Crna Gora
Ministarstvo javne uprave

Praktična pravila o pružanju usluge izrade kvalifikovanih elektronskih vremenskih pečata (TimeStamp Practice Statment GovME CA TSPS)

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 vremenskog 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, izmedu ostalog, vrši kvalifikovane elektronske usluge povjerenja za organe državne uprave.

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

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

1.1. PREGLED

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

Ovaj dokument predstavlja praktična pravila o postupcima pružanja usluge - izrade kvalifikovanog elektronskog vremenskog pečata, definiše način na koji GovME CA ispunjava tehničke, organizacione i proceduralne zahtjeve, koji su propisani za kvalifikovane elektronske usluge povjerenja, u skladu sa Zakono o elektronskoj identifikaciji i elektronskom potpisu i standardima koji su navedeni na kraju dokumenta. Sadrži opis pravila, proceduralne i kadrovske politike i prakse koje GovME CA koristi u svom radu.

Ovaj dokument je javno dostupan i namijenjen svima kojima su potrebne informacije za procjenu povjerenja u datu uslugu.

1.1.1. OSNOVNE DEFINICIJE

U ovom dokumentu pojedini izrazi imaju sljedeće značenje:

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

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

Skraćenice koje se koriste u ovom dokumentu:

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

1.1.2. NAZIV DOKUMENTA I IDENTIFIKACIONI PODACI

Naziv dokumenta: Praktična pravila o pružanju usluge izrade kvalifikovanih elektronskih vremenskih pečata (TimeStamp Practice Statment GovME CA TSPS). Takode, dokument se može kratko nazvati GovME CA TSPS .

Struktura ovog dokumenta zasniva se na standardizovanom dokumentu IETF RFC 3647, uz izvjesne modifikacije neophodne da bi se opisali zahtjevi za pružanje izrade kvalifikovanih elektronskih vremenskih pečata, propisani Zakonom o elektronskoj identifikaciji i elektronskom potpisu.

Ažuriranje ovog pravilnika će se vršiti od strane GovME CA periodično, a minimum jednom godišnje ili prilikom provjere ukladenosti.

1.1.3. KONTAKT OSOBA

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

1.2. KORISNICI I PRIMJENJIVOST

Naručilac je organ državne uprave, odnosno starješina organa koji podnosi zahtjev za izdavanje kvalifikovanog elektronskog vremenskog pečata.

Kada je u pitanju usluga izrade kvalifikovanih elektronskih vremenskih pečata, naručilac može biti istovremeno i korisnik, s obzirom da se ova usluga može koristiti od strane organa državne uprave ili od strane zaposlenog u tom organu.

Naručilac/korisnik snosi krajnju odgovornost za upotrebu ove elektronske usluge povjerenja.

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

Kvalifikovani elektronski vremenski pečat koji izdaje GovME CA koristi se kada postoji potreba dokazivanja postojanja podataka ili postojanja elektronskog potpisa podataka u trenutku formiranja kvalifikovanog elektronskog vremenskog pečata, odnosno kada postoji potreba za očuvanjem dugoročnosti podataka u elektronskom obliku i osiguranje usklađenosti sa zahtjevima norme ETSI EN 319 122 ili drugih normi.

Ova elektronska usluga povjerenja kao i sve elektronske usluge povjerenja koje pruža GovME CA namijenjena je organima državne uprave koje imaju potrebu za istima.

1.3. USKLAĐENOST

Pružanje kvalifikovane usluge izrade kvalifikovanog elektronskog vremenskog pečata usklađeno je sa Zakonom o elektronskoj identifikaciji i elektronskom potpisu, podzakonskom regulativom i ovim dokumentom.

2. OBAVEZE I ODGOVORNOSTI

2.1. OBAVEZE SERTIFIKACIONOG TIJELA

2.1.1. OPŠTE OBAVEZE SERTIFIKACIONOG TIJELA

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 ispunjavati sopstveno preuzete obaveze,
- da će komunicirati sa naručiocem/korisnikom i obezbjediti podršku u skladu sa ovim dokumentom i praktičnim pravilima za elektronske usluge povjerenja, pojedinačno,
- 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, kao i sva dokumenta relevantna za rad GovME CA.

GovME CA nije odgovoran za neodgovarajuću upotrebu elektronskih usluga povjerenja od strane korisnika, kao i načina na koje se treće strane po pouzdaju u elektronske usluge povjerenja koje pruža GovME CA.

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

2.1.2. OBAVEZE DAVAOCA USLUGA SERIFIKACIJE PREMA KORISNICIMA I TREĆIM LICIMA

Opšte obaveze GovME CA su opisane u poglavlju 2.1.1.

Dodatno, kada je u pitanju kvalifikovana usluga izrade kvalifikovanog elektronskog vremenskog pečata GovME CA garantuje:

- da će nastojati da bude dostupan svim korisnicima vremenskog pečata u režimu 24/7, sa izuzetkom najavljenih prekida zbog intervencija na infrastrukturi, nepredviđenih kvarova i drugih dogadaja koje su izvan kontrole sertifikacionog tijela ili više sile;
- da UTC vrijeme koje se nalazi u svakom tokenu, ne odstupa više od +/- 1s;
- vjerodostojnost podataka potpisanim kvalifikovanim elektronskim vremenskim pečatom.

2.2. OBAVEZE KORISNIKA

Naručilac odnosno korisnik se obavezuje da na pouzdan i propisan način koristi elektronske usluge povjerenja, što podrazumijeva da:

- posjeduje odgovarajuća znanja za upotrebu elektronskih usluga povjerenja za koje je odobren zahtjev;
- je upoznat sa sadržajem ovog dokumenta i da elektronske usluge povjerenja koristi u skladu sa istim;
- u procesu podnošenja zahtjeva za izdavanje elektronskih usluga povjerenja i utvrđivanja identiteta, tijelu GovME CA RA dostavi sve potrebne podatke;
- elektronske usluge povjerenja koristi isključivo u poslovne svrhe, u skadu sa ovim dokumentom, praktičnim pravilima, Zakonom o elektronskoj identifikaciji i elektronskom potpisu i pravilnicima koji proizilaze iz zakona;

- obustavi korišćenje elektronskih usluga povjerenja ukoliko nastane promjena bilo kojih podataka koji su ranije dostavljeni i o tome u najkraćem roku obavijesti GovME CA;
- prilikom dobijanja tokena vremenskog pečata provjeriti da li je token vremenskog pečata ispravno elektronski potpisan i da sertifikat kojim se provjerava potpis tokena vremenskog pečata nije opozvan do trenutka provjere.

2.3. TREĆA LICA

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 kvalifikovanog elektronskog vremenskog pečata, a koja se može provjeriti na osnovu javno dostupnih informacija.

Kada se treća lica oslanjaju na kvalifikovani elektronski vremenski pečat, u obavezi su da:
- provjere da je zapis kvalifikovanog elektronskog vremenskog pečata ispravno potpisan;
- provjere validnost javnog ključa provjerom CRL ili korišćenjem OCSP servisa;
- vjeruju vremenskom pečatu samo u granicama utvrđenim u ovom dokumentu.

2.4. ODGOVORNOST

2.4.1. ODGOVORNOST SERTIFIKACIONOG TIJELA

GovME CA je odgovorno za sve obaveze utvrđene u poglavlju 2.1.

2.4.2. OGRANIČENJE ODGOVORNOSTI SERTIFIKACIONOG TIJELA

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.

2.4.3. FINANSIJSKA ODGOVORNOST

Nije primjenjivo.

2.5. CJENOVNIK

Nije primjenjivo.

3. USLOVI POSLOVANJA SERTIFIKACIONOG TIJELA

3.1. POSTUPANJE SA DOKUMENTACIJOM

3.1.1. POSTUPCI ZA PROMJENU SADRŽAJA DOKUMENTACIJE

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 3.1.2.

GovME CA će obavijestiti korisnike o promjenama koje imaju uticaj na njih, putem e-maila i treća lica putem Repozitorijuma.

3.1.2. OBJAVLJIVANJE DOKUMENTACIJE

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.

3.2. UPRAVLJANJE KLJUČEVIMA

3.2.1. KREIRANJE PARA KLJUČEVA

Par kriptografskih ključeva za elektronsko potpisivanje kvalifikovanih elektronskih vremenskih pečata je generisan prilikom instaliranja aplikacije TSU i tokom postupka generisanja ključa (Key Generatian Ceremony) po definisanoj proceduri. U toku generisanja para kriptografskih ključeva za elektronsko potpisivanje koristi se zaštita koja važi za prostorije GovME CA, višestruka autentifikacija ovlašćenih lica i hardverski kriptografski modul (Hardware Security Module - HSM).

Generisanje TSU privatnog ključa za potpisivanje se izvodi sa pouzdanim kriptografskim uređajem, HSM modulom, koji posjeduje sertifikat o usaglašenosti sa standardom FIPS 140-2 nivo 3 i zadovoljava EAL 4 nivo sigurnosti, u skladu sa ISO/IEC 15408 standardom. Algoritam za kreiranje TSU ključeva, dužina ključeva i algoritam za potpisivanje TSU sertifikata u potpunosti odgovaraju specifikaciji u ETSI TS 119 312. TSU privatni ključ se isključivo čuva u HSM modulu i ne radi se import u bilo koji drugi kriptografski modul. U jednom trenutku može biti aktivan samo jedan ključ koji se koristi za kreiranje kvalifikovanih elektronskih vremenskih pečata.

3.2.2. ZAŠTITA PRIVATNOG KLJUČA

Privatni ključ GovME CA kreiran je i upotrebljava se isključivo na hardveru koji ima sertifikat o usaglašenosti sa FIPS 140-2 nivo 3.

U operacijama u kojima se upravlja hardverskim kriptografskim modulom uvijek je potrebno prisustvo najmanje dva lica sa odgovarajućim punomoćjem koji se identifikuju sa pametnom karticom hardverskog kriptografskog modula i tajnom lozinkom kartice (Aktivacijski podaci).

Aktivacijski podaci za privatni ključ TSU koji su smjesteni na odgovarajuće upravljačke kartice HSM modula, zaštićeni su odgovarajućim lozinkama. Lozinke se generišu u bezbjednom prostoru Ministarstva od strane službenika GovME CA OA. Upravljačke kartice HSM modula i pripadajuće lozinke dodjeljuju se ovlašćenim licima sa povjerljivim ulogama.

3.2.3. PRISTUP JAVNOM KLJUČU

Javni ključevi GovME CA koji izdaje kvalifikovani elektronski vremenski pečat su dostupni u obliku X.509 sertifikata na Repozitorijumu GovME CA i u svakom izdatom tokenu vremenskog pečata.

3.2.4. OBNOVA KLJUČA VREMENSKOG PEČATA

Rok važenja javnih ključeva kvalifikovanog elektronskog vremenskog pečata je 5 godina.

Prije isteka sertifikata usluge kvalifikovanog elektronskog vremenskog pečata vrši se obnova ključa. U postupku obnove se kreira novi par ključeva. Stari par ključeva se posle obnove uništi (briše iz HSM).

Sertifikat javnog ključa kvalifikovanog elektronskog vremenskog pečata se čuva trajno, što omogućava potvrdu valjanosti potpisa na tokenima kvalifikovanog elektronskog vremenskog pečata izdatih prije isteka sertifikata.

3.2.5. POSTUPAK UNIŠTENJA KLJUČEVA

U toku uništavanja ključeva jedinice za izradu kvalifikovanog elektronskog vremenskog pečata (TSU), uništavaju se sve kopije ključeva. Proces uništavanja ključeva vrši se pod strogom kontrolom sertifikacionog tijela odnosno GovME CA.

3.2.6. UPRAVLJANJE HARDVERSKIM SIGURNOSNIM MODULOM (HSM – HARDWARE SECURITY MODULE)

Tokom procesa aktiviranja i generisanja ključeva koristi se dvostruka autorizacija. Postupak se izvodi uz prisustvo svjedoka.

Privatni ključ jedinice za izradu kvalifikovanog elektronskog vremenskog pečata generiše se i uvijek se koristi samo na hardverskom sigurnosnom modulu (HSM). Privatni ključ se nikada ne pojavljuje u čitljivom obliku izvan HSM-a.

3.3. VREMENSKO PEČATIRANJE

3.3.1. IZRADA KVALIFIKOVANOG ELEKTRONSKOG VREMENSKOG PEČATA

GovME CA izrađuje kvalifikovani elektronski vremenski pečat na siguran način i isti sadrži tačno vrijeme.

Glavne karakteristike svakog kvalifikovanog elektronskog vremenskog pečata su:

- sadrži identifikacionu oznaku politike kao što je definisano u skladu sa ovim dokumentom;
- sadrži jedinstvenu identifikacijsku oznaku tokena kvalifikovanog elektronskog vremenskog pečata (serialnumber);
- sadrži UTC vrijeme preuzeto iz jedinice za izradu kvalifikovanog elektronskog vremenskog pečata koje je uporedivo sa UTC tačnim vremenom uz maksimalno dozvoljeno odstupanje od 1 sekunde;
- kvalifikovani elektronski vremenski pečat je potpisan privatnim ključem koji je kreiran samo za tu namjenu;
- profil tokena kvalifikovanog elektronskog vremenskog pečata je usklađen sa RFC 3161 (Time-S Stamp Protocol) i ETSI EN 319 422 (Time-stamping protocol and time-stamp token profiles).

3.3.2. SINHRONIZACIJA VREMENA SA UTC

Sinhronizacija vremena se obavlja automatski u skladu sa specifikacijom NTP protokola. GovME CA koristi izvor tačnog vremena sa NTP sinhronizacijom i internim satom, a NTP sinhronizacija se vrši sa Stratum 1 i/ili Stratum 2 serverima.

GovME CA ima uspostavljenu kontrolu koja omogućava otkrivanje u odstupanju vremena jedinice za izradu kvalifikovanog elektronskog vremenskog pečata od referentnog vremenskog izvora.

3.4. ORGANIZACIJA I UPRAVLJANJE

3.4.1. FIZIČKA SIGURNOST SISTEMA I SIGURNOST NJEGOVOG OKRUŽENJA

TSTU sistem je smješten u istom prostoru gdje je smještena infrastruktura GovME CA.

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

3.4.2. SIGURNOSNO UPRAVLJANJE

TSTU sistem je dio cjelokupne infrastrukture GovME CA.

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

3.4.3. BEZBJEDNOST RAČUNARSKE MREŽE

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

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

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

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

Mrežni segment TSTU sistema 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 konfigurisan tako da dozvoljava samo protokole i komande koje su neophodne za pristup CA servisima.

Primjenjuju se mjere bezbjednosti računarske mreže na način, opisan u dokumentu Praktična pravila o postupcima izdavanja kvalifikovanih sertifikata (GovME CA CPS – Certification Practice Statement).

3.4.4. UPRAVLJANJE INCIDENTIMA

GovME CA ima implementirane procedure reagovanja na bezbjednosne incidente i kvarove u skladu sa internim procedurama.

3.4.5. KOMPROMITOVANJE SERVISA VREMENSKOG PEČATA

U slučaju da se desi kompromitovanje ključa, GovME CA će sprovesti sledeće korake:

- opozvati sertifikat kompromitovanog kvalifikovanog elektronskog vremenskog pečata;
- objaviti opoziv sertifikata;
- obavijestiti cjelokupno osoblje GovME CA;
- obavijestiti sve korisnike;
- kreirati nove ključeve za usluge kvalifikovanog elektronskog vremenskog pečata i novi sertifikat kvalifikovanog elektronskog vremenskog pečata.

U slučaju da se ugrozi izvor vremena ili u slučaju neusaglašenosti izmedu jedinice za izradu kvalifikovanog elektronskog vremenskog pečata i referentnog UTC izvora, GovME CA će obustaviti izdavanje tokena kvalifikovanog elektronskog vremenskog pečata do ponovne sinhronizacije.

U slučaju većih nepravilnosti u radu servisa, GovME CA će korisnicima pružiti informacije koje će omogućiti identifikaciju ugroženih tokena kvalifikovanog elektronskog vremenskog pečata.

3.4.6. PRESTANAK IZDAVANJA KVALIFIKOVANOG ELEKTRONSKOG VREMENSKOG PEČATA

U slučaju prestanka izdavanja usluge kvalifikovanog elektronskog vremenskog pečata, 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 raspoloživost i dostupnost podataka potrebnih za provjeru valjanosti izdatih tokena vremenskog pečata;
- osigurati da se arhivirani podaci čuvaju 10 godina od dana prestanka rada, ukoliko drugačije nije predvideno važećim propisima;
- osigurati raspoloživost liste opozvaih sertifikata u periodu od godinu dana poslije opoziva svih TSTU sertifikata.

3.5. USKLAĐENOST SA ZAKONODAVSTVOM

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

3.6. CJENOVNIK

Nije primjenjivo.

3.7. SIGURNOSNE KONTROLE RAČUNARA

3.7.1. SPECIFIČNI ZAHTJEVI ZA SIGURNOST RAČUNARA

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

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

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

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

3.7.2. RANGIRANJE SIGURNOSTI RAČUNARA

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

3.7.3. KONTROLA UPRAVLJANJA SIGURNOŠĆU

GovME CA nadgleda i kontroliše sigurnost i upravljanje sigurnošću sistema za pružanje usluge kvalifikovanog elektronskog vremenskog pečata.

3.7.4. UNUTRAŠNJA ORGANIZACIJA I UPRAVLJANJE BEZBJEDNOŠĆU

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

4. FIZIČKE BEZBJEDNOSNE KONTROLE

4.1. LOKACIJA I KONSTRUKCIJA

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

4.1.1. KONTROLA FIZIČKOG PRISTUPA

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

4.1.2. NAPAJANJE I KLIMATIZACIJA

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

4.1.3. ZAŠTITA OD POPLAVE

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

4.1.4. PREVENCIJA I ZAŠTITA OD POŽARA

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

4.1.5. SMJEŠTANJE MEDIJA

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

4.1.6. ODLAGANJE OTPADA

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

4.1.7. KONTROLA OSOBLJA

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

4.1.8. KVALIFIKACIJE, ISKUSTVA I POVJERE

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

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

4.1.9. POSTUPCI ZA KONTROLU OSOBLJA

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

4.1.10. OBUKA OSOBLJA

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

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

4.1.11. DODATNA OBUKA I UČESTALOST OBUKE OSOBLJA

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

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

4.1.12. UČESTALOST I REDOSLJED ROTACIJE ULOGA

Nije primjenjivo.

4.1.13. SANKCIJE ZA NEOVLAŠĆENE AKTIVNOSTI

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

4.1.14. KRITERIJUMI ZA OSOBLJE ANGAŽOVANO PO UGOVORU O DJELU

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

4.1.15. DOKUMENTACIJA ZA POTREBE OSOBLJA

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

4.2. KOMPROMITOVANJE I OPORAVAK SISTEMA OD NEPREDVIĐENIH SITUACIJA

4.2.1. PROCEDURE KOD KOMPROMITOVANJA ILI INCIDENATA

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

4.2.2. 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).

4.2.3. PRESTANAK RADA SERTIFIKACIONOG TIJELA

U slučaju dobrovoljnog prekida poslovanja, GovME CA će:

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

4.2.4. USKLAĐENOST SA ZAKONODAVSTVOM

Pružanje kvalifikovane usluge izrade kvalifikovanog elektronskog vremenskog pečata usklađeno je sa Zakonom o elektronskoj identifikaciji i elektronskom potpisu, podzakonskom regulativom i ovim dokumentom.

4.2.5. USAGLAŠENOST SA MEĐUNARODNIM STANDARDIMA

U procesu pružanja pružanje kvalifikovane usluge elektronskih vremenskih pečata, poslovanje GovME CA je usklađeno sa sljedećim međunarodnim standardima:

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

Broj: 01-050/25-1058

U Podgorici, 11. marta 2025. godine

MINISTAR

mr Marash Dukaj