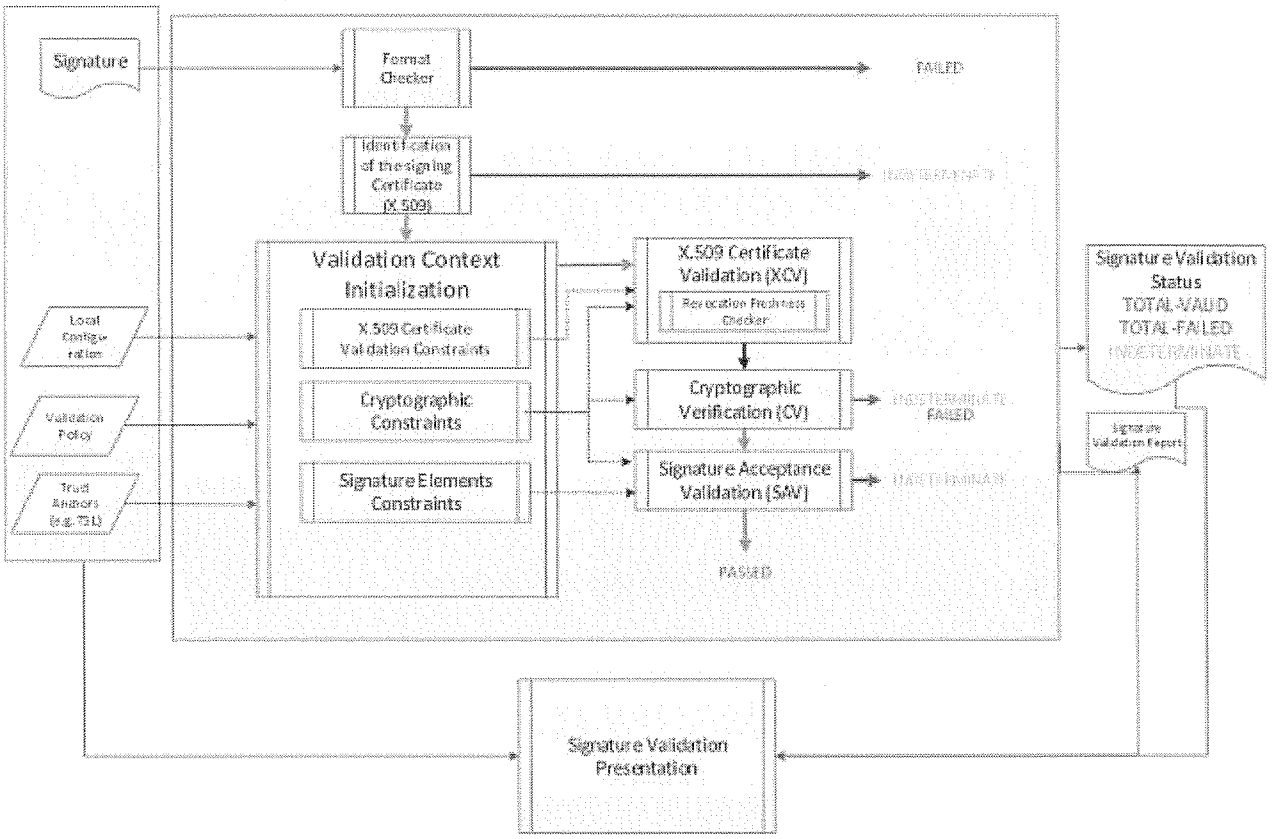
3.1. ZAHTJEVI ZA VERIFIKACIJU

CTrust QSVA, u procesu pružanja usluge verifikacije, koristi politiku verifikacije kroz postupak utvrđivanja tehničke ispravnosti kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata koji je u skladu sa tehničkom specifikacijom ETSI TS 119 102-1.

Ovaj dokument u nastavku opisuje način na koji tijelo koje vrši uslugu verifikacije sprovodi pojedine faze postupka provjere, kao i tehničke kriterijume koji se koriste prilikom procesa verifikacije.

3.1.1. MODEL PROVJERE VALIDNOSTI KVALIFIKOVANOG ELEKTRONSKOG POTPISA I KVALIFIKOVANOG ELEKTRONSKOG PEČATA

Konceptualni model provjere validnosti kvalifikovanog elektronskog potpisa/pečata prikazan je na slici 2. i u potpunosti je preuzet iz standarda ETSI TS 119 102-1.



Slika 2. - Konceptualni model verifikacije kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata

Konceptualni model prikazuje da se tokom verifikacije provjeravaju: format kvalifikovanog elektronskog potpisa, odnosno kvalifikovanog elektronskog pečata, certifikat potpisnika ili autora elektronskog pečata , X.509 kriterijumi za verifikaciju certifikata, kriptografski kriterijumi i kriterijumi vezani za elemente kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata. Na osnovu provjere ovih kriterijuma aplikacija za verifikaciju prikazuje rezultat verifikacije i izdaje izvještaj o verifikaciji.

CTrust QSVA istovremeno prihvata samo jednu datoteku za verifikaciju, koja sadrži elektronske potpise, odnosno pečate i datoteke sa potpisanim sadržajem u sebi.

3.1.2. STATUS VERIFIKACIJE I IZVJEŠTAJ O VERIFIKACIJI

CTrust QSVA izdaje sveobuhvatni izvještaj o verifikaciji kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata na elektronskom dokumentu. Aplikacija za verifikaciju, na osnovu politike verifikacije, detaljno provjerava kvalifikovani elektronski potpis i ta provjera obuhvata utvrđivanje da je korišćenje pseudonima, ako je pseudonim korišćen u trenutku potpisivanja, naznačeno korisniku, odnosno kvalifikovani elektronski pečat i preko upravljačke aplikacije prezentuje izvještaj o verifikaciji, koji može biti u formi čitljive HTML stranice, XML ili PDF dokumenta.

Izlazni izvještaj procesa verifikacije kvalifikovanog elektronskog potpisa, odnosno kvalifikovanog elektronskog pečata sadrži:

- listu potpisa/pečata;
- status koji pokazuje rezultate postupka provjere potpisa/pečata;

- neispunjeni kriterijumi na osnovu kojih je potpis/pečat nevalidan (TOTAL-FAILED) ili upozorenja koja opisuju zašto se nije mogao utvrditi status potpisa/pečata (INDETERMINATE);
- OID oznaku usluge verifikacije.

Status verifikacije kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata može imati jednu od tri vrijednosti: USPJEŠNO (TOTAL-PASSED), NEODREĐENO (INDETERMINATE) i NEUSPJEŠNO (TOTAL-FAILED), a u skladu sa tehničkim specifikacijama ETSI TS 119 102-1.

Status verifikacije USPJEŠNO označava da su sve kriptografske provjere elektronskog potpisa, odnosno elektronskog pečata, kao i sve druge provjere u skladu sa propisanim politikama i pravilima za verifikaciju.

Status verifikacije NEODREĐENO označava da nijesu ispunjeni svi uslovi za status verifikacije USPJEŠNO, s tim da postoji mogućnost da se steknu uslovi za status verifikacije USPJEŠNO na osnovu dodatnih činjenica koje su se u postupku verifikacije smatrale nepoznatim.

Status verifikacije NEUSPJEŠNO označava da nijesu ispunjeni uslovi ni za status verifikacije USPJEŠNO, ni za status verifikacije NEODREĐENO.

Struktura i semantika osnovnih statusa verifikacije data je u Tabeli 1. – Struktura i semantika osnovnih statusa verifikacije :

Indikator statusa	Semantika	Podaci izvještaja o verifikaciji
USPJEŠNO (TOTAL-PASSED)	Proces verifikacije rezultira statusom USPJEŠNO (TOTAL-PASSED) ukoliko je ispunjeno sljedeće: • kriptografska provjera potpisa, odnosno pečata je bila uspješna; • svi kriterijumi koji se odnose na provjeru identiteta potpisnika ili autora elektronskog pečata pozitivno su potvrđeni; • potpis/pečat je pozitivno potvrđen u odnosu na sve kriterijume iz politike verifikacije.	Izlaz iz procesa verifikacije je: certifikat za potpisivanje korišćen u procesu, zajedno sa specifičnim potpisanim atributima, ukoliko su prisutni i rezultati provjera svih kriterijuma iz politike verifikacije.
NEUSPJEŠNO (TOTAL-FAILED)	Proces verifikacije rezultira statusom TOTAL-FAILED ukoliko su kriptografske provjere potpisa/pečata neuspješne ili može biti dokazano da je generisanje potpisa/pečata nastalo nakon opoziva certifikata potpisnika ili autora elektronskog pečata.	Izlaz iz procesa verifikacije su dodatne informacije koje objašnjavaju status TOTAL-FAILED za svaki kriterijum iz politike verifikcije za koji je rezultat provjere negativan.
NEODREĐENO (INDETERMINATE)	Dostupne informacije nijesu dovoljne da bi proces verifikacije potpisa/pečata rezultirao statusom TOTAL-PASSED ili TOTAL-FAILED.	Izlaz iz procesa verifikacije su dodatne informacije koje objašnjavaju status INDETERMINATE i od pomoći su naručiocu da identifikuje nedostajuće podatke neophodne da bi se verifikacija izvršila uspješno.

Tabela 1. – Struktura i semantika osnovnih statusa verifikacije

Pored osnovnih statusa, izvještaj o verifikaciji uključuje i sekundarnu indikaciju sa semantikom prikazanom u Tabeli 2. – Sekundarne indikacije procesa verifikacije:

Osnovna indikacija	Subindikacija	Povezani podaci u verifikacionom izvještaju	Semantika
TOTAL_FAILED	FORMAT_FAILURE	The validation process shall provide any information available why parsing of the signature failed. Proces verifikacije će obezbijediti sve dostupne informacije zašto analiza potpisa nije uspjela.	The signature is not conformant to one of the base standards to the extent that the cryptographic verification building block is unable to process it. Potpis nije u skladu sa jednim od osnovnih standarda do te mjere da blok za kriptografsku verifikaciju nije u mogućnosti da ga obradi.
	HASH_FAILURE	The validation process shall provide: An identifier (s) (e.g. an URI or OID) uniquely identifying the element within the signed data object (such as the signature attributes, or the SD) that caused the failure. Proces verifikacije će obezbijediti: Identifikator(e) (npr. URI ili OID) koji jedinstveno identifikuju element unutar potpisanog objekta podataka (kao što su atributi potpisa, ili SD) koji su uzrokovali neuspjeh.	The signature validation process results into TOTAL-FAILED because at least one hash of a signed data object(s) that has been included in the signing process does not match the corresponding hash value in the signature. Proces verifikacije potpisa rezultira TOTAL-FAILED, jer se najmanje jedan heš potpisanih objekata podataka koji su bili uključeni u proces potpisivanja ne podudaraju sa odgovarajućom heš vrijednošću u potpisu.

Osnovna indikacija	Subindikacija	Povezani podaci u verifikacionom izvještaju	Semantika
	SIG_CRYPTO_ FAILURE	The validation process shall output: The signing certificate used in the validation process. Izlaz procesa verifikacije: Certifikat potpisnika ili autora elektronskog pečata koji se koristi u procesu verifikacije.	The signature validation process results into TOTAL-FAILED because the signature value in the signature could not be verified using the signer's public key in the signing certificate. Proces verifikacije potpisa rezultira TOTAL-FAILED, jer vrijednost potpisa nije mogla biti verifikovana pomoću javnog ključa potpisnika ili autora elektronskog pečata u certifikatu potpisnika ili autora elektronskog pečata.
	REVOKED	The validation process shall provide the following: • The certificate chain used in the validation process. • The time and, if available, the reason of revocation of the signing certificate. Proces verifikacije će obezbijediti sljedeće: • Lanac certifikata koji se koristi u procesu verifikacije. • Vrijeme i, ako je dostupan, razlog opoziva certifikata potpisnika ili autora elektronskog pečata.	The signature validation process results into TOTAL-FAILED because: • the signing certificate has been revoked; and • there is proof that the signature has been created after the revocation time. Proces verifikacije potpisa rezultira TOTAL-FAILED, jer: • certifikat potpisnika ili autora elektronskog pečata je opozvan; • postoji dokaz da je kreiranje potpisa nastalo nakon opoziva certifikata potpisnika ili autora elektronskog pečata .

Osnovna indikacija	Subindikacija	Povezani podaci u verifikacionom izvještaju	Semantika
	EXPIRED	The process shall output: The validated certificate chain Izlaz procesa: Potvrđeni lanac certifikata	The signature validation process results into TOTAL-FAILED because there is proof that the signature has been created after the expiration date (notAfter) of the signing certificate. Proces verifikacije potpisa rezultira TOTAL-FAILED, jer postoji dokaz da je potpis kreiran nakon datuma isteka (vrijednost notAfter atributa) certifikata potpisnika ili autora elektronskog pečata .
	NOT_YET_VALID		The signature validation process results into TOTAL-FAILED because there is proof that the signature was created before the issuance date (notBefore) of the signing certificate. Proces verifikacije potpisa rezultira TOTAL-FAILED, jer postoji dokaz da je potpis kreiran prije datuma izdavanja (vrijednost notBefore atributa) certifikata potpisnika ili autora elektronskog pečata .
INDETERMINATE	SIG_CONSTRAINTS_ FAILURE	The validation process shall provide: The set of constraints that have not been met by the signature. Proces verifikacije će obezbijediti: skup ograničenja koja nijesu ispunjena potpisom.	The signature validation process results into INDETERMINATE because one or more attributes of the signature do not match the validation constraints. Proces verifikacije potpisa rezultira INDETERMINATE jer se jedan ili više atributa potpisa ne podudaraju sa ograničenjima verifikacije.

Osnovna indikacija	Subindikacija	Povezani podaci u verifikacionom izvještaju	Semantika
	CHAIN_CONSTRAINTS_ FAILURE	The validation process shall output: • The certificate chain used in the validation process. • The set of constraints that have not been met by the chain. Izlaz procesa verifikacije: • Lanac certifikata koji se koristi u procesu verifikacije. • Skup ograničenja koja lanac nije ispunio.	The signature validation process results into INDETERMINATE because the certificate chain used in the validation process does not match the validation constraints related to the certificate. Proces verifikacije potpisa rezultira INDETERMINATE jer se lanac certifikata koji se koristi u procesu verifikacije ne podudara sa ograničenjima verifikacije povezanim sa certifikatom.
	CERTIFICATE_CHAIN_ GENERAL_FAILURE	The process shall output: Additional information regarding the reason. Izlaz procesa: Dodatne informacije vezane za razlog.	The signature validation process results into INDETERMINATE because the set of certificates available for chain validation produced an error for an unspecified reason. Proces verifikacije potpisa rezultira INDETERMINATE, jer je skup certifikata dostupan za verifikaciju lanca proizveo grešku iz neodređenog razloga.
	CRYPTO_CONSTRAINTS_ FAILURE	The process shall output: • Identification of the material (signature, certificate) that is produced using an	The signature validation process results into INDETERMINATE because at least one of the algorithms that have been used in material (e.g. the signature value, a certificate...) involved in validating

Osnovna indikacija	Subindikacija	Povezani podaci u verifikacionom izvještaju	Semantika
		algorithm or key size below the required cryptographic security level. • If known, the time up to which the algorithm or key size were considered secure. Izlaz procesa: • Identifikacija materijala (potpis, certifikat) koja se izrađuje pomoću algoritma ili dužine ključa ispod zahtijevanog nivoa kriptografske sigurnosti. • Ako je poznato, vrijeme do kada su se algoritam ili dužina ključa smatrali sigurnim.	the signature, or the size of a key used with such an algorithm, is below the required cryptographic security level, and: • this material was produced after the time up to which this algorithm/key was considered secure (if such a time is known); and • the material is not protected by a sufficiently strong time-stamp applied before the time up to which the algorithm/key was considered secure (if such a time is known). Proces verifikacije potpisa rezultira INDETERMINATE, jer je barem jedan od algoritama korišćenih u materijalu (npr. vrijednost potpisa, certifikat ...) i uključenih u verifikaciju potpisa ili dužina ključa koji se koristi sa takvim algoritmom, ispod potrebnog nivoa kriptografske sigurnosti i: • ovaj materijal je izrađen nakon vremena do kada se primjenjeni algoritam/ključ smatrao sigurnim (ako je takvo vrijeme poznato); i • predmet nije zaštićen dovoljno jakim vremenskim pečatom primijenjenim prije vremena do kada se algoritam/ključ smatrao sigurnim (ako je takvo vrijeme poznato).
	POLICY_PROCESSING_	The validation process shall provide additional	The signature validation process results into INDETERMINATE

Osnovna indikacija	Subindikacija	Povezani podaci u verifikacionom izvještaju	Semantika
	ERROR	information on the problem. Proces verifikacije će obezbijediti dodatne informacije o problemu.	because a given formal policy file could not be processed for any reason (e.g. not accessible, not parseable, digest mismatch, etc.). Proces verifikacije potpisa rezultira INDETERMINATE, jer se dati formalni fajl politike nije mogao obraditi iz bilo kog razloga (npr. nije dostupan, nije ga moguće analizirati, nepodudaranje sažetka, itd.).
	SIGNATURE_POLICY_ NOT_AVAILABLE		The signature validation process results into INDETERMINATE because the electronic document containing the details of the policy is not available. Proces verifikacije potpisa rezultira INDETERMINATE, jer elektronski dokument koji sadrži detalje politike nije dostupan.
	TIMESTAMP_ORDER_ FAILURE	The validation process shall output the list of time-stamps that do no respect the ordering constraints. Izlaz procesa verifikacije će biti lista vremenskih pečata kojima nijesu ispoštovana ograničenja redosljeda.	The signature validation process results into INDETERMINATE because some constraints on the order of signature time-stamps and/or signed data object(s) time-stamps are not respected. Proces verifikacije potpisa rezultira INDETERMINATE, jer neka ograničenja u redosljedu vremenskih pečata za potpis i/ili vremenskih pečata za potpisane objekte podataka, nijesu ispoštovana.
	NO_SIGNING_		The signature validation process results into INDETERMINATE

Osnovna indikacija	Subindikacija	Povezani podaci u verifikacionom izvještaju	Semantika
	CERTIFICATE_FOUND		because the signing certificate cannot be identified. Proces verifikacije potpisa rezultira INDETERMINATE, jer se certifikat potpisnika ili autora elektronskog pečata ne može identifikovati.
	NO_CERTIFICATE_ CHAIN_FOUND		The signature validation process results into INDETERMINATE because no certificate chain has been found for the identified signing certificate. Proces verifikacije potpisa rezultira INDETERMINATE, jer nije pronađen lanac certifikata za identifikovani certifikat potpisnika ili autora elektronskog pečata .
	REVOKED_NO_ POE	The validation process shall provide the following: • The certificate chain used in the validation process. • The time and the reason of revocation of the signing certificate. Proces verifikacije će obezbijediti sljedeće: • Lanac certifikata koji se koristi u procesu verifikacije.	The signature validation process results into INDETERMINATE because the signing certificate was revoked at the validation date/time. However, the Signature Validation Algorithm cannot ascertain that the signing time lies before or after the revocation time. Proces verifikacije potpisa rezultira INDETERMINATE, jer je certifikat potpisnika ili autora elektronskog pečata opozvan na datum/vrijeme verifikacije. Međutim, algoritam za verifikaciju potpisa ne može utvrditi da je vrijeme potpisivanja prije ili poslije vremena opoziva.

Osnovna indikacija	Subindikacija	Povezani podaci u verifikacionom izvještaju	Semantika
		• Vrijeme i razlog opoziva certifikata potpisnika ili autora elektronskog pečata .	
	REVOKED_CA_ NO_POE	The validation process shall provide the following: • The certificate chain which includes the revoked CA certificate. • The time and the reason of revocation of the certificate. Proces verifikacije će obezbijediti sljedeće: • Lanac certifikata koji uključuje opozvani CA certifikat. • Vrijeme i razlog opoziva certifikata.	The signature validation process results into INDETERMINATE because at least one certificate chain was found but an intermediate CA certificate is revoked. Proces verifikacije potpisa rezultira INDETERMINATE, jer je pronađen barem jedan lanac certifikata, ali je opozvan certifikat podređenog CA tijela.
	OUT_OF_BOUNDS_ NOT_REVOKED		The signature validation process results into INDETERMINATE because the signing certificate is expired or not yet valid at the validation date/time and the Signature Validation Algorithm cannot ascertain that the signing time lies within the validity interval of the signing certificate. The certificate is known not to be revoked.

Osnovna indikacija	Subindikacija	Povezani podaci u verifikacionom izvještaju	Semantika
			Proces verifikacije potpisa rezultira INDETERMINATE, jer je istekao certifikat potpisnika ili autora elektronskog pečata ili još nije validan na datum/vrijeme verifikacije i algoritam za verifikaciju potpisa ne može utvrditi da je vrijeme potpisivanja unutar intervala validnosti certifikata potpisnika ili autora elektronskog pečata . Poznato je da certifikat nije opozvan.
	OUT_OF_BOUNDS_ NO_POE		The signature validation process results into INDETERMINATE because the signing certificate is expired or not yet valid at the validation date/time and the Signature Validation Algorithm cannot ascertain that the signing time lies within the validity interval of the signing certificate. Proces verifikacije potpisa rezultira INDETERMINATE, jer je istekao certifikat potpisnika ili autora elektronskog pečata ili još nije validan na datum/vrijeme verifikacije i Algoritam za verifikaciju potpisa ne može utvrditi da je vrijeme potpisivanja unutar intervala validnosti certifikata potpisnika ili autora elektronskog pečata .
	CRYPTO_CONSTRAINTS_ FAILURE_NO_POE	The process shall output: • Identification of the material (signature, certificate) that is	The signature validation process results into INDETERMINATE because at least one of the algorithms that have been used in objects (e.g. the signature value, a

Osnovna indikacija	Subindikacija	Povezani podaci u verifikacionom izvještaju	Semantika
		produced using an algorithm or key size below the required cryptographic security level. If known, the time up to which the algorithm or key size were consider secure. Izlaz procesa: • Identifikacija materijala (potpis, certifikat) koji se izrađuje pomoću algoritma ili dužine ključa ispod zahtijevanog nivoa kriptografske sigurnosti. • Ako je poznato, vrijeme do kada su se algoritam ili veličina ključa smatrali sigurnim.	certificate, etc.) involved in validating the signature, or the size of a key used with such an algorithm, is below the required cryptographic security level, and there is no proof that this material was produced before the time up to which this algorithm/key was considered secure. Proces verifikacije potpisa rezultira INDETERMINATE, jer je barem jedan od algoritama korišćenih u materijalu (npr. vrijednost potpisa, certifikat, itd.) i uključenih u verifikaciju potpisa ili dužina ključa koji se koristi sa takvim algoritmom, ispod potrebnog nivoa kriptografske sigurnosti i nema dokaza da je ovaj materijal izrađen prije vremena do kada se ovaj algoritam/ključ smatrao sigurnim.
	NO_POE	The validation process shall identify at least the signed objects for which the POEs are missing. • The validation process should provide additional information on the problem. Procesom verifikacije će se identifikovati bar potpisani objekti za koje	The signature validation process results into INDETERMINATE because a proof of existence is missing to ascertain that a signed object has been produced before some compromising event (e.g. broken algorithm). Proces verifikacije potpisa rezultira INDETERMINATE, jer nedostaje dokaz o postojanju da bi se utvrdilo da je potpisani objekt izrađen prije

Osnovna indikacija	Subindikacija	Povezani podaci u verifikacionom izvještaju	Semantika
		nedostaju dokazi o postojanju. • Proces verifikacije treba da obezbijedi dodatne informacije o problemu.	nekog kompromitujućeg događaja (npr. kompromitovani algoritam).
	TRY_LATER	The validation process shall output the point of time, where the necessary revocation information is expected to become available. Izlaz procesa verifikacije će biti vremenski trenutak u kojem se očekuje da će postati dostupni potrebni podaci o opozivu.	The signature validation process results into INDETERMINATE because not all constraints can be fulfilled using available information. However, it may be possible to do so using additional revocation information that will be available at a later point of time. Proces verifikacije potpisa rezultira INDETERMINATE, jer se sva ograničenja ne mogu ispuniti pomoću dostupnih informacija. Međutim, to može biti moguće pomoću dodatnih informacija o opozivu koje će biti dostupne kasnije.
	SIGNED_DATA _NOT_FOUND	The process should output when available: The identifier(s) (e.g. an URI) of the signed data that caused the failure. Izlaz procesa, kada je dostupan: Identifikator (i) (npr. URI) potpisanih podataka	The signature validation process results into INDETERMINATE because signed data cannot be obtained. Proces verifikacije potpisa rezultira INDETERMINATE, jer se potpisani podaci ne mogu dobiti.

Osnovna indikacija	Subindikacija	Povezani podaci u verifikacionom izvještaju	Semantika
		koji su uzrokovali neuspjeh.	

Tabela 2. – Sekundarne indikacije procesa verifikacije

Napomena: U slučaju neslaganja objašnjenja na zvaničnom jeziku koji je u upotrebi u Crnoj Gori i engleske verzije, prednost ima engleska verzija

3.1.3. PROCES VERIFIKACIJE

CTrust usluga verifikacije podržava provjeru za elektronske potpise i pečate, elektronske potpise i pečate sa elektronskim vremenskim pečatom i elektronske potpise i pečate za pouzdano elektronsko čuvanje dokumenata.

U kontekstu zakonodavstva Crne Gore i Evropske unije, CTrust usluga verifikacije podržava sljedeće formate elektronskog potpisa i elektronskog pečata:

1. ETSI TS 103 171 V2.1.1 (2012-03) Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile;
2. ETSI TS 103 172 V2.2.2 (2013-04) Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile;
3. ETSI TS 103 173 V2.1.1 (2012-03) Electronic Signatures and Infrastructures (ESI); CAdES Baseline Profile.

Postupak verifikacije kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata sprovodi se na sljedeći način:

1. Usluga verifikacije sprovodi postupak verifikacije za sve elektronske potpise, odnosno pečate, nezavisno od njihovog nivoa;
2. Ukoliko je provjera odabranim postupkom verifikacije vratila indikaciju PASSED, usluga dodjeljuje statusu verifikacije vrijednost TOTAL-PASSED;
3. Ukoliko je provjera odabranim postupkom verifikacije vratila indikaciju NOT PASSED, usluga dodjeljuje statusu verifikacije vrijednost TOTAL-FAILED;
4. U suprotnom, usluga dodjeljuje statusu verifikacije vrijednost INDETERMINATE.

Proces verifikacije kvalifikovanih elektronskih potpisa i kvalifikovanih elektronskih pečata sastoji se od sljedećih koraka, kada se ista obavlja upotrebom eTrust portala:

1. Provjera identiteta klijenta na eTrust portalu i prijava na upravljačku aplikaciju (DA);
2. Naručilac bira dokument čiji će elektronski potpis, odnosno elektronski pečat biti verifikovan. DA računa heš vrijednost odabranog dokumenta i šalje dokument aplikaciji za verifikaciju (SVA);
3. SVA verifikuje kriptografsku strukturu primljenog materijala i lanac certifikata potpisnika/autora elektronskog pečata;
4. SVA šalje serijski broj certifikata potpisnika/autora elektronskog pečata OCSP servisu, kako bi provjerila njegov status;
5. OCSP komponenta vraća rezultat provjere;
6. SVA učitava CRL (lista opozvanih certifikata);
7. SVA koristi serijski broj certifikata potpisnika/autora elektronskog pečata da bi u listi povučenih certifikata provjerila da li je certifikat opozvan;

8. SVA provjerava listu certifikata od povjerenja (Trust List) da li se certifikatu certifikacionog tijela koje je potpisalo certifikat potpisnika/autora elektronsko pečata može vjerovati;
9. SVA određuje da li se certifikatu certifikacionog tijela koje je potpisalo certifikat potpisnika/autora elektronsko pečata može vjerovati;
10. SVA konstruiše izvještaj o verifikaciji, izvještaj se elektronski potpisuje privatnim ključem SVU i rezultat verifikacije se vraća DA;
11. DA prezentuje klijentu rezultat verifikacije i elektronski potpisan izvještaj o verifikaciji.

3.1.4. POLITIKA VERIFIKACIJE – KRITERIJUMI ZA VERIFIKACIJU

CTrust QSVA primjenjuje politiku verifikacije kvalifikovanih elektronskih potpisa, odnosno kvalifikovanih elektronskih pečata koja je definisana ETSI politikom verifikacije označenom OID 0.4.0.19441.1.2 (itu-t(0) identified-organization(4) etsi(0) val-service-policies(19441) policy-identifiers(1) qualified (2)).

Jedna usluga verifikacije ne prihvata više politika verifikacije.

Strategija definisana u politici verifikacije slijedi sljedeće principe:

- Za isti ulaz, primjenjujući politiku verifikacije, usluga verifikacije će vratiti isti izlaz.
- Sistem za verifikaciju može za provjeru potpisa prihvatiti različite elemente kao dokaz postojanja potpisa.

Kriterijumi koji su sastavni dio CTrust QSVA politike verifikacije kvalifikovanih elektronskih potpisa, odnosno kvalifikovanih elektronskih pečata, a na osnovu kojih CTrust QSVA verifikuje kvalifikovane elektronske potpise i kvalifikovane elektronske pečate definisani su u kontrolnim podacima specifičnim za SVA , kao i samom implementacijom.

Svi kriterijumi za provjeru u okviru usluge, koji se ne podrazumijevaju implementacijom, potiču iz samog sadržaja potpisa (uključeno u atribute potpisa/pečata) ili indirektno, pozivanjem na spoljni dokument, dat u mašinski obradivom obliku. Dodatni kriterijumi mogu biti definisani preko parametara odabranih od strane aplikacije ili naručioca.

Opšti kriterijumi

CTrust QSVA usluga povjerenja verifikacije kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata podržava maksimalnu veličinu datoteke dokumenata od 100 MB.

X.509 kriterijumi

CTrust QSVA usluga povjerenja verifikacije kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata implementira X.509 kriterijume verifikacije, koji ukazuju na zahtjeve provjere lanca certifikata, kako je određeno tehničkim specifikacijama ETSI TS 119 172-1, klauzula A.4.2.1, tabela A.2, red m.

Kriterijum	Vrijednost pri verifikaciji
m)1. X509CertificateValidationConstraints: This set of constraints indicates requirements for use in the certificate path validation process as defined in IETF RFC 5280. These constraints may be different for different certificate types (e.g. certificates issued to signer, to CAs, to OCSP responders, to CRL Issuers, to Time-	Trust List Crne Gore Trust List Evropske Unije * Trust List ostalih zemalja **

Kriterijum	Vrijednost pri verifikaciji
Stamping Units). Semantic for a possible set of requirement values used to express such requirements is defined as follows: Ovaj skup ograničenja ukazuje na zahtjeve koje treba koristiti u procesu verifikacije certifikata kako je definisano u IETF RFC 5280. Ova ograničenja mogu se razlikovati za različite tipove certifikata (npr. certifikati izdati potpisniku ili autoru elektronskog pečata, CA tijelima, OCSP jedinicama, izdavaocima CRL lista, jedinicama za izradu zapisa vremenskog pečata). Semantika za mogući skup zahtijevanih vrijednosti koje se koriste za izražavanje takvih zahtjeva definisana je na sljedeći način: (m)1.1. SetOfTrustAnchors: This constraint indicates a set of acceptable trust anchors (TAs) as a constraint for the validation process. Ovo ograničenje ukazuje na skup prihvatljivih strana od povjerenja (trust anchors - TA) kao ograničenje za proces verifikacije.	
(m)1.2. CertificationPath: This constraint indicates a certification path required to be used by the SVA for validation of the signature. The certificate path is of length 'n' from the trust anchor (TA) down to the certificate used in validating a signed object (e.g. the signer's certificate or a time stamping certificate). This constraint can include the path to be considered or indicate the need for considering the path provided in the signature if any. Ovo ograničenje ukazuje na put certifikata koji SVA treba da koristi za validaciju potpisa. Put certifikata je dužine 'n' od „strane od povjerenja" (Trust Anchor -TA) do certifikata koji se koristi za validaciju potpisanog objekta (npr. certifikat potpisnika ili certifikat vremenskog pečata). Ovo ograničenje može sadržati putanju koju treba razmotriti ili ukazati na potrebu razmatranja putanje predviđene potpisom, ako postoji. • (m)1.3. user-initial-policy-set: This constraint is as described in IETF RFC 5280 clause 6.1.1 item (c) Ovo ograničenje je opisano u IETF RFC 5280 klauzula 6.1.1 stavka (c)	None

Kriterijum	Vrijednost pri verifikaciji
• (m)1.4. initial-policy-mapping-inhibit: This constraint is as described in IETF RFC 5280 clause 6.1.1 item (e) Ovo ograničenje je opisano u IETF RFC 5280 klauzula 6.1.1 stavka (e) • (m)1.5. initial-explicit-policy: This constraint is as described in IETF RFC 5280 clause 6.1.1 item (f) Ovo ograničenje je opisano u IETF RFC 5280 klauzula 6.1.1 stavka (f) • (m)1.6. initial-any-policy-inhibit: This constraint is as described in IETF RFC 5280 clause 6.1.1 item (g) Ovo ograničenje je opisano u IETF RFC 5280 klauzula 6.1.1 stavka (g) • (m)1.7. initial-permitted-subtrees: This constraint is as described in IETF RFC 5280 clause 6.1.1 item (h) Ovo ograničenje je opisano u IETF RFC 5280 klauzula 6.1.1 stavka (h) • (m)1.8. initial-excluded-subtrees: This constraint is as described in IETF RFC 5280 clause 6.1.1 item (i) Ovo ograničenje je opisano u IETF RFC 5280 klauzula 6.1.1 stavka (i) • (m)1.9. path-length-constraints: This constraint indicates restrictions on the number of CA certificates in a certification path. This may need to define initial values for this or to handle such constraint differently (e.g. ignore it) Ovo ograničenje ukazuje na ograničenja broja CA certifikata na putu certifikata. Ovo će možda zahtijevati definisanje početne vrijednosti ili drugačije postupanje sa takvim ograničenjem (npr. zanemariti ga) • (m)1.10. policy-constraints: This constraint indicates requirements for certificate policies referenced in the certificates. This may need to define initial values for this or to handle such constraint differently (e.g. ignore it). This should also allow the ability to require a (possible set of) specific certificate policy extension value(s) in end-entity certificates (without requiring such values appearing in certificate of authorities in the certification path). Ovo ograničenje ukazuje na zahtjeve za certifikacione politike na koje se referenciraju certifikati. Ovo će možda zahtijevati definisanje početne vrijednosti ili drugačije postupanje s takvim	

Kriterijum	Vrijednost pri verifikaciji
ograničenjem (npr. zanemariti ga). Ovo bi takođe trebalo dozvoliti mogućnost zahtevanja (mogućeg skupa) specifičnih vrijednosti ekstenzija certifikacionih politika u certifikatima krajnjih korisnika (bez potrebe da se takve vrijednosti pojavljuju u certifikatima certifikacionih tijela na putu certifikacije).	
(m)2. RevocationConstraints: This set of constraints indicates requirements applicable when verifying the certificate validity status of the certificates during the certificate path validation process. These constraints may be different for different certificate types (e.g. certificates issued to signer, to CAs, to OCSP responders, to CRL Issuers, to Time-Stamping Units). Semantic for a possible set of requirement values used to express such requirements is defined as follows: Ovaj skup ograničenja ukazuje na zahtjeve koji se primenjuju prilikom provjere statusa valjanosti certifikata tokom procesa verifikacije lanca certifikata. Ova ograničenja mogu biti različita za različite tipove certifikata (npr. certifikati izdati potpisniku ili autoru pečata, CA tijelima, OCSP jedinicama, izdavaocima CRL lista, jedinicama za izradu zapisa vremenskog pečata). Semantika za mogući skup zahtijevanih vrijednosti koje se koriste za izražavanje takvih zahtjeva definisana je na sljedeći način: (m)2.1. RevocationCheckingConstraints: This constraint indicates requirements for checking certificate revocation. Such constraints may specify if revocation checking is required or not and if OCSP responses or CRLs have to be used. Semantic for a possible set of requirement values used to express such requirements is defined as follows: Ovo ograničenje ukazuje na zahtjeve za provjeru opoziva certifikata. Takva ograničenja mogu odrediti da li je potrebna provjera opoziva ili ne i da li se moraju koristiti OCSP odgovori ili CRL. Semantika za mogući skup zahtijevanih vrijednosti koje se koriste za izražavanje takvih zahtjeva definisana je na sljedeći način: • clrCheck: Checks shall be made against current CRLs (or Authority Revocation Lists); Provjeriće se važeće CRL liste (ili Liste opozvanih certifikata certifikacionih tijela)	eitherCheck

Kriterijum	Vrijednost pri verifikaciji
• ocspCheck: The revocation status shall be checked using OCSP IETF RFC 6960; Status opoziva provjeriće se korišćenjem OCSP IETF RFC 6960; • bothCheck: Both OCSP and CRL checks shall be carried out; Izvršiće se i OSCP I CRL provjere; • eitherCheck: Either OCSP or CRL checks shall be carried out; Izvršiće se bilo OCSP ili CRL provjere; • noCheck: No check is mandated. Nije zahtijevana nijedna provjera.	
(m)2.2. RevocationFreshnessConstraints: This constraint indicates time requirements on revocation information. The constraints may indicate the maximum accepted difference between the issuance date of the revocation status information of a certificate and the time of validation or require the SVA to only accept revocation information issued a certain time after the signature has been created. Ovo ograničenje ukazuje na vremenske zahtijeve u informacijama o opozivu. Ograničenja mogu ukazivati na maksimalnu prihvaćenu razliku između datuma izdavanja informacija o statusu opoziva certifikata i vremena verifikacije ili zahtijevati da SVA prihvati samo informacije o opozivu izdate određeno vrijeme nakon kreiranja potpisa.	None
(m)2.3. RevocationInfoOnExpiredCerts: This constraint mandates the signer's certificate used in validating the signature to be issued by a certification authority that keeps revocation notices for revoked certificates even after they have expired for a period exceeding a given lower bound. Ovo ograničenje nalaže da certifikat potpisnika ili autora elektronskog pečata koji se koristi za verifikaciju potpisa izdaje certifikaciono tijelo koje čuva obavještenja o opozivu opozvanih certifikata čak i nakon što isteknu za period duži od date donje granice.	None
(m)3. LoAOnTSPPractices: This constraint indicates the required LoA on the practices implemented by the TSP(s) having issued	None

Kriterijum	Vrijednost pri verifikaciji
the certificates to be validated during the certificate path validation process, i.e. the certificates present in the certificate path of the signer's certificate, and optionally those present in all or some of the other certificate chain. Ovo ograničenje ukazuje na zahtijevan nivo sigurnosti u praksama koje su primjenjivali davaoci usluga povjerenja koji su izdali certifikate koji će biti potvrđeni tokom procesa verifikacije lanca certifikata, tj. certifikati prisutni u lancu certifikata potpisnika ili autora elektronskog pečata , a opciono i oni prisutni u svim ili nekom drugom lancu certifikata.	
EUQualifiedCertificateRequired	Yes
EUQualifiedCertificateSigRequired	Yes
EUQualifiedCertificateSealRequired	Yes
EUQSCDRequired 1	Yes if using QES validation policy, no if using AdES validation policy Yes ako se koristi QES politika verifikacije, no ako se koristi AdES politika verifikacije

Tabela 3. – X.509 kriterijumi verifikacije

* Biće dostupna od dana pristupanja Crne Gore Evropskoj Uniji shodno Zakonu

** Trust Liste zemalja sa kojima Crna Gora ima sklopljene bilateralne sporazume, koji su implementirani u pogledu interoperabilnosti

Napomena: U slučaju neslaganja objašnjenja na zvaničnom jeziku koji je u upotrebi u Crnoj Gori i engleske verzije, prednost ima engleska verzija

Na osnovu Aneksa C iz ETSI TS 119 172-1 sljedeći kriterijumi ukazuju na zahtjeve za specifične meta podatke certifikata čija se semantička primjena odnosi na kontekst zakonodavstva EU:

- EUQualifiedCertificateRequired: Ovo ograničenje ukazuje da je potrebno da certifikat potpisnika ili autora elektronskog pečata , koji se koristi za verifikaciju potpisa, bude kvalifikovan elektronski certifikat, kako je definisano u važećem zakonodavstvu EU;
- EUQualifiedCertificateSigRequired: Ovo ograničenje ukazuje na to da je potrebno da certifikat potpisnika ili autora elektronskog pečata koji se koristi za provjeru potpisa bude kvalifikovani certifikat za elektronski potpis, kako je definisano u važećem zakonodavstvu EU;
- EUQualifiedCertificateSealRequired: Ovo ograničenje ukazuje da je potrebno da certifikat autora elektronskog pečata, koji se koristi za provjeru elektronskog pečata bude kvalifikovani elektronski certifikat za elektronski pečat, kako je definisano u važećem zakonodavstvu EU;
- EUQSCDRequired: Ovo ograničenje ukazuje da certifikat potpisnika ili autora elektronskog pečata ili autora pečata, koji se koristi za provjeru elektronskog potpisa, mora biti povezan sa privatnim ključem koji se čuva u QSCD uređaju, kao što je definisano u važećem zakonodavstvu EU.

Kriptografska ograničenja

CTrust QSVA usluga povjerenja verifikacije kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata implementira kriptografska ograničenja koja ukazuju na zahtjeve vezane za algoritme i parametre koji se koriste prilikom kreiranja elektronskog potpisa i elektronskog pečata, ili koji se koriste prilikom provjere potpisanog objekta kako je navedeno u ETSI TS 119 172-1, klauzula A.4.2.1, tabela A.2 red p.

Kriterijum	Vrijednost pri verifikaciji
(p)1. CryptographicSuitesConstraints: This constraint indicates requirements on algorithms and parameters used when creating signatures or used when validating signed objects included in the validation or augmenting process (e.g. signature, certificates, CRLs, OCSP responses, time-stamps). Ovo ograničenje ukazuje na zahtjeve u vezi sa algoritmima i parametrima koji se koriste prilikom kreiranja potpisa/pečata ili koji se koriste prilikom verifikacije potpisanih objekata uključenih u procesu verifikacije ili nadogradnje elektronskog potpisa (npr. potpis, certifikati, CRL-ovi, OCSP odgovori, vremenski pečati).	Based on ETSI TS 119 312

Tabela 4. – Kriptografska ograničenja

Napomena: U slučaju neslaganja objašnjenja na zvaničnom jeziku koji je u upotrebi u Crnoj Gori i engleske verzije, prednost ima engleska verzija

Kriterijumi vezani za elemente kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata

CTrust QSVA usluga povjerenja verifikacije kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata podržava kriterijume koji ukazuju na zahtjeve specificirane u ETSI TS 119 172-1 [ETSI, klauzula A.4.2.1, tabela A.2 red b.

Kriterijum	Vrijednost pri verifikaciji
(b)1. ConstraintOnDTBS: This constraint indicates requirements on the type of the data to be signed by the signer. Ovo ograničenje ukazuje na zahtjeve o tipu podataka koje potpisnik ili autor elektronskog pečata potpisuje, odnosno pečatira.	None
(b)2. ContentRelatedConstraintsAsPartOfSignatureElements: This set of constraints indicate the required content related information elements under the form of signed or unsigned qualifying properties that are mandated to be present in the signature. This includes:	None

Kriterijum	Vrijednost pri verifikaciji
Ovaj skup ograničenja ukazuje na zahtijevane informativne elemente u vezi sa sadržajem u obliku potpisanih ili nepotpisanih kvalifikovanih svojstava koja su obavezna da budu prisutna u potpisu. Ovo uključuje: (b)2.1 MandatedSignedQProperties-DataObjectFormat to require a specific format for the content being signed by the signer. zahtijeva određeni format za sadržaj koji potpisnik ili autor elektronskog pečata potpisuje, odnosno pečatira. (b)2.2 MandatedSignedQProperties-content-hints to require specific information that describes the innermost signed content of a multi-layer message where one content is encapsulated in another for the content being signed by the signer. zahtijeva specifične informacije koje opisuju najdublje potpisani sadržaj višeslojne poruke gdje je jedan sadržaj enkapsuliran u drugi za sadržaj koji potpisnik ili autor elektronskog pečata potpisuje, odnosno pečatira. (b)2.3 MandatedSignedQProperties-content-reference to require the incorporation of information on the way to link request and reply messages in an exchange between two parties, or the way such link has to be done, etc. zahtijeva ugradnju informacija o načinu povezivanja zahtjeva za odgovor i odgovora u razmjeni između dvije strane ili o načinu na koji takva veza mora da se ostvari, itd. (b)2.4 MandatedSignedQProperties-content-identifier to require the presence of, and optionally a specific value for, an identifier that can be used later on in the signed qualifying property "content-reference" attribute. zahtijeva prisutnost i, opciono određenu vrijednost za, identifikator koji se kasnije može koristiti u potpisanom atributu kvalifikovanog svojstva "content-reference".	
(b)3. DOTBSAsAWholeOrInParts: This constraint indicates whether the whole data or only certain part(s) of it have to be signed. Semantic for a possible set of requirement values used to express such requirements is defined as follows: • whole: the whole data has to be signed; • parts: only certain part(s) of the data have to be signed. In this case,	None

Kriterijum	Vrijednost pri verifikaciji
additional information should be used to express which parts have to be signed. Ovo ograničenje ukazuje na to da li moraju biti potpisani cjelokupni podaci ili samo određeni njihov dio/djelovi. Semantika za mogući skup zahtijevanih vrijednosti koje se koriste za izražavanje takvih zahtjeva definisana je na sljedeći način: • cjelina: cjelokupni podaci moraju biti potpisani; • djelovi: moraju se potpisati samo određeni djelovi podataka. U ovom slučaju, treba koristiti dodatne informacije da se ukaže koji djelovi moraju biti potpisani.	

Tabela 5. – Kriterijumi vezani za elemente kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata
Napomena: U slučaju neslaganja objašnjenja na zvaničnom jeziku koji je u upotrebi u Crnoj Gori i engleske verzije, prednost ima engleska verzija

3.2. PROTOKOL ZA PROCES VERIFIKACIJE

Komunikacioni kanal između naručioca i sistema za verifikaciju kvalifikovanog elektronskog potpisa, odnosno kvalifikovanog elektronskog pečata prenosi zahtjeve za verifikaciju u jednom smjeru i vraća odgovor, u drugom. CTrust QSVA koristi namjenski protokol za uslugu verifikacije kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata koji se zasniva na zahtjevima standarda ETSI EN 119 442.

CTrust QSVA usluga verifikacije kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata dostupna je preko korisničkog interfejsa (eTrust portal).

3.3. INTERFEJSI

3.3.1. KOMUNIKACIONI KANAL

Komunikacioni kanal između naručioca i sistema za provjeru validnosti kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata obezbijeđen je korišćenjem TLS bezbjednosnog kanala. Sistem za provjeru validnosti garantuje uspostavljanje bezbjednog kanala i očuvanje povjerljivosti i integriteta podataka naručioca.

eTrust portal zahtijeva autentifikaciju od klijenta. Naručilac može pristupiti usluzi verifikacije tek nakon uspješno izvršenog procesa autentifikacije. Na ovaj način se obezbjeđuje da su informacije koje se razmjenjuju dostupne samo konkretnom autentifikovanom naručiocu. Podržana su dva mehanizma bazirana na dvofaktorskoj (korisničko ime/lozinka i OTP) autentifikaciji.

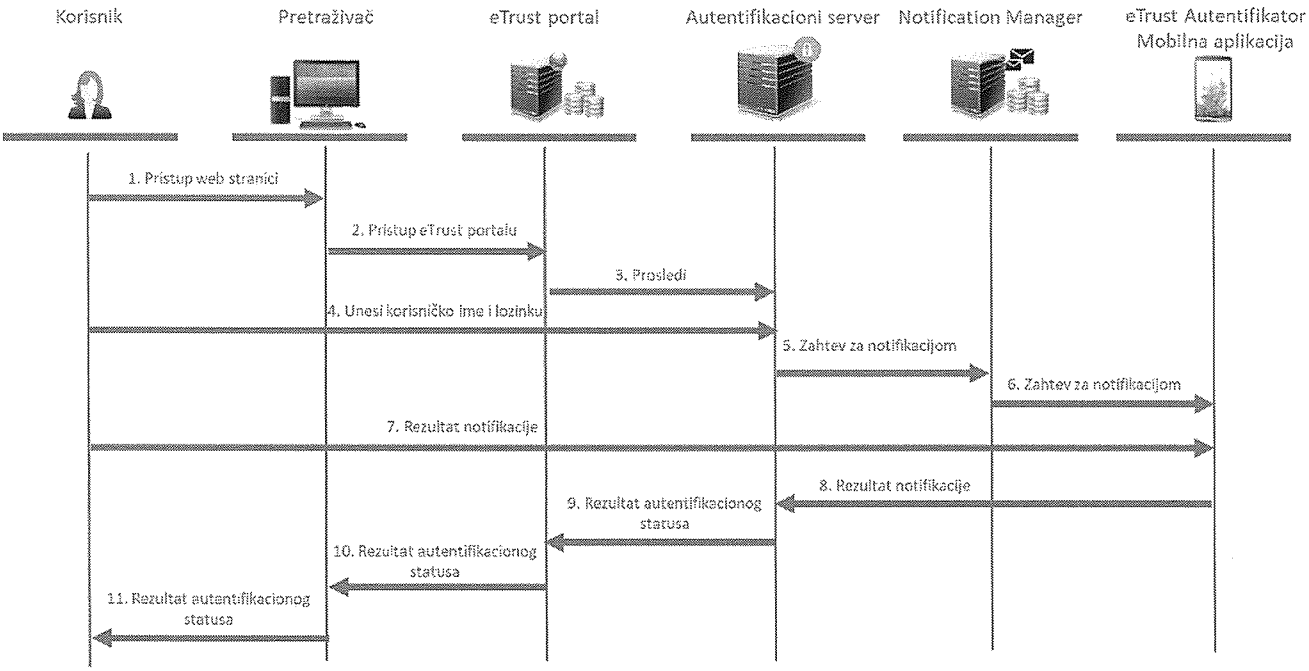
3.3.1.1. DVOFAKTORSKA (KORISNIČKO IME I LOZINKA, OTP) AUTENTIFIKACIJA

Sistem podržava dva tipa dvofaktorske autentifikacije. Oba tipa se baziraju na OTP generatoru i podrazumevaju unos korisničkog imena i lozinke, kao i korišćenje eTrust autentifikator mobilne aplikacije.

Prva opcija je zasnovana na korišćenju mobilne notifikacije, gde korisnik dobija notifikaciju na mobilnoj aplikaciji nakon unošenja korisničkog imena i lozinke na Autentifikacioni server. Korisnik mora da odobri notifikaciju sa telefona kako bi potvrdio akciju logovanja na sistem.

Drugi opcija se zasniva na korišćenju OTP-a (One Time Password), gde korisnik, nakon unosa korisničkog imena i lozinkee, mora da pristupi OTP kodu na svojoj eTrust autentifikator mobilnoj aplikaciji i zatim taj kod unese direktno na web stranicu Autentifikacionog servera.

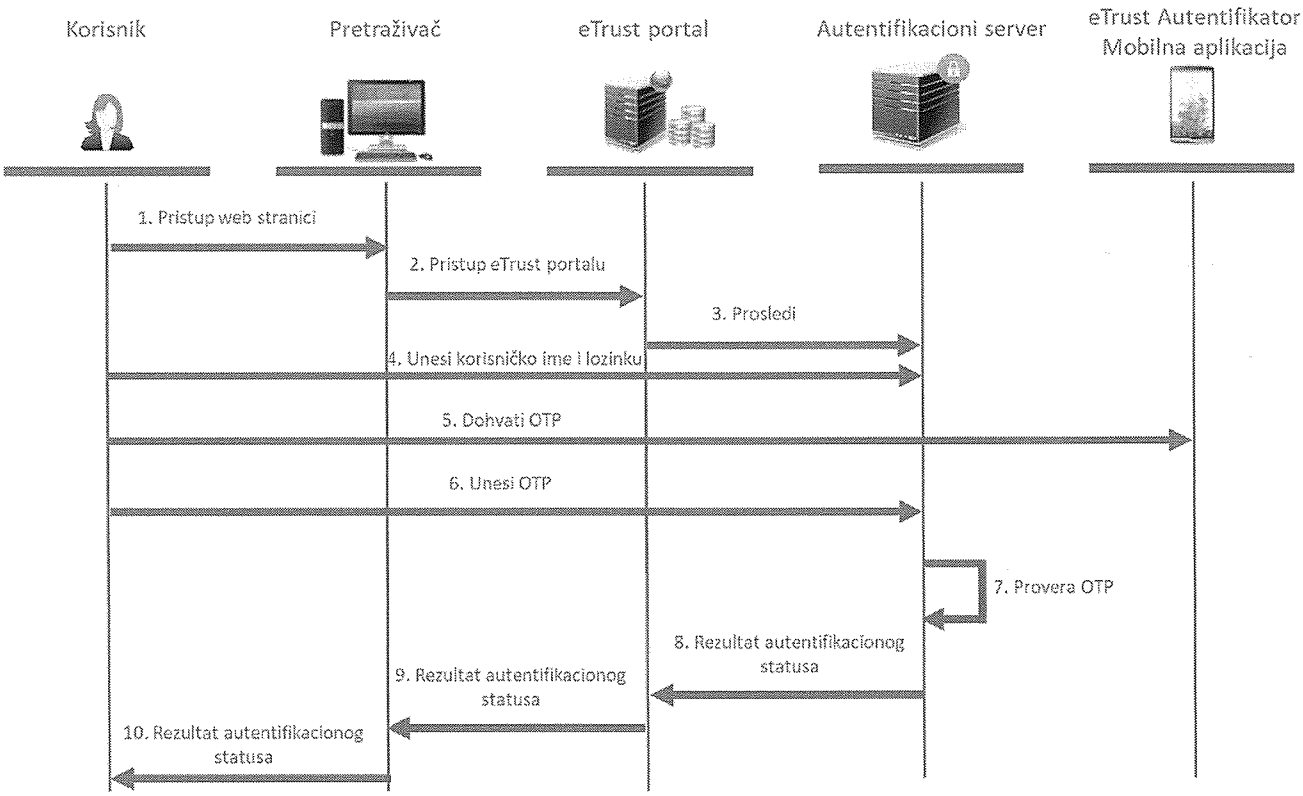
Mobilna notifikacija



Proces autentifikacije putem mobilne notifikacije se može opisati na sledeći način:

1. Korisnik preko pretraživača pristupa eTrust portalu.
2. Ako ne postoji aktivan autentifikacioni token, onda eTrust portal prebacuje korisnika na Autentifikacioni server.
3. Korisnik unosi korisničko ime i lozinku na Autentifikacioni server.
4. Autentifikacioni server šalje zahtev za notifikacijom do Notification Manager.
5. Notification Manager šalje notifikaciju ka eTrust Autentifikator mobilnoj aplikaciji.
6. eTrust Autentifikator mobilna aplikacija prikazuje notifikaciju korisniku koji bira da li da odobri ili odbaci zahtev za logovanjem.
7. eTrust Autentifikator mobilna aplikacija šalje rezultat izbora korisnika do Autentifikacionog servera.
8. Autentifikacioni server šalje status rezultata ka eTrust portalu.
9. eTrust portal šalje status rezultata pretraživaču.
10. Web pretraživač prikaže poruku greške u slučaju da je korisnik odbio akciju na mobilnoj aplikaciji, ili vodi korisnika na željenu web stranu.

One Time Password (OTP)



Proces autentifikacije putem OTP se može opisati na sledeći način:

1. Korisnik preko pretraživača pristupa eTrust portalu.
2. Ako ne postoji aktivan autentifikacioni token, onda eTrust portal prebacuje korisnika na Autentifikacioni server.
3. Korisnik unosi korisničko ime i lozinku na Autentifikacioni server.
4. eTrust portal prikazuje web stranicu na kojoj korisnik može da unese svoj OTP kod. Korisnik treba da pristupi svojoj mobilnoj aplikaciji kako bi našao OTP kod.
5. Korisnik unosi OTP kod na Autentifikacioni server.
6. Autentifikacioni server proverava da li je OTP kod ispravan.
7. Autentifikacioni server šalje status rezultata ka eTrust portalu.
8. eTrust portal šalje status rezultata pretraživaču.
9. Web pretraživač prikaže poruku greške u slučaju da je korisnik uneo pogrešan OTP kod, ili vodi korisnika na željenu web stranu.

3.3.2. ODNOS SA DRUGIM DAVAOCIMA USLUGA POVJERENJA

Na status verifikacije kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata, kao i na izvještaj o verifikaciji mogu da utiču prakse, politike i sporazumi o usaglašenosti sa drugim davaocima usluga povjerenja, koji su van kontrole CTrust sistema. Ostali davaoci usluga povjerenja mogu uključivati: tijela za označavanje tačnog vremena, CRL i OCSP davaoce usluga i druge davaoce usluga povjerenja. CTrust QSVA usluga verifikacije garantuje status verifikacije kvalifikovanog elektronskog potpisa, kvalifikovanog elektronskog pečata i izvještaja o verifikaciji samo u vrijeme stvarne provjere potpisa, odnosno pečata.

Komunikacioni kanali između CTrust QSVA usluge verifikacije i drugih davalaca usluga povjerenja je izvan opsega ovog dokumenta.

3.4. ZAHTJEVI ZA IZVJEŠTAJ O VERIFIKACIJI KVALIFIKOVANOG ELEKTRONSKOG POTPISA I KVALIFIKOVANOG ELEKTRONSKOG PEČATA

CTrust QSVA usluga verifikacije pruža tri vrste izvještaja o verifikaciji:

1. Jednostavan izvještaj o verifikaciji - pruža neophodne informacije u vezi sa identitetom potpisnika ili autora elektronskog pečata i indikacijom statusa verifikovanog kvalifikovanog elektronskog potpisa, odnosno kvalifikovanog elektronskog pečata, uključujući podindikaciju.
2. Detaljan izvještaj o verifikaciji - pruža izvještaj o svakom kriterijumu verifikacije koji se obrađuje, uključujući sve kriterijume verifikacije koji su implicitno primijenjeni.
3. Izvještaj o verifikaciji koji je mašinski čitljiv - pruža detaljan izvještaj o verifikaciji u formatu koji je mašinski čitljiv.

CRNOGORSKI TELEKOM A.D.
1
PODGORICA

Dzina Tsybulskaja
Izvršni direktor