Crna Gora
Ministarstvo javne uprave

Praktična pravila o postupcima izdavanja kvalifikovanih sertifikata (GovME CA CPS – Certification Practice Statement)

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 – izrada kvalifikovanog elektronskog potpisa, odnosno kvalifikovanog elektronskog 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), 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. KRATAK 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 sljedeće usluge povjerenja:

1. izrada kvalifikovanog sertifikata za elektronski potpis;
2. izrada kvalifikovanog sertifikata za elektronski pečat.

Od 2024. godine, Ministarstvo vrši elektronsku uslugu povjerenja „izrada sertifikata za autentifikaciju internet stranica". Ova usluga je upisana u Evidenciju davalaca elektronskih usluga povjerenja. U aneksu ovog dokumenta navedene su informacije od značaja za ovu uslugu povjerenja.

Ovaj dokument predstavlja praktična pravila o postupcima izdavanja sertifikata za GovME CA, definiše način na koji GovME CA ispunjava tehničke, organizacione i proceduralne zahtjeve, koji su propisani za kvalifikovane elektronske usluge povjerenja, u skladu sa standardima koji su navedeni na kraju dokumenta. Sadrži opis pravila, procedura i uslova izdavanja i opoziva sertifikata i opisuje

tehničke, proceduralne i kadrovske politike i prakse koje GovME CA koristi u izdavanju i upravljanju sertifikatima. Numerisanje poglavlja i sekcija je isto kao u RFC 3647.

Svaka kategorija sertifikata ima dodijeljenu jedinstvenu politiku sertifikata koja reguliše kome se može izdati sertifikat za tu kategoriju, koje informacije moraju biti obezbijeđene i druge faktore koji utiču na pouzdanost sertifikata.

Ove politike, definisane u ovom dokumentu, biće identifikovane u sertifikatima izdatim u okviru ovog dokumenta time što će sadržati identifikatore objekta (OIDs) u CP ekstenziji sertifikata.

1.2. NAZIV DOKUMENTA I IDENTIFIKACIONI PODACI

Naziv dokumenta: Praktična pravila o postupcima izdavanja sertifikata (CPS – Certification Practice Statement; u daljem tekstu: GovME CA CPS).

Sledeći identifikatori objekata (OIDs) su dodijeljeni kategorijama sertifikata izdatim pod ovim GovME CA CPS:

Naziv tipa sertifikata	Identifikacija politike sertifikata (OID)	Kriptografski uređaj	Period važenja
Kvalifikovani sertifikat za napredni elektronski potpis fizičkog lica u organu državne uprave	1.3.6.1.4.1.34324.2.2.1	NE	3 godine
Kvalifikovani sertifikat za napredni elektronski pečat organa državne uprave	1.3.6.1.4.1.34324.2.2.2	NE	3 godine
Kvalifikovani sertifikat za kvalifikovani elektronski potpis fizičkog lica u organu državne uprave (token QSCD)	1.3.6.1.4.1.34324.2.2.4	DA	3 godine
Sertifikat za autentifikaciju fizičkog lica u sklopu organa državne uprave (token QSCD)	1.3.6.1.4.1.34324.2.2.5	DA	3 godine
Kvalifikovani sertifikat za kvalifikovani elektronski potpis fizičkog lica u organu državne uprave (remote signing QSCD)	1.3.6.1.4.1.34324.2.2.6	DA	3 godine

Kvalifikovani sertifikat za kvalifikovani elektronski pečat organa državne uprave (token QSCD)	1.3.6.1.4.1.34324.2.2.7	DA	3 godine
Sertifikat za OCSP servis (HSM)	1.3.6.1.4.1.34324.2.1.1	DA	5 godina
Sertifikat za uslugu vremenskog pečata (HSM)	1.3.6.1.4.1.34324.2.1.2	DA	5 godina
Sertifikat za uslugu verifikacije elektronskog potpisa i pečata (HSM)	1.3.6.1.4.1.34324.2.1.3	DA	5 godina
Sertifikat za uslugu elektronske preporučene dostave	1.3.6.1.4.1.34324.2.1.4	DA	5 godina

1.3. UČESNICI INFRASTRUKTURE JAVNIH KLJUČEVA

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

GovME CA koristi primarni CA (Root CA) koji je izdao self-signed sertifikat prilikom ceremonije generisanja glavnog ključa i jedan podređeni CA (Sub CA) za izdavanje sertifikata svim krajnjim entitetima.

Učesnici u infrastrukturi javnih ključeva Ministarstva su:

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

1.3.1. SERTIFIKACIONA TIJELA (CERTIFICATION AUTHORITIES)

Sertifikaciona tijela na koje se odnosi ovaj dokument je Korijensko sertifikaciono tijelo (GovME Root CA) i podređeno sertifikaciono tijelo (GovME Sub CA).

1.3.1.1. 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.

1.3.1.2. TIJELO ZA OPERATIVNE POSLOVE MINISTARSTVA JAVNE UPRAVE ZA PRUŽANJE ELEKTRONSKIH USLUGA POVJERENJA (OA)

GovME CA OA (Operations Authority) je odgovorno za:

- generisanje CA para ključeva, sigurno upravljanje CA privatnim ključevima i distribuciju javnih CA ključeva;
- uspostavljanje okruženja za izdavanje sertifikata;
- potpisivanje i izdavanje X.509 sertifikata koji povezuju korisnike sa njihovim javnim ključevima kao odgovor na odobrene zahtjeve za izdavanje sertifikata;
- pokretanje opoziva sertifikata, u komunikaciji sa svim tijelima GovME CA,
- opoziv sertifikata uključujući izdavanje i objavljivanje liste opozvanih sertifikata (CRL) i upravljanje OCSP servisom (Online Certificate Status Protocol);
- 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.

Za usluge koje se ne pružaju Portala GovME CA, tj. za usluge izdavanja kvalifikovanog sertifikata za napredni elektronski potpis fizičkog lica u organu državne uprave/napredni elektronski pečat organa državne uprave/kvalifikovani elektronski potpis fizičkog lica u organu državne uprave (token QSCD)/kvalifikovani elektronski pečat organa državne uprave (token QSCD), GovME CA OA odobrava zahtjev odmah nakon okončane procedure identifikacije i provjere podataka od strane GovME CA RA, a njihovu aktivaciju vrši korisnik uz pomoć GovME CA OA.

1.3.2. REGISTRACIONA TIJELA (REGISTRATION AUTHORITIES)

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

- prihvatanje ili odbijanje zahtjeva za izdavanje/opoziv sertifikata;
- komunikaciju sa naručiocima i korisnicima po osnovu podnijetih zahtjeva za izdavanje/opoziv sertifikata;
- provjeru podataka u zahtjevu za izdavanje/opoziv sertifikata naručioca;
- identifikaciju „licem u lice" korisnika za kojeg naručilac zahtijeva izdavanje sertifikata;
- 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;
- pokretanje opoziva sertifikata na zahtjev naručioca/korisnika ili na sopstvenu inicijativu, u komunikaciji sa svim tijelima GovME CA;
- izvještavanje o radu prema GovME CA PMA;
- edukaciju korisnika za korišćenje kvalifikovanih elektronskih sertifikata.

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.

1.3.3. NARUČIOCI I KORISNICI (END USERS AND SUBSCRIBERS)

Naručilac je organ državne uprave, odnosno starješina organa koji podnosi zahtjev za izdavanje elektronskog sertifikata u ime organa državne uprave za zaposlenog u tom organu.

Korisnik je zaposleni u organu državne uprave koji upotrebljava elektronski sertifikat za koji je naručiocu odobren zahtjev od strane GovME CA. Korisnik je subjekt identifikovan u sertifikatu kao vlasnik privatnog ključa povezanog sa javnim ključem koji je dat u sertifikatu.

Naručilac/korisnik snosi krajnju odgovornost za korišćenje privatnog ključa povezanog sa javnim ključem korisnika sertifikata.

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

1.3.4. TREĆA LICA (RELYING PARTIES)

Treća lica su pouzdajuće strane odnosno entiteti koji uključuju fizička lica (pojedince) i/ili pravna lica (državne institucije, ustanove, kompanije), koja se oslanjaju na kvalifikovanu uslugu izrade elektronskih sertifikata, a koja se može provjeriti na osnovu javno dostupnih informacija.

U cilju provjere validnosti elektronskog sertifikata, treća lica uvijek moraju da provjere Registar opozvanih elektronskih sertifikata (GovME CA CRL) ili putem OCSP servisa prije nego se oslone na informacije u sertifikatu.

1.3.5. OSTALI UČESNICI

Nije primjenjivo.

1.4. UPOTREBA SERTIFIKATA

1.4.1. DOZVOLJENA UPOTREBA SERTIFIKATA

Sertifikati izdati od strane GovME CA upotrebljavaju se u skladu sa Zakonom o elektronskoj identifikaciji i elektronskom potpisu u skladu sa ovim dokumentom, isključivo za potrebe poslova u okviru organa državne uprave.

1.4.2. NEDOZVOLJENA UPOTREBA SERTIFIKATA

Upotreba sertifikata koji se izdaju od strane GovME CA nije dozvoljena za korišćenje u druge svrhe, osim onih koje su definisane ovim dokumentom.

1.5. UPRAVLJANJE POLITIKAMA I PRAKTIČNIM PRAVILIMA

1.5.1. ORGANIZACIJA KOJA UPRAVLJA DOKUMENTOM

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.

1.5.2. KONTAKT 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

1.5.3. SUBJEKT KOJI UTVĐUJE USAGLAŠENOST DOKUMENTA SA ZAKONOM

Ministarstvo utvrđuje usaglašenost dokumenta sa Zakonom.

1.5.4. PROCEDURA ODOBRAVANJA DOKUMENTA

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 primjenjenih kriptografskih algoritama ili dužina kriptografskih ključeva.

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

1.6. DEFINICIJE I SKRAĆENICE

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 izraduje 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 odredenu 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
Jedinstveni sistem za elektronsku razmjenu podataka (JSERP)	Informacioni sistem kojim se omogućava i obezbjeđuje razmjena podataka između više različitih informacionih sistema državnih organa i organa državne uprave, nezavisno od njihove kompatibilnosti.

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	Oniine Sertificate Status Provider
OID	Object Identifier
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
CN	Common Name
DN	Distinguished Name
HSM	Hardware Security Module

2. OBJAVLJIVANJE I ODGOVORNOSTI ZA REPOZITORIJUM

2.1. 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 kao i objavu sertifikata sertifikacionih tijela i liste opozvanih sertifikata 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.

2.2. OBJAVA INFORMACIJA O SERTIFIKATIMA

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 izdavanje/opoziv sertifikata;
- ostale javne informacije vezane za rad sertifikacionog tijela GovME CA.

2.3. VRIJEME I UČESTALOST OBJAVLJIVANJA

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.

Učestalost objave CRL za sertifikate koje izdaje GovME CA specificirano je u Sekciji 4.9.7. ovog dokumenta.

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

2.4. KONTROLA PRISTUPA DO REPOZITORIJUMA

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 obezbjedivanje 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.

3. IDENTIFIKACIJA I AUTENTIFIKACIJA

Procedure identifikacije i autentifikacije krajnjih korisnika navedene u ovom dokumentu se odnose na sertifikate koje izdaje GovME CA.

3.1. DODJELJIVANJE IMENA

3.1.1. VRSTE IMENA

Atributi CA sertifikata i sertifikata izdatog naručiocu su u formi X.501 jedinstvenog imena (Distinguished Name - DN). DN je upisan u formi X.501 UTF8String ili štampanog stringa i mora biti prisutan u svim izdatim sertifikatima.

3.1.2. POTREBA ZA REALNIM IMENIMA

Skup atributa u jedinstvenom imenu upisanim u polje Subject sertifikata, na jedinstven način identifikuje vlasnika sertifikata i ima realnu vrijednost.

Tip atributa serijski broj, kada je prikazan, koristi se za razlikovanje imena u kojima bi polje Subject inače bilo identično.

3.1.3. ANONIMNOST KORISNIKA I UPOTREBA PSEUDONIMA

GovME CA ne podržava anonimnost korisnika. Takođe sertifikaciono tijelo ne podržava ni pseudonime za korisnike sertifikata. U sertifikate koje izdaje GovME CA ne upisuju se pseudonimi korisnika.

3.1.4. PRAVILA ZA PRIKAZIVANJE RAZNIH FORMI IMENA

Polje Subject je definisano kao X.501 tip imena (x.500 Distinguished Name) u skladu sa RFC 5280. x.500 jedinstveno ime za GovME CA ima sledeći format:

Za fizičko lice u organu državne uprave:

Komponente jedinstvenog imena	Vrijednost
Country (C =)	ISO3155-1 alpha-2 oznaka države
Organization (O =)	Registrovani puni ili skraćeni naziv organa državne uprave koje je povezano sa korisnikom sertifikata (fizičkim licem)

organizationIdentifier	Registrovani poreski identifikacioni broj (PIB) organa državne uprave u formatu "VATDvoslovna ISO3155-1 oznaka države u kojoj se nalazi organ državne uprave-PIB"
Organizational Unit (OU=)	opcionalno
Given name	Ime potpisinka
Surname	Prezime potpisnika
Common Name (CN=)	Ime + Prezime + tip sertifikata (Autentifikacija ili Potpis)
Serial Number (serialNumber=)	Jedinstveni serijski broj (osmocifreni jedinstveni identifikator) korisnika definisan članom 4 Uredbe o načinu određivanja identifikacionog broja potpisnika kvalifikovanog elektornskog sertifikata za potpis sa prefiksom PNOME, kojeg određuje organ državne uprave nadležan za unutrašnje poslove

Organ državne uprave:

Komponente jedinstvenog imena	Vrijednost
Country (C =)	ISO3155-1 alpha-2 oznaka države
Organization (O =)	Registrovani puni ili skraćeni naziv organa državne uprave
organizationIdentifier	Registrovani poreski identifikacioni broj (PIB) organa državne uprave u formatu "VATDvoslovna ISO3155-1 oznaka države u kojoj se nalazi organ državne uprave-PIB"
Organizational Unit (OU=)	opcionalno
Common Name (CN=)	Vrijednost atributa commonName može sadržati ime kojim subjekt predstavlja sebe + tip sertifikata ili JSERP identifikator domena
Serial Number (serialNumber=)	JSERP identifikator subjekta/člana (alfanumerički zapis)
BussinessCategory	JSERP kategorija subjekta/člana – tip organizacije

3.1.5. JEDINSTVENOST IMENA

GovME CA za svakog vlasnika sertifikata određuje jedinstveno ime (DN), kao što je definisano u poglavlju 3.1.2 i 3.1.4 da osigura nedvosmislenost i jedinstvenost imena.

Set atributa u jedinstvenom imenu (DN) predstavlja svakog vlasnika sertifikata.

3.1.6. PREPOZNAVANJE, AUTENTIFIKACIJA I ULOGA ZAŠTITNIH ZNAKOVA

GovME CA će preduzimati razumne mjere za rješavanje sporova koji mogu nastati zbog dodjele imena, na primjer GovME CA može kontaktirati podnosioca zahtjeva za izdavanje sertifikata i dogovoriti da se traženo ime u sertifikatu promjeni tako da se razlikuje od imena u sertifikatu već izdatom drugom korisniku.

GovME CA zadržava pravo da po svojoj procjeni, odbije zahtjev, ponovo izda ili opozove sertifikat.

3.2. INICIJALNA VALIDACIJA IDENTITETA

3.2.1. METODA ZA DOKAZIVANJE VLASNIŠTVA PRIVATNOG KLJUČA

Dokaz o posjedovanju privatnog ključa naručioca je osiguran putem bezbjedne komunikacije između CA aplikacije i PKI klijentske aplikacije koristeći PKCS#10 u skladu sa RSA PKCS#10 Certification Request Syntax standardom.

U ovom slučaju kada su privatni ključ i sertifikat generisani od strane CA, tada je kartica sa ključem i pinom poslata onome ko je zahtijevao sertifikat, što osigurava da naručilac/korisnik dobije privatni ključ. Kada je u pitanju Kvalifikovani sertifikat za kvalifikovani elektronski potpis fizičkog lica u organu državne uprave (remote signing QSCD), privatni ključ se čuva na HSM uređaju – hardverskom uređaju koji je dizajniran za upravljanje i zaštitu kriptografskih ključeva.

3.2.2. 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.

3.2.3. PROVJERA IDENTITETA FIZIČKOG LICA U ORGANU DRŽAVNE UPRAVE

Fizičko lice za koje naručilac zahtijeva izdavanje elektronskog sertifikata je zaposleni u organu državne uprave.

Provjera identiteta vrši se po principu "licem u lice", dolaskom u prostorije Ministarstva na identifikaciju.

On 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).

Procedura provjere identiteta i izdavanje sertifikata opisana je u poglavlju 4.1.2 Proces obrade zahtjeva i odgovornosti.

3.2.4. PODACI O KORISNICIMA KOJI SE NE PROVJERAVAJU

Svi podaci koju su opisani u poglavlju 3.1.4 su verifikovani u procesu registracije.

GovME CA RA ne provjerava podatke koji nijesu navedeni u poglavlju 3.2.3.

3.2.5. VALIDACIJA OVLAŠĆENJA

Nije primjenljivo.

3.2.6. KRITERIJUMI ZA INTEROPERABILNOST

Nije primjenljivo.

3.3. PROVJERA IDENTITETA KOD ZAHTJEVA ZA OBNOVU SERTIFIKATA

3.3.1. PROVJERA IDENTITETA KOD RUTINSKE OBNOVE SERTIFIKATA

Obnova sertifikata predstavlja izradu novog sertifikata, što obuhvata proceduru provjere identiteta definisanu kao što je specificirano u poglavlju 3.2.2. Provjera identiteta organa državne uprave i 3.2.3. Provjera identiteta fizičkog lica u organu državne uprave.

3.3.2. PROVJERA IDENTITETA KOD OBNOVE SERTIFIKATA NAKON OPOZIVA

Obnova sertifikata nakon opoziva predstavlja izradu novog sertifikata, što obuhvata proceduru provjere identiteta definisanu kao što je specificirano u poglavlju 3.2.2. Provjera identiteta organa državne uprave i 3.2.3. Provjera identiteta fizičkog lica u organu državne uprave.

3.4. IDENTIFIKACIJA I AUTENTIFIKACIJA KOD ZAHTJEVA ZA OPOZIV

Zahtjev za opoziv se podnosi u elektronskoj formi, u situaciji:

- kada je korisniku prestao radni odnos u organu;
- kada je došlo do potrebe za promjenom informacija u elektronskom sertifikatu;
- kada je prestala potreba za korišćenjem elektronskog sertifikata;
- kada postoji sumnja da je privatni ključ koji odgovara elektronskom sertifikatu kompromitovan;
- kada naručilac procijeni da je potrebno opozvati elektronski sertifikat.

GovME CA vrši opoziv elektronskih sertifikata shodno podnesenom zahtjevu za opoziv. Izuzetno, kada se radi o elektronskom sertifikatu koji je aktivan na Portalu GovME CA, korisnik može samostalno izvršiti njegov opoziv.

Naručilac ili korisnik sertifikata koji zahtijevaju opoziv elektronskim putem, autentifikuju se na osnovu svog elektronskog potpisa koji je aktivan.

Provjera zahtjeva za opoziv sertifikata se radi na osnovu dostavljenih informacija, kao i informacija koje se nalaze u evidenciji korisnika.

4. ŽIVOTNI CIKLUS UPRAVLJANJA SERTIFIKATIMA

4.1. APLICIRANJE ZA IZDAVANJE SERTIFIKATA

4.1.1. KO MOŽE APLICIRATI ZA IZDAVANJE SERTIFIKAT

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

4.1.2. PROCES OBRADE ZAHTJEVA I ODGOVORNOSTI

GovME CA vrši izdavanje sertifikata nakon provjere identiteta naručioca i uspješnog završetka procesa registracije korisnika.

Koraci prilikom izdavanja sertifikata su sljedeći:

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 elektronskog sertifikata.
        - 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 se ne pružaju Portala GovME CA, tj. za usluge izdavanja kvalifikovanog sertifikata za napredni elektronski potpis fizičkog lica u organu državne uprave/napredni elektronski pečat organa državne uprave/kvalifikovani elektronski potpis fizičkog lica u organu državne uprave (token QSCD)/kvalifikovani elektronski pečat organa državne uprave (token QSCD), GovME CA OA odobrava zahtjev odmah nakon okončane procedure identifikacije i provjere podataka od strane GovME CA RA, a njihovu aktivaciju vrši korisnik uz pomoć GovME CA OA.
- 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").

4.2. PROCESUIRANJE ZAHTJEVA ZA IZDAVANJE SERTIFIKATA

4.2.1. POSTUPAK IDENTIFIKACIJE I AUTENTIFIKACIJE

GovME CA izvršava identifikaciju i autentifikaciju kao što je definisano u poglavljima 3.2.2 Provjera identiteta organa državne uprave i 3.2.3 Provjera identiteta fizičkog lica u organu državne uprave.

4.2.2. ODOBRAVANJE ILI ODBIJANJE ZAHTJEVA ZA IZDAVANJE SERTIFIKATA

Odobravanje ili odbijanje zahtjeva za izdavanje sertifikata vrši se u skladu sa procedurom opisanom u poglavlji 4.1.2 – Proces obrade zahtjeva i odgovornosti.

4.2.3. VRIJEME ZA OBRADU ZAHTJEVA

Inicijalna obrada zahtjeva počinje od trenutka dodjeljivanja predmeta kroz eDMS službeniku GovME CA RA.

Zahtjevi će biti inicijalno procesuirani od strane GovME CA RA u okviru pet radnih dana od prijema zahtjeva.

Maksimalno ukupno vrijeme za kompletnu obradu zahtjeva je 10 radnih dana, pod uslovom da su svi dostavljeni podaci tačni i da je dokumentacija kompletirana.

4.3. IZDAVANJE SERTIFIKATA

4.3.1. AKTIVNOSTI CA U FAZI IZDAVANJA SERTIFIKATA

Obaveza GovME CA je da postupa u skladu sa procedurom opisanom u poglavlju 4.1.2 – Proces obrade zahtjeva i odgovornosti.

4.3.2. OBAVJEŠTAVANJE KORISNIKA O IZDAVANJU SERTIFIKATA OD STRANE CA

Naručioci će biti blagovremeno obaviješteni o svim neophodnim informacijama u vezi izdavanja sertifikata, shodno proceduri opisanoj u poglavlju 4.1.2 – Proces obrade zahtjeva i odgovornosti.

4.4. PRIHVATANJE SERTIFIKATA

4.4.1. POSTUPAK PRIHVATANJA SERTIFIKATA OD STRANE KORISNIKA

Podnosilac zahtjeva će dobiti sve sertifikate za vrijeme trajanja procesa izdavanja sertifikata. Dodatna potvrda prihvatanja sertifikata nije potrebna.

U slučaju neuspješnog preuzimanja, odnosno aktivacije, korisnik mora prijaviti problem GovME CA.

4.4.2. OBJAVLJIVANJE SERTIFIKATA OD STRANE CA

Nije primjenjivo.

4.4.3. OBAVJEŠTAVANJE OSTALIH UČESNIKA O IZDAVANJU SERTIFIKATA

GovME CA neće obavještavati ostale entitete.

4.5. UPOTREBA PARA KLJUČEVA I SERTIFIKATA

4.5.1. UPOTREBA PARA KLJUČEVA I SERTIFIKATA OD STRANE KORISNIKA

Naručioci moraju iskoristiti elektronske sertifikate u skladu sa zahtjevima navedenim u poglavlju 1.4. Privatne ključeve mogu da koriste samo vlasnici kojima je izdat elektronski sertifikat pripadajućeg javnog ključa.
GovME CA izdaje sertifikate koji mogu podržati više namjena za upotrebu ključa. Podrška je obezbijeđena upotrebom odgovarajućih ekstenzija za namjenu ključa.

Naručilac treba da koristi sertifikat u skladu sa keyUsage i extKeyUsage x.509 ekstenzijama sertifikata i za namjene definisane u poglavlju 1.4.1 Dozvoljena upotreba sertifikata.
Naručilac mora čuvati privatni ključ i preduzeti sve mjere opreza kako bi se spriječilo otkrivanje i neovlašćeno korišćenje.
Nakon isteka validnosti sertifikata ili u slučaju opoziva sertifikata, dodijeljeni privatni ključ se smatra nevalidnim.

4.5.2. UPOTREBA PARA KLJUČEVA I SERTIFIKATA OD STRANE TREĆIH LICA

Sertifikati izdati od strane GovME CA upotrebljavaju se u skladu sa Zakonom o elektronskoj identifikaciji i elektronskom potpisu i u skladu sa ovim dokumentom, isključivo za potrebe poslova u okviru organa državne uprave.

U cilju provjere validnosti elektronskog sertifikata, treća lica uvijek moraju da izvrše:

- provjeru perioda validnosti sertifikata,
- provjeru lanca sertifikata,
- provjeru opozvanosti sertifikata upotrebom OCSP servisa ili provjeru opozvanosti sertifikata upotrebom liste opozvanih sertifikata.

U slučaju sumnje ili poznate zloupotrebe bilo kojeg sertifikata kojeg je izdao GovME CA, treća lica su dužna o tome obavijestiti GovME CA.

4.6. OBNOVA SERTIFIKATA (BEZ PROMJENE KLJUČA)

Obnova sertifikata nije dozvoljena i podržana od strane GovME CA.

4.6.1. OKOLNOSTI POD KOJIMA SE MOŽE OBNOVITI SERTIFIKAT

Nije podržano, kao što je navedeno u 4.6 Obnova sertifikata.

4.6.2. KO MOŽE TRAŽITI OBNOVU

Nije podržano, kao što je navedeno u 4.6 Obnova sertifikata.

4.6.3. PROCES OBRADE ZAHTJEVA ZA OBNOVU SERTIFIKATA

Nije podržano kao što je navedeno u 4.6 Obnova sertifikata.

4.6.4. OBAVJEŠTAVANJE KORISNIKA O OBNOVI SERTIFIKATA

Nije podržano kao što je navedeno u 4.6 Obnova sertifikata.

4.6.5. POSTUPAK POTVRDE PRIHVATANJA OBNOVLJENOG SERTIFIKATA

Nije podržano kao što je navedeno u 4.6 Obnova sertifikata.

4.6.6. OBJAVA OBNOVLJENOG SERTIFIKATA OD STRANE CA

Nije podržano kao što je navedeno u 4.6 Obnova sertifikata.

4.6.7. OBAVJEŠTAVANJE O IZDAVANJU OBNOVLJENOG SERTIFIKATA OD STRANE CA DRUGIM LICIMA

Nije podržano kao što je navedeno u 4.6 Obnova sertifikata.

4.7. OBNOVA SERTIFIKATA (UZ GENERISANJE NOVOG KLJUČA)

Obnova sertifikata je proces u kom GovME CA izdaje novi sertifikat korisniku. Novi sertifikat sadrži iste identifikacione oznake kao stari sertifikat i novi javni ključ.

4.7.1. OKOLNOSTI POD KOJIMA SE MOŽE OBNOVITI SERTIFIKAT

Obnova elektronskog sertifikata predstavlja izradu novog sertifikata.

Izrada novog elektronskog sertifikata se vrši na osnovu zahtjeva korisnika i to:

- nakon opoziva sertifikata,
- prije isteka elektronskog sertifikata,
- u slučaju promjene podataka u elektronskog sertifikatu.

4.7.2. KO MOŽE TRAŽITI OBNOVU SERTIFIKATA UZ GENERISANJE NOVOG KLJUČA

Izdavanje novog elektronskog sertifikata može zatražiti naručilac.

4.7.3. PROCES OBRADE ZAHTJEVA ZA OBNOVU SERTIFIKATA

Obnova elektronskog sertifikata predstavlja izradu novog sertifikata. Izdavanje se vrši u skladu sa procedurom definisanom u poglavlju 4.1.2 - Proces obrade zahtjeva i odgovornosti.

4.7.4. OBAVJEŠTAVANJE KORISNIKA O IZDAVANJU SERTIFIKATA

Kao što je opisano u poglavlju 4.3.2. Obavještavanje korisnika o izdavanju sertifikata od strane CA.

4.7.5. POSTUPAK POTVRDE PRIHVATANJA OBNOVLJENOG SERTIFIKATA UZ GENERISANJE NOVOG KLJUČA

Kao što je opisano u poglavlju 4.4.1. Postupak prihvatanja sertifikata od strane korisnika.

4.7.6. OBJAVA OBNOVLJENOG SERTIFIKATA UZ GENERISANJE NOVOG KLJUČA OD STRANE CA

Kao što je opisano u poglavlju 4.4.2. Objavljivanje sertifikata od strane CA.

4.7.7. OBAVJEŠTAVANJE O IZDAVANJU OBNOVLJENOG SERTIFIKATA OD STRANE CA DRUGIM LICIMA

Kao što je opisano u poglavlju 4.4.3. Obavještavanje ostalih učesnika o izdavanju sertifikata.

4.8. PROMJENA SERTIFIKATA

Korisnik elektronskog sertifikata može da zahtijeva promjenu informacija u sertifikatu, ali taj proces predstavlja izdavanje novog sertifikata i obrađuje se kao inicijalni zahtjev za izdavanje sertifikata. GovME CA ne vrši modifikacije sertifikata na već izdatim elektronskim sertifikatima, već isključivo vrši izradu novog.

4.8.1. OKOLNOSTI ZA PROMJENU SERTIFIKATA

Naručilac sertifikata može zahtijevati promjenu elektronskog sertifikata u slučaju:

- da je GovME CA greškom izdalo sertifikat sa nevalidnim podacima u sertifikatu,
- da je došlo do promjene podataka koji se nalaze u sertifikatu,
- drugi razlozi.

4.8.2. KO MOŽE ZAHTIJEVATI PROMJENU SERTIFIKATA

U slučaju da je neophodna promjena sertifikata, to isključivo može zahtijevati naručilac koji je zahtijevao inicijalno izdavanje sertifikata.

4.8.3. PROCESUIRANJE ZAHTJEVA ZA PROMJENU SERTIFIKATA

Promjena sertifikata se obrađuje kao i inicijalno izđavanje sertifikata.

4.8.4. OBAVJEŠTAVANJE KORISNIKA O IZDAVANJU IZMIJENJENOG SERTIFIKATA

Obavještavanje korisnika o izdavanju sertifikata od strane GovME CA se obavlja na način opisan u poglavlju 4.3.2.

4.8.5. POSTUPAK POTVRDE PRIHVATANJA PROMIJENJENOG SERTIFIKATA

Postupak prihvatanja sertifikata od strane korisnika kao što je opisano u poglavlju 4.4.1.

4.8.6. OBJAVLJIVANJE PROMIJENJENOG SERTIFIKATA OD STRANE CA

Objavljivanje sertifikata od strane CA se obavlja kao što je opisano u poglavlju 4.4.2.

4.8.7. OBAVJEŠTAVANJE DRUGIH LICA O PROMJENI SERTIFIKATA OD STRANE CA

Obavještavanje ostalih učesnika o izdavanju sertifikata se obavlja na način opisan u poglavlju 4.4.3.

4.9. OPOZIV I SUSPENZIJA SERTIFIKATA

4.9.1. OKOLNOSTI ZA OPOZIV SERTIFIKATA

U skladu sa Zakonom o elektronskoj identifikaciji i elektronskom potpisu, GovME CA vrši opoziv izdatog sertifikata u sljedećim slučajevima:

- ukoliko je to traženo od strane naručioca ili korisnika elektronskog sertifikata;
- ukoliko se utvrdi da je podatak u elektronskom sertifikatu pogrešan ili je elektronski sertifikat izdat na osnovu pogrešnih podataka;
- ukoliko GovME CA primi obavještenje da je vlasnik elektronskog sertifikata preminuo, izgubio poslovnu sposobnost ili su izmijenjene činjenice koje imaju veliki uticaj na validnost elektronskog sertifikata;
- ukoliko se utvrdi da je korisnik završio radni angažman u organu državne uprave;
- ukoliko se utvrdi da su podaci za izradu elektronskog potpisa ili informacioni sistem potpisnika ugroženi na način koji utiče na pouzdanost i bezbjednost izrade elektronskog potpisa ili kad treće lice te podatke koristi na neprimjeren način;
- ukoliko se utvrdi da su podaci za provjeru elektronskog potpisa ili informacioni sistem davaoca elektronskih usluga povjerenja ugroženi na način koji utiče na bezbjednost i pouzdanost certifikata;
- ukoliko GovME CA prestaje sa radom ili mu je rad zabranjen, a izdatim elektronskim sertifikatima nije istekao rok važenja;
- istekne rok važenja certifikata;

- ukoliko je kompromitovan neki od aktivacionih podataka, kao što su lozinka ili PIN, koji se koriste za zaštitu privatnog ključa ili se sumnja da je kompromitovan;
- ukoliko se desi da je kompromitovan privatni ključ koji je dodijeljen sa sertifikatom, ili se sumnja da je kompromitovan;
- ukoliko naručilac ili vlasnik sertifikata krše odredbe definisane GovME CA politikom sertifkata ili primjenjivim zakonom.
- ukoliko primi sudsku odluku ili upravni akt koji se odnose na važenje certifikata ili ukoliko postoje drugi pravni razlozi predviđeni internim aktima.

4.9.2. KO MOŽE ZAHTIJEVATI OPOZIV SERTIFIKATA

Opoziv sertifikata može zahtijevati:

- Naručilac ili korisnik sertifikata
- GovME CA PMA
- GovME CA OA
- GovME CA RA
- Organi prepoznati zakonom
- Treća lica

4.9.3. PROCEDURA OPOZIVA SERTIFIKATA

U situaciji kada je neophodno izvršiti opoziv sertifikata usljed ispunjenja uslova za opoziv iz stavova navedenih u ovom poglavlju, naručilac ili korisnik sertifikata dužni su da u najkraćem mogućem roku kontaktiraju ovlašćenog službenika ili GovME CA RA radi dostavljanja Zahtjeva za opoziv.

Zahtjev za opoziv sertifkata je identifikovan kao što je opisano u poglavlju 3.4 Identifikacija i autentifikacija kod zahtjeva za opoziv.

Opozivom sertifikata njegov serijski broj pojavljuje se u listi opozvanih sertifikata, a njegov status putem OCSP servisa postaje opozvan.

4.9.4. VRIJEME PREDVIĐENO ZA PODNOŠENJE ZAHTJEVA ZA OPOZIV

Subjekat koji je svjestan okolnosti koje zahtijevaju opoziv sertifikata mora zatražiti opoziv u najkraćem roku i bez nepotrebnog odlaganja.

4.9.5. VRIJEME ZA KOJE CA MORA PROCESUIRATI ZAHTJEV ZA OPOZIV

U slučaju opoziva sertifkat će biti objavljen u CRL i OSCP najkasnije 24h od trenutka kada je GovME CA primio validan zahtjev za opoziv.

4.9.6. OBAVEZA PROVJERE REGISTRA OPOZVANIH SERTIFIKATA OD STRANE TREĆIH LICA

Da bi se uvjerila u validnost samog sertifikata, treća lica su u obavezi da provjere GovME CA CRL ili OCSP prije upotrebe bilo kojeg sertifkata izdatog od strane GovME CA.

U slučaju da ne postoji mogućnost utvrdivanja statusa sertifikata zbog otkaza sistema ili servisa, nijedan GovME CA sertifikat ne treba da bude prihvaćen kao validan.

Treća strana će provjeriti CRL ili OCSP odgovor tako što će provjeriti digitalni potpis sa pridruženim GovME CA sertifkatom i period validnosti sertifikata.

4.9.7. UČESTALOST IZDAVANJA REGISTRA OPOZVANIH SERTIFIKATA (CRL)

Kada se sertifikat opozove, ažuriranje CRL se vrši odmah ili u najkraćem roku nakon što je obraden validni zahtjev za opoziv.

4.9.8. MAKSIMALNA ZAKAŠNJENJA U OBJAVI REGISTRA OPOZVANIH SERTIFIKATA (CRL)

Nije primjenjivo (vidjeti poglavlje 4.9.7).

4.9.9. DOSTUPNOST ON-LINE PROVJERE STATUSA OPOZVANIH SERTIFIKATA

OCSP servis obezbjeđuje CA. Lokacija servisa je označena sa URL-om uključenim u svakom izdatom sertifikatu. Adresa OCSP je https://ocsp.ca.gov.me.

4.9.10. OBAVEZA ON-LINE PROVJERE OPOZVANIH SERTIFIKATA

Pogledaj poglavlju 4.5.2. Upotreba para ključeva i sertifikata od trećih lica.

4.9.11. OSTALE FORME OBJAVLJIVANJA OPOZVANIH SERTIFIKATA KOJE SU DOSTUPNE

Nije primjenjivo.

4.9.12. POSEBNI ZAHTJEVI U SLUČAJU KOMPROMITOVANJA KLJUČA

Nema posebnih zahtjeva potrebnih u slučaju kompromitovanja privatnog ključa vlasnika sertifikata.

4.9.13. OKOLNOSTI ZA SUSPENZIJU SERTIFIKATA

Nije primjenjivo.

4.9.14. KO MOŽE ZAHTIJEVATI SUSPENZIJU SERTIFIKATA

Nije primjenjivo.

4.9.15. PROCEDURA ZA SUSPENZIJU SERTIFIKATA

Nije primjenjivo.

4.9.16. OGRANIČENJA PERIODA TRAJANJA SUSPENZIJE

Nije primjenjivo.

4.10. SERVISI ZA STATUS SERTIFIKATA

4.10.1. OPERATIVNE KARAKTERISTIKE

GovME CA daje infromacije o statusu sertifikata putem OCSP sevisa i objave CRL.

CRL se objavljuje ne Repozitorijumu. Tačna lokacija (http URLs) se objavljuje uz pomoć X.509 CRL Distribution Point ekstenzije. Lokacija OCSP servisa je označena sa URL-om uključenim u svakom izdatom sertifikatu.

4.10.2. RASPOLOŽIVOST SERVISA

GovME CA garantuje da je status sertifikata raspoloziv 24/7 uz maksimalne neplanirane prekide rada od (5) dana u godini.

4.10.3. OPERATIVNE KARAKTERISTIKE

Nije primjenjivo.

4.11. PREKID DOGOVORA/UGOVORA/SPORAZUMA

Sertifikat prestaje da važi nakon isteka korisnikovog sertifikata, ili u slučaju da dođe do opoziva sertifikata. GovME CA čuva dokumenta vezana za korisnika, sertifikate i status sertifikata najmanje 10 godina od trenutka isticanja posljednjeg sertifikata.

Organ državne uprave koji je zahtijevao sertifikat za svog zaposlenog mora obavijestiti GovME CA da je radni odnos prestao ili da više ne postoji potreba za sertifikatom.

4.12. DEPONOVANJE (ESCROW) I POVRATAK KLJUČA

Nije primjenjivo.

4.12.1. POLITIKE I PRAKSE ZA DEPONOVANJE (ESCROW) I POVRATAK KLJUČA

Nije primjenjivo.

4.12.2. POLITIKA I PRAKSA ZA UPRAVLJANJE ENKAPSULACIJE I OPORAVKA SESIJE KLJUČA

Nije primjenjivo.

5. OBJEKTI, UPRAVLJANJE I OPERATIVNE KONTROLE

5.1. FIZIČKA ZAŠTITA

5.1.1. LOKACIJA I KONSTRUKCIJA

Definisano u dokumentu "Plan fizičke zaštite objekata, odnosno prostora za smještaj i funkcionisanje računarske i komunikacione opreme".

5.1.2. KONTROLA FIZIČKOG PRISTUPA

Definisano u dokumentu "Plan fizičke zaštite objekata, odnosno prostora za smještaj i funkcionisanje računarske i komunikacione opreme".

5.1.3. NAPAJANJE I KLIMATIZACIJA

Definisano u dokumentu "Plan fizičke zaštite objekata, odnosno prostora za smještaj i funkcionisanje računarske i komunikacione opreme".

5.1.4. ZAŠTITA OD POPLAVE

Definisano u dokumentu "Plan fizičke zaštite objekata, odnosno prostora za smještaj i funkcionisanje računarske i komunikacione opreme".

5.1.5. PREVENCIJA I ZAŠTITA OD POŽARA

Definisano u dokumentu "Plan fizičke zaštite objekata, odnosno prostora za smještaj i funkcionisanje računarske i komunikacione opreme".

5.1.6. SMJEŠTANJE MEDIJA

Definisano u dokumentu "Plan fizičke zaštite objekata, odnosno prostora za smještaj i funkcionisanje računarske i komunikacione opreme".

5.1.7. 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.

5.1.8. 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.

5.2. PROCEDURALNE KONTROLE

5.2.1. POVJERLJIVE ULOGA OSOBLJA CA

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 su:

Oblast	Uloga	Minimalni broj osoba	Osoba
Upravljanje setifikatima	HSM Administrator	4	A, B, C, D
	HSM kripto korisnik	2	A, B
	CA Administrator	1	G
	CA Superadmin	1	D
	RA Administrator	1	J
	SCD Administrator	1	I
	Root CA/ unix root, Issuing CA / unix root	2	B, D
Sigurnost i kontrola	HSM administrator particije	1	E
	Čuvar bezbjednosnog sefa	1	H
	Interni revizor	1	F

5.2.2. POTREBAN BROJ OSOBA ZA OPERATIVNE POSTUPKE

Za izvršenje sljedećih zadataka potrebna su odobrenja dva (2) korisnika:

- HSM inicijalizacija
- Inicijalno generisanje CA sertifikata i ključa
- Backup CA ključa i vraćanje
- Ažuriranje CA ključa i sertifikata
- Aktivacija CA ključa

Jedna osoba može izvršiti sve ostale zadatke. Sve aktivnosti koje obavljaju pouzdani nosioci uloga se evidentiraju i provjeravaju.

5.2.3. IDENTIFIKACIJA I AUTENTIFIKACIJA OSOBLJA ZA POJEDINE ULOGE

Svaka osoba sa povjerljivom CA ulogom se identifikuje i autentifikuje 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.

5.2.4. POVJERLJIVE ULOGE KOJE MORAJU IMATI ODVOJENE DUŽNOSTI

Sistem administrator mora imati potrebna prava za instalaciju, konfiguraciju i upravljanje CA računarskim hardverom i softverom. 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.

5.3. KONTROLA OSOBLJA

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

5.3.1. KVALIFIKACIJE, ISKUSTVA I PROVJERE

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.

5.3.2. PROCEDURA POZADINSKIH I BEZBJEDONOSNIH PROVJERA

Prije početka rada na poslovima GovME CA, Ministarstvo sprovodi odgovarajuće provjere kandidata u cilju procjene njihove stručnosti, sposobnosti i pouzdanosti u skladu s potrebama poslova GovME CA.

5.3.3. OBUKE

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.

5.3.4. UČESTALOST PONOVNIH OBUKA

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.

5.3.5. UČESTALOST I REDOSLJED ROTACIJE ULOGA

Rotacija uloga nije implementirana.

5.3.6. SANKCIONISANJA ZA NEOVLAŠĆENE AKTIVNOSTI

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

5.3.7. KRITERIJUMI ZA OSOBLJE ANGAŽOVANO PO UGOVORU O DJELU

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

5.3.8. DOKUMENTACIJA ZA POTREBE OSOBLJA

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 CPS-u.

5.4. PROCEDURA UPRAVLJANJA LOGOVIMA ZA REVIZIJU

5.4.1. 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.

5.4.2. 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.

5.4.3. VRIJEME ČUVANJA LOGOVA

Logovi se zadržavaju i čuvaju u periodu koji je definisan u poglavlju 5.5.

5.4.4. ZAŠTITA REVIZIJSKIH 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.

5.4.5. 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.

5.4.6. SISTEM PRIKUPLJANJA LOGOVA

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

5.4.7. OBAVJEŠTAVANJE LICA KOJE JE IZAZVALO DOGAĐAJ

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

5.4.8. PROCJENA RANJIVOSTI SISTEMA

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

5.5. ARHIVIRANJE PODATAKA

5.5.1. PODACI KOJI SE ARHIVIRAJU

GovME CA čuva sledeće tipove podataka:

- Informacije za reviziju specificirane u poglavlju 5.4. Procedura upravljanja logovima za reviziju;
- Korisničke zahtjeve;
- Sertifikate, status opozvanog sertifikata;
- Izvještaje o nepodudarnosti i kompromitovanjima.

5.5.2. PERIOD ČUVANJA PODATAKA U ARHIVI

GovME CA čuva revizorske logove najmanje 10 godina nakon isteka sertifikata. Status opoziva sertifikata se čuvaju najmanje 10 godina nakon isteka sertifikata. Zahtjevi korisnika i CA korespodencija se čuvaju minimum 10 godina nakon isteka sertifikata.

5.5.3. 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.

5.5.4. PROCEDURA ČUVANJA REZERVNIH KOPIJA ARHIVIRANIH PODATAKA

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.

5.5.5. POTREBA ZA VREMENSKIM PEČATOM ARHIVIRANIH PODATAKA

Arhivirani podaci se obilježavaju u vrijeme njihovog nastanka koristeći sistemsko vrijeme u kom je događaj zabilježen. Svi sistemi su sinhronizovani sa vremenskim izvorom koji se oslanja na UTC.

5.5.6. SISTEM ARHIVIRANJA (INTERNI ILI EKSTERNI)

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

5.5.7. PROCEDURA ZA PRISTUP I VERIFIKACIJU ARHIVIRANIH PODATAKA

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

5.6. OBNOVA CA KLJUČA

Obnova privatnog ključa će se izvršiti prije isteka sertifikata. Nakon promjene privatnog ključa, novi javni ključ biće dostupan vlasnicima sertifikata putem javnog repozitorijuma.

5.7. KOMPROMITOVANJE I OPOROVAK SISTEMA OD NEPREDVIĐENIH SITUACIJA

5.7.1. PROCEDURE KOD KOMPROMITOVANJA ILI INCIDENATA

GovME CA ima implementirane procedure reagovanja na bezbjednosne incidente i kvarove u skladu sa pozitivnim zakonskim pravilima.

5.7.2. 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).

5.7.3. KOMPROMITOVANJE PRIVATNOG KLJUČA SERTIFIKACIONIOG TIJELA

U slučaju da je privatni ključ za potpisivanje kompromitovan, CA će opozvati sve korisničke sertifikate koji nijesu istekli i sertifikate koji su trenutno u upotrebi i obustaviti izdavanje novih sertifikata upotrebom kompromitovanog ključa.

5.7.4. KONTINUITET POSLOVANJA U SLUČAJU PRIRODNE I DRUGE KATASTROFE

Nakon prirodne ili neke druge katastrofe, CA funkcionalnosti i procesi će biti ponovo uspostavljeni na rezervnoj lokaciji koristeći sigurnosne kopije podataka koje se svakodnevno preuzimaju sa primarne lokacije. GovME CA će preduzeti sve razumne mjere tako da vrijeme oporavka ne bude duže od 10 radnih dana.

5.8. PRESTANAK RADA CA ILI RA

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;
- 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.

6. TEHNIČKO BEZBJEDONOSNE KONTROLE

U ovom poglavlju su definisane mjere, postupci i metodi, kao i druge tehničke bezbjednosne kontrole koje se primjenjuju prilikom upravljanja ključevima i sertifikatima.

Tehničke kontrole uključuju životni ciklus bezbjednosnih kontrola kao i operativne bezbjednosne kontrole.

6.1. FORMIRANJE PARA KLJUČEVA I INSTALACIJA

6.1.1. FORMIRANJE PARA KLJUČEVA

Prilikom generisanja i upravljanja sopstvenim privatnim ključevima GovME CA primjenjuje odredbe Zakona o elektronskoj identifikaciji i elektronskom potpisu, podzakonskih akata i propisanih standarda.

Privatni kriptografski ključevi za potpisivanje stvoreni su na hardverskom sigurnosnom modulu HSM (Hardware Security Module) za vrijeme inicijalne instalacije CA aplikacije.

Privatni ključ koji se korsiti za kvalifikovani elektronski potpis ili kvalifikovani elektronski pečat, generiše se u hardverskom tokenu koji je u skladu sa QSCD standardima. Privatni ključ koji se koristi za ostale tipove sertifikata, kreira se u softverskom kripto tokenu na korisničkoj strani ili bilo kojem hardverskom tokenu.

6.1.2. ISPORUKA PRIVATNOG KLJUČA KORISNIKU

Privatni ključevi generisani od strane korisnika i preuzeti koristeći PCKS#10 format, se ne dostavljaju. Privatni ključevi generisani u QSCD-u od strane CA, dostavljaju se korisnicima.

Kada je u pitanju Kvalifikovani sertifikat za kvalifikovani elektronski potpis fizičkog lica u organu državne uprave (remote signing QSCD), privatni ključ se čuva na HSM uređaju – hardverskom uređaju koji je dizajniran za upravljanje i zaštitu kriptografskih ključeva.

6.1.3. DOSTAVLJANJE JAVNOG KLJUČA DAVAOCU USLUGE SERTIFIKOVANJA

Javni ključ treba da bude na siguran način isporučen CA aplikaciji kako bi se generisao javni ključ sertifikata. Javni ključ se dostavlja CA aplikaciji u PCKS#10 formatu.

6.1.4. DOSTAVLJANJE JAVNOG KLJUČA DAVAOCA USLUGA SERTIFIKOVANJA TREĆIM LICIMA

GovME CA javni ključ za verifikaciju potpisa se dostavlja trećim licima u sertifikatu u PKCS#7 ili X.509 formatu.

6.1.5. DUŽINA KLJUČEVA

Ključevi koje GovME CA koristi za potpisivanje sertifikata su RSA ključevi sa dužinom od 3072 bita. Vlasnički RSA ključevi imaju dužinu 2048 bit-ova.

Za potrebe elektronske identifikacije i formiranja kvalifikovanog elektronskog potpisa korisnika koristi se RSA asimetrični par ključeva dužine 2048 bita i periodom validnosti sertifikata do 3 godina.

6.1.6. EPARAMETRI ZA GENERISANJE JAVNOG KLJUČA I PROVJERA KVALITETA

GovME CA ne generiše DSA ključeve.

6.1.7. NAMJENA UPOTREBE KLJUČEVA (X.509 v3 upotreba ključa)

GovME CA je u mogućnosti da izdaje sertifikate koji podržavaju različite slučajeve upotrebe. Ova podrška se ostvaruje uključivanjem odgovarajućih dodataka za korišćenje ključa.

GovME CA ključ za potpisivanje je jedini dozvoljeni ključ za potpisivanje sertifikata i CRL-ova. CA javni ključ za verifikaciju potpisa sertifikata sadrži keyCertSign cRLSign bitove.

Korisnički ključevi mogu se koristiti u svrhe zasnovane na keyUsage i extKeyUsage poljima u sertifikatu (takođe pogledati poglavlje 7).

Kategorija sertifikata	keyUsage	extKeyUsage
Kvalifikovani sertifikat za napredni elektronski potpis i autentifikaciju fizičkog lica u sklopu organa državne uprave	nonRepudiation digitalSignature	-
Kvalifikovani sertifikat za napredni elektronski pečat i autentifikaciju organa državne uprave	nonRepudiation digitalSignature	-
Kvalifikovani sertifikat za kvalifikovani elektronski potpis fizičkog lica u sklopu organa državne uprave (token)	nonRepudiation	-
Sertifikat za autentifikaciju fizičkog lica u sklopu organa državne uprave (token)	digitalSignature	-
Kvalifikovani sertifikat za kvalifikovani elektronski potpis fizičkog lica u sklopu organa državne uprave (remote signing)	nonRepudiation	-
Sertifikat za OCSP servis	digitalSignature	OCSP Signer
Sertifikat za uslugu vremenskog pečata	digitalSignature nonRepudiation	TimeStamping

Sertifikat za uslugu verifikacije elektronskog potpisa i pečata	digitalSignature nonRepudiation	-
Sertifikat za uslugu elektronske preporučene dostave	digitalSignature nonRepudiation	-
Sertifikat za JSERP autentifikaciju organa državne uprave	digitalSignature	-
Kvalifikovani sertifikat za napredni elektronski pečat organa državne uprave (JSERP pečat)	nonRepudiation	-

6.2. ZAŠTITA PRIVATNOG KLJUČA I KONTROLE KRIPTOGRAFSKIH MODULA

6.2.1. STANDARDI I KONTROLE KRIPTOGRAFSKIH MODULA

Generisanje digitalnih ključeva za potpisivanje i potpisivanje sertifikata vrši se na hardverskom kriptografskom modulu koji zadovoljava sigurnosne standarde FIPS 140-2 Nivoa 3. Poštovanje ovog standarda garantuje, da je bilo koji pokušaj narušavanja integriteta uređaja ili kriptografske memorije istovremeno detektovan.

Odgovornost vlasnika sertifikata jeste da obezbijedi čuvanje privatnog ključa u okruženju koje ima dovoljno nivoa fizičke zaštite. U svakom slučaju, preporuka je da vlasnik sertifikata koristi hardverski kriptografski modul (pametna kartica...) jer privatni ključ koji se koristi za kvalifikovani elektronski potpis ili kvalifikovani elektronski pečat, generiše se i koristi u hardverskom kriptografskom modulu sertifikovanom na osnovu QSCD specifikacije. Privatni ključ vlasnika sertifikata za ostale tipove sertifikata, oslanja se na fizičke i logičke kontrole koje štite računarski sistem vlasnika sertifikata.

Definisano je da HSM uređaji ne smiju da napuštaju bezbjednu zonu sertifikacionog tijela osim u posebnim prilikama, koje su unaprijed definisane, a koje se odnose na premještanje, preseljenje, popravku ukoliko nije moguće odraditi na licu mjesta. Sertifikaciono tijelo je zaduženo da vodi računa u vezi svih tih premještanja ili preseljenja.

6.2.2. KONTROLA PRIVATNOG KLJUČA (N OD M)

Potreban broj osoba za operativne postupke na način kako je definisano u poglavlju 5.2.2.

6.2.3. DEPONOVANJE (ESCROW) PRIVATNOG KLJUČA

Nije dozvoljeno deponovanje privatnog ključa.

6.2.4. SIGURNOSNE KOPIJE PRIVATNOG KLJUČA

Procedura čuvanja privatnog ključa zahtijeva da se izvršava backup CA privatnog ključa odmah nakon generisanja. Backup je zaštićen mehanizmom kontrole pristupa i koristeći sigurnosne mehanizme koje omogućava HSM.

GovME CA ne backup-uje korisničke privatne ključeve za potpisivanje.

6.2.5. ARHIVIRANJE PRIVATNOG KLJUČA

Privatni ključevi se ne arhiviraju.

6.2.6. TRANSFER PRIVATNOG KLJUČA NA KRIPTOGRAFSKI MODUL

U okviru hardverskog sigurnosnog modula (HSM) generisan je GovME CA privatni ključ za potpisivanje. Privatni ključ za potpisivanje se nikada ne pojavljuje u čitljivom obliku van HSM-a.
Ne postoji zahtjev za prenos korisničkih privatnih ključeva za potpisivanje jer se generišu u okviru kriptografskog modula korisnika.

6.2.7. ČUVANJE PRIVATNOG KLJUČA NA KRIPTOGRAFSKOM MODULU

Privatni ključ sertifikacionog tijela za potpisivanje se koristi samo na hardverskom sigurnosnom modulu (HSM). CA privatni ključ za potpisivanje može biti sačuvan u enkriptovnoj formi na CA sistemu jedino za potrebe backup-a i oporavka. CA privatni ključ je zaštićen sa hardverskim sigurnosnim modulom (HSM) i jedino se koristi na HSM-u. Master ključ za enkripciju/dekripciju koji se koristi u backup svrhe, zaštićen je pametnim karticama HSM-a i politikom.

6.2.8. NAČIN AKTIVIRANJA PRIVATNOG KLJUČA

Startovanjem CA aplikacije, što takođe zahtijeva HSM lozinku aktivira se i privatni ključ za potpisivanje. Korisnik sertifikata je u obavezi da koristi PKI klijentsku aplikaciju ili pametne kartice koje aktiviraju privatne ključeve kao dio procesa prijave tokom kojeg se korisnik autentifikuje pomoću lozinke ili PIN-a.

6.2.9. NAČIN DEAKTIVIRANJA PRIVATNOG KLJUČA

Privatni ključevi se deaktiviraju kada se CA aplikacija ugasi i HSM zatvori sesiju.

Korisnik sertifikata nakon što odradi odjavu, restart aplikacije ili deaktivira (plug-out) kriptografski token na taj način će se deaktivirati i privatni ključevi.

6.2.10. METODA UNIŠTAVANJA PRIVATNOG KLJUČA

Trajno brisanje CA privatnih ključeva će biti uništeno pozivanjem odgovarajuće HSM operacije brisanja.

6.2.11. REJTING KRIPTOGRAFSKIH MODULA

Standardi i kontrole kriptografskih modula kao što je opisano u poglavlju 6.2.1.

6.3. OSTALI ASPEKTI UPARAVLJANJA PAROM KLJUČEVA

6.3.1. ARHIVIRANJE JAVNOG KLJUČA

Arhiviranje javnih ključeva za verifikaciju potpisa kao što je opisano u poglavlju 5.5 Arhiviranje podataka.

6.3.2. ROK VAŽENJA SERTIFIKATA I PERIOD UPOTREBE PARA KLJUČEVA

Vrijem korišćenja javnih i privatnih ključeva koje je izdao MJU sertifikaciono tijelo je sljedeći:

SERTIFIKAT	VRIJEME
Root CA privatni ključ, javni ključ za verifikaciju potpisa i sertifikat	30 (trideset) godina
Privatni ključ podređenog (Subordinate) CA, javni ključ za verifikaciju potpisa i sertifikat:	20 (dvadeset) godina
Privatni ključ krajnjeg entiteta, javni ključ za verifikaciju potpisa i sertifikat:	3 (tri) godine

Period važenja podređenog sertifikacionog tijela se uvijek izdaje na kraći period važenja u odnosu na korijensko sertifikaciono tijelo.

Upotreba privatnih ključeva nije dozvoljena nakon isteka perioda važenja pripadajućih sertifikata, kao ni nakon opoziva sertifikata ili za vrijeme dok je sertifikat suspendovan.

6.4. AKTIVACIJSKI PODACI

6.4.1. GENERISANJE I INSTALACIJA AKTIVACIJSKIH PODATAKA

Sertifikaciono tijelo generiše aktivacione kodove u softveru i čuva ih u bazi zaštićene i šifrovane dok se ne izvrši inicijalizacija korisnika. Brojevi i kodovi su jedinstveni.
Svaki korisnik sertifikata bira svoju lozinku za ključeve koje generiše lično.

Za ključ generisan na kriptografskom uređaju, PIN generiše CA, šalje ga ili predaje korisniku kao dio procesa isporuke kao što je definisano udijelu Proces obrade zahtjeva i odgovornosti, u poglavlju 4.1.2.

Nakon što prvi put izvrši upotrebu kriptografskog tokena korisnik sertifikata je u obavezi da primijeni lozinku.

6.4.2. ZAŠTITA AKTIVACIJSKIH PODATAKA

Generisanje i instalacija aktivacijskih podataka kao što je definisano u poglavlju 6.4.1

6.4.3. OSTALI ASPEKTI AKTIVACIJSKIH PODATAKA

Nije primjenjivo.

6.5. RAČUNARSKE BEZBJEDONOSNE KONTROLE

6.5.1. SPECIFIČNI BEZBJEDONOSNO TEHNIČKI ZAHTJEVI

GovME CA je implementiralo brojne tehničke, računarske bezbjednosne kontrole koje koristi CA operativni sistem i CA aplikacija, ubrajajući:

- Kontrola pristupa CA servisima i PKI ulogama
- Striktna podjela PKI uloga
- Korišćenje pametnih kartica za čuvanje kredencijala CA superadmina
- Enkriptovane sesije između CA aplikacije i korisničke PKI klijentske aplikacije
- Kriptografska zaštita osjetljivih podataka koji se čuvaju u CA (ili RA) bazi
- Revizija sigurnosih događaja

6.5.2. RANGIRANJE NIVOA ZAŠTITE

Serveri i operativni sistemi koje koristi GovME CA su komercijalni proizvodi koji su dodatno bezbjednosno ojačani.

6.6. TEHNIČKE KONTROLE TOKOM UPOTREBE SISTEMA

6.6.1. KONTROLA RAZVOJA SISTEMA

Sve aplikacije i proizvodi koje koristi GovME CA su komercijalni proizvodi ili custom proizvodi napravljeni pod kontrolom i procedurama Ministarstva javne uprave.

6.6.2. KONTROLA UPRAVLJANJA BEZBJEDNOŠĆU

GovME CA, u skladu sa ISO/IEC 27001 preporukama, upravlja i kontroliše bezbjednost i upravljanje bezbjednošću GovME CA sistema.

6.6.3. KONTROLA BEZBJEDNOSTI TOKOM UPOTREBE SISTEMA

Ministarstvo ima usvojen plan testiranja za sve softvere i procedure u kontrolisanim uslovima.

6.7. KONTROLA MREŽNE BEZBJEDNOSTI

GovME CA mreža se sastoji od namjenskog segmenta vezanog za korporativnu TCP/IP mrežu kroz firewall uređaj. Server sa CA aplikacijom je konektovan na taj segment.

Firewall uređaj je iskonfigurisan tako da dozvoljava samo protokole i komande koje su neophodne za pristup CA servisima.

6.8. VREMENSKI PEČAT (TIME-STAMPING)

Sve informacije o vremenskom pečatu su definisane u posebnom dokumentu „Praktična pravila o pružanju usluge izrade kvalifikovanih elektronskih vremenskih pečata (TimeStamp Practice Statment MJU TSPS)".

7. SERTIFIKAT, CRL I OCSP PROFILI

7.1. PROFIL SERTIFIKATA

7.1.1. BROJ VERZIJE

Sertifikaciono tijelo MJU izdaje X.509 v3 sertifikate u skladu sa RFC 5280.
Koriste se sledeća X.509 osnovna polja:

X.509 ekstenzije	Opis
signature	Potpis sertifikacionog tijela
issuer	Ime sertifikacionog tijela
valid from	Datum aktivacije sertifikata
valid to	Datum isteka sertifikata
subject	Jedinstveno ime korisnika sertifikata
subjectPublicKeyInformation	ID algoritma, ključ
version	X.509 verzija sertifikata, verzija 3
serialNumber	Jedinstveni serijski broj sertifikata

7.1.2. EKSTENZIJE SERTIFIKATA

Koriste se sledeće ekstenzije sertifikata:

X.509 Ekstenzije		Opis
authorityKeyIdentifier		Identifikator javnog ključa CA
subjectKeyIdentifier		Identifikator javnog ključa sertifikata
keyUsage		Kao što je specificirano u poglavlju 6.1.7.
extendedKeyUsage		Opcionalno Kao što je specificirano u RFC 5280 u skladu sa specifičnim zahtjevima aplikacije.
privateKeyUsagePeriod		Koristi se samo u sertifikatu za vremenski pečat
sertificatePolicies:		Politika sertifikata OID, kao što je specificirano u poglavlju 1.2 Naziv dokumenta i identifikacioni podaci
	CertPolicyID	
	CPS URI	
Subject Alternative Name		Alternativno ime korisnika. Može biti i email adresa korisnika.
CRLDistributionPoints		CRL lokacija

basicConstraints	CA=true u CA sertifikatu, CA=false u svim ostalim sertifikatima
Authority Information Access	id-ad-calssuers i id-ad-ocsp u skladu sa RFC 5280
qcStatement	U skladu sa ETSI EN 319 412-5

7.1.3. IDENTIFIKATORI ALGORITAMSKIH OBJEKATA

Algoritam	Identifikacijska oznaka
RSA Encryption	1.2.840.113549.1.1.1
RSA with SHA-1signature	1.2.840.113549.1.1.5
SHA256 with RSA Encryption	1.2.840.113549.1.1.11

7.1.4. FORME IMENA

Sertifikati koje izdaje GovME CA sadrže potpuno X.500 jedinstveno ime izdavača i korisnika sertifikata u poljima namijenjenim za izdavača i korisnika. Jedinstvena imena su tesktualna polja u X.501 UTF8 formtu. (Pogledaj poglavlju 3.1.4.)

7.1.5. OGRANIČENJA ZA IME

Ekstenziju nameConstraints GovME CA koristi samo u unakrsnim sertifikatima, ako je primjenjivo.

7.1.6. IDENTIFIKATOR OBJEKTA ZA POLITIKU SERTIFIKOVANJA

Svi sertifikati koje je izdao CA sadrže OID politike sertifikata pod kojom se izdao. OID za svaku politiku sertifikata je definsan u poglavlju 1.2. Naziv dokumenta i identifikacioni podaci. Mogu biti prisutni dodatni OID-ovi za identifikaciju specifičnih komercijalnih uslova ili ako to zahtijeva posebna aplikacija.

7.1.7. KORIŠĆENJE POLITIKE OGRANIČENJA EKSTENZIJA

Ekstenziju policyConstraints GovME CA koristi samo u unakrsnim sertifikatima, ako je primjenjivo.

7.1.8. SINTAKSA I SEMANTIKA ZA KVALIFIKATORE POLITIKE

Ne koristi se.

7.1.9. PROCESUIRANJE SEMANTIKE ZA KRITIČNE EKSTENZIJE POLITIKE SERTIFIKOVANJA

PKI klijentska aplikacija mora procesuirati ekstenzije označene kao kritične u skladu sa RFC 5280.

7.2. CRL PROFIL

7.2.1. BROJ VERZIJE

X.509 ekstenzija	Opis
Version	V2
Signature	Identifikator algoritma koji se koristi da potpiše CRL
Issuer	CA jedinstveno ime
thisUpdate	Vrijeme izdavanja CRL-a
nextUpdate	Vrijeme izdavanja sledećeg CRL-a
revokedSertificates	Serijski brojevi opozvanih sertifikata

7.2.2. CRL I CRL EKSTENZIJE

X.509 ekstenzije	Opis
CRLNumber	Redni broj CRL-a
reasonCode	Razlog opoziva sertifikata
invalidityDate	Datum kompromitovanja ili sumnje u kompromitovanje privatnog ključa ili datum kada je sertifikat na neki drugi način prestao biti važeći

7.3. OCSP PROFILI

Profil odgovora OSCP servis je definisan u dokumentu RFC 6960.

7.3.1. BROJ VERZIJE

Profil odgovora OSCP v1 sevris je definisan u dokumentu RFC 6960.

7.3.2. OCSP EKSTENZIJE

OCSP ekstenzije su podržane u skladu sa RFC 6960.

8. REVIZIJA USAGLAŠENOSTI I DRUGE PROCJENE

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

8.1. UČESTALOST I OKOLNOSTI ZA PROCJENU (REVIZIJU)

GovME CA PMA tijelo koje je osnovano da upravlja politikama je odgovorno za sprovođenje revizija usaglašenosti.

Jednom godišnje se održava interni pregled koji inicira GovME CA PMA.

Ukoliko postoji potreba ili GovME CA PMA zahtijeva, moguće je održati i više od jedne revizije godišnje.

Eksterna revizija se vrši najmanje jednom u dvije godine od strane nezavisnog tijela, koje je akreditovano za poslove revizije iz oblasti elektronskih usluga povjerenja, u skladu sa eIDAS i nacionalnom regulativom.

8.2. IDENTITET/KVALIFIKACIJE REVIZORA

Provjera rada GovME CA se vrši u skladu sa Zakonom o elektronskoj identifikaciji i elektronskom potpisu.

Ministarstvo javne uprave će za internog revizora odrediti osobu sa odgovarajućim IT znanjem i revizorskim iskustvom.

Interni ili eksterni revizori treba da ispunjavaju sljedeće kriterijume:

Značajno iskustvo u primjeni PKI i kriptografskih tehnologija
Iskustvo u radu sa CA aplikacijom
Iskustvo u obavljanju sertifikacionih aktivnosti ili revizija sistema informacionih tehnologija

8.3. REVIZOREVA POVEZANOST SA PREDMETOM PROCJENE (REVIZIJA)

Nije primjenjivo.

8.4. OBLASTI KOJE POKRIVA PROCJENA (REVIZIJA)

Zadatak revizije jeste da utvrdi usaglašenost rada GovME CA sa Zakonom, podzakonskim aktivma i ovim dokumentom.

8.5. AKTIVNOSTI KOJE SE PREDUZIMAJU U SLUČAJU NEUSAGLAŠENOSTI

U skladu sa nalazom i preporukama revizije GovME CA PMA preduzima potrebne mjere za rješavanje nedostataka ili eventualnih neuskladenosti utvrdenih kao rezultat revizije.

8.6. OBJAVLJIVANJE REZULTATA PROCJENE (REVIZIJE)

Rezultati revizije se dostavljaju GovME CA tijelu za upravljanje politikama (GovME CA PMA).

9. OSTALI POSLOVNI I PRAVNI ASPEKTI

9.1. NAKNADE

9.1.1. NAKNADE ZA IZDAVANJE I OBNOVU SERTIFIKATA

Nije primjenjivo.

9.1.2. NAKNADE ZA PRISTUP SERTIFIKATU

Nije primjenjivo.

9.1.3. NAKNADE ZA OPOZIV ILI PRISTUP INFORMACIJAMA O STATUSU

Nije primjenjivo.

9.1.4. NAKNADE ZA OSTALE USLUGE

Nije primjenjivo.

9.1.5. POLITIKA REFUNDIRANJA

Nije primjenjivo.

9.2. FINANSIJSKA ODGOVORNOST

9.2.1. OSIGURANJE

Nije primjenjivo.

9.2.2. OSTALA SREDSTVA

Nije primjenjivo.

9.2.3. OSIGURANJE ILI GARANCIJE KORISNIKA

Nije primjenjivo.

9.3. POVJERLJIVOST POSLOVNIH INFORMACIJA

9.3.1. OBIM POVJERLJIVIH INFORMACIJA

Infomacije koje je GovME CA prikupilo smatraju se povjerljivim, osim podataka navedenih u poglavlju 9.3.2.

9.3.2. INFORMACIJE KOJE NIJESU U OPSEGU POVERLJIVIH INFORMACIJA

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, neće se smatrati povjerljivim.

9.3.3. ODGOVORNOST ZA ZAŠTITU POVJERLJIVIH INFORMACIJA

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

9.4. PRIVATNOST LIČNIH INFORMACIJA

9.4.1. PLAN PRIVATNOSTI

Ministarstvo je u obavezi da sve lične podatke koje daje korisnik tretira u skladu sa Zakonom o zaštiti ličnih podataka.

9.4.2. INFORMACIJE KOJE SE TRETIRAJU KAO LIČNE

Informacije koje nisu objavljene u okviru sertifikata, a odnose se na vlasnika sertifikata tj. korisnika, smatraju se privatnim.

9.4.3. INFORMACIJE KOJE SE NE 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.

9.4.4. ODGOVORNOST ZA ZAŠTITU LIČNIH INFORMACIJA

Kako što je utvrđeno u poglavlju 9.3.3.

9.4.5. OBAVJEŠTENJE I DAVANJE SAGLASNOSTI ZA KORIŠTENJE LIČNIH INFORMACIJA

Prije izdavanja elektronskih sertifikata korisnici su upoznati o podacima koji će biti sastavni dio sertifikata. Korisnik 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.

9.4.6. OTKRIVANJE LIČNIH INFORMACIJA U SKLADU SA SUDSKIM ILI ADMINISTRATIVNOM PROCESOM

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

9.4.7. OSTALE OKOLNOSTI KADA SE MOGU OTKRIVATI LIČNE INFORMACIJE

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

9.5. 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.

9.6. GARANCIJE

9.6.1. GARANCIJE SERTIFIKACIONOG TIJELA

GovME CA garantuje da će izdavati sertifikate, izvršavati ostale procedure vezane za upravljanje sertifikatima, upravljati cjelokupnom infrastrukturom GovME CA u skladu sa Zakonom o elektronskoj identifikaciji i elektronskom potpisu i ovim dokumentom.

GovME CA se obavezuje da će:

- pružiti elektronske usluge povjerenja u skladu sa Zakonom o elektronskoj identifikaciji i elektronskom potpisu i podzakonskim aktima,
- da će obezbjediti potreban softver i hardver za funkcionisanje GovME CA,
- da će obezbjediti Repozitorijum za objavljivanje svih potrebnih informacija i sadržaja za podršku elektronskim uslugama povjerenja,
- da će objaviti kontakt informacije GovME CA,
- da će u skladu sa standardima koji regulišu ovu oblast i dobrom kriptografskom praksom obezbjediti sigurne mehanizme koji uključuju mehanizam generisanja korisničkih ključeva i ključeva CA tijela i adekvatnu kriptografsku zaštitu pomenutih ključeva,
- da će uspostaviti proceduru dijeljenja tajni za sve povjerljive role u skladu sa svojom PKI infrastrukturom,
- u najkraćem mogućem roku, ukoliko se to desi, obavijestiti korisnike i treće strane o kompromitaciji sopstvenog privatnog ključa, po mogućnosti po više komunikacionih kanala,
- da će izdavati elektronske sertifikate korisnicima u skladu sa Zakonom o elektronskoj identifikaciji i elektronskom potpisu i procedurama definisanim ovim dokumentom,
- da će ispunjavati sopstveno preuzete obaveze,
- da će komunicirati sa naručiocem/korisnikom, u skladu sa procedurom opisanom u poglavlju 4.1.2 - Proces obrade zahtjeva i odgovornosti,
- da će nakon prijema validnog zahtjeva za opoziv elektronskog sertifikata opozvati isti,
- da će obezbjediti podršku korisnicima u skladu sa ovim dokumentom,
- da će redovno i periodično objavljivati informacije o statusu sertifikata putem CRL, a da će isto tako informacije o statusu sertifikata biti dostupne putem OCSP servisa u realnom vremenu,
- da će redovno ažurirati ovaj dokument.

GovME CA nije odgovoran za neodgovarajuću provjeru validnosti sertifikata od treće strane koja se pouzdaje u sertifikate izdate od strane GovME CA.

GovME CA nije odgovorno za neizvršavanje svojih obaveza kao posledice više sile.

9.6.2. GARANCIJE REGISTRACIONOG TIJELA

Odgovornosti GovME CA RA tijela su definisane u poglavlju 1.3.2 Registraciona tijela (Registration Authorities).

9.6.3. GARANCIJE KORISNIKA SERTIFIKATA

Naručilac odnosno korisnik sertifikata se obavezuje da na pouzdan i propisan način mora voditi računa o svom sertifikatu, što podrazumijeva da:

- posjeduje odgovarajuća znanja za upotrebu izdatih elektronskih sertifikata;
- je upoznat sa sadržajem ovog dokumenta i da koristi elektronski sertifikat u skladu sa istim;
- u procesu podnošenja zahtjeva za izdavanje elektronskog sertifikata i utvrđivanja identiteta, tijelu GovME CA RA dostavi sve potrebne podatke;
- je odgovaran za čuvanje lozinke koja je povezana sa elektronskim sertifikatom;
- elektronski sertifikat koristi isključivo u poslovne svrhe, u skadu sa ovim dokumentom i Zakonom o elektronskoj identifikaciji i elektronskom potpisu i pravilnicima koji proizilaze iz zakona;
- u najkraćem roku obavijesti GovME CA o promjenama bilo kojih podataka koji su ranije dostavljeni;
- obustavi korišćenje izdatog ili izdatih sertifikata ukoliko bilo koji podatak u sertifikatu postane nevalidan;
- spriječi kompromitaciju, gubljenje, objavljivanje, modifikaciju ili bilo koje drugo nevalidno korišćenje svojih privatnih ključeva;
- podnese zahtjev za opoziv certifikata ako dođe do nekog događaja koji utiče na integritet izdatog sertifikata;
- prijavi svaku moguću zloupotrebu svojih privatnih ključeva i da u tom slučaju podnesu zahtjev za opoziv pripadajućeg sertifikata.

9.6.4. ODGOVORNOST TREĆIH LICA

Treće lice koje se oslanja na sertifikate izdate od strane GovME CA obavezuje se da:

- posjeduje odgovarajuća znanja za upotrebu izdatih certifikata;
- se upozna i da poštuje politiku i praktična pravila rada objavljena od strane GovME CA;
- verifikuje izdate sertifikate od strane GovME CA primjenom svih raspoloživih metoda provjere sertifikata: da provjeri da li je certifikat validan (da provjeri period važenja sertifikata; da provjeri da li je sertifikat izdat od strane GovME CA; da provjeri da li je potpis elektronskog sertifikata vjerodostojan; da provjeri status datog sertifkata na važećoj listi opozvanih sertifikata ili putem OCSP servisa sertifikacionog tijela, a u skladu sa procedurom validacije sertifikata i potpunog lanca sertifkata);
- vjeruje u izdati sertifikat samo ukoliko se sve informacije koje se odnose na taj sertifikat mogu provjeriti da su tačne i ažurne;
- odmah obavijesti GovME CA o bilo kakvoj zloupotrebi bilo kojeg sertifikata izdatog od strane GovME CA.

9.6.5. GARANCIJE OSTALIH UČESNIKA

Nije primjenjivo.

9.7. IZUZEĆA GARANCIJA

GovME CA isključuje svu odgovornost i garancije i ne odgovara za štetu:

- ako je elektronski sertifikat korišćen nakon isteka;
- ako nije bilo provjere statusa podataka i validnosti sertifikata u Listi opozvanih sertifikata (CRL ili OCSP) prilikom korišćenja elektronskog sertifikata;
- ako je elektronski sertifikat korišćen nakon opoziva i objavljivanja u Listi opozvanih sertifikata (CRL ili OCSP);
- za upotrebu sertifikata sa netačnim podacima zbog promjena (npr. elektronska adresa, imena, prezimena ili drugih podataka korisnika);
- ako se dogodila zloupotreba, upad u informacioni sistem korisnika sertifikata ili trećih lica, a samim tim i zloupotreba informacija o sertifikatima od strane neovlašćenih lica;
- ako je korisnik otkrio privatni ključ ili se sumnja da je to uradio;
- ako se elektronski sertifikat ne koristi u skladu sa ograničenjima koja su utvrđena u ovoj politici ili važećem zakonu (vidjeti 9.14.);
- ako korisnik ili treće lice nisu postupili u skladu sa ovim dokumentom;
- ako je oštećenje prouzrokovano neispravnošću hardvera ili softvera korisnika;
- ako je šteta nastala uslijed više sile kako je opisano u poglavlju 9.16.5;
- ako je šteta nastala kao rezultat dešavanja van kontrole GovME CA.

9.8. OGRANIČENJA ODGOVORNOSTI

GovME CA nije odgovoran za bilo kakvu štetu koja je nastala zbog nepoštovanja uslova definisanim u ovom dokumentu i zakonskim propisima iz ove oblasti od strane korisnika ili trećeg lica.

9.9. OBEŠTEĆENJA

Svaka strana snosi isključivu odgovornost za obeštećenja drugih strana za gubitke ili štetu nastalu kao rezultat neovlašćenog korišćenja sertifikata, neadekvatne upotrebe sertifikata ili nepostupanja u skladu sa ovim dokumentom i važećim zakonima.

9.10. ROK I PREKID

9.10.1. ROK

Ovaj dokument stupa na snagu danom donošenja i objave na Repozitorijumu.

9.10.2. PREKID

Ovaj dokument nije vremenski ograničen. Trenutna verzija je na snazi do objavljivanja nove verzije.

9.10.3. EFEKTI ZAVRŠETKA I PONOVNOG RADA

Elektronski sertifikat se koristi u skladu sa verzijom dokumenta (CPS) koja je bila aktivna na datum izdavanja elektronskog sertifikata.

Izuzetno, ukoliko se jave okolnosti kada to nije moguće, GovME CA će blagovremeno obavijestiti korisnike kao što je opisano u poglavlju 9.12.2. Mehanizmi obavještavanja i vremenski periodi, a treća lica putem internet stranice, kao što je definisano u poglavlju 2.1. Repozitorijumi.

9.11. INDIVIDUALNO OBAVJEŠTAVANJE I KOMUNIKACIJA SA UČESNICIMA

GovME CA distribuira trenutnu verziju ovog dokumenta i trenutnu verziju svih ostalih javnih dokumenata putem svoje internet stranice opisane u poglavlju 2.1 Repozitorijumi.

Takođe, treba uzeti u obzir i poglavlje 9.12.2 Mehanizmi obavještavanja i vremenski periodi.

9.12. IZMJENE

9.12.1. PROCEDURA ZA IZMJENU

Dokument „Praktična pravila o postupcima izdavanja sertifikata (CPS – Certification Practice Statement)" sertifikacionog tijela GovME CA se periodično pregleda i ažurira po potrebi.

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.

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

9.12.2. MEHANIZMI OBAVJEŠTAVANJA I VREMENSKI PERIODI

GovME CA PMA može odlučiti da ne obavještava korisnike i treća lica u slučaju izmjena sa malim ili nepostojećim uticajem. GovME CA tijelo odlučuje o tome da li izmjene imaju bilo kakav uticaj na korisnike i treća lica, na sopstvenu odgovornost.

Sve izmjene ovog dokumenta biće objavljene kao što je opisano u poglavlju „2. Objave i odgovornosti repozitorijuma". GovME CA će obavijestiti korisnike o promjenama koje imaju uticaj na njih, putem e-maila i treća lica putem Repozitorijuma.

9.12.3. OKOLNOSTI POD KOJIMA OID MORA BITI PROMIJENJEN

Nije primjenjivo.

9.13. RJEŠAVANJA U SLUČAJU SPORA

Nije primjenjivo.

9.14. PRIMJENA ZAKONA

Ovaj dokument je u skladu sa Zakonom o elektronskoj identifikaciji i elektronskom potpisu i njegovim podzakonskim aktima.

9.15. USAGLAŠENOST SA PRIMJENLJIVIM ZAKONIMA

Sertifikaciono tijelo GovME CA radi u skladu sa sljedećim zakonima:

- Zakon o elektronskoj identifikaciji i elektronskom potpisu
- Zakon o zaštiti podataka o ličnosti
- Ostali propisi iz ove oblasti

9.16. RAZNE ODREDBE

9.16.1. CJELOKUPNI UGOVOR

Ovaj dokument obuhvata sve relevantne elemente koji definišu odnos između GovME CA i korisnika sertifikata.

9.16.2. PRENOS PRAVA

Korisnicima nije dozvoljeno da prava i obaveze koji proističu iz ovog dokumenta u cijelosti ili parcijalno prenesu na treća lica po bilo kom osnovu.

9.16.3. KLAUZULA O VALJNOSTI

Nevalidnost jednog ili više djelova ovog dokumeta ne treba da utiču na validnost ostalih odredbi, pod uslovom da nemaju uticaj na materijalne odredbe (povjerenje u sertifikat i upotreba sertifikata).

9.16.4. IZVRŠENJE (NADOKNADE ZA PRAVNOG ZASTUPNIKA I ODRICANJE OD PRAVA)

Nije primjenjivo.

9.16.5. VIŠA SILA

Višu silu predstavljaju vanredne okolnosti i nepredvidive situacije kao što su prirodne katastrofe, terorizam, nedostatak napajanja ili prekid telekomunikacionih veza, požar, nepredvidivi incidenti kao što su virusi ili napadi sa ciljem onemogućavanja servisa, greške u kriptografskim algoritmima itd.

9.17. OSTALE ODREDBE

Nije primjenjivo.

Aneks
SERTIFIKAT ZA AUTENTIFIKACIJU INTERNET STRANICE

A1. KRATAK PREGLED

Autentifikacija internet stranica, shodno Zakonu o elektornskoj identifikaciji i elektronskom potpisu, je elektronski postupak koji omogućava potvrđivanje cjelovitosti podataka internet stranice i pouzdanosti korišćenja internet stranice i zasniva se na sertifikatu za autentifikaciju internet stranica.

Sertifikat za autentifikaciju internet stranice je potvrda pomoću koje se može izvršiti autentifikacija internet stranice i kojom se internet stranica povezuje sa fizičkim ili pravnim licem kojem je izdat sertifikat.

Sertifikat za autentifikaciju internet stranice koji izdaje GovME CA, namijenjen je organima državne uprave koji imaju potrebu za istim, u smislu obezbjeđivanja sigurne interne komunikacije između web servera.

A2. IDENTIFIKACIONI PODACI

Ovoj kategoriji sertifikata dodijeljen je identifikacioni broj (OID): 1.3.6.1.4.1.34324.2.2.3.

Ova vrsta sertifikata ne zahtijeva kriptografski uređaj, a njegov period važenja je 13 mjeseci.

A3. PRAVA KORIŠĆENJA DOMENA

Za potrebe provjere identiteta i izdavanja sertifikata za domene neophodna je identifikacija domena organa državne uprave.

Provjera da li domen priprada organu državne uprave vrši se na osnovu postojeće baze DNS-ova definisanih za organe državne uprave. Ukoliko domen organa državne uprave nije ranije definisan, vrši se provjera ispunjenosti uslova za njegovo definisanje. Ovaj proces obično uključuje DNS, e-mail ili HTTP validaciju.

A4. UPRAVLJANJE ŽIVOTNIM CIKLUSOM SERTIFIKATA

Koraci prilikom izdavanja sertifikata su sljedeći:

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.

Korak 6 – Službenik GovME CA RA unosi zahtjev kroz RA portal i isti prosljeđuje ka GovME CA OA na obradu.

Korak 7 – GovME CA OA službenik vrši provjeru podataka, u skladu sa procedurom opisanom u A3. Prava korišćenja domena.

- Ukoliko nije uspješno utvrđeno vlasništvo nad domenom ili dostavljeni podaci nijesu validni, GovME CA OA službenik komunicira sa naručiocem, u cilju otklanjanja nedostataka.
- Ukoliko je uspješno utvrđeno vlasništvo nad domenom i ostali podaci su validni, GovME CA OA službenik kreira sertifikat.

Korak 8 – GovME CA OA službenik komunicira sa naručiocem, u cilju pružanja instrukcija za aktivaciju sertifikata i nakon uspješne aktivacije obavještava GovME CA RA službenika o istom.

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

Procedure koje se odnose na obnavljanje i opoziv sertifikata su analogne procedurama u poglavlju 4, a koje važe za sve tipove sertifikata koji su opisani u ovom dokumentu.

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

Broj: 01-050/25-1057

U Podgorici, 11. marta 2025. godine

MINISTAR

mr Marash Dukaj