Crna Gora
Ministarstvo javne uprave

Praktična pravila o pružanju kvalifikovane usluge verifikacije kvalifikovanih elektronskih potpisa i kvalifikovanih elektronskih pečata (GovME CA Verify)

Verzija: 1.0

Vlasnik dokumenta:
Ministarstvo javne uprave

Istorijat izmjena

Verzija	Datum	Broj promjena	Opis promjena

Preispitivanje dokumenta

Datum sljedećeg zakazanog preispitivanja	

Distribucija

Naziv		Naslov

Odobrio

Ime	Pozicija	Potpis	Datum

SADRŽAJ

1. UVOD

Ovim dokumentom se definišu praktična pravila pružanja kvalifikovane usluge verifikacije kvalifikovanih elektronskih potpisa i kvalifikovanih elektronskih pečata od strane Ministarstva javne uprave (u daljem tekstu: Ministarstva), kao organa koji u skladu sa Uredbom o organizaciji i načinu rada državne, između ostalog, vrši poslove koji se odnose na oblast elektronskih usluga povjerenja.

Na osnovu Zakona o elektronskoj identifikaciji i elektronskom potpisu („Sl. list CG", br. 31/17 i 72/19), Ministarstvo, pored ostalog, vrši kvalifikovane elektronske usluge povjerenja za organe državne uprave.

Stručni poslovi koji se odnose na pružanje elektronskih usluga povjerenja za organe državne uprave vrše se u okviru Direktorata za infrastrukturu, informacionu bezbjednost, digitalizaciju i e-servise, kao posebne organizacione jedinice u Ministarstvu, koji uspostavlja i organizuje rad sertifikacionog tijela GovME Certification Authority (u daljem tekstu: GovME CA),

Ministarstvo kao kvalifikovani davalac elektronskih usluga povjerenja omogućava stvaranje odnosa povjerenja, koji je neophodan preduslov za razvoj elektronske javne uprave i elektronskog poslovanja.

1.1. PREGLED

Ministarstvo je uspostavilo i upravlja insfrastrukturom javnih ključeva (PKI), tj. sistemom za pružanje kvalifikovanih elektronskih usluga povjerenja. U skladu sa Zakonom o elektronskom potpisu („Službeni list RCG", br. 55/2003, 31/2005), Ministarstvo je 2009. godine upisano u Evidenciju davalaca elektronskih usluga povjerenja za vršenje elektronske usluge povjerenja izrada certifikata za napredni elektronski potpis. Od 2024. godine, Ministarstvo je steklo status kvalifikovanog davaoca elektronskih usluga povjerenja i za organe državne uprave, u skladu sa ovim dokumentom, vrši kvalifikovanu uslugu verifikacije kvalifikovanih elektronskih potpisa i kvalifikovanih elektronskih pečata.

Ovaj dokument opisuje nivo bezbjednosti infrastrukture GovME CA, tehničke karakteristike kao i procedure koje se koriste za pružanje kvalifikovane usluge verifikacije kvalifikovanih elektronskih potpisa i kvalifikovanih elektronskih pečata (u daljem tekstu: usluga verifikacije).

Koristeći ovu elektronsku uslugu povjerenja i pravila opisana u ovom dokumentu, korisnici odnosno zaposleni u organima državne uprave imaće mogućnost da izvrše provjeru validnosti dokumenta u elektronskom obliku, odnosno kvalifikovanog elektronskog potpisa/pečata ili vremenskog pečata koji se na njemu nalazi. To podrazumijeva provjeru:

- integriteta - da nije izvršena nikakva modifikacija potpisanih podataka nakon što su potpisani kvalifikovanim elektronskim potpisom ili pečatom;
- autentičnosti - da je elektronski potpis/pečat podržan kvalifikovanim sertifikatom koji nedvosmisleno identifikuje potpisnika.

Pregled koraka uključenih u proces usluge verifikacije bi bio:

- Provjera integriteta podataka;
- Provjera validnosti sertifikata;
- Verifikacija kvalifikovanog statusa sertifikata;

Provjera da li je elektronski potpis kreiran pomoću kvalifikovanog uredaja za kreiranje elektronskog potpisa.

Konačno, pošto su brojni koraci uključeni u ovaj proces verifikacije, odgovor na zahtjev za verifikaciju može imati oblik izvještaja koji sadrži skup odgovora na različite verifikacije i korake uključene tokom tog procesa.

1.1.1. OSNOVNE DEFINICIJE

U ovom dokumentu pojedini izrazi imaju sljedeće značenje:

POJAM	OPIS
Aktivacija (inicijalizacija) podataka	Aktivacioni kodovi koje izdaje GovME CA i koji se koriste jednom tokom procesa inicijalizacije naručioca, za autentifikaciju naručioca i generisanje njihovih sertifikata.
Arhiva	Specifična baza podataka za čuvanje zapisa za određeni period vremena u cilju bezbjednosti, backup-a ili audit-a.
Autorizacija	Procedura utvrđivanja prava koje neki autentifikovani korisnik ima za korišćenje odgovarajuće aplikacije ili servisa.
Deponovanje ključa	Aranžman u kojem se ključevi potrebni za dešifrovanje šifrovanih podataka čuvaju deponovani od treće strane, tako da ih neko drugi može dobiti za dešifrovanje poruke.
Elektronski pečat	Sertifikat za elektronski pečat je elektronska potvrda koja povezuje podatke za verifikaciju elektronskog pečata sa pravnim licem i potvrđuje naziv tog pravnog lica.
Elektronski potpis	Elektronski potpis je skup podataka u elektronskom obliku koji su pridruženi ili su logički povezani sa elektronskim dokumentom i služe za potpis i elektronsku identifikaciju potpisnika. Elektronski potpis se izrađuje pomoću sredstva za izradu elektronskog potpisa i zasniva se na sertifikatu za izradu elektronskog potpisa.
Elektronski sertifikat	Sertifikat za elektronski potpis je dokument u elektronskom obliku potpisan od davaoca elektronskih usluga povjerenja koji povezuje podatke za provjeru elektronskog potpisa sa nekim licem i potvrđuje identitet tog lica.
Identifikator objekta (OID)	Jedinstveni alfanumerički/numerički identifikator registrovan od strane ISO standarda za registraciju i upućuje na određeni objekat ili klasu objekata

Infrastruktura javnog ključa (PKI)	Struktura hardvera, softvera, ljudi, procesa i politika kako bi se olakšala povezanost javne komponente asimetričnog javnog ključa sa određenim entitetom.
Integritet podataka	Osiguranje da su podaci ostali nepromijenjeni od samog stvaranja.
Korisnik	Zaposleni u organu državne uprave koji koristi i oslanja se na kvalifikovane usluge povjerenja, a za koji je naručiocu odobren zahtjev od strane GovME CA.
Lista opozvanih sertifikata (CRL)	Potpisana lista koja pokazuje skup sertifikata javnih ključeva koje izdavalac sertifikata više ne smatra validnim.
Naručilac	Naručilac je organ državne uprave, odnosno starješina organa koji podnosi zahtjev za pružanje elektronske usluge povjerenje u ime organa državne uprave.
Operativno tijelo Ministarstva javne uprave za pružanje elektronskih usluga povjerenja (GovME CA OA)	Tijelo koje je primarno odgovorno za funkcionisanje kompletne GovME CA infrastrukture.
Par ključeva za enkripciju	Par asimetričnih ključeva sastavljenih od javnog ključa za šifrovanje i odgovarajućegeg privatnog ključa za dešifrovanje. Takođe se naziva i par ključeva povjerljivosti.
Politika sertifikata (CP)	Imenovani skup pravila koji ukazuje na primjenjivost sertifikata na određenu zajednicu i / ili klasu aplikacija sa zajedničkim sigurnosnim zahtjevima
Praktična pravila o postupcima izdavanja sertifikata (CPS)	Praktična pravila o praksama koje sertifikaciono tijelo koristi za izdavanje sertifikata. CPS opisuje opremu, politike i procedure koje su implementirane od strane GovME CA kako bi zadovoljio specifikacije u politikama sertifikata podržane od strane GovME CA.
Protokol za online status sertifikata (OCSP)	Internet protokol koji se koristi za dobijanje statusa X.509 digitalnog sertifikata.
Registraciono tijelo Ministarstva javne uprave (GovMe CA RA)	Tijelo koje je odgovorno za identifikaciju i autentifikaciju naručioca odnosno korisnika prije pružanja elektronskih usluga povjerenja.
Repozitorijum	Lokacija gdje su sačuvani CRLs, ARLs i sertifikati kojima pristupaju krajnji entiteti.
Sertifikaciono tijelo (CA)	Tijelo koje kreira i dodjeljuje sertifikate i kome vjeruje jedan ili više korisnika.
Treća lica (Relying party)	Primaoci sertifikata koji postupaju oslanjajući se na taj sertifikat i/ili elektronske potpise provjerene upotrebom tog sertifikata.
Upravljačko tijelo Ministarstva javne uprave za pružanje elektronskih usluga povjerenja (GovME CA PMA)	Tijelo koje je primarno odgovorno za postavljanje, sprovođenje i upravljanje

	politikama i praksama koje se odnose na rad GovME CA

Skraćenice koje se koriste u ovom dokumentu:

POJAM	OPIS
CA	Certification Authority
PMA	Policy Management Authority
OA	Operations Authority
RA	Registration Authority
CSP	Sertification Service Provider
PKI	Public Key Infrastructure
QSCD	Qualified Signature Creation Device
CRL	Sertificate Revocation List
OCSP	Online Sertificate Status Provider
OID	Object Identifier
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
CN	Common Name
DN	Distinguished Name
HSM	Hardware Security Module

1.2. PRIMJENLJIVOST PRAKTIČNIH PRAVILA

Za izradu i ažuriranje ovog dokumenta odgovorno je Ministarstvo. Tijelo za upravljanje GovME CA PMA ovaj dokument izrađuje, ažurira i dostavlja na odobrenje i potpis ministru.

Promjene sadržaja ovog dokumenta obavljaju se na osnovu internih predloga i zahtjeva za usklađivanjem sa zakonskom regulativom.

1.3. IDENTIFIKACIONI PODACI

GovME CA kontakt informacije:
Adresa: Ministarstvo javne uprave
Rimski trg 45
81000 Podgorica, Crna Gora
Email: ca@mju.gov.me
Internet: https://gov.me/mju/ca

GovME CA RA kontakt informacije:
Adresa: Ministarstvo javne uprave
Rimski trg 45
81000 Podgorica, Crna Gora
Email: ca@mju.gov.me
Internet: https://gov.me/mju/ca

2. UČESNICI

GovME CA za pružanje usluga povjerenja ima uspostavljenu sopstvenu infrastrukturu javnih ključeva.

Učesnici u infrastrukturi javnih ključeva Ministarstva su:

- Sertifikaciona tijela Ministarstva,
- Registraciono tijelo Ministarstva,
- Naručioci i Korisnici,
- Treća lica.

2.1. SERTIFIKACIONA TIJELA (CERTIFICATION AUTHORITIES)

U okviru Ministarstva javne uprave, uspostavljeno je sertifikaciono tijelo GovME CA za pružanje kvalifikovanih elektronskih usluga povjerenja, između ostalih i kvalifikovane usluge verifikacije kvalifikovanih elektronskih potpisa i kvalifikovanih elektronskih pečata za potrebe organa državne uprave.

2.1.1. UPRAVLJAČKO TIJELO MINISTARSTVA JAVNE UPRAVE ZA PRUŽANJE ELEKTRONSKIH USLUGA POVJERENJA I USLUGA ELEKTRONSKE IDENTIFIKACIJE (GovME CA PMA)

GovME CA PMA (Policy Management Authority) je odgovoran za:

- izradu i ažuriranje GovME CA CPS i CP;
- izradu i ažuriranje GovME CA javnih dokumenata;
- podnošenje internih akata (CPS i CP) na usvajanje ministru javne uprave;
- GovME CA registraciju i akreditaciju;
- predlaganje članova OA i RA;
- odobravanje izdavanja sertifikata za korijensko i podređena sertifikaciona tijela, kao i OCSP servise korijenskog i podređenih sertifikacionih tijela;
- pokretanje procedure obnove sertifikata za korijensko i podređena sertifikacionih tijela;
- izradu i održavanje definicija profila sertifikata;
- nadzor i organizovanje revizije usklađenosti pružanja elektronskih usluga povjerenja sa Zakonom, CPS i CP.

Članovi GovME CA PMA obavljaju i druge poslove upravljanja neophodne za funkcionisanje GovME CA.

Članovi Upravljačkog tijela prate rad Tijela za Operativne poslove (GovME CA OA) i Registracionog tijela (GovME CA RA) u cilju utvrđivanja obavljanja poslova u skladu sa Zakonom o elektronskoj identifikaciji i elektronskom potpisu, podzakonskim aktima, Politikom pružanja elektronskih usluga povjerenja kvalifikovanog davaoca elektronskih usluga povjerenja Ministarstva, Praktičnim pravila rada i drugim internim aktima.

2.1.2. TIJELO ZA OPERATIVNE POSLOVE MINISTARSTVA JAVNE UPRAVE ZA PRUŽANJE ELEKTRONSKIH USLUGA POVJERENJA

GovME CA OA (Operations Authority) je odgovorno za:

- instalaciju, konfiguraciju i održavanje IT okruženja sistema za verifikaciju;
- instalaciju, konfiguraciju i održavanje komunikacione mreže;
- funkcionisanje CA u skladu sa propisima i politikama;
- administracija korisničkih naloga za članove GovME CA OA i GovME CA RA tijela;
- administracija naloga za korisnike GovME CA portala za pružanje elektronskih usluga povjerenja (Portal GovME CA);
- izdavanje sertifikata za interne infrastrukturne usluge;
- primanje i distribuciju korisničkih aktivacionih kodova dobijenih od strane GovME CA i pomoć pri aktivaciji u vremenskom periodu predviđenom za to;
- upotrebu Trust liste Crne Gore u funkcionisanju usluge verifikacije odnosno njenog softvera.

2.2. TIJELO ZA UPRAVLJANJE REGISTRACIJOM KORISNIKA

GovME CA posjeduje jedno Registraciono tijelo (GovME CA RA), odgovorno za:

- prihvatanje ili odbijanje zahtjeva za pružanje usluge verifikacije;
- komunikaciju sa naručiocima i korisnicima po osnovu podnijetih zahtjeva za pružanje usluge verifikacije;
- provjeru podataka u zahtjevu za pružanje usluge verifikacije;
- identifikaciju korisnika „licem u lice";
- upoznavanje korisnika sa politikama i praktičnim pravilima rada GovME CA;
- administraciju Portala za rad Registracionog tijela (u daljem tekstu: RA portal);
- komunikaciju sa GovME CA OA tijelom;
- izvještavanje o radu prema GovME CA PMA;
- edukaciju korisnika za korišćenje GovME CA portala.

Za usluge koje su na GovME CA portalu za pružanje elektoronskih usluga povjerenja, GovME CA RA odobrava zahtjev odmah nakon okončane procedure identifikacije i provjere podataka, a njihovu aktivaciju vrši korisnik samostalno na svom računaru.

Na GovME CA portalu korisnik ima mogućnost da:

- elektronski potpisuje dokumenta koristeći kvalifikovanu elektronsku uslugu povjerenja „izrada kvalifikovanog sertifikata za elektronski potpis" (tzv. udaljeni kvalifikovani elektronski potpis);
- izvrši verifikaciju elektronskog potpisa/pečata/vremenskog pečata na dokumentu, koristeći kvalifikovanu elektronsku uslugu povjerenja „kvalifikovana usluga verifikacije kvalifikovanih elektronskih potpisa i kvalifikovanih elektronskih pečata";
- pošalje elektronski dokument koristeći kvalifikovanu elektronsku uslugu povjerenja „kvalifikovana elektronska preporučena dostava".

Uzimajući u obzir značaj pomenutih usluga povjerenja, za potrebe procesa rada, odlučeno je da se odobrenjem zahtjeva za izradu kvalifikovanog sertifikata za elektronski potpis, korisniku u isto vrijeme omogući da na GovME CA portalu koristi i kvalifikovanu uslugu verifikacije kvalifikovanih elektronskih

potpisa i kvalifikovanih elektronskih pečata, kao i kvalifikovanu uslugu elektronske preporučene dostave.

2.3. NARUČIOCI I KORISNICI (END USERS AND SUBSCRIBERS)

Naručilac je organ državne uprave, odnosno starješina organa koji podnosi zahtjev za pružanje elektronske usluge povjerenja u ime organa državne uprave, u ovom slučaju usluge verifikacije.

Korisnik je zaposleni u organu državne uprave koji upotrebljava elektronsku uslugu povjerenja za koju je naručiocu odobren zahtjev od strane GovME CA.

Naručilac snosi krajnju odgovornost za korišćenje ove elektronske usluge povjerenja

Korisnik mora biti upoznat sa Politikom pružanja kvalifikovanih elektronskih usluga povjerenja, kao i ovim dokumentom.

2.4. TREĆA LICA

Nije primjenjivo.

3. PROCES I KOMPONENTE USLUGE ZA VERIFIKACIJU

3.1. ULOGE U PRUŽANJU USLUGE VERIFIKACIJE

Komponente sistema za pružanje Usluge verifikacije imaju sljedeće uloge:

- GovME CA Portal - softverska komponenta koja obezbjeđuje korisnički interfejs (Signature Validation Client – SVC) i kao upravljačka aplikacija koja koristi aplikaciju za verifikaciju i naručiocu obezbjeđuje funkcionalnost verifikacije (Driving Application - DA),
- Protokol za verifikaciju - predstavlja bezbjedan komunikacioni kanal za razmjenu informacija naručioca i servera za verifikaciju (Signature Validation Service Protocol - SVSP),
- Verifikacioni server - je komponenta koja implementira protokol verifikacije na strani davaoca usluge verifikacije (Signature Validation Service Server - SVSServ).
- GovME CA Verify Back-end predstavlja softversku komponentu koja je odgovorna za verifikaciju potpisa/pečata, implementira verifikacioni algoritam i kreira izvještaj o verifikaciji (Signature Validation Application – SVA)
- Eksterni učesnici – Sertifikaciona tijela, tijela za izradu vremenskih pečata, zvanična Trust lista Crne Gore.

3.2. ZAHTJEVI ZA VERIFIKACIJU

GovME CA, u procesu pružanja usluge verifikacije, obavlja provjeru i utvrđivanje tehničke ispravnosti kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata koji je u skladu sa tehničkim zahtjevima propisanim u ETSI TS 119 102-1.

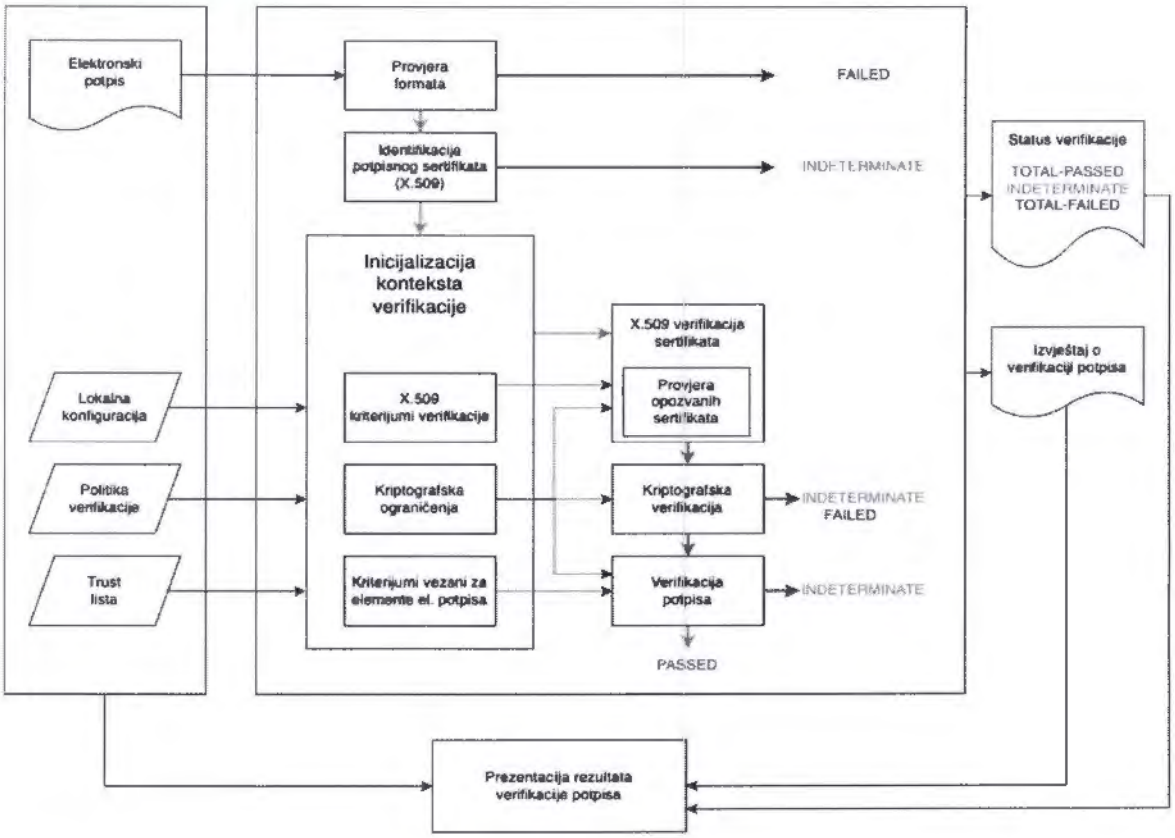
Članom 23 Zakona o elektronskoj identifikaciji i elektronskom potpisu, propisano je da se validnost kvalifikovanog elektronskog potpisa/pečata potvrđuje verifikacijom kvalifikovanog elektronskog potpisa/pečata koja obuhvata utvrđivanje da:

- je sertifikat na kojem se zasniva elektronski potpis u trenutku potpisivanja bio kvalifikovani certifikat za elektronski potpis izdat u skladu sa navedenim Zakonom;
- je kvalifikovani sertifikat za elektronski potpis izdao kvalifikovani davalac usluge sertifikovanja za elektronske transakcije i da je validan u trenutku potpisivanja;
- podaci za verifikaciju potpisa odgovaraju podacima koji se daju korisniku;
- je jedinstveni skup podataka koji predstavljaju potpisnika u kvalifikovanom certifikatu za elektronski potpis ispravno dostavljen korisniku;
- je korišćenje pseudonima, ako je pseudonim korišćen u trenutku potpisivanja, naznačeno korisniku; je kvalifikovani elektronski potpis izrađen kvalifikovanim sredstvom za izradu elektronskog potpisa;
- nije ugrožen integritet potpisanih podataka;
- su zahtjevi iz člana 10 Zakona o elektronskoj identifikaciji i elektronskom potpisu ispunjeni u trenutku izrade potpisa.

Verifikacija kvalifikovanog elektronskog potpisa sprovodi se na način koji korisniku obezbjeđuje tačan rezultat verifikacije. Rezultati postupka verifikacije potpisuju se naprednim elektronskim pečatom davaoca usluge verifikacije.

3.3. MODEL PROVJERE VALIDNOSTI KVALIFIKOVANOG ELEKTRONSKOG POTPISA I PEČATA

Na Slici 1 je prikazan model provjere validnosti kvalifikovanog elektronskog potpisa i pečata:



Slika 1 - Model provjere validnosti elektronskog potpisa/pečata

Konceptualni model prikazuje da se tokom verifikacionog procesa provjeravaju:

- format elektronskog potpisa/pečata,
- sertifikat potpisnika,
- X.509 kriterijumi za verifikaciju sertifikata,
- kriptografski kriterijumi
- kriterijumi vezani za elemente potpisa/pečata.

Na osnovu provjere navedenih kriterijuma aplikacija za verifikaciju prikazuje rezultat verifikacije i izdaje izvještaj o verifikaciji. GovME CA usluga verifikacije kvalifikovanog elektronskog potpisa ili pečata istovremeno prihvata samo jednu datoteku za provjeru validnosti, koja sadrži elektronske potpise/pečate i datoteke sa potpisanim sadržajem u sebi.

3.4. STATUS VERIFIKACIJE I IZVJEŠTAJ O VERIFIKACIJI

Usluga verifikacije izdaje sveobuhvatni izvještaj o provjeri validnosti kvalifikovanog elektronskog potpisa/pečata na elektronskom dokumentu. Aplikacija za verifikaciju, na osnovu kriterijuma validacije, detaljno provjerava elektronski potpis/pečat i preko upravljačke aplikacije prezentuje izvještaj o verifikaciji, koji može biti u formi čitljive HTML stranice ili PDF dokumenta. Izlazni izvještaj procesa provjere validnosti potpisa/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);
- identifikaciona oznaka politike koju je potpis potvrdio;

Status provjere validnosti kvalifikovanog elektronskog potpisa/pečata može imati jednu od tri vrijednosti:

- USPJEŠNO (TOTAL – PASSED) - znači da su sve kriptografske provjere potpisa, odnosno pečata, kao i sve druge provjere u skladu sa propisanim politikama i pravilima za verifikaciju.

- NEODREĐENO (INDETERMINATE) - znači da nisu 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.

- NEUSPJEŠNO (TOTAL – FAILED) - znači da nisu ispunjeni uslovi ni za status verifikacije uspješno, ni za status verifikacije neodredeno.

U tabeli 1 je prikazana struktura i semantika osnovnih statusa verifikacije:

Indikator statusa	Semantika	Podaci izvještaja o provjeri validnosti
USPJEŠNO (TOTAL-PASSED)	Verifikacioni proces 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 pozitivno su potvrdeni; potpis/pečat je pozitivno potvrđen u odnosu na kriterijume verifikacije.	Izlaz iz procesa verifikacije je sertifikat za potpisivanje korišćen u procesu, zajedno sa specifičnim potpisanim atributima, ukoliko su prisutni i razmatranim dokazima verifikacije.
NEUSPJEŠNO (TOTAL-FAILED)	Verifikacioni proces rezultira statusom TOTAL-FAILED ukoliko su kriptografske provjere potpisa/pečata neuspješne ili može biti dokazano da je generisanje potpisa/pečata nastalo nakon opoziva sertifikata potpisnika ili pečatioca.	Izlaz iz verifikacionog procesa su dodatne informacije koje objašnjavaju status TOTAL-FAILED za svaki verifikacioni kriterijum za koji je rezultat provjere negativan.
NEODREĐENO (INDETERMINATE)	Dostupne informacije nisu dovoljne da bi provjera validnosti potpisa bila u statusu TOTAL- PASSED ili TOTAL-FAILED.	Izlaz iz verifikacionog procesa su dodatne informacije koje objašnjavaju status INDETERMINATE i od pomoći su korisniku da identifikuje nedostajuće podatke neophodne da bi se verifikacija izvršila uspješno.

Tabela 1 – Struktura i semantika osnovnih statusa verifikacije

U tabeli 2 su pored osnovnih statusa, prikazani izveštaj o verifikaciji uključuje i sekundarnu indikaciju sa semantikom

Osnovna indikacija	Podindikacija	Povezani podaci u verifikacionom izvještaju	Semantika
TOTAL_FAILED	FORMAT_FAILURE	The validation process shall provide any information available why parsing of the signature failed. **Prevod:** Proces validacije će obezbijediti sve dostupne informacije zašto raščlanjivanje potpisa nije uspjelo.	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. **Prevod:** Potpis nije u skladu sa jednim od osnovnih standarda u kriptografske verifikacije, stoga ga nije moguće obraditi.
	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. **Prevod:** Proces validacije će obezbediti: identifikator(e) (npr. URI ili OID) koji jedinstveno identifikuje elemente unutar potpisanog skupa podataka (kao što su atributi potpisa ili SD) koji su izazvali grešku.	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. **Prevod:** Proces verifikacije potpisa rezultira u TOTAL- FAILED jer se najmanje jedan heš potpisanog(ih) objekta(a) podataka koji je uključen u proces potpisivanja ne podudara sa odgovarajućom heš vrijednošću u potpisu.
	SIG_CRYPTO_ FAILURE	The validation process shall output: The signing certificate used in the validation process. **Prevod:** Proces validacije će prikazati: Potpisni sertifikat koji se koristi u procesu validacije.	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.

			Prevod: Proces provjere valjanosti potpisa rezultira u TOTAL-FAILED jer potpis nije mogao biti verifikovan korišćenjem javnog ključa potpisnika u sertifikatu za potpisivanje.
	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. **Prevod:** Proces validacije će prikazati sljedeće: Lanac sertifikata koji se koristi u procesu validacije. Vreme i, ako postoji, razlog opoziva sertifikata za potpisivanje.	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. **Prevod:** Proces verifikacije potpisa rezultira u TOTAL- FAILED jer je sertifikat za potpisivanje opozvan; i postoji dokaz da je potpisivanje odrađeno nakon vremena opoziva.
	EXPIRED	The process shall output: The validated certificate chain **Prevod:** Proces će dati: verifikocaioni lanac sertifikata	The signature validation process results into TOTAL- FAILED because there is proof that the signature has been created after the expiration date of the signing certificate **Prevod:** Proces provjere valjanosti potpisa rezultira u TOTAL-FAILED jer postoji dokaz da je potpis kreiran nakon datuma isteka certifikata za potpisivanje.
	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. **Prevod:** Proces verifikacije potpisa rezultira u TOTAL- FAILED jer postoji dokaz da je potpis kreiran prije datuma izdavanja sertifikata za potpisivanje.
INDETERMINATE	SIG_CONSTRAINTS_ FAILURE	The validation process shall provide: The set of constraints that have not been met by the signature. **Prevod:** Proces validacije će obezbediti: Skup uslova koje potpis nije ispunio.	The signature validation process results into INDETERMINATE because one or more attributes of the signature do not match the validation constraints. **Prevod:** Proces verifikacije potpisa rezultira u INDETERMINATE jer jedan ili više atributa potpisa ne odgovaraju ograničenjima verifikacije.
	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. **Prevod:** Proces validacije će dati: Lanac sertifikata koji se koristi u procesu validacije. Skup uslova 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. **Prevod:** Proces verifikacije potpisa rezultira u INDETERMINATE jer lanac sertifikata koji se koristi u procesu verifikacije ne odgovara uslovima verifikacije koji se odnose na sertifikat.
	CERTIFICATE_CHAIN_ GENERAL_FAILURE	The process shall output: Additional information regarding the reason **Prevod:** Dodatne informacije o razlogu	The signature validation process results into INDETERMINATE because the set of certificates available for chain validation produced an error for an unspecified reason.

			Prevod: Proces verifikacije potpisa rezultira u INDETERMINATE jer je skup sertifikata dostupnih za lančanu verifikaciju proizveo grešku iz neodređenog razloga.
	CRYPTO_CONSTRAINTS_FAILURE	The process shall output: Identification of the materia (signature, certificate) that is 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 considered secure. **Prevod:** Identifikacija objekta (potpisa, sertifikata) koji se proizvodi korišćenjem algoritma ili veličine ključa je ispod potrebnog nivoa kriptografske bezbednosti. Ako je poznato, prikazaće se vrijeme do kojeg su se algoritam ili veličina ključa smatrali sigurnim.	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 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). **Prevod:** Proces verifikacije potpisa rezultira u INDETERMINATE jer je bar jedan od algoritama koji su korišćeni u objektu (npr. potpis, sertifikat...) uključen u verifikaciju potpisa, ili veličina ključa koji se koristi sa takvim algoritmom, ispod zahtijevanog nivoa kriptografske bezbjednosti, i:

			ovaj materijal je proizveden nakon vremena do kojeg se ovaj algoritam/ključ smatrao sigurnim (ako je takvo vrijeme poznato); i materijal nije zaštićen dovoljno jakim vremenskim žigom primijenjenim prije vremena do kojeg se algoritam/ključ smatrao sigurnim (ako je takvo vrijeme poznato).
	POLICY_PROCESSING_ ERROR	The validation process shall provide additional information on the problem. **Prevod:** Proces verifikacije će prikazati dodatne informacije o problemu.	The signature validation process results into INDETERMINATE because a given formal policy file could not be processed for any reason (e.g. not accessible, not parse- able, digest mismatch, etc.). **Prevod:** Proces verifikacije potpisa rezultira u INDETERMINATE jer data formalna datoteka politike nije mogla biti obrađena iz bilo kog razloga (npr. nije dostupna, nije raščlanjiva, 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. **Prevod:** Proces verifikacije potpisa rezultira u 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	The signature validation process results into INDETERMINATE

		respect the ordering constraints. **Prevod:** Proces validacije će dati listu vremenskih oznaka koje ne ispunjavaju uslove.	because some constraints on the order of signature time-stamps and/or signed data object(s) time-stamps are not respected. **Prevod:** Proces verifikacije potpisa rezultira u INDETERMINATE jer se ne poštuju neka ograničenja u pogledu redosljeda vremenskih oznaka potpisa i/ili potpisanih objekata podataka.
	NO_SIGNING_ CERTIFICATE_FOUND		The signature validation process results into INDETERMINATE because the signing certificate cannot be identified. **Prevod:** Proces verifikacije potpisa rezultira u INDETERMINATE jer se sertifikat za potpisivanje 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. **Prevod:** Proces verifikacije potpisa rezultira u INDETERMINATE jer nije pronađen lanac sertifikata za identifikovani sertifikat za potpisivanje.
	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.	The signature validation process results into INDETERMINATE because the signing certificate was revoked at the validation date/time. However, the Signature Validation Algorithm

		Prevod: Proces verifikacije će obezbijediti sljedeće: Niz sertifikata koji se koristi u procesu verifikacije. Vrijeme i razlog opoziva sertifikata za potpisivanje.	cannot ascertain that the signing time lies before or after the revocation time. **Prevod:** Proces verifikacije potpisa rezultira u INDETERMINATE jer je sertifikat za potpisivanje opozvan na datum/vrijeme validacije. Međutim, algoritam za verifikaciju potpisa ne može da utvrdi da li je vrijeme potpisivanja prije ili posle vremena opoziva.
	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. **Prevod:** Proces verifikacije će obezbijediti sljedeće: Niz sertifikata koji uključuje opozvani CA sertifikat. Vrijeme i razlog opoziva sertifikata.	The signature validation process results into INDETERMINATE because at least one certificate chain was found but an intermediate CA certificate is revoked. **Prevod:** Proces verifikacije potpisa rezultira u INDETERMINATE jer je pronađen najmanje jedan niz sertifikata ali je posredni CA sertifikat opozvan.
	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. **Prevod:** Proces verifikacije potpisa rezultira u INDETERMINATE

			jer je sertifikat za potpisivanje istekao ili još uvek nije važeći na datum/vrijeme verifikacije i algoritam za provjeru valjanosti potpisa ne može da utvrdi da je vrijeme potpisivanja u intervalu važenja sertifikata za potpisivanje. Poznato je da sertifikat 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. **Prevod:** Proces verifikacije potpisa rezultira u INDETERMINATE jer je sertifikat za potpisivanje istekao ili još nije važeći na datum/vrijeme verifikacije i algoritam za provjeru valjanosti potpisa ne može da utvrdi da je vrijeme potpisivanja u intervalu važenja sertifikata za potpisivanje.
	CRYPTO_CONSTRAINTS_ FAILURE_NO_POE	The process shall output: Identification of the material (signature, certificate) that is 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.	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 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

		Prevod: Proces će prikazati: Identifikacija objekta (potpis, sertifikat) je proizveden korišćenjem algoritma ili veličine ključa koji je ispod potrebnog nivoa kriptografske bezbjednosti. Ako je poznato, vrijeme do kojeg su se algoritam ili veličina ključa smatrali sigurnim.	is no proof that this material was produced before the time up to which this algorithm/key was considered secure. **Prevod:** Proces validacije potpisa rezultira u INDETERMINATE jer bar jedan od algoritama koji su korišćeni u objektima (npr. vrednost potpisa, sertifikat, itd.) uključenim u verifikaciju potpisa, ili veličina ključa koji se koristi sa takvim algoritmom, je ispod je potrebnog nivoa kriptografske bezbjednosti, i nema dokaza da je ovaj objekat proizveden prije vremena do kojeg 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. **Prevod:** Proces validacije će identifikovati najmanje potpisane objekte za koje nedostaju POE. Proces validacije treba da pruži dodatne informacije o problemu.	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). **Prevod:** Proces verifikacije potpisa rezultira u INDETERMINATE jer nedostaje dokaz postojanja da bi se utvrdilo da je potpisani objekat nastao prije nekog kompromitujućeg događaja (npr. pokvareni algoritam)
	TRY_LATER	The validation process shall output the point of time, where the necessary revocation information is expected to become available.	The signature validation process results into INDETERMINATE because not all constraints can be fulfilled using available

		Prevod: Proces validacije će dati trenutak kada se očekuje da će potrebne informacije o opozivu postati dostupne.	information. However, it may be possible to do so using additional revocation information that will be available at a later point of time. **Prevod:** Proces verifikacije potpisa rezultira u INDETERMINATE jer se ne mogu svi uslovi ispuniti korišćenjem dostupnih informacija. Međutim, to je moguće učiniti pomoću dodatnih informacije 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. **Prevod:** Proces treba da prikaže kada bude dostupno: Identifikator(e) (npr. URI) potpisanih podataka koji su uzrokovali grešku.	The signature validation process results into INDETERMINATE because signed data cannot be obtained. **Prevod:** Proces verifikacije potpisa rezultira u INDETERMINATE jer se ne mogu dobiti potpisani podaci.

Tabela 2 – Sekundarne indikacije procesa verifikacije

3.5. PROCES VERIFIKACIJE

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

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

Usluga verifikacije sprovodi postupak verifikacije za sve elektronske potpise/pečate, nezavisno od njihovog nivoa. Ukoliko je provjera odabranim postupkom verifikacije vratila indikaciju PASSED, usluga dodjeljuje statusu verifikacije vrijednost TOTAL-PASSED. Ukoliko je provjera odabranim

postupkom verifikacije vratila indikaciju NOT PASSED, usluga dodjeljuje statusu verifikacije vrijednost TOTAL-FAILED.

U suprotnom, usluga dodjeljuje statusu verifikacije vrijednost INDETERMINATE.

Provjera verifikacije kvalifikovanih elektronskih potpisa/pečata na portalu GovME CA sastoji se od sljedećih koraka:

1. Korisnik se prijavljuje na GovME CA portal upotrebom korisničkog imena i lozinke;
2. Korisnik bira dokument čiji će elektronski potpis/pečat biti verifikovan. Dokument dobija hash vrijednost, koja se prosljeđuje aplikaciji za verifikaciju (SVA);
3. SVA verifikuje kriptografsku strukturu primljenog materijala i lanac sertifikata potpisnika;
4. SVA šalje serijski broj sertifikata potpisnika OCSP servisu, kako bi provjerila njegov status;
5. OCSP komponenta vraća rezultat provjere koji može biti: Good, Unknown i Revoked;
6. SVA učitava CRL;
7. SVA koristi serijski broj sertifikata da bi u listi povučenih sertifikata provjerila da li je sertifikat potpisnika opozvan;
8. SVA provjerava u Trust listi da li se Root sertifikatu koji je potpisao sertifikat korisnika može vjerovati;
9. SVA određuje da li je Root sertifikat od povjerenja;
10. SVA konstruiše izvještaj o verifikaciji i vraća rezultat verifikacije;
11. GovME CA portal prezentuje klijentu rezultat verifikacije i izvještaj o verifikaciji.

3.5.1. POLITIKA VERIFIKACIJE - KRITERIJUMI ZA VERIFIKACIJU

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

Jedna usluga verifikacije ne prihvata više izvora verifikacione politike.

Strategija definisana u politici verifikacije slijedi sljedeće principe:

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

Kriterijumi na osnovu kojih GovME CA usluga verifikacije vrši provjeru validnosti kvalifikovanih potpisa/pečata definisani su u kontrolnim podacima specifičnim za sistem, 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 korisnika.

3.5.2. OPŠTI KRITERIJUMI

GovME CA usluga provjere validnosti kvalifikovanog elektronskog potpisa/pečata podržava maksimalnu veličinu datoteke dokumenata od 100 MB.

3.5.3. X.509 KRITERIJUMI

GovME CA usluga provjerenja validosti kvalifikovanog elektronskog potpisa/pečata implementira X.509 kriterijume verifikacije, koji ukazuju na zahtjeve provjere lanca sertifikata, 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-Stamping Units). Semantic for a possible set of requirement values used to express such requirements is defined as follows: m)1.1. SetOfTrustAnchors: This constraint indicates a set of acceptable trust anchors (TAs) as a constraint for the validation process. **Prevod:** m)1. X509CertificateValidationConstraints: Ovaj skup ograničenja ukazuje na zahteve u procesu verifikacije putanje sertifikata kao što je definisano u IETF RFC 5280. Ova ograničenja mogu biti različita za različite tipove sertifikata (npr. sertifikate izdate potpisnicima, sertifikacionim tijelima, sertifiaktima za CRL i OCSP, vremenskim pečatima). Semantika za mogući skup vrijednosti koji se koristi za izražavanje takvih zahtjeva je definisana na sledeći način: m)1.1. SetOfTrustAnchors: Ovo ograničenje označava skup prihvatljivih izdavačkih sertifikata kao ograničenje za proces validacije.	Trust lista Crne Gore
(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. • (m)1.3. user-initial-policy-set: This constraint is as described in IETF RFC 5280 clause 6.1.1 item (c) • (m)1.4. initial-policy-mapping-inhibit: This	None

constraint is as described in IETF RFC 5280 clause 6.1.1 item (e) • (m)1.5. initial-explicit-policy: This constraint is as described in IETF RFC 5280 clause 6.1.1 item (f) • (m)1.6. initial-any-policy-inhibit: This constraint is as described in IETF RFC 5280 clause 6.1.1 item (g) • (m)1.7. initial-permitted-subtrees: This constraint is as described in IETF RFC 5280 clause 6.1.1 item (h) • (m)1.8. initial-excluded-subtrees: This constraint is as described in IETF RFC 5280 clause 6.1.1 item (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) • (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). **Prevod:** (m)1.2. CertificationPath: Ovo ograničenje označava put sertifikacije koji treba da bude koristi SVA za verifikaciju potpisa. Putanja sertifikata je dužine 'n' od izdavačkog sertifikata do sertifikata koji je predmet verifikacije potpisanog objekta (npr. sertifikat potpisnika ili sertifikat sa vremenskim pečatom). Ovo ograničenje može uključiti putanju koju treba uzeti u obzir ili ukazati na potrebu za razmatranjem putanje date u potpisu ako postoji. • (m)1.3. user-initial-polici-set: Ovo ograničenje je kao što je opisano u IETF RFC 5280 klauzula 6.1.1 tačka (c) • (m)1.4. initial-policy-mapping-inhibit: Ovo ograničenje je kao što je opisano u IETF RFC 5280 klauzula 6.1.1 tačka (e) • (m)1.5. initial-explicit-policy: Ovo ograničenje je kao što je opisano u IETF RFC 5280 klauzula 6.1.1 tačka (f) • (m)1.6. initial-any-policy-inhibit: Ovo ograničenje je kao što je opisano u IETF RFC 5280 klauzula 6.1.1 tačka (g)	

• (m)1.7. initial-permitted-subtrees: Ovo ograničenje je kao što je opisano u IETF RFC 5280 klauzula 6.1.1 tačka (h) • (m)1.8. initial-excluded-subtrees: Ovo ograničenje je kao što je opisano u IETF RFC 5280 klauzula 6.1.1 tačka (i) • (m)1.9. path-length-constraints: Ovo ograničenje ukazuje na ograničenje broja sertifikata u putanji. Za ovo ograničenje se moraju definisati početne vrijednosti ili će se drugačije obrađivati takvo ograničenje (npr. ignorisaće se) • (m)1.10. Policy-constraints: Ovo ograničenje ukazuje na zahtjeve vezane za politike sertifikata na koje se upućuje u sertifikatima. Za ovo ograničenje se moraju definisati početne vrijednosti ili će se drugačije obrađivati takvo ograničenje (npr. ignorisaće se). Ovo takođe omogućava da se zahtijevaju (mogući skup) specifične vrijednosti politike u sertifikatima krajnjeg entiteta (bez zahtjeva da se takve vrednosti pojavljuju u sertifikatima izdavaoca na nizu sertifikata).	
(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: (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: • clrCheck: Checks shall be made against current CRLs; • ocspCheck: The revocation status shall be checked using OCSP IETF RFC 6960; • bothCheck: Both OCSP and CRL checks shall be carried out; • eitherCheck: Either OCSP or CRL checks shall be carried out; • noCheck: No check is mandated. **Prevod:** (m)2. RevocationConstraints: Ovaj skup ograničenja ukazuje na zahtjeve koji se primenjuju kada se provjerava status validnosti sertifikata tokom procesa	eitherCheck

verifikacije putanje sertifikata. Ova ograničenja mogu biti različita za različite tipove sertifikata (npr. sertifikate izdate potpisnicima, sertifikacionim tijelima, sertifiaktima za CRL i OCSP, vremenskim pečatima). Semantika za mogući skup vrijednosti koji se koristi za izražavanje takvih zahtjeva je definisan na sledeći način: (m)2.1. RevocationCheckingConstraints: Ovo ograničenje ukazuje na zahtjeve za proveru opoziva sertifikata. Takva ograničenja mogu specificirati da li je provera opoziva potrebna ili ne i da li se moraju koristiti OCSP odgovori ili CRL-ovi. Semantika za mogući skup vrijednosti koje se koriste za provjeru takvih zahtjeva je definisana na sledeći način: • clrCheck: Provjerva se trenutna CRL; • ocspCheck: Status opoziva će biti proveren korišćenjem OCSP IETF RFC 6960; • bothCheck: I OCSP i CRL provjere će biti sprovedene; • AniCheck: OCSP ili CRL provjere će biti sprovedene; • noCheck: Provjera nije obavezna.	
(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. **Prevod:** m)2.2. RevocationFreshnessConstraints: Ovo ograničenje ukazuje na vremenske zahtjeve za informacije o opozivu. Ograničenja mogu ukazivati na maksimalnu prihvaćenu razliku između datuma izdavanja informacija o statusu opoziva sertifikata i vremena verifikacije ili zahtijevati od SVA da prihvati samo informacije o opozivu izdate za 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.	None

Prevod: (m)2.3. RevocationInfoOnEkpiredCerts: Ovo ograničenje nalaže da sertifikat potpisnika koji se koristi u verifikaciji potpisa izdaje autoritet za izdavanje sertifikata koji čuva obavještenja o opozivu za opozvane sertifikate čak i nakon što su istekli u periodu koji prelazi datu donju granicu.	
(m)3. LoAOnTSPPractices: This constraint indicates the required LoA (Level of Acceptance) on the practices implemented by the TSP(s) having issued the certificates to be validated during the certificate path validation process. **Prevod:** (m)3. LoAOnTSPPractices: Ovo ograničenje ukazuje na potrebnu LoA (nivo prihvatanja/pouzdavanja) na prakse koje implementiraju TSP(i) (kvalifikovani pru\aoci usluga povjerenja) koji su izdali sertifikate koji će biti verifikovani tokom procesa verifikacije niza sertifikata.	None
EUQualifiedCertificateRequired	Yes
EUQualifiedCertificateSigRequired	Yes
EUQualifiedCertificateSealRequired	Yes
EUQSCDRequired 1	Yes if using QES validation policy, no if using AdES validation policy Prevod: Yes ukoliko se koristi QES politika verifikacije, No ako se koristi AdES politika verifikacije

Tabela 3 – Kriterijumi verifikacije X.509

Sljedeći kriterijumi, na osnovu Aneksa C iz ETSI 119 172-1, ukazuju na zahtjeve za specifične meta podatke sertifikata čija se semantička primjena odnosi na kontekst zakonodavstva EU:

- EUQualifiedCertificateRequired: Ovo ograničenje ukazuje da je potrebno da sertifikat potpisnika, koji se koristi za verifikaciju potpisa, bude kvalifikovan elektronski sertifikat, kako je definisano u važećem zakonodavstvu EU;
- EUQualifiedCertificateSigRequired: Ovo ograničenje ukazuje na to da je potrebno da sertifikat potpisnika koji se koristi za provjeru potpisa bude kvalifikovani sertifikat za elektronski potpis, kako je definisano u važećem zakonodavstvu EU;
- EUQualifiedCertificateSealRequired: Ovo ograničenje ukazuje da je potrebno da sertifikat potpisnika, koji se koristi za provjeru elektronskog pečata bude kvalifikovani elektronski sertifikat za elektronski pečat, kako je definisano u važećem zakonodavstvu EU;
- EUQSCDRequired: Ovo ograničenje ukazuje da se sertifikat potpisnika, 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.

3.5.4. KRIPTOGRAFSKA OGRANIČENJA

GovME CA usluga za provjeru validnosti kvalifikovanog elektronskog potpisa/pečata implementira kriptografska ograničenja koja ukazuju na zahtjeve vezane za algoritme i parametre koji se koriste prilikom kreiranja elektronskog potpisa/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, timestamps). They will be typically be represented by a list of entries as in table A.3. **Prevod:** p)1. CryptographicSuitesConstraints: Ovo ograničenje ukazuje na zahtjeve u vezi algoritama i parametara koji se koriste prilikom kreiranja potpisa ili se koriste prilikom verifikacije potpisanih objekata uključenih u proces verifikacije ili nadogradnje potpisa (npr. potpis, sertifikati, CRL-ovi, OCSP odgovori, vremenski pečati). Oni će obično biti predstavljeni listom unosa kao u tabeli A.3	Based on ETSI TS 119 312 **Prevod:** Bazirano na ETSI TS 119 312

Tabela 4 – Kriptografska ograničenja

3.5.5. KRITERIJUMI VEZANI ZA ELEMENTE ELEKTRONSKOG POTPISA I ELEKTRONSKOG PEČATA

GovME CA usluga za provjeru validnosti kvalifikovanog elektronskog potpisa/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.	None

Prevod: (b)1. ConstraintOnDTBS: Ovo ograničenje ukazuje na zahtjeve o vrsti podataka koji se potpisuju.	
(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: (b)2.1MandatedSignedQProperties-DataObjectFormat to require a specific format for the content being signed by the signer. (b)2.2 MandatedSignedQPropertiescontent- hints to require specific information that describes the innermost signed content of a multi-layer message where one content is encapsulated in another or the content being signed by the signer. (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. (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" atribute. **Prevod:** (b)2.ContentRelatedConstraintsAsPartOfSignatureElements: Ovaj skup ograničenja ukazuje na potreban sadržaj povezanim informacionim elementima pod formom potpisanih ili nepotpisanih kvalifikovinih svojstva koja su obavezna biti prisutana u potpisu. Ovo uključuje: b)2.1 MandatedSignedQProperties-DataObjectFormat Zahtijeva se specifičan format za sadržaj koji se potpisuje od strane potpisnika (b)2.2 MandatedSignedQPropertiescontent- Zahtijevaju se specifične informacije koje opisuju najdublje potpisani sadržaj višeslojne poruke gdje je jedan sadržaj integrisan u drugi sadržaj koji se potpisuje od strane potpisnika (b)2.3 MandatedSignedQProperties-content-reference Zahtijevaju se informacije prilikom povezivanja zahtievanog i dobijenog odgovora u razmjeni podataka izmedu dvije strane, ili o načinu kako će ta razmjena podataka biti ostvarena, itd. (b)2.4 MandatedSignedQProperties-content-identifier Zahtijeva se prisustvo ili specifična vrijednost za identifikator koji će se kasnije koristiti u potpisanom atributu kvalifikovanog svojstva "content-reference".	None
(b)3. DOTBSAsAWholeOrInParts: This constraint indicates whether the whole data or only certain part(s) of it have to be	None

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, additional information should be used to express which parts have to be signed. **Prevod:** Ovo ograničenje ukazuje na to da li svi podaci ili samo dio podataka mora biti potpisan. Semantika za moguć skup zahtijevanih vrijednosti koje se koriste prilikom ovog ograničenja je sledeća: • cijeli: cijeli podaci moraju biti potpisani; • djelovi: samo odredeni dio podataka mora biti potpisan. U ovom slučaju, dodatne informacije treba da ukažu koji djelovi moraju biti potpisani.	

Tabela 5 – Kriterijumi vezani za elemente kvalifikovanog elektronskog potpisa/pečata

3.6. PROTOKOL ZA PROCES VERIFIKACIJE

Kanal za informacije između korisnika i sistema za provjeru validnosti potpisa/pečata prenosi zahtjeve za provjeru kvalifikovanog elektronskog potpisa/pečata u jednom smjeru i vraća odgovor, u drugom. GovME CA koristi namjenski protokol za uslugu provjere validnosti elektronskog potpisa/pečata koji se zasniva na zahtjevima standarda ETSI EN 119 442.

Usluge provjere kvalifikovanog elektronskog potpisa/pečata GovME CA dostupne su preko korisničkog interfejsa (GovME CA portal).

3.7. INTERFEJS

3.7.1. KANAL ZA INFORMACIJE

Kanal za informacije između korisnika i sistema za provjeru validnosti kvalifikovanog elektronskog potpisa/pečata obezbijeđen je korišćenjem TLS bezbjednosnog kanala. Sistem za provjeru validnosti potpisa/pečata garantuje uspostavljanje bezbjednog kanala i očuvanje povjerljivosti i integriteta podataka korisnika.
Nakon uspješno izvršenog procesa autentifikacije na GovME CA portalu, korisnik može pristupiti usluzi verifikacije. Na ovaj način se obezbjeđuje da su informacije koje se razmjenjuju dostupne samo konkretnom autentifikovanom klijentu.

3.7.2. ODNOS SA DRUGIM PRUŽAOCIMA USLUGA POVJERENJA

Na status verifikacije potpisa i izveštaj o provjeri validnosti potpisa/pečata mogu da utiču autoriteti za označavanje tačnog vremena, prakse, politike i drugih pružaoca elektronskih usluga povjerenja, koji su van kontrole sistema GovME CA, odnosno njihove CRL liste i OCSP servisi. GovME CA sistem za provjeru validnosti potpisa/pečata garantuje status provjere validnosti potpisa i izveštaja o provjeri validnosti potpisa/pečata samo u vrijeme stvarne provjere potpisa, odnosno pečata.

3.8. ZAHTJEVI ZA IZVJEŠTAJ O VERIFIKACIJI KVALIFIKOVANOG ELEKTRONSKOG POTPISA/PEČATA

Usluga verifikacije na portalu GovME CA pruža tri vrste izvještaja o verifikaciji:

1. Jednostavan izvještaj o verifikaciji - pruža neophodne informacije u vezi sa identitetom potpisnika i indikacijom statusa verifikovanog potpisa, 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 provjeri validnosti u formatu koji je mašinski čitljiv.

4. USLOVI POSLOVANJA SERTIFIKACIONOG TIJELA

4.1. ORGANIZACIJA I UPRAVLJANJE

4.1.1. UNUTRAŠNJA ORGANIZACIJA I UPRAVLJANJE BEZBJEDNOŠĆU

Fizička zaštita, upravljanje i operativne kontrole koje se odnose na rad GovME CA su definisane internom dokumentu „Plan fizičke zaštite objekata, odnosno prostora za smještaj i funkcionisanje računarske i komunikacione opreme".

4.1.2. SIGURNOSNI NADZOR OPREME

Fizička zaštita, upravljanje i operativne kontrole koje se odnose na rad GovME CA su definisane internom dokumentu „Plan fizičke zaštite objekata, odnosno prostora za smještaj i funkcionisanje računarske i komunikacione opreme".

4.1.3. KONTROLA OSOBLJA

4.1.3.1. KVALIFIKACIJE, ISKUSTVA I POVJERE

Osoblje GovME CA predstavljaju stalno zaposleni službenici, imenovani rješenjem ministra javne uprave, kojim su određena njihove radne dužnosti. Oni su angažovani na poslovima certifikacionog tijela i adekvatno osposobljeni za izvršavanje radnih dužnosti.

PKI osoblje sa pouzdanom CA ulogom podvrgnuto je sigurnosnim provjerama prije nego što budu imenovani za člana GovME CA osoblja.

4.1.3.2. POSTUPCI ZA KONTROLU OSOBLJA

GovME CA prati provjeru osoblja i provjeru pozadine u skladu sa internim dokumentima i procedurama Ministartsva javne uprave.

4.1.3.3. OBUKA OSOBLJA

Svi članovi GovME CA osoblja su obučeni na odgovarajući način. Za CA osoblje trening obuhvata hardver, softver i CA aplikaciju.

Osoblje CA pruža obuku drugim članovima o CA procesima, postupanjima u kriznim situacijama i slučajevima oporavka od katastrofe. Takođe, pružaju obuku članovima GovME CA RA.

4.1.3.4. DODATNA OBUKA I UČESTALOST OBUKE OSOBLJA

Zaposleni će redovno, a najmanje jednom godišnje pohađati obuke ili seminare radi obnavljanja znanja o aktuelnim bezbjednosnim procedurama i novim bezbjednosnim prijetnjama.

Potrebe za obuku GovME CA osoblja se redovno revidiraju da bi se prilagodili promjenama PKI okruženja.

4.1.3.5. UČESTALOST I REDOSLJED ROTACIJE ULOGA

Nije primjenjivo.

4.1.3.6. SANKCIJE ZA NEOVLAŠĆENE AKTIVNOSTI

Neovlašćene radnje i kršenja rješavaju se u skladu sa važećom zakonskom regulativom.

4.1.3.7. KRITERIJUMI ZA OSOBLJE ANGAŽOVANO PO UGOVORU O DJELU

GovME CA ne zapošljava osoblje po ugovoru o djelu na bilo kojoj osjetljivoj poziciji.

4.1.3.8. DOKUMENTACIJA ZA POTREBE OSOBLJA

CA osoblje, u skladu sa ulogama, ima pristup dokumentaciji, uključujući hardver, softver i dokumentaciju vezanu za aplikaciju, operativnim procedurama, procedurama za bezbijednost, procedurama za kontrolu pristupa i ovom dokumentu.

4.1.4. FIZIČKA ZAŠTITA

4.1.4.1. LOKACIJA I KONSTRUKCIJA

Fizička zaštita, upravljanje i operativne kontrole koje se odnose na rad GovME CA su definisane internom dokumentu „Plan fizičke zaštite objekata, odnosno prostora za smještaj i funkcionisanje računarske i komunikacione opreme".

4.1.4.2. KONTROLA FIZIČKOG PRISTUPA

Fizička zaštita, upravljanje i operativne kontrole koje se odnose na rad GovME CA su definisane internom dokumentu „Plan fizičke zaštite objekata, odnosno prostora za smještaj i funkcionisanje računarske i komunikacione opreme".

4.1.4.3. NAPAJANJE I KLIMATIZACIJA

Fizička zaštita, upravljanje i operativne kontrole koje se odnose na rad GovME CA su definisane internom dokumentu „Plan fizičke zaštite objekata, odnosno prostora za smještaj i funkcionisanje računarske i komunikacione opreme".

4.1.4.4. ZAŠTITA OD POPLAVE

Fizička zaštita, upravljanje i operativne kontrole koje se odnose na rad GovME CA su definisane internom dokumentu „Plan fizičke zaštite objekata, odnosno prostora za smještaj i funkcionisanje računarske i komunikacione opreme".

4.1.4.5. PREVENCIJA I ZAŠTITA OD POŽARA

Fizička zaštita, upravljanje i operativne kontrole koje se odnose na rad GovME CA su definisane internom dokumentu „Plan fizičke zaštite objekata, odnosno prostora za smještaj i funkcionisanje računarske i komunikacione opreme".

4.1.4.6. SMJEŠTANJE MEDIJA

Fizička zaštita, upravljanje i operativne kontrole koje se odnose na rad GovME CA su definisane internom dokumentu „Plan fizičke zaštite objekata, odnosno prostora za smještaj i funkcionisanje računarske i komunikacione opreme".

4.1.4.7. ODLAGANJE OTPADA

Fizička zaštita, upravljanje i operativne kontrole koje se odnose na rad GovME CA su definisane internom dokumentu „Plan fizičke zaštite objekata, odnosno prostora za smještaj i funkcionisanje računarske i komunikacione opreme".

4.1.4.8. SMJEŠTANJE KOPIJA MEDIJA NA UDALJENOJ LOKACIJI

GovME CA koristi sigurnosne kontrole za siguran transport i skladištenje svih rezervnih i arhivskih medija van primarne lokacije. Pristup i čitanje rezervnih kopija vrši se jednom godišnje u okviru vježbe kontinuiteta poslovanja.

Operativne sigurnosne kopije (Backups) cjelokupnog CA sistema (konfiguracija sistema, arhivski zapisi, zapisi revizije) snimaju se mjesečno i čuvaju na sigurnom mjestu za skladištenje van primarne lokacije. Operativne sigurnosne kopije mogu se koristiti za oporavak kompletnog CA sistema.

4.1.5. UPRAVLJANJE INFRASTRUKTUROM

Sertifikaciono tijelo ima uspostavljene procedure upravljanja infrastrukturom u skladu sa ISO/IEC 27001 standardom. Procedure su opisane u internim dokumentima koja su povjerljiva i nisu javno dostupna.

4.1.6. UPRAVLJANJE PRISTUPOM SISTEMIMA

Kao što je opisano u dijelu 3.4.4.2. Kontrola fizičkog pristupa u okviru ovog dokumenta.

4.1.7. SISTEM PRIKUPLJANJA LOGOVA ZA REVIZIJU

GovME CA je uspostavio mehanizme za prikupljanje revizorskih logova za sve događaje koji se odnose na vršenje Usluga verifikacije.

4.2. PRESTANAK RADA SERTIFIKACIONOG TIJELA

U slučaju prestanka rada pružanja usluga povjerenja, GovME CA će:

- obavijestiti Vladu Crne Gore i sve organe državne uprave najmanje 90 dana prije namjere da se prestane sa radom;
- opozvati sve validne sertifikate do ili nakon isteka otkaznog roka;
- osigurati pristup i dostupnost relevantnih CRL-ova i OCSP u periodu od 6 mjeseci nakon opoziva svih sertifikata;
- osigurati da sva dokumentacija i arhive budu zadržane 10 godina od poslednjeg dana rada, ukoliko drugačije nije predviđeno važećim propisima.

4.3. USKLADENOST SA ZAKONODAVSTVOM

Pružanje kvalifikovane usluge verifikacije kvalifikovanih elektronskih potpisa i pečata usklađeno je sa Zakonom o elektronskoj identifikaciji i elektronskom potpisu, podzakonskom regulativom i ovim dokumentom.

4.4. USAGLAŠENOST SA MEĐUNARODNIM STANDARDIMA

ETSI EN 319 401	General Policy Requirements for Trust Service Providers;
ETSI EN 119 442	Protocol profiles for trust service providers providing AdES digital signature validation services;
ETSI TS 119 102-1	Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation
ETSI TS 103 171	XAdES Baseline Profile
ETSI TS 103 172	PAdES Baseline Profile
ETSI TS 103 173	CAdES Baseline Profile
ETSI EN 319 411-1	Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements;
ETSI EN 319 411-2	Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates;
ETSI EN 319 412-1	Certificate Profiles; Part 1: Overview and common data structures;
ETSI EN 319 412-2	Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
ETSI EN 319 412-3	Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
ETSI EN 319 412-5	Certificate Profiles; Part 5: QCStatements
ETSI TS 119 312	Cryptographic Suites
ETSI EN 319 421	Policy and Security Requirements for Trust Service Providers issuing ElectronicTime-Stamps;
ETSI EN 319 422	Time stamping protocol and electronic time-tamp profiles;
ETSI EN 319 522	Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services
RFC 2580	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;
RFC 3161	Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP);
RFC 6960	X.509 Internet Public Key - Infrastructure Online Certificate Status Protocol - OCSP.

Broj: 01-050/25-1059

U Podgorici, 11. marta 2025. godine

MINISTAR

mr Marash Dukaj