Crna Gora
Ministarstvo javne uprave

Praktična pravila o pružanju kvalifikovane usluge elektronske preporučene dostave (eDelivery Certificate Practice Statment – GovME CA eDelivery CPS)

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 elektronske usluge povjerenja kvalifikovane usluge elektronske preporučene dostave od strane Ministarstva javne uprave (u daljem tekstu: Ministarstva), kao organa koji u skladu sa Uredbom o organizaciji i načinu rada državne, izmedu 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), koje kreira i dodjeljuje sertifikate. Njegovim uspostavljenjem omogućava se upotreba kvalifikovanog elektronskog potpisa, kvalifikovanog elektronskog pečata, kao i ostalih elektronskih usluga povjerenja od strane organa državne uprave.

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 elektronske preporučene dostave.

Ovaj dokument opisuje nivo bezbjednosti infrastrukture GovME CA, tehničke karakteristike kao i procedure koje se koriste za pružanje kvalifikovane usluge elektronske preporučene dostave.

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

1.1.2. SKRAĆENICE

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

1.1.3. NAZIV DOKUMENTA I IDENTIFIKACIONI PODACI

Ovaj dokument predstavlja Praktična pravila o pružanju kvalifikovane usluge elektronske preporučene dostave (eDelivery Certificate Practice Statment – GovME CA eDelivery CPS).

Struktura ovog dokumenta zasniva se na standardizovanom dokumentu IETF RFC 3647, uz izvjesne modifikacije neophodne da bi se opisali zahtjevi za pružanje kvalifikovane usluge elektronske preporučene dostave propisani Zakonom o elektronskoj identifikaciji i elektronskom potpisu.

Ažuriranje ovog dokumenta će se vršiti od strane GovME CA PMA periodično, a minimum jednom godišnje ili prilikom provjere uklađenosti.

1.1.4. KONTAKT OSOBA

Kontakt podaci za administraciju i sadržaj ovog dokumenta su:

Ministarstvo javne uprave GovME CA
Rimski trg 45
81000 Podgorica, Crna Gora
URL: https://gov.me/mju/ca
E-mail: ca@mju.gov.me

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

Učesnici u cjelokupnom sistemu pružanja usluga kvalifikovane usluge elektronske preporučene dostave GovME CA 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 elektronske preporučene dostave 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 podredenih 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

GovME CA OA (Operations Authority) je odgovorno za:

- instalaciju, konfiguraciju i održavanje IT okruženja sistema za preporučenu elektronsku dostavu;
- 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.

2.1.3. TIJELO ZA UPRAVLJANJE REGISTRACIJOM KORISNIKA

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

- prihvatanje ili odbijanje zahtjeva za pružanje kvalifikovane usluge elektronske preporučene dostave;
- komunikaciju sa naručiocima i korisnicima po osnovu podnijetih zahtjeva za kvalifikovane usluge elektronske preporučene dostave;
- provjeru podataka u zahtjevu za pružanje kvalifikovane usluge elektronske preporučene dostav;
- 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".

2.2. 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 kvalifikovane usluge elektronske preporučene dostave.

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.

2.3. TREĆA LICA

Nije primjenjivo.

3. KVALIFIKOVANA USLIGA ELEKTRONSKE PREPORUČENE DOSTAVE

Kvalifikovana usluga elektronske preporučene dostave podliježe zakonskoj regulativi i standardima. Mapiranje relevantnijih zahtjeva sa opisima ispunjenosti istih dat je u Tabeli 1.

Regulatorni okvir je referenciran po osnovu Zakona o elektronskoj identifikaciji i elektronskom potpisu („Službeni list CG", br. 31/17 i 72/19) i Pravilnika o bližim zahtjevima koje mora da ispunjava kvalifikovana usluga elektronske preporučene dostave („Službeni list CG", br. 53/18 i 20/20).

OPIS ZAHTJEVA	REGULATORNI OKVIR	OPIS ISPUNJENOSTI
Cjelovitost podataka	Član 30, stav 1 tačka 1 Zakona; Član 31, stav 1 tačka 4 Zakona	Integritet sadržaja poruke korisnika
Slanje podataka od strane identifikovanog pošiljaoca	Član 30, stav 1 tačka 2 Zakona; Član 31, stav 1 tačka 2 Zakona; Član 2 i 4 Pravilnika	Procedura vršenja kvalifikovane usluge elektronske preporučene dostave Autentifikacija korisnika

Prijem podataka od strane identifikovanog primaoca	Član 30, stav 1 tačka 3 Zakona; Član 31, stav 1 tačka 2 Zakona Član 2, 3 i 4 Pravilnika	Procedura vršenja kvalifikovane usluge elektronske preporučene dostave Autentifikacija korisnika
Tačnost datima i vremena slanja i prijema podataka	Član 30, stav 1 tačka 4 Zakona; Član 31, stav 1 tačka 6 Zakona; Član 4 Pravilnika	Obezbjeđivanje kvalifikovanih elektronskih vremenskih pečata
Dokaz o slanju i primanju podataka	Član 4, stav 1 tačka 1 Pravilnika	Evidencija događaja
Prikupljanje i čuvanje podataka	Član 4, stav 1 tačka 2 Pravilnika	Evidencija događaja

Tabela 1 - Matrica regulatornih zahtjeva i opisa ispunjenosti istih

3.1. IDENTIFIKACIJA USLUGE

Identifikaciona oznaka (OID) za kvalifikovanu uslugu elektronske preporučene dostave po ovom dokumentu je: 1.3.6.1.4.1.34324.2.1.4.

3.2. PROCEDURA VRŠENJA KVALIFIKOVANE USLUGE ELEKTRONSKE PREPORUČENE DOSTAVE

Nakon uspješne registracije na GovME CA portalu, korisnik ima mogućnost, između ostalog, da pošalje elektronski dokument koristeći kvalifikovanu elektronsku uslugu povjerenja „kvalifikovana elektronska preporučena dostava".

Pružanje kvalifikovane usluge elektronske preporučene dostave se odvija po osnovu standarda ETSI 319 522.

3.3. INTEGRITET SADRŽAJA PORUKE KORISNIKA

GovME CA u okviru svakog dokaza o slanju i primanju sadržaja poruke korišćenjem kvalifikovane usluge elektronske preporučene dostave šalje hash vrijednost poslatog/primljenog sadržaja poruke. Dokazi o slanju i primanju sadržaja poruke, uključujući datum i vrijeme slanja i primanja obezbjeđuju se kvalifikovanim elektronskim pečatom kvalifikovanog davaoca elektronskih usluga povjerenja i ovjeravaju kvalifikovanim elektronskim vremenskim pečatom. Na ovaj način se obezbjeđuje integritet sadržaja poruke na prenosnom putu od jednog do drugog korisnika.

3.4. AUTENTIFIKACIJA KORISNIKA

Proces autentifikacije predstavlja dio vršenja kvalifikovane usluge elektronske preporučene dostave i zasniva se na bezbjednosnom parametru dvofaktorske autentifikacije.

3.5. DVOFAKTORSKA AUTENTIFIKACIJA

Autentifikacija korisnika prilikom korišćenja kvalifikovane usluge elektronske preporučene dostave vrši se korišćenjem korisničkog imena i lozike, kao prvog faktora autentifikacije i koda koji se dobija SMS porukom, kao drugog faktora autentifikacije.

Korisničko ime predstavlja e-mail adresu korisnika. Nakon uspješne autentifikacije, korisnik se loguje na GovME CA portal i 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".

3.6. EVIDENCIJA DOGAĐAJA

Za kvalifikovanu uslugu elektronske preporučene dostave GovME CA razlikuje sljedeće tipove dogadaja:

- Prihvatanje sadržaja elektronske preporučene dostave za slanje od strane davaoca usluga podrazumijeva da davalac usluga prima i prihvata sadržaj elektronske preporučene dostave od jednog krajnjeg korisnika kako bi ga otpremio nekom drugom krajnjem korisniku. Vrijeme prihvatanja predstavlja vrijeme kada je i zadnji bajt sadržaja elektronske peporučene dostave prihvaćen od strane davaoca usluge.
- Slanje sadržaja elektronske preporučene dostave predstavlja isporuku sadržaja elektronske preporučene dostave do email-a krajnjeg korisnika kome je dostava namijenjena. Vrijeme slanja sadržaja elektronske preporučene dostave predstavlja vrijeme kada je posljednji bajt sadržaja elektronske preporučene dostave upućen sa sistema pružaoca usluge prema email-u krajnjeg korisnika.
- Obavještenje krajnjem korisniku u vezi prijema elektronske preporučene dostave predstavlja obavještenje kojim se krajnji korisnik upoznaje da za njega postoji elektronska preporučena dostava, te da može da istu primi ili da je odbije. Vrijeme obavještenja je vrijeme kada je krajnjem korisniku sadržaj elektronske preporučene dostave isporučen putem email-a.
- Prijem sadržaja elektronske preporučene dostave podrazumijeva da je krajnjem korisniku, kome je dostava namijenjena, isporučen sadržaj elektronske preporučene dostave u njegovom email-u i krajnji korisnik se eksplicitno izjasnio da li će istu da primi ili odbije. Vrijeme prijema je vrijeme eksplicitnog izjašnjavanja primaoca da prihvata/odbija sadržaj elektronske preporučene dostave.
- Preuzimanje sadržaja elektronske preporučene dostave predstavlja upoznavanje krajnjeg korisnika sa sadržajem elektronske preporučene dostave. Vrijeme preuzimanja je vrijeme

kada je sadržaj elektronske preporučene dostave napustio sistem pružaoca usluge i uspješno je predat aplikaciji koju koristi primalac za prikaz sadržaja elektronske preporučene dostave.

Dokaze o slanju, primanju i preuzimanju podataka prilikom pružanja kvalifikovane usluge elektronske preporučene dostave izrađuje sistem GovME CA i to:

- Potvrda o prihvatanju sadržaja elektronske proporučene dostave za slanje (od strane pružaoca usluge);
- Obavještenje krajnjem korisniku za prihvatanje elektronske preporučene dostave;
- Potvrdu o slanju sadržaja elektronske proporučene dostave;
- Potvrdu o prijemu sadržaja elektronske preporučene dostave;
- Potvrdu krajnjem korisniku da je rok za prijem sadržaja elektronske preporučene dostave istekao;
- Potvrdu o preuzimanju sadržaja elektronske proporučene dostave.

Navedene potvrde moraju minimalno da sadrže sljedeće podatake:

- Jedinstveni identifikator sadržaja elektronske preporučene dostave koji je dodijelio davalac kvalifikovane usluge elektronske preporučene dostave;
- Naziv davaoca kvalifikovane usluge elektronske preporučene dostave;
- Identifikaciona oznaka (OID) za kvalifikovanu uslugu elektronske preporučene dostave;
- Naziv sadržaja elektronske preporučene dostave;
- Kod i opis akcije koja je izvršena (prihvatanje pošiljke za slanje, slanje, prijem, preuzimanje)
- Metod koji je korišćen za autentifikaciju pošiljaoca i primaoca;
- Elektronske adrese pošiljaoca i primaoca;
- Podatak koji jedinstveno identifikuje sadržaj elektronske preporučene dostave (hash);
- Datum i vrijeme kada je akcija izvršena;
- Podatke o pošiljaocu i primaocu

Vrijeme prijema sadržaja elektronske preporučene dostave je unaprijed definisano i iznosi 15 dana od slanja sadržaja elektronske preporučene dostave. U slučaju da ovaj rok istekne, sadržaj pošiljke više nije dostupan i neće se moći primiti.

GovME CA PMA zadržava pravo da u dokaze uvrsti i dodatne podatke, ukoliko su oni iz nekog razloga potrebni i ukoliko je njihovo objavljivanje u skladu sa važećom zakonskom regulativom Crne Gore. Potvrde se primarno šalju u PDF formatu, a može biti i formatu XML.

GovME CA je u obavezi da sve dokaze o slanju, primanju i preuzimanju podataka prilikom pružanja kvalifikovane usluge elektronske preporučene dostave čuva u sistemu u periodu od najmanje 10 godina od vremena njihovog nastanka.

Sadržaj elektronske preporučene dostave se čuva na sistemu u periodu od najmanje 45 dana od vremena prihvatanja sadržaja elektronske proporučene dostave.

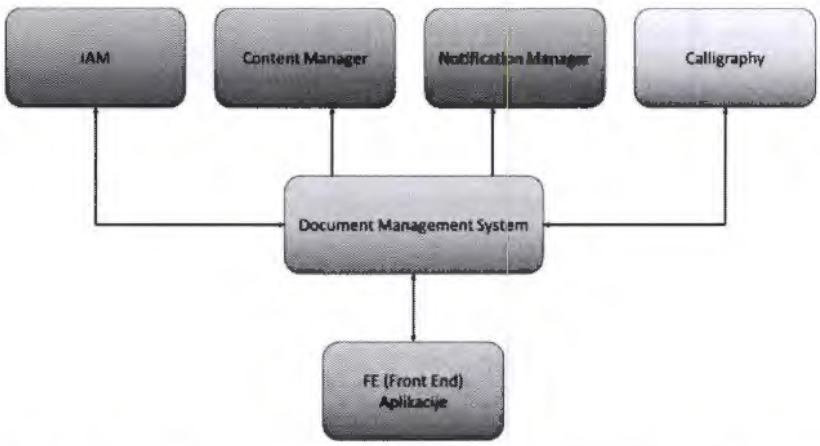
3.7. INTEROPERABILNOST

GovME CA pruža kvalifikovanu uslugu elektronske preporučene dostave samo svojim registrovanim korisnicima.

4. PROCES I KOMPONENTE USLUGE ZA PREPORUČENU DOSTAVU

4.1. ULOGE U PRUŽANJU USLUGE ELEKTRONSKE PREPORUČENE DOSTAVE

Komponente sistema za pružanje usluge kvalifikovane elektronske preporučene dostave su prikazane na sljedećoj slici:



Slika 1 – Komponente sistema za pružanje Usluge preporučene dostave

Osnovne komponente sistema GovME CA eDelivery su:

- Identity access management (IAM) predstavlja softversku komponentu koja služi za upravljanje nalozima krajnjih korisnika. Ona sadrži funkcionalnosti kao što su kreiranje, izmjena i brisanje krajnjeg korisnika. Sa Back office sistemo ima direktnu komunikaciju, u cilju da operaterima obezbijedi neophodne funkcionalnosti, prije svega verifikaciju korisničkog identiteta.
- Content Manager (CM) predstvalja modul koji se koristi za skladištenje binarnih podataka učitanih, potpisanih i pečatiranih dokumenata. CM koristi API metode za učitavanje i povlačenje binarnih podataka preko zadatih referenci.
- Document Management System (DMS) predstvalja modul čije su funkcionalnosti dostupne jedino preko GovME CA portala, odakle krajnji korisnici mogu da kreiraju workflow za razmjenu dokumenata i izvršavaju različite vrste akcija u okviru workflow-a u kome participiraju.
- Caligraphy Service Manager je API gateway koji prikuplja sve zahtjeve krajnjih korisnika i prevodi ih u odgovarajuće servisne zahtjeve. Ova komponenta predstavlja jedinstvenu tačku kontakta za sve vitalne funkcionalnosti koje sistem pruža krajnjim korisnicima.
- Notification Manager predstvalja komponentu sistema koja je odgovorna za prosljeđivanje sistemskih obavještenja krajnjim korisnicima. Ona se prvenstveno koristi za autentifikaciju krajnjih korisnika koji pristupaju sistemu, kao i za autorizaciju digitalnih transakcija od strane

krajnjih korisnika preko mobilnog telefona, čime se postiže dodatni nivo sigurosti u identitet krajnjih korisnika i volju krajnjih korisnika da izvrši započetu operaciju.
- FE (Front End) aplikacije čine aplikativne komponente koje koriste krajnji korisnici, administratori i operateri sistema i one su detaljnije opisane u ovom dokumentu.

4.2. UTVRĐIVANJE USAGLAŠENOSTI DOKUMENTA SA ZAKONOM

Ovaj dokument je usklađen sa Zakonom o elektronskoj identifikaciji i elektronskom potpisu i podzakonskim aktima.

4.3. PROCEDURA ODOBRAVANJA DOKUMENATA

Ovaj dokument se periodično pregleda i ažurira po potrebi.

Period pregleda i ažuriranja ovog dokumenta se vrši najmanje jednom godišnje ili prilikom pripreme provjere usklađenosti.

Dokument se može pregledati i po potrebi ažurirati i češće ukoliko dođe do promjena u zakonskoj regulativi ili se javi potreba za promjenu primijenjenih kriptografskih algoritama ili dužina kriptografskih ključeva.

Na osnovu predloga GovME CA PMA, ovaj dokument odobrava ministar javne uprave.

5. REGISTRACIJA KORISNIKA

5.1. PODNOŠENJE ZAHTJEVA I REGISTRACIJA KORISNIKA

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

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.

5.2. PROCES OBRADE ZAHTJEVA I ODGOVORNOSTI

Kada se odradi provjera identiteta krajnjih korisnika i uspješno završi proces registracije GovME CA nakon toga pruža kvalifikovane elektronske usluge povjerenja.
Da bi mogli da koriste uslugu kvalifikovane elektronske preporučene dostave krajnji korisnici moraju da imaju kreiran nalog na GovME CA portalu.

Koraci u procesu obrade zahtjeva su detaljnije opisani u ovom dokumentu, u poglavlju 5.3.

5.3. OBRADA ZAHTJEVA

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.

Koraci prilikom obrade zahtjeva su:

Korak 1 - Naručilac ispunjava zahtjev na propisanom obrascu i isti potpisuje kvalifikovanim elektronskim potpisom.

Korak 2 - Naručilac potpisan zahtjev dostavlja putem email-a na adresu arhiva@mju.gov.me.

Korak 3 - Arhiva Ministarstva dostavljeni zahtjev unosi u Sistem za elektronsko upravljanje dokumentima (u daljem tekstu: eDMS) i dodjeljuje predmet službeniku GovME CA RA.

Korak 4 - GovME CA RA službenik dobija notifikaciju na e-mail o dodijeljenom predmetu i isti obrađuje.

Korak 5

- GovME CA RA službenik provjerava da li je zahtjev ispunjen na propisan način.
- GovME CA RA službenik provjerava da li u bazi podataka postoji aktivan korisnički nalog na ime korisnika.
    - Ukoliko postoji, GovME CA RA službenik provjerava status elektronske usluge povjerenja.
        - ukoliko je status „Aktivan", GovME CA RA službenik obavještava naručioca da je usluga aktivna i zatvara predmet u eDMS-u (dobija status „Riješen").
        - ukoliko je status „Povučen", GovME CA RA službenik prelazi na sledeći korak.
    - Ukoliko ne postoji, GovME CA RA službenik prelazi na sledeći korak.
- GovME CA RA službenik obavještava naručioca koji je podnio zahtjev putem email-a da je zahtjev validan i zakazuje termin u kojem korisnik može doći u prostorije Ministarstva u cilju

identifikacije „licem u lice". U okviru ovog obavještenja, GovME CA RA službenik naručiocu dostavlja standardizovanu informaciju o tačnoj lokaciji i kontakt informacijama GovME CA RA službenika.

Korak 6 - Korisnik dolazi u prostorije Ministarstva na identifikaciju. Korisnik je dužan da sa sobom ponese važeći identifikacioni dokument (ličnu kartu), kao i dokument izdat od strane Ministarstva unutrašnjih poslova, a koji sadrži njegov IB (identifikacioni broj).

- GovME CA RA službenik upoređuje informacije sa obrasca podnijetog zahtjeva sa podacima na ličnoj karti korisnika.
- Ukoliko prilikom utvrđivanja identiteta GovME CA RA službenik utvrdi nepravilnosti, o tome usmeno obavještava korisnika i šalje obavještenje naručiocu da ispravi greške i dostavi dopunu zahtjeva, vezujući se za isti predmet u eDMS-u. Nakon toga, ponavlja se postupak iz koraka 5 i 6.
- Ukoliko je sve u redu, GovME CA RA službenik unosi sve informacije sa podnijetog zahtjeva kroz RA portal i generiše potvrdu, koju potpisuje korisnik da je upoznat sa pravilima korišćenja i da Ministarstvo njegove lične podatke može koristiti isključivo u svrhu izdavanja elektronskih sertifikata, kao i GovME CA RA službenik da je izvršio identifikaciju korisnika na propisan način. Potpisana potvrda se izdaje u dva primjerka (po jedan za obje strane), nakon čega GovME CA RA službenik istu skenira i unosi u predmet na eDMS-u.

Korak 7 - Kada službenik GovME CA RA unese zahtjev kroz RA portal, isti stiže na obradu.

- Za usluge koje su na Portalu GovME CA 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.

Korak 8 - GovME CA RA službenik informiše korisnika da je zahtjev odobren, putem email-a i u prilogu dostavlja korisnička uputstva adekvatna za uslugu povjerenja za koju je podnijet zahtjev.

Korak 9 - GovME CA RA službenik zatvara predmet na eDMS-u (dobija status „Riješen").

5.4. PROVJERA IDENTITETA FIZIČKOG LICA U ORGANU DRŽAVNE UPRAVE

Zadatak ovlašćenog lica organa državne uprave jeste da izvrši provjeru identiteta fizičkog lica u okviru organa državne uprave, odnosno budućeg korisnika kvalifikovane usluge elektronske preporučene dostave.

Fizička lica će biti identifikovana po prinicipu „licem u lice", na način opisan u okviru poglavlja 5.3 i koraka 6.

5.5. PROVJERA IDENTITETA ORGANA DRŽAVNE UPRAVE

Organi državne uprave su definisani Uredbom o organizaciji i načinu rada državne uprave i kao takvi se ne moraju identifikovati posebno.

6. USLOVI POSLOVANJA SERTIFIKACIONOG TIJELA

6.1. ORGANIZACIJA I UPRAVLJANJE

6.1.1. REPOZITORIJUM

Repozitorijumom GovME CA upravlja Ministarstvo kao kvalifikovani davalac elektronskih usluga povjerenja. Sertifikaciono tijelo je odgovorno za dostupnost Repozitorijuma, objavu dokumenata i informacija na Repozitorijumu.

U okviru normalnog funkcionisanja Repozitorijuma, on je dostupan za upotrebu 24 sata na dan, 7 dana u nedelji.

U slučaju nedostupnosti Repozitorijuma setifikaciono tijelo će preduzeti sve potrebne mjere i postupke da Repozitorijum učini dostupnim u najkraćem mogućem roku.

GovME CA objavljuje sve relevantne informacije vezane za pružanje kvalifikovanih elektronskih usluga povjerenja na sljedećoj adresi: https://gov.me/mju/ca.

6.1.2. OBJAVA INFORMACIJA

Na repozitorijumu su javno objavljeni dokumenti i informacije o pružanju kvalifikovane usluge elektronske preporučene dostave.

6.1.3. SADRŽAJ REPOZITORIJUMA

Na Repozitorijumu javno su objavljeni dokumenti i informacije o pružanju elektronskih usluga povjerenja.

GovME CA objavljuje:

- sve verzije dokumenta „Politika pružanja kvalifikovanih elektronskih usluga povjerenja za organe državne uprave (GovME CA Certificate Policy - GovME CA CP)";
- sve verzije dokumenta „Praktična pravila o postupcima izdavanja kvalifikovanih sertifikata (GovME CA CPS – Certification Practice Statement)";
- ažuriranu CRL – Listu opozvanih sertifikata;
- CA sertifikate za RootCA i SubCA;
- korisnička uputstva za upotrebu elektronskih usluga povjerenja;
- obrazac zahtjeva za pružanje elektronskih usluga povjerenja;
- ostale javne informacije vezane za rad sertifikacionog tijela GovME CA.

U okviru repozitorijuma se ne objavljuju povjerljivi podaci.

6.1.4. POSTUPCI OBJAVE SADRŽAJA I UPRAVLJANJA REPOZITORIJUMOM

Da bi se dokumenta objavila na Repozitorijumu potrebno je da budu odobrena od strane ministra javne uprave, na predlog GovME CA PMA.

6.1.5. UČESTALOST OBJAVLJIVANJA PODATAKA

GovME CA na godišnjem nivou pregleda i po potrebi ažurira ovaj dokument. Prethodne verzije ovih dokumenata ostaju objavljene na Repozitorijumu najmanje 10 godina poslije isteka sertifikata izdatih u skladu s tim dokumentima.

Drugi GovME CA dokumenti i ostale relevantne informacije objavljuju se po potrebi, nakon odobrenja GovME CA PMA.

Sve informacije se objavljuju odmah nakon što su se promijenile ili postale dostupne.

6.1.6. KONTROLA PRISTUPA REPOZITORIJUMU

Sva javna dokumenta i informacije objavljene na Repozitorijumu su javno dostupne svim učesnicima uspostavljene PKI infastrukture, bez ograničenja.

Repozitorijum posjeduje uspostavljene odgovarajuće tehničke i bezbjednosne mehanizme kontrole pristupa u cilju zaštite od neovlašćenih promjena podataka i mehanizme za obezbjeđivanje raspoloživosti podataka. Pristup objavljenim dokumentima i informacijama na Repozitorijumu omogućen je samo za čitanje.

Pravo dodavanja, promjene ili brisanja informacija na Repozitorijumu imaju ovlašćena lica GovME CA.

6.2. CJENOVNIK

Nije primjenjivo.

6.3. SIGURNOSNE KONTROLE RAČUNARA

6.3.1. SPECIFIČNI ZAHTJEVI ZA SIGURNOST RAČUNARA

Ministarstvo javne uprave primjenjuje mehanizme kontrole pristupa računarskim sistemima koji se koriste u okviru GovME CA sistema.

Računarska i komunikaciona oprema koja se koristi u okviru GovME CA sistema fizički je obezbijeđena u prostorijama Ministarstva.

GovME CA koristi i mehanizme logičke kontrole pristupa putem firewall uređaja.

Neautorizovan pristup opremi nije dozvoljen. Kritične softverske i hardverske komponente GovME CA sistema mogu startovati samo dvije ili više ovlašćenih osoba koje posjeduju odgovarajuće smart kartice i koje znaju njihove PINove ili odgovarajuće lozinke.

6.3.2. RANGIRANJE SIGURNOSTI RAČUNARA

GovME CA koristi računare i operativne sisteme koji su komercijalni proizvodi i dodatno su bezbjednosno ojačani.

6.3.3. KONTROLA UPRAVLJANJA SIGURNOŠĆU

GovME CA nadgleda i kontroliše sigurnost i upravljanje sigurnošću sistema za pružanje kvalifikovane usluge elektronske preporučene dostave.

6.3.4. 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".

6.3.5. 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".

6.4. PRIVATNOST I ZAŠTITA LIČNIH PODATAKA

GovME CA naročito vodi računa o zaštiti ličnih podataka koje prikuplja, skladišti i upotrebljava u cilju pružanja usluga iz opsega opisanog u ovom dokumentu i sa ličnim podacima postupa u skladu sa odgovarajućim zakonima.

U postupku registracije, odnosno obrade zahtjeva za pružanje elektronske usluge povjerenja, korisnik se upoznaje i prihvata uslove korišćenja potpisivanjem potvrde prilikom identifikacije od strane GovME CA RA. GovME CA koristi lične informacije isključivo u svrhe za koje je korisnik dao saglasnost tokom postupka registracije.

6.4.1. PLAN PRIVATNOSTI

Ministarstvo je u obavezi da sve lične podatke koje obrađuje tretira u skladu sa Zakonom o zaštiti podataka o ličnosti.

6.4.2. INFORMACIJE KOJE SE TRETIRAJU KAO LIČNE

Informacije koje se ne nalaze na elektronskom sertifikatu, a odnose se na vlasnika elektronskog sertifikata tj. korisnika, smatraju se privatnim.

6.4.3. INFORMACIJE KOJE NE SE TRETIRAJU KAO LIČNE

Informacije koje su objavljene i čine sastavni dio sertifikata, CRL-a, ovog dokumenta, uključujući i sertifikate korisnika i druge informacije objavljene u CA javnom repozitorijumu, ne smatraju se ličnim.

6.4.4. ODGOVORNOST ZA ZAŠTITU LIČNIH PODATAKA

GovME CA je odgovoran za zaštitu povjerljivih podataka u skladu sa važećim propisima i Zakonom o zaštiti ličnih podataka.

6.4.5. OTKRIVANJE INFORMACIJA SHODNO PRAVNIM I ADMINISTRATIVNIM PROCESIMA

GovME CA je ovlašćeno da koristi ili objavljuje lične podatke samo na osnovu saglasnosti korisnika ili na pravno validan zahtjev nadležnog organa.

6.4.6. OSTALE OKOLNOSTI KADA SE MOGU OTKRIVATI LIČNE INFORMACIJE

GovME CA ustupiće podatke sudu, tužilaštvu i drugim nadležnim državnim organima u slučajevima propisanim odgovarajućim zakonima.

6.4.7. PRAVA NA INTELEKTUALNU SVOJINU

Ministarstvo ima sva prava intelektualnog vlasništva nad ovim dokumentom, sertifikatima koje izdaje, Repozitorijumom na kojem objavljuje informacije i svim dokumentima i informacijama koje su objavljene na Repozitorijumu.

7. FIZIČKE BEZBJEDNOSNE KONTROLE

7.1. 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".

7.1.1. 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".

7.1.2. 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".

7.1.3. 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".

7.1.4. 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".

7.1.5. 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".

7.1.6. ODLAGANJE OTPADA

U zavisnosti od tipa dokumenta koje je potrebno uništiti, dokumenta se uništavaju odgovarajućom metodom. U slučaju da su dokumenta koja više nisu potrebna za rad u papirnom obliku, tada se uništavaju kroz mašine za sječenje papira, dok se elektronski mediji uništavaju mehanički ili koristeći poseban uređaj koji zadovoljava najstrože sigurnosne standarde iz ove oblasti.

7.1.7. 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.

7.2. ORGANIZACIONE MJERE ZAŠTITE

GovME CA sprovodi kontrolu svojih zaposlenih radi obezbjeđivanja razumne sigurnosti, povjerljivosti i kompetencija zaposlenih.

Zaposleni u GovME CA sistem potpisuju izjavu da će se pridržavati pravne regulative u vezi zaštite podataka, kao i da će zadovoljiti sve postavljene zahtjeve u vezi sa povjerljivošću i svojim zaduženjima u okviru GovME CA sistema.

7.2.1. POVJERLJIVE ULOGE

Zavisno od svoje uloge, GovME CA osoblje može imati nalog na CA operativnom sistemu ili CA aplikaciji ili na oboje. CA aplikacija koju koristi GovME CA, implementira niz uloga koje dodjeljuje CA osoblju u zavisnosti od njihovih odgovornosti. Prava pristupa na operativnom sistemu CA ograničavaju osoblje na radnje koje su im potrebne u obavljanju njihovih dužnosti.

Različiti nivoi sistemskog i fizičkog pristupa se kontrolišu na osnovu uloga dodijeljenih od strane CA aplikacije i prava pristupa koje ima nalog na sistemu.

Povjerljive uloge koje su ključne za rad sistema elektronske preporučene dostave, definisane su obrazovanjem Tijela za operativne poslove (GovME CA OA) i Registracionog tijela (GovME CA RA).

Za potrebe funkcionisanja sistema elektronske preporučene dostave moguće je definisati i dodatne uloge.

7.2.2. IDENTIFIKACIJA I AUTENTIFIKACIJA OSOBLJA ZA POJEDINE ULOGE

Svaka osoba sa povjerljivom CA ulogom se identifikuje i autentifikuje sa korisičkim imenom i lozinkom ili sa digitalnim sertifikatom. Sistemski CA nalozi i aplikativni CA nalozi su direktno povezani sa pojedincem u čijem su vlasništvu. Nalozi se ne dijele i prava koja su im dodijeljena ograničena su na ona koja su im potrebna da izvršavaju svoje funkcije.

7.2.3. POVJERLJIVE ULOGE KOJE MORAJU IMATI ODVOJENE DUŽNOSTI

Povjerljive uloge koje su ključne za rad sistema elektronske preporučene dostave, definisane su obrazovanjem Tijela za operativne poslove (GovME CA OA) i Registracionog tijela (GovME CA RA).

Pri dodjeli korisničkih uloga i fizičkih prava pristupa strogo se poštuje princip segregacije dužnosti tako da jedna osoba ne može koristiti kriptografske materijale za izvršavanje sigurnosnih osjetljivih operacija, već je uvijek potrebno osigurati prisustvo najmanje dvije osobe.

7.2.4. KONTROLA OSOBLJA

Ministarstvo imenuje članove GovME CA i pismeno ih obavještava o njihovim obavezama.

7.2.5. 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.

7.2.6. POSTUPCI ZA KONTROLU OSOBLJA

GovME CA prati provjeru osoblja u skladu sa internim dokumentima i procedurama.

7.2.7. 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.

7.2.8. 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.

7.2.9. UČESTALOST I REDOSLJED ROTACIJE ULOGA

Nije primjenjivo.

7.2.10. SANKCIJE ZA NEOVLAŠĆENE AKTIVNOSTI

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

7.2.11. KRITERIJUMI ZA OSOBLJE ANGAŽOVANO PO UGOVORU O DJELU

GovME CA ne zapošljava osoblje pod ugovorom o djelu na bilo kojoj osjetljivoj poziciji.

7.2.12. DOKUMENTACIJA ZA POTREBE OSOBLJA

GovME CA zaposleni imaju pristup CA dokumentaciji, uključujući hardver, softver i dokumentaciju vezanu za aplikaciju, operativnim procedurama, procedurama za bezbijednost, procedurama za kontrolu pristupa i ovom dokumentu.

7.3. PROCEDURA UPRAVLJANJA LOGOVIMA ZA REVIZIJU

7.3.1. VRSTA DOGAĐAJA KOJI SE BILJEŽE

Logovi za potrebe revizije su dostupni za istraživanje u slučaju neautorizovanog pristupa informacijama sistema i za potrebe revizije. Za potrebe revizije, bilježe se sledeći tipovi događaja:

- Logovi koji su vezani za upravljanje životnim ciklusom sertifikata koji uključuje, ali nije ograničen na:
    - Registracija korisnika
    - Izdavanje sertifikata
    - Opoziv sertifikata
    - Izdavanje i objavljivanje CRL-a
- Logovi koji su vezani za administraciju sistema i upravljanje aktivnostima koje uključuju, ali nisu ograničene na:

- Pokretanje i zaustavljanje aplikacije
- Nadzor funkcionisanja sistema (upozorenja, alarmi, prekidi, greške...)
- Promjene u kritičnoj konfiguraciji sistema
- Backup i oporavak podataka

Revizorski zapisi sadrže minimum sledeće zapise:

- Identifikacija korisnika
- Tip događaja
- Vrijeme i datum događaja
- Uspješne i neuspješne događaje
- Ishod događaja
- Identifikacija podataka, komponenti sistema i resursa kojima je pristupljeno.

7.3.2. UČESTALOST PROCESUIRANJA LOGOVA

Skladištenje, zaštita i obrada revizorskih logova vrši se u realnom vremenu uz automatsko upozorenje na pojavu sigurnosnih događaja za sve kritične aktivnosti.

Za manje kritične aktivnosti vrši se periodična provjera.

7.3.3. VRIJEME ČUVANJA LOGOVA

Logovi se zadržavaju i čuvaju u periodu koji je definisan u poglavlju 7.4.

7.3.4. ZAŠTITA REVIZORSKIH LOGOVA

Logovi su adekvatno zaštićeni i vjerodostojni i mogu se predočiti kao dokazni materijal na sudu. Oni obuhvataju sledeće zaštitne mehanizme:

- Svi sistemski satovi i vremena su međusobno usklađeni tako da logovi sadrže zapise sa važećim datumom i vremenom.
- Povjerljivi podaci su isključeni ili maskirani tako da nisu sadržani u logovima.
- Implementirana je kriptografska zaštita integriteta svih kritičnih zapisa kako bi se zaštitili od bilo kakvih izmjena ili brisanja u okviru pojedinog zapisa.
- Administratori sistema ne smiju da mijenjaju ili brišu manje kritične zapise koji nisu obuhvaćeni sistemom za upravljanje revizijskim zapisima.

7.3.5. IZRADA REZERVNIH KOPIJA REVIZIJSKIH LOGOVA

Backup revizijskih logova se vrši automatski kako bi se osigurao kontinuitet poslovanja.

Postupak vraćanja sigurnosnih kopija je poznat, testiran i pouzdan i osigurava vraćanje podataka u razumnom vremenu.

Backup pravi više rezervnih kopija koje se čuvaju na primarnoj i udaljenoj lokaciji.

7.3.6. SISTEM PRIKUPLJANJA LOGOVA

Uspostavljen je sistem za upravljanje logovima i vrši automatsko skladištenje i zaštitu zapisa u realnom vremenu.

7.3.7. OBAVJEŠTAVANJE LICA KOJE JE IZAZVALO DOGAĐAJ

Lice koje je izazvalo događaj se ne obaviještava o audit aktivnosti.

7.3.8. PROCJENA RANJIVOSTI SISTEMA

GovME CA sprovodi procjene ranjivosti kao dio postupka obrade revizorskih logova.

7.4. ARHIVIRANJE PODATAKA

7.4.1. PODACI KOJI SE ARHIVIRAJU

GovME CA čuva sledeće tipove podataka:

- Informacije za reviziju specificirane u poglavlju 7.3.
- Korisničke zahtjeve
- Izvještaje o nepodudarnosti i kompromitovanjima

7.4.2. PERIOD ČUVANJA ARHIVE

GovME CA čuva revizorske logove najmanje deset (10) godina.

Zahtjevi korisnika, potvrde i GovME CA korespodencija se čuvaju minimum deset (10) godina.

7.4.3. ZAŠTITA ARHIVE

Podaci sa arhive se prikupljaju u bezbjednoj zoni. Pristup bezbjednoj zoni je dozvoljen samo ovlašćenim osobama, kako je to definisano internim procedurama za pristup.

Za arhive operativnog sistema se upotrebljavaju zaštite koje omogućava sam operativni sistem. Logovi aplikacija GovME CA sistema su zaštićeni tehnologijom kriptografije javnih kriptografskih ključeva.

7.4.4. PROCEDURA PRAVLJENJA REZERVNIH KOPIJA ARHIVE

Arhivirani materijal se čuva van primarne lokacije u sigurnom objektu gdje su fizičke i bezbjedonosne kontrole uporedive sa onima koje su implementirane na primarnoj lokaciji.

7.4.5. POTREBA ZA VREMENSKIM PEČATOM ARHIVIRANIH PODATAKA

Arhivirani podaci se obilježavaju u vrijeme njihovog nastanka koristeći sistemsko vrijeme u kom je događaj zabilježen.

Sistemi su sinhronizovani sa vremenskim izvorom koji se oslanja na UTC.

7.4.6. SISTEM SKUPLJANJA ZAPISA

GovME CA koristi interni backup za arhiviranje. Arhivirani podaci su skladišteni na offline medijumu.

7.4.7. PROCEDURE ZA PRISTUP I VERIFIKACIJU INFORMACIJA IZ ARHIVE

Pristup sačuvanim podacima je dozvoljen GovME CA službeniku na osnovu potreba ili u skladu sa važećim zakonom.

7.5. KOMPROMITOVANJE I OPOROVAK SISTEMA OD NEPREDVIĐENIH SITUACIJA

7.5.1. PROCEDURE KOD KOMPROMITOVANJA ILI INCIDENATA

GovME CA ima implementirane procedure reagovanja na bezbjednosne incidente i kvarove u skladu sa važećom zakonskom regulativom.

7.5.2. GREŠKE U RADU SISTEMA, PROGRAMSKE OPREME ILI OŠTEĆENJA PODATAKA

Procedure koje se sprovode kod kompromitacije sistema su propisane internim dokumentom, Plan neprekidnog funkcionisanja, odnosno poslovanja za vraćanje informacionog sistema i podataka u prvobitno stanje nakon incidenta (Plan za oporavak od katastrofe - Disaster Recovery Plan).

7.5.3. PRESTANAK RADA GOVME CA

U slučaju dobrovoljnog prekida poslovanja, GovME CA će:

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

7.5.4. USKLADENOST SA ZAKONODAVSTVOM

Pružanje kvalifikovane usluge elektronske preporučene dostave usklađeno je sa Zakonom o elektronskoj identifikaciji i elektronskom potpisu, podzakonskom regulativom i ovim dokumentom.

7.5.5. USAGLAŠENOST SA MEĐUNARODNIM STANDARDIMA

U procesu pružanja usluga elektronske preporučene dostave, poslovanje GovME CA je usklađeno sa sledećim 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;
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: 01-050/25-1060

U Podgorici, 11. marta 2025. godine

MINISTAR

mr Marash Dukaj