Pošta Crne Gore SLUŽBENI POŠTANSKI GLASNIK

IZLAZI JEDNOM U TRI MJESECA I PO POTREBI	POŠTA CRNE GORE AD PODGORICA	RUKOPISI SE PRIMAJU DO 20. U MJESECU U KOME IZLAZI

Pošta Crne Gore AD Podgorica
Odbor direktora
Broj: 00010-15142/8
Podgorica, 28.12.2016. godine

Na osnovu člana 28 i 30 Statuta Pošte Crne Gore AD Podgorica, Odbor direktora Pošte je na sjednici održanoj dana 28.12.2016.godine, donio

O D L U K U
o usvajanju Pravilnika o postupcima izdavanja certifikata i zaštiti sistema certifikovanja (Certification Practice Statement-CPS)

Član 1

Usvaja se prečišćeni tekst Pravilnika o postupcima izdavanja certifikata i zaštiti sistema certifikovanja (Certification Practice Statement-CPS) u tekstu koji čini sastavni dio ove Odluke.

Član 2

Za realizaciju ove Odluke zadužuje se izvršni direktor.

Član 3

Ova Odluka stupa na snagu danom donošenja.

PREDSJEDNIK
Prof. dr Igor Radusinović

Pošta Crne Gore AD Podgorica
Odbor direktora
Broj: 00010-15142/8-1
Podgorica, 28.12.2016. godine

Projekat:	Javni PKI - Pošta Crne Gore AD
Naziv dokumenta:	**Pravilnik o postupcima izdavanja certifikata i zaštiti sistema certifikovanja (Certification Practice Statement - CPS)**
Verzija:	Verzija 7.0
Datum:	01.12.2016.
Autor:	Stevan Ljumović - Ministarstvo javne uprave Tatjana Popović, Andreja Vujačić, Ivan Brković - Pošta CG Dragomir Stevanović - S&T Crna Gora

Revizije dokumenta:

1. Radna verzija 1.0:
- workshop Bečići,
- datum 11.10.2010-13.10.2010.
- Obrađena poglavlja 1, 2, 3, 4, 8 i 9.

2. Radna verzija 1.0.2:
- sastanci radne grupe u periodu 14.10.2010 – 20.10.2010.
- Obrađena poglavlja 5, 6, i 7.

3. Radna verzija 1.0.3:
- dodati tipovi o OID i certifikata,
- datum 21.10.2010 (Rudi Ponikvar)
- dopunjeni opisi vezani na cert profile u 6. i 7,
- datum 21.10.2010 (Rudi Ponikvar)
  - Sekcija "3.1.4. Pravila za tumačenje različitih vrsta imena", dodata tabela "Oblik za SSL Server digitalne certifikate"
  - Sekcija "6.1.7. Namjena upotrebe ključeva (X.509 keyUsage), dodate tablice keyUsage i ExtendeKeyUsage
  - Sekcija "7.1.2. Ekstenzije certifikata", usaglašavanje sa odabranim modelom certifikata

4. Radna verzija 2.0:
- verifikacija teksta dokumenta i otklanjanje tipografskih grešaka i unifikacija pisma kojim je napisan dokument.
- Prihvatanje svih promjena na početnoj verziji dokumenta
- Definisanje značenja pojmova
  - Centralno registraciono tijelo
  - Lokalno registraciono tijelo
  - Kriptografski modul
  - Kriptografski token
  - PIN

5. Radna verzija 3.0
- sastanci radne grupe Pošte CG u periodu 21.10.2010 – 9.11.2010.
- prečišćen tekst Pravilnika
- definisani komentari

6. Radna verzija 4.0
- prečišćen konačan tekst Pravilnika koji je upućen Odboru direktora Pošte CG na usvajanje.

7. Konačna verzija 5.0
- prečišćen konačan tekst Pravilnika koji je usvojio Odbor direktora Pošte CG.

8. Konačna verzija 6.0 od 12.06.2012 godine
- prečišćen konačan tekst Pravilnika koji je usvojio Odbor direktora Pošte CG.
-

9. Pravilnik o izmjenama i dopunama Pravilnika o postupcima izdavanja certifikata i zaštiti sistema certifikovanja (Certification Practice Statement – CPS) od 23.12.2014 godine
- prečišćen konačan tekst Pravilnika o izmjenama i dopunama koji je usvojio Odbor direktora Pošte CG.

10. Pravilnik o izmjenama i dopunama Pravilnika o postupcima izdavanja certifikata i zaštiti sistema certifikovanja (Certification Practice Statement – CPS) od 10.12.2015 godine
- prečišćen konačan tekst Pravilnika o izmjenama i dopunama koji je usvojio Odbor direktora Pošte CG.

11. Konačna verzija 7.0 od 01.12.2016 godine
- prečišćen konačan tekst Pravilnika o izmjenama i dopunama koji je usvojio Odbor direktora Pošte CG.

Sadržaj

Na osnovu Zakona o elektronskom potpisu (Sl. list RCG 55/03), Zakona o izmjenama i dopunama zakona o elektronskom potpisu (Sl. list RCG 41/010) i člana 12. Pravilnika 2 o mjerama i postupcima upotrebe i zaštite elektronskog potpisa, sredstava za izradu elektronskog potpisa i sistema certifikovanja (Sl. list RCG 25/05) Odbor direktora Pošte Crne Gore na sjednici od 28.12.2016. donio je

Pravilnik o postupcima izdavanja certifikata
i zaštiti sistema certifikovanja
(Certification Practice Statement - CPS)

1. UVOD

1.1. Kratak pregled

Pošta Crne Gore upravlja infrastrukturom javnih ključeva [PoštaCG-PKI] za javne potrebe.
U okviru [Pošte CG-PKI] za potrebe davanja usluga certifikovanja uspostavljeno je certifikaciono tijelo sa samo-potpisanim certifikatom (*Single Rooted Certification Authority*) [PoštaCG-CA], koje izdaje kvalifikovane certifikate zainteresovanim fizičkim i pravnim licima.
Certifikaciono tijelo [PoštaCG-CA] izdaje slijedeće tipove digitalnih certifikata:

- kvalifikovani digitalni certifikat izdat na pametnoj kartici;
- kvalifikovani digitalni certifikati;
- kvalifikovani digitalni certifikat za poverljivost izdat na pametnoj kartici;
- kvalifikovani digitalni certifikat za poverljivost;
- digitalni certifikat za SSL server.
- digitalni certifikat za Microsoft Windows Domain Controllera (DC) server
- digitalni certifikat za SmartLogon

1.2. Naziv dokumenta i identifikacioni podaci

Ovaj dokument nosi naziv „Pravilnik o postupcima izdavanja certifikata i zaštite sistema certifikovanja“ i sadrži opšta pravila pružanja usluga certifikovanja, pravila o postupcima izdavanja certifikata i pravila o zaštiti sistema certifikovanja u daljem tekstu: Pravilnik.
Ovaj Pravilnik definiše slijedeće politike digitalnih certifikata (*Certificate policy identification - OID*), koje se međusobno razlikuju po tipu certifikata i namjeni upotrebe. Identifikacione oznake digitalnih certifikata sa opisom su dati u slijedećoj tabeli:

Kvalifikovani digitalni certifikati	
Kvalifikovani digitalni certifikat izdat na pametnoj kartici	
Opis:	Kvalifikovani digitalni certifikat izdat na pametnoj kartici
Namjena:	Napredni elektronski potpis definisan u Zakonu o elektronskom potpisu Član 7. i verifikacija identiteta korisnika
Period važenja:	Jedna (1) do pet (5) godina
Identifikaciona oznaka:	1.3.6.1.4.1.36737.1.1.1.1
Kvalifikovani digitalni certifikat	
Opis:	Kvalifikovani digitalni certifikat
Namjena:	Elektronski potpis definisan u Zakonu o elektronskom potpisu Član 6. i verifikacija identiteta korisnika
Period važenja:	Jedna (1) do pet (5) godina
Identifikaciona oznaka:	1.3.6.1.4.1.36737.1.1.1.2
Kvalifikovani digitalni certifikat za povjerljivost	
Kvalifikovani digitalni certifikat za povjerljivost izdat na pametnoj kartici	
Opis:	Kvalifikovani digitalni certifikat za povjerljivost izdat na pametnoj kartici sa mogućnošću oporavka istorije privatnih ključeva
Namjena:	Povjerljivost (šifriranje) podataka
Period važenja:	Jedna (1) do pet (5) godina
Identifikaciona oznaka:	1.3.6.1.4.1.36737.1.2.1.1.1
Kvalifikovani digitalni certifikat za povjerljivost	
Opis:	Kvalifikovani digitalni certifikat za povjerljivost sa mogućnošću oporavka istorije privatnih ključeva
Namjena:	Povjerljivost (šifriranje) podataka

Period važenja:	Jedna (1) do pet (5) godina
Identifikaciona oznaka:	1.3.6.1.4.1.36737.1.2.1.1.2
Digitalni certifikati za SSL	
Digitalni certifikat za SSL server	
Opis:	Digitalni certifikat za SSL servere
Namjena:	Identifikacija SSL servera i uspostavljanje SSL/TLS sesije
Period važenja:	Jedna (1) do pet (5) godina
Identifikaciona oznaka:	1.3.6.1.4.1.36737.1.3.1.1
Digitalni certifikat za DC (Microsoft Windows Domain Controllera) server	
Digitalni certifikat za DC (Microsoft Windows Domain Controllera) server	
Opis:	Digitalni certifikat za DC (Microsoft Windows Domain Controllera) servere
Namjena:	Verifikacija identiteta DC (Microsoft Windows Domain Controllera) servera i uspostavljanje SmartLogon funkcionalnosti
Period važenja:	Jedna (1) do pet (5) godina
Identifikaciona oznaka:	1.3.6.1.4.1.36737.1.3.1.2
Digitalni certifikat za SmartLogon	
Digitalni certifikat za SmartLogon izdat na pametnoj kartici	
Opis:	Digitalni certifikat za SmartLogon izdat na pametnoj kartici
Namjena:	Verifikaciju identiteta ili funkcije korisnika i uspostavljanje SmartLogon funkcionalnosti
Period važenja:	Jedna (1) do pet (5) godina
Identifikaciona oznaka:	1.3.6.1.4.1.36737.1.4.1.1.1

1.3. Učesnici infrastrukture javnih ključeva

1.3.1. Certifikaciono tijelo (*Certification Authority*)

Certifikaciono tijelo [PoštaCG] CA izdaje digitalne certifikate u skladu sa zakonom i ovim Pravilnikom.
Certifikaciono tijelo [PoštaCG] CA koristi za obavljanje svoje djelatnosti jedan izdavač certifikata sa samo-potpisanim certifikatom (*Single Rooted Certification Authority*), povjerljivu infrastrukturu i angažuje pojedince odgovorne za:

- Ukupni rad [PoštaCG] CA (*Policy Management Authority* - PMA);
- Izvođenje postupaka upravljanja certifikatima i upravljanje infrastrukturom, privatnih kriptografskih ključeva, servera i programa [PoštaCG] CA (*Operations Authority* - OA);
- Identifikaciju korisnika (*Registration Authority* - RA).

[PoštaCG] CA PMA je odgovoran za:

- Izradu i održavanje Pravilnika;
- Izradu i održavanje ostalih javnih dokumenata [PoštaCG] CA, kao što su Ugovor sa krajnjim korisnikom (*End-User Agreement*) ili izjava o davanju usluga certifikovanja (*PKI Disclosure Statement* - PDS);
- Podnošenje Pravilnika na usvajanje Odboru direktora Pošte Crne Gore;
- Predlaže za imenovanje osoblje [PoštaCG] CA OA na njihove dužnosti;
- Nadzor i reviziju usklađenosti davanja usluga certifikovanja [PoštaCG] CA sa ovim Pravilnikom;
- Autorizaciju oporavka i povratka istorije privatnih korisničkih ključeva za dešifriranje, koji su bili certifikovani po ovom Pravilniku;

- Rješavanje sporova između [PoštaCG] CA OA i [PoštaCG] CA RA.

[PoštaCG] CA OA odgovoran je za:

- Generisanje i sigurno upravljanje kriptografskim ključevima certifikacionog tijela i distribuciju javnih ključeva certifikacionog tijela;
- Uspostavljanje okoline i procedura za prihvat i obradu obrasca sa zahtjevima korisnika;
- Potpisivanje i izdavanje X.509 certifikata za povezivanje identiteta korisnika sa njihovim javnim kriptografskim ključevima;
- Objavljivanje certifikata u javnom LDAP imeniku;
- Opoziv certifikata na osnovu zahtjeva korisnika ili na svoju inicijativu;
- Izdavanje i objavljivanje liste opozvanih certifikata;
- Upravljanje infrastrukturom certifikacionog tijela u skladu sa ovim Pravilnikom;
- Rješavanje sporova između korisnika i certifikacionog tijela;
- Zahtijevanje opoziva certifikata članova operativnog osoblja certifikacionog tijela.

1.3.2. Registraciona tijela (*Registration Authorities*)

[PoštaCG] CA koristi jedno registraciono tijelo, koje radi u sastavu Pošte Crne Gore AD i koje je ovlašćeno za provjeru identiteta korisnika u postupcima upravljanja certifikata kao što su prvo izdavanje certifikata, obnova certifikata, opoziv certifikata i za odobravanje zahtjeva za izdavanje certifikata. Registraciono tijelo proslijeđuje odobrene zahtjeve operativnom. S obzirom da RA prikuplja zahtjeve u papirnom obliku, jedna kopija originalnih zahtjeva proslijeđuje se u [PoštaCG] CA. Način proslijeđivanja može biti ličnom dostavom ili internom poštom.

Registraciona tijela (Registration Authorities - RA) Certifikacionog tijela Pošte CG su:

- Centralno registraciono tijelo *(Central Registration Authority - CRA),* koje radi u sjedištu Certifikacionog tijela Pošte i koje je ovlašćeno za odobravanje i pro-sledjivanje podataka za izdavanje kvalifikovanih elektronskih certifikata i zahtjeva za promjenu statusa certifikata prema aplikaciji certifikacionog tijela.

- Lokalna registraciona tijela (*Local Registration Authority - LRA*) koja rade u poštama i na udaljenim lokacijama, ovlašćena su za provjeravanje identiteta korisnika i za proslijedjivanje podataka za izdavanje kvalifikovanih elektronskih certifikata i zahtjeva za promjenu statusa certifikata prema centralnom registracionom tijelu.

1.3.3. Naručioci i korisnici

[PoštaCG] Certifikaciono tijelo izdaje certifikate zaiteresovanim fizičkim i pravnim licima.

[PoštaCG] Certifikaciono tijelo izdaje certifikate naručiocu (*subscriber)* koji može biti fizičko lice ili pravno lice. Izdati certifikat upotrebljava korisnik (subject) čije ime ili funkcija je navedeno u certifikatu.Kada certifikat traži naručilac koji je fizičko lice, tada je naručilac istovremeno i korisnik.

Kada se certifikat izda naručiocu koji je pravno lice, tada naručilac daje certifikat na upotrebu korisniku.

Punu odgovornost za upotrebu certifikata snosi naručilac, bez obzira da li je naručilac fizičko ili pravno lice.

1.3.4. Treća lica (*Relying parties*)

Treća lica su subjekti, uključujući fizička i pravna lica, koji imaju certifikat izdat od strane [PoštaCG] CA, kao i subjekti koji nemaju certifikat izdat od strane [PoštaCG] CA i oslanjaju se na certifikat izdat od strane [PoštaCG] CA drugim korisnicima.

Da bi provjerili validnost certifikata koji su primili, treća lica moraju uvijek da konsultuju [PoštaCG] CA CRL listu prije nego što usvoje kao tačne informacije sadržane u certifikatu.

1.3.5. Ostali učesnici

Ostali učesnici su pravna lica koja, na neki način, doprinose ili učestvuju u obezbijedjivanju kvaliteta rada certifikacionog tijela.

1.4. Upotreba certifikata

1.4.1. Dozvoljena upotreba certifikata

Certifikati koje izdaje [PoštaCG] CA se mogu koristiti za različite namjene u zavisnosti od politike certifikata. Politika certifikata je u svakom izdatom korisničkom certifikatu označena u ekstenziji *certificatePolicies* u skladu sa specifikacijom u RFC-u (*Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*).

Certifikate izdate od strane [PoštaCG] CA je dozvoljeno koristiti za verifikaciju digitalnog potpisa, verifikaciju identiteta ili funkcije i obezbjeđivanje povjerljivosti podataka.. Dozvoljena namjena upotrebe pojedinog tipa certifikata koje izdaje [PoštaCG] CA je definisana u tablici u odjeljku 1.2. Naziv dokumenta i identifikacioni podaci.

1.4.2. Zabranjena upotreba certifikata

Svi certifikati izdati od strane [PoštaCG] CA treba da se koriste u skladu sa zakonom i drugim propisima iz ove oblasti .

1.5. Upravljanje pravilnika

1.5.1. Tijelo koje upravlja Pravilnikom

Ovim Pravilnik upravlja [PoštaCG] CA *Polica Managent Authority* (PMA).

1.5.2. Kontakt

Kontaktni podaci davaoca usluga certifikovanja [PoštaCG] CA su:

Adresa: Pošta Crne Gore

Certification Authority PMA
Slobode 1
81000 Podgorica
Crna Gora
E-mail: pma@postacg-ca.me
Internet: http://www. postacg-ca.me/
Kontaktni podaci [PoštaCG] CA Registracionog tijelo (RA):
Adresa: Pošta Crne Gore
Certification Authority RA
Slobode 1
81000 Podgorica
Crna Gora
E-mail: ra@postacg-ca.me

1.5.3. Subjekt koji utvrđuje usaglašenost Pravilnika sa zakonom

Nadležni organ shodno zakonu i propisima iz ove oblasti.

1.5.4. Postupci odobravanja Pravilnika

[PoštaCG] CA *Policy Management Authority* (PMA) odgovoran je za upravljanje svih aspekata [PoštaCG] CA i za usklađenost Pravilnika sa zakonom i drugim propisima iz ove oblasti.

1.6. Definicije i skraćenice

Aplikacija certifikacionog tijela - "Entrust Authority" aplikacija na serverima certifikacionog tijela koja generiše i potpisuje certifikate.
Centralno registraciono tijelo (Central Registration Authority - CRA) - tijelo koje radi u sjedištu [PostaCG] CA i koje je ovlašćeno za:

- odobravanje i prosleđivanje podataka za izdavanje kvalifikovanih elektronskih certifikata i zahtjeva za promjenu statusa certifikata prema aplikaciji certifikacionog tijela,
- kreiranje kvalifikovanih certifikata na kriptografskom tokenu za korisnike koji su izabrali ovaj model,
- prosleđivanje registracionog i autentikacionog koda, praznog kriptografskog tokena ili popunjenog kriptografskog tokena i PIN-a na adresu navedenu u zahtjevu ili lokanom registracionom tijelu.

Certifikaciono tijelo – pravno ili fizičko lice (preduzetnik) koje izdaje certifikate ili pruža druge usluge povezane s elektronskim potpisom, uključujući sisteme davalaca usluga certifikovanja za upravljanje certifikata.
Certifikat – potvrda u elektronskom obliku koja povezuje podatke za provjeru elektronskog potpisa sa nekim licem i potvrđuje identitet tog lica.
Elektronski dnevnik - elektronska forma zapisa o sprovedenim aktivnostima.
Elektronski dokument – dokument u elektronskom obliku koji se koristi u pravnom prometu, upravnim, sudskim i drugim postupcima, a uključuje sve oblike pisanog i drugog teksta, podatke, slike, crteže, karte, zvuk, muziku, govor, računarske baze podataka i sl.
Elektronski potpis – skup podataka u elektronskom obliku koji su pridruženi ili su logički povezani sa elektronskim dokumentom i koji služe za identifikaciju potpisnika.
Javni imenik – javno dostupan imenik LDAP koji sadrži certifikate koje je izdalo certifikaciono tijelo.
Kompromitovanje privatnog kriptografskog ključa - narušavanje bezbjednosti kojim se privatni kriptografski ključ izlaže mogućem neovlašćenom pristupu (neovlašćeno otkrivanje, mijenjanje, korišćenje i sl.).
Korisnička klijent aplikacija - aplikacija koju koristi korisnik za preuzimanje i rad sa certifikatom.
Korisnik - fizičko ili pravno lice koje će koristiti izdati certifikat i čiji se podaci nalaze u certifikatu.
Kriptografski modul – Aplikacija certifikacionog tijela koja omogućava kreiranje certifikata na kriptografskom tokenu ili drugom davaocu kriptografskih usluga.
Kriptografski token – Uređaj na kome se kreira digitalni certifikat, a koji zadovoljava sve tehničke zahtjeve za naprednim elektronskim potpisom navedene u Zakonu o elektronskom potpisu, podzakonskim aktima i ovom dokumentu. Kriptografski token može da bude u obliku pametne kartice, čitača pametnih kartica i pametne kartice ili token uređaja sa integrisanom pametnom karticom. Samo sa kriptografskim tokenom moguće je formirati napredni elektronski potpis.
Kvalifikovani digitalni certifikat - digitalni certifikat koji je izdat od strane certifikacionog tijela za izdavanje kvalifikovanih digitalnih certifikata i sadrži podatke predviđene zakonom.
Lokalno registraciono tijelo - (*Local Registration Authority - LRA*) – tijelo u okviru jedinstvene poštanske mreže ovlašćeno za provjeravanje identiteta korisnika i za prosljeđivanje podataka za izdavanje kvalifikovanih elektronskih certifikata i zahtjeva za promjenu statusa certifikata prema centralnom registracionom tijelu.
Napredni elektronski potpis - elektronski potpis kojim se pouzdano garantuje identitet potpisnika, integritet elektronskih dokumenata i onemogućava naknadno poricanje odgovornosti za njihov sadržaj, a koji ispunjava uslove utvrđene zakonom.
Naručilac - je fizičko ili pravno lice koje naručuje certifikat od certifikacionog tijela.
PIN – šifra koja se koristi za zaštitu pristupa privatnim ključevima korisnika koji se nalaze na kriptografskom tokenu.
Podaci za izradu elektronskog potpisa – jedinstveni podaci, kao što su kodovi ili privatni kriptografski ključevi koje potpisnik koristi za izradu elektronskog potpisa.
Podaci za provjeru elektronskog potpisa – podaci kao što su kodovi ili javni kriptografski ključevi koji se koriste za provjeru elektronskog potpisa.

Potpisnik – lice koje posjeduje sredstva za izradu elektronskog potpisa kojim se potpisuje u svoje ime ili u ime fizičkog ili pravnog lica koje predstavlja.
Registar opozvanih certifikata (*Certificate Revocation List - CRL*) - lista u koju se upisuju serijski brojevi i drugi podaci svih opozvanih certifikata koje je izdao [PoštaCG] CA tj. koje davalac usluga više ne smatra validnim.
Sredstva za izradu elektronskog potpisa – odgovarajuća računarska oprema ili računarski program koje potpisnik koristi pri izradi elektronskog potpisa uz korišćenje podataka za izradu elektronskog potpisa.
Sredstva za provjeru elektronskog potpisa – odgovarajuća računarska oprema ili program koji se koriste za provjeru elektronskog potpisa.
Vremenski pečat - dokument u elektronskom obliku potpisan od davaoca usluga certifikovanja kojim potvrđuje da su podaci bili sadržaj elektronskog dokumenta u vremenu navedenom u vremenskom pečatu.

Skraćenice:

ARL	Authoroty Revocation List
CA	Certification Authority
CN	Common Name
CRL	Certificate Revocation List
CSP	Certification Service Provider
DN	Distinguished Name
OCSP	Online Certificate Status Provider
OID	Object IDentifier
PDS	PKI Disclosure Statement
PKI	Public Key Infrastructure
PKIX	Internet X.509 Public Key Infrastructure
PMA	Policy Management Authority
RDN	Relative Distinguished Name
SHA-1	Secure Hash Algorithm 1 (see annex E on cryptographic algorithms)
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

2. OBJAVE I ODGOVORNOSTI REPOZITORIJUMA

2.1. Repozitoriji

[PoštaCG] CA objavljuje informacije vezane za upravljanje certifikata u repozitorijima na slijedećim adresama:
Javne web stranice: http://www.postacg-ca.me
Javni imenik LDAP: ldap://ldap.postacg-ca.me

2.2. Objava informacija o certifikatima

[PoštaCG] CA objavljuje:

- Izdate certifikate javnog ključa za šifrovanje;
- Razdjeljenu (*partitioned*) i sastavljenu (*combined*) listu opozvanih certifikata (CRL);
- Certifikat certifikacionog tijela;
- Pravilnik;
- Ugovor sa krajnjim korisnicima (*End User Agreement*);
- Formulare zahtjeva za upravljanje certifikatima;
- Korisnička uputstva;
- Korisničke klijent aplikacije za preuzimanje, obnovu i oporavak certifikata;
- Listu [PoštaCG] CA registracionih tijela;
- Cjenovnik proizvoda i usluga;
- Ostale javne informacije vezane za davanje usluga certifikovanja.

2.3. Vrijeme ili frekvencija objava

Certifikati se objavljuju odmah nakon što su izdati (gledaj i odjeljak 4.4). Lista opozvanih certifikata se objavljuje odmah nakon što je izdata (gledaj i odjeljak 4.9.7). Sve informacije se objavljuju odmah nakon što su se promijenile ili postale dostupne [PoštaCG] CA.

2.4. Kontrole pristupa do repozitorija

Sve javne informacije su dostupne za čitanje bez ograničenja.
Repozitoriji su dodatno zaštićeni od neovlašćenih promjena.

3. IDENTIFIKACIJA I AUTENTIFIKACIJA

3.1. Dodjeljivanje imena

3.1.1. Vrste imena

Stvarno ime koje se koristi u [PoštaCG] CA certifikatima, je ovjereno ime ili funkcija korisnika koje je definisano za naziv (Common Name - CN) u tabeli u odjeljku 3.1.4. Pravila za tumačenje različitih vrsta imena. U certifikatima je ime ili funkcija korisnika certifikata, polje Subject, upisano kao jedinstveno ime (Distinguished Name - DN), u obliku X.509 printableString, teletextString ili UTF8String i mora biti prisutno u svim certifikatima..

3.1.2. Potreba za smislenim imenima

Set atributa u jedinstvenom imenu upisanom u polje *Subject* jedinstveno identifikuje korisnika svakog certifikata i ima smislenu vrijednost. Atribut *serialNumber* se inkrementalno povećava za jedan za svakog novog korisnika.

3.1.3. Anonimnost korisnika i upotreba pseudonima

Nije primenljivo.

3.1.4. Pravila za tumačenje različitih vrsta imena

Polje *Subject* je upisano kao X.501 tip *Name* (*X.500 Distinguished Name - DN*) u skladu sa RFC3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

X.500 jedinstveno ime u certifikatima koje izdaje [PoštaCG] CA ima slijedeće oblike:

Oblik za fizička lica:

Atribut jedinstvenog imena	Sadržaj
Country (C =)	ME
Organization (O =)	PostaCG
Organizational Unit (OU =)	Fizičko lice
Common Name (CN=)	Ime i prezime ili funkcija korisnika
Serial Number (serialNumber =)	Jedinstveni serijski broj

Oblik za pravna lica:

Atribut jedinstvenog imena	Sadržaj
Country (C =)	ME
Organization (O =)	PostaCG
Organizational Unit (OU =)	Puno ime ili skraćeno ime i Matični broj pravnog lica
Common Name (CN=)	Ime i prezime ili funkcija korisnika
Serial Number (serialNumber =)	Jedinstveni serijski broj

Oblik za SSL server digitalne certifikate:

Atribut jedinstvenog imena	Sadržaj
Country (C =)	ME
Organization (O =)	PostaCG
Organizational Unit (OU =)	SSL Serveri
Common Name (CN=)	SSL server hostname sa domenom (FQDN)

Oblik za DC server digitalne certifikate:

Atribut jedinstvenog imena	Sadržaj
Country (C =)	ME
Organization (O =)	PostaCG
Organizational Unit (OU =)	Puno ime ili skraćeno ime i Matični broj pravnog lica
Common Name (CN=)	DC server hostname sa domenom (FQDN)

U kvalifikovanim elektronskim certifikatima su imena korisnika vjerno predstavljena odgovarajućim latiničnim slovima iz crnogorskog jezika.

Specijalni znaci čije korišćenje u imenima nije dozvoljeno su: ? (upitnik), \ (*backslash*), # (taraba), $ (dolar), % (procenat), = (jednako), + (plus), | (uspravna crta), ; (tačka-zarez), < (manje), > (veće) i , (zarez). Iste je potrebno izostaviti ili zamijeniti drugim znacima.

3.1.5. Jedinstvenost imena

[PoštaCG] CA garantuje jedinstvenost imena u svom domenu. [PoštaCG] CA dodjeljuje svakom korisniku jedinstveno ime (*Distinguished Name - DN*), koje se upisuje u polje *Subject* certifikata i polje *serialNumber*.

3.1.6. Prepoznavanje, verifikacija i uloga zaštitnih znakova

[PoštaCG] CA će preduzeti aktivnosti za rješavanje sporova koji mogu nastati tokom dodjele imena, npr. certifikaciono tijelo može kontaktirati podnosioca zahtjeva za izdavanje certifikata i dogovoriti se da se traženo ime u certifikatu promijeni tako da se razlikuje od imena u certifikatu već izdatom drugom korisniku.

[PoštaCG] CA zadržava pravo da po svojoj procjeni, odbije, promijeni, ponovo izda ili opozove certifikat.

3.2. Inicijalna provjera identiteta

3.2.1. Metoda za dokazivanje posjedovanja privatnog ključa

Dokaz o posjedovanju privatnog ključa je osiguran putem bezbjedne komunikacije između aplikacije certifikacionog tijela i korisnikove klijent aplikacije sa upotrebom *Certificate Management Protocols* protokola u skladu sa PKIX-CMP, Netscape SPKC, ili PKCS#10 u skladu sa RSA PKCS#10 Certification Request Syntax Standard.

3.2.2. Provjera identiteta pravnog lica

Pravno lice koje zahtijeva izdavanje certifikata mora da obezbijedi dovoljno dokaza o svom identitetu. Provjera identiteta pravnog lica može se vršiti koristeći jedan od slijedećih načina:

- Sačuvane informacije ako je bila provjera identiteta pravnog lica prethodno utvrđivana od strane [PoštaCG] CA;
- Original ili ovjerena kopija zvaničnih dokumenata koji pružaju dokaz o identitetu pravnog lica – rješenje, odnosno izvod o registraciji ne starije od šest mjeseci, odnosno za javne ustanove i nevladine organizacije i druge pravne subjekte, dokaz o registraciji od ovlašćenog nadležnog organa.

Pravno lice mora da podnese zahtjev preko fizičkog lica koje mora imati važeće ovlašćenje da djeluje u ime pravnog lica. [PoštaCG] CA RA će provjeriti identitet ovlašćenog lica kao što je definisano u odjeljku 3.2.3. Provjera identiteta fizičkog lica, i njegovo ovlašćenje da djeluje u ime pravnog lica kao što je definisano u odjeljku 3.2.5. Provjera ovlašćenja.

3.2.2a Ovlašćenje za predaju dokumentacije za izdavanje kvalifikovanog digitalnog certifikata.

Predaju dokumentacije za izdavanje kvalifikovanog digitalnog certifikata osim lica na čije ime glasi zahtjev i ovlašćenje za izdavanje/obnovu kvalifikovanog digitalnog certifikata može predati i fizičko lice koje mora imati važeće ovlašćenje na memorandumu pravnog lica, ovjereno pečatom i potpisano.

3.2.2.b Provjera identiteta stranog pravnog lica

Ukoliko se zahtjev za izdavanje certifikata podnosi za strano pravno lice za potrebe rada sa odredjenim pravnim licem iz Crne Gore potrebno je dostaviti:

- potvrdu/izjavu od ovlašćenog predstavnika pravnog lica iz Crne Gore da se traženi kvalifikovani digitalni certifikat za strano pravno lice izdaje za potrebe rada sa pravnim licem iz Crne Gore koje daje predmetnu izjavu / potvrdu;
- original ili ovjerenu kopiju zvaničnih dokumenata koji pružaju dokaz o identitetu pravnog lica – rješenje o registraciji iz domicilne države i prevod na engleski jezik od ovlašćenog lica;
- kopiju pasoša osobe na čije ime glasi kvalifikovani digitalni certifikat;
- zahtjev i ovlašćenje (shodno odjeljku 3.2.2. Provjera identiteta pravnog lica).

[PoštaCG] CA RA čuva kopiju ili original dokumenata na osnovu kojih je izvršena provjera identiteta pravnog lica.

3.2.3. Provjera identiteta fizičkog lica

Sva fizička lica koja žele da postanu korisnici certifikata koje izdaje [PoštaCG] CA će biti identifikovani licem u lice. Pojedinci moraju da se identifikuje koristeći jedan od slijedećih dokumenata koje je izdala država:

- Lična karta
- Pasoš

Prilikom identifikacije korisnik mora da posjeduje važeći identifikacioni dokument sa fotografijom (važeća lična karta ili pasoš).

3.2.4. Podaci o korisniku koji se ne provjeravaju

[PoštaCG] CA ne provjerava podatke koji se ne nalaze na identifikacionom dokumentu (npr. e-mail adresa).

3.2.5. Provjera ovlašćenja

Pojedinac koji zahtijeva certifikat u ime pravnog lica mora da obezbijedi validnu dokumentaciju na ime pravnog lica koje će biti upisano u certifikate, u skladu sa odjeljkom 3.2.2. Provjera identiteta pravnog lica. Ime pravnog lica koje će biti uključeno u certifikat mora biti identično punom ili skraćenom imenu pravnog lica kako je u prezentiranim dokumentima.

Podnosioci koji zahtijevaju certifikat za upotrebu u svoje ime moraju biti identifikovani kao lice čije ime će biti uključeno u certifikat.

3.2.6. Kriterijumi za povezivanje

Procedure i praksa povezanih certifikacionih tijela moraju biti materijalno ekvivalentni procedurama i praksi [PoštaCG] CA kao što je definisano u ovom Pravilniku. [PoštaCG] CA PMA treba da uradi procjenu procedura i prakse CA sa kojim se povezuje od slučaja do slučaja.

3.3. Provjera identiteta kod zahtjeva za obnovu certifikata

3.3.1. Provjera identiteta kod rutinske obnove certifikata

Rutinska obnova se odvija kad se valjanost certifikata ili privatnog ključa približava kraju.
Za certifikate koji se upravljaju koristeći protokol PKIX-CMP, novi ključevi i certifikati će se generisati automatski. Autorizacija korisnika se izvede na osnovu validnih ključeva za digitalni potpis.

Identifikacija korisnika certifikata koji se upravljaju koristeći protokol PKCS#10 ili Netscape SPKC se provjerava kao što je definisano u odjeljcima 3.2.2. Provjera identiteta 3.2.3. Provjera identiteta fizičkog lica ili slanjem digitalno potpisanog zahtjeva sa validnim ključevima za digitalni potpis korisnika koji zahtijeva obnovu certifikata. Digitalno potpisani zahtjev mora biti u propisanim formatima definisanim na Repozitoriju.

3.3.2. Provjera identiteta kod zahtjeva za obnovu certifikata poslije opoziva

Identifikacija korisnika koji zahtijevaju obnovu certifikata poslije opoziva se provjerava kao što je definisano u odjeljcima 3.2.2. Provjera identiteta pravnog lica i 3.2.3. Provjera identiteta fizičkog lica.

3.4. Provjera identiteta kod zahtjeva za opoziv

Korisnik certifikata koji želi da opozove certifikat, šalje elektronski potpisan zahtjev za opoziv registracionom tijelu sa validnim ključevima za digitalni potpis korisnika koji zahtijeva opoziv certifikata ili se lično identifikuje kao u odjeljku 3.2.3. Provjera identiteta fizičkog lica.
U slučaju da pravno lice koje je vlasnik certifikata traži opoziv, autentifikuje se kao u odjeljku 3.2.2. Provjera identiteta pravnog lica.

4. Upravljanje certifikatima

4.1. Zahtjev za izdavanje certifikata

4.1.1. Ko može da zahtijeva izdavanje certifikata

Zahtjev za izdavanje certifikata može podnijeti:

- Fizičko lice koje ispunjava zahtjeve navedene u obrascu za registraciju, [PoštaCG] CA CPS-a i relevantnom ugovoru sa korisnikom (*End-User Agreement*)
- Pravno lice koje ispunjava zahtjeve navedene u obrascu za registraciju, [PoštaCG] CA CPS-a i relevantnom ugovoru.

4.1.2. Proces obrade zahtjeva i odgovornosti

4.1.2.1. Proces obrade zahtjeva i odgovornosti za certifikate koje korisnik preuzima sam

[PoštaCG] CA izdaje certifikate tek nakon provjere identiteta korisnika i uspješnog završetka procesa registracije. Glavni koraci u procesu obrade zahtjeva za izdavanje certifikata su:

- korisnik podnese potpisan obrazac za prijavu i priloži valjan dokument za identifikaciju kao što je opisano u 3.2. Inicijalna provjera identiteta;
- korisnik prihvata [PoštaCG] CA CPS-a i uslove potpisivanjem ugovora sa korisnikom (*End-User Agreement*);
- Zahtjev za izdavanje certifikata je prihvaćen i odobren od strane [PoštaCG] CA Local Registration Authority;
- Local Registration Authority podnosi zahtjev za certifikat [PoštaCG] CA Central Registration Authority službi (Centralna Služba za Registraciju CRA);
- [PoštaCG] CA CRA dodaje i aktivira korisnika u aplikaciji certifikacionog tijela sa odgovarajućim profilom certifikata. Aplikacija certifikacionog tijela generiše kodove za aktiviranje, koji se sastoje od referentnog broja i autorizacionog koda. Kodovi za aktiviranje trebaju korisniku u tehničkom postupku preuzimanja certifikata;
- kodove za aktiviranje certifikata koje korisnik preuzima sam je potrebno poslati korisniku koji je tražio izdavanje certifikata:
  - Referentni broj šalje CRA elektronskim putem na e-mail adresu koju je korisnik naveo na obrascu zahtjeva za izdavanje certifikata;
  - autorizacijski kod je odštampan i zatvoren u kovertu. CRA isporučuje kovertu preporučeno putem pošte ili je korisnik preuzima lično u LRA kancelariji.

Korisnik koristi kodove za aktiviranje u svojoj aplikaciji (klijent aplikacija [PoštaCG] CA, ili internet pretraživaču) kad preuzima certifikat od certifikacionog tijela. Popis podržanih klijentskih aplikacija i internet pretraživača je objavljen, zajedno sa korisničkim uputstvima, na [PoštaCG] CA javnim web stranicama na adresi navedenoj u odjeljku 2.1. Repozitoriji.

4.1.2.2. Proces obrade zahtjeva i odgovornosti za certifikate koji se izdaju na kriptografskom tokenu

[PoštaCG] CA izdaje certifikate tek nakon provjere identiteta korisnika i uspješnog završetka procesa registracije. Glavni koraci u procesu obrade zahtjeva za izdavanje certifikata su:

- korisnik podnese potpisan obrazac za prijavu i priloži valjan dokument za identifikaciju kao što je opisano u 3.2. Inicijalna provjera identiteta;
- korisnik prihvata [PoštaCG] CA CPS-a i uslove potpisivanjem ugovora sa korisnikom (*End-User Agreement*);
- Zahtjev za izdavanje certifikata je prihvaćen i odobren od strane [PoštaCG] CA Local Registration Authority;
- Local Registration Authority podnosi zahtjev za certifikat [PoštaCG] CA Central Registration Authority službi (Centralna Služba Za Registraciju CRA);
- [PoštaCG] CA CRA dodaje i aktivira korisnika u aplikaciji certifikacionog tijela sa odgovarajućim profilom certifikata. Aplikacija certifikacionog tijela generiše kodove za aktiviranje, koji se sastoje od referentnog broja i autorizacionog koda. Kodovi za aktiviranje trebaju korisniku u tehničkom postupku preuzimanja certifikata;
- Kriptografski token i PIN za zaštitu kriptografskog tokena na koji je preuzet certifikat je potrebno poslati korisniku koji je tražio izdavanje certifikata:
  - Kriptografski token CRA isporučuje u koverti preporučeno putem pošte ili je korisnik preuzima lično u LRA kancelariji;
  - PIN za zaštitu kriptografskog tokena na koji je preuzet certifikat je odštampan i zatvoren u kovertu. CRA isporučuje Post Express-om ili je korisnik preuzima lično u LRA kancelariji.

4.2. Procesuiranje zahtjeva za certifikat

4.2.1. Postupak identifikacije i autentifikacije

[PoštaCG] CA vrši identifikaciju i autentifikaciju kao što je definisano u odjeljku 3.2.2. Provjera identiteta pravnog lica i 3.2.3. Provjera identiteta fizičkog lica.

4.2.2. Odobravanje ili odbijanje zahtjeva za izdavanje certifikata

Zahtjev za [PoštaCG] CA certifikat će biti odobren ako su ispunjeni svi slijedeći uslovi:

- Podnosilac zahtjeva je predao popunjen obrazac zahtjeva za izdavanje i priložio važeće dokumente za identifikaciju u skladu sa odjeljkom 3.2.2. Provjera identiteta pravnog lica i 3.2.3. Provjera identiteta fizičkog lica;
- Podnosilac zahtjeva ima odgovarajuće ovlašćenje, ako djeluje u ime pravnog lica;
- Podaci na obrascu zahtjeva za izdavanje su potpuni;
- Identifikacija identiteta korisnika i po potrebi ovlašćenja je uspješna;
- Podnosilac zahtjeva je potpisom ugovora sa korisnikom potvrdio da je upoznat sa uslovima [PoštaCG] CA CPS i da ih prihvata.

U slučaju da bilo koji od navedenih kriterijuma nije ispunjen ili ako postoji opravdana sumnja da podnosilac zahtjeva ne ispunjava uslove ovog Pravilnika, Ugovora sa korisnikom ili važećim zakonima Crne Gore, [PoštaCG] CA Registration Authority će odbiti zahtjev. [PoštaCG] CA zadržava pravo odbiti zahtjev bez navođenja razloga.

4.2.3. Vrijeme za obradu zahtjeva

Inicijalna obrada zahtjeva za izdavanje certifikata počinje u toku prisustva podnosioca zahtjeva u [PoštaCG] CA LRA, tj. obavezno se u dijelu inicijalne obrade mora obaviti provjera identiteta podnosioca zahtjeva.
[PoštaCG] CA će kompletnu obradu zahtjeva, pod uslovom da su svi podaci u zahtjevu tačni i u skladu sa ovim Pravilnikom, završiti u roku od najviše 15 dana od dana prijema zahtjeva.

4.3. Izdavanje certifikata

4.3.1. Postupci CA u fazi izdavanja certifikata

[PoštaCG] CA aplikacija će po prijemu zahtjeva za izdavanje certifikata:

- provjeriti valjanost kodova za aktiviranje uključenih u zahtjevu;
- provjeriti da korisnik posjeduje privatni ključ povezan s javnim ključem uključenim u zahtjev za izdavanje certifikata, kao što je propisano u odjeljku 3.2.1. Metoda za dokazivanje posjedovanja privatnog ključa ;
- ovjeriti sadržaj zahtjeva u skladu s protokolom PKIX-CMP, Netscape SPKC ili PKCS#10;
- izdati traženi certifikat, ako su ispunjeni svi gore navedeni uslovi.

Kvalifikovani digitalni certifikat može podići samo lice na čije ime isti glasi (samo lično).

Ne predvidja se mogućnost podizanja certifikata uz ovlašćenje drugog lica.

Izuzetno, kvalifikovani digitalni certifikat izdat za strano pravno lice može se preuzeti uz ovlašćenje podnosioca zahtjeva (stranog pravnog lica), dato pravnom licu iz Crne Gore identifikovanom u tački 3.2.2.b poglavlje 3 ovjerenog kod nadležnog organa domicilne države (notar, sud).

4.3.2. Obavještavanje korisnika o izdavanju certifikata od strane CA

Aplikacija certifikacionog tijela [PoštaCG] CA će izdati certifikat odmah posle prijema zahtjeva od klijent aplikacije korisnika i odmah slati certifikat klijent aplikaciji korisnika, tako da je korisnik odmah obaviješten i nije potrebno slati dodatno obavještenje.
Za certifikate izdate na kriptografskom tokenu, [PoštaCG] CA CRA će poslati odgovarajuće obavještenje na e-mail adresu iz zahtjeva za izdavanje kvalifikovanog digitalnog certifikata.

4.4. Prihvatanje certifikata

4.4.1. Postupak potvrde prihvata certifikata od strane korisnika

Korisnik će primiti sve potrebne certifikate u toku on-line procesa preuzimanja certifikata (vidi odjeljak 4.3). Dodatna potvrda prihvatanja certifikata od strane korisnika nije potrebna.
U slučaju neuspješnog preuzimanja certifikata, mora korisnik o problemu obavijestiti [PoštaCG] RA (vidi RA kontakt informacije u odjeljku 1.5.2 Kontakt).
U slučaju certifikata izdatog na kriptografskom tokenu korisnik svojeručnim potpisom potvrđuje preuzimanje kriptografskog tokena.
Ukoliko se naknadno utvrdi da u kvalifikovanom certifikatu postoje pogrešni podaci, korisnik je dužan da se obrati [PoštaCG] RA radi opoziva i eventualnog izdavanja novog certifikata (vidi RA kontakt informacije u odjeljku 1.5.2 Kontakt).

4.4.2. Objava certifikata od strane certifikacionog tijela

[PoštaCG] CA će objaviti sve certifikate koji imaju postavljen bit za enkripciju u javnom LDAP direktorijumu navedenom u odjeljku 2.1 Repozitoriji. Certifikati koji se koriste samo za digitalni potpis (postavljen samo bit (0) *digitalSignature* za digitalni potpis ili samo bit (1) *nonRepudiation* za ne-poricanje) ili autentifikaciju neće biti objavljeni.

4.4.3. Obavještavanje ostalih učesnika o izdavanje certifikata

[PoštaCG] CA neće obavijestiti nijednog drugog učesnika.

4.5. Upotreba para ključeva i certifikata

4.5.1. Upotreba privatnog ključa i certifikata sa strane korisnika

[PoštaCG] CA izdaje certifikate koji mogu podržavati jedan ili više namjena upotrebe ključa. Podrška za različite namjene je implementirana upotrebom ekstenzija u certifikatu u skladu sa Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile preporukama.
Korisnik treba da koristi certifikate u skladu sa *keyUsage* i *extKeyUsage* X.509 ekstenzijama u certifikatu i za namjene definisane u odjeljku 1.4.1. Dozvoljena upotreba certifikata. Korisnik mora čuvati privatni ključ, te preduzeti mjere opreza kako bi se spriječilo otkrivanje i neovlašćeno korišćenje njegovog privatnog ključa.

4.5.2. Upotreba javnog ključa i certifikata sa strane trećih lica

Treća lica trebaju da ograniče oslanjanje na javne ključeve sadržane u certifikatima koje izdaje [PoštaCG] CA za namjene definisane u odjeljku 1.4.1. Dozvoljena upotreba certifikata. Treća lica također trebaju da:

- budu svjesni ograničenja certifikata i odgovornosti [PoštaCG] CA definisanih u ovom dokumentu;
- provjere da certifikat nije opozvan, koristeći bilo koju važeću evidenciju opozvanih certifikata (CRLs) koju objavljuje [PoštaCG] CA;
- odmah obavijeste CA u slučaju sumnje ili poznate zloupotrebe bilo kojeg certifikata kojeg je izdao [PoštaCG] CA.

4.6. Obnova certifikata bez promjene ključa

Obnova certifikata bez promjene ključa je proces u kojem certifikaciono tijelo izdaje certifikat za isti javni ključ, što za certifikate koje izdaje [PoštaCG] CA nije dozvoljeno.

4.7. Obnova certifikata

Obnova certifikata je proces u kojem certifikaciono tijelo izdaje korisniku novi certifikat. Novi certifikat sadrži iste identifikacione podatke o korisniku kao stari certifikat i korisnikov novi javni ključ.

4.7.1. Okolnosti pod kojima se može obnoviti certifikat

Obnova certifikata se vrši:

- nakon opoziva certifikata ili
- nakon što je istekao vremenski period važnosti certifikata ili privatnog ključa.

4.7.2. Ko može da zahtijeva obnovu certifikata

Obnovu certifikata mogu tražiti korisnik ili ovlašćeni predstavnik pravnog lica koji je zatražio izdavanje prvog certifikata.

4.7.3. Proces obrade zahtjeva za obnovu certifikata

Obnova certifikata kojim se upravljaju pomoću PKIX-CMP se obavlja automatski prije isteka razdoblja korišćenja certifikata ili privatnog ključa. Ako istekne razdoblje korišćenja privatnog ključa prije nego što se izvrši obnova certifikata, postupak je isti kao i za početni zahtjev za certifikat.

Obnova certifikata kojim se upravljaju pomoću PKCS # 10 izvodi se na isti način kao početni zahtjev za certifikat.

4.7.4. Obavještavanje korisnika o izdavanju obnovljenog certifikata

Kao što je opisano u odjeljku 4.3.2. Obavještavanje korisnika o izdavanju certifikata od strane CA.

4.7.5. Postupak potvrde prihvatanja obnovljenog certifikata

Kao što je opisano u odjeljku 4.4.1. Postupak potvrde prihvata certifikata od strane korisnika.

4.7.6. Objava obnovljenog certifikata

Kao što je opisano u odjeljku 4.4.2. Objava certifikata od strane certifikacionog tijela.

4.7.7. Obavještavanje ostalih učesnika o izdavanju obnovljenog certifikata

Kao što je opisano u odjeljku 4.4.3. Obavještavanje ostalih učesnika o izdavanje certifikata.

4.8. Promjena certifikata

Promjena certifikata je postupak koji omogućava korisnicima da zahtijevaju promjenu podataka sadržanih u certifikatu. Promjena certifikata traži obnovu certifikata i obrađuje se kao početni zahtjev za certificiranje.

4.8.1. Okolnosti pod kojima se može promjeniti certifikat

Korisnik može zahtijevati promjenu certifikata kada se promijeni bilo koji od identifikacionih podataka (npr. ime, e-mail adresa).

4.8.2. Ko može da zahtijeva promjenu certifikata

Promjenu certifikata mogu tražiti korisnik ili ovlašćeni predstavnik pravnog lica koji je tražio izdavanje prvog certifikata.

4.8.3. Proces obrade zahtjeva za promjenu certifikata

Zahtjev za promjenu certifikata je obrađen kao početni zahtjev za certifikovanje.

4.8.4. Obavještavanje korisnika o izdavanju promijenjenog certifikata

Kao što je opisano u odjeljku 4.4.1. Postupak potvrde prihvata certifikata od strane korisnika.

4.8.5. Postupak potvrde prihvata promijenjenog certifikata

Kao što je opisano u odjeljku 4.4.1. Postupak potvrde prihvata certifikata od strane korisnika.

4.8.6. Objava promijenjenog certifikata

Kao što je opisano u odjeljku 4.4.2. Objava certifikata od strane certifikacionog tijela.

4.8.7. Obavještavanje ostalih učesnika o izdavanju promijenjenog certifikata

Kao što je opisano u odjeljku 4.4.3. Obavještavanje ostalih učesnika o izdavanje certifikata.

4.9. Opoziv i suspenzija certifikata

4.9.1. Okolnosti pod kojima se vrši opoziv certifikata

Izdati certifikat se opoziva u slijedećim slučajevima:

- ako opoziv traži korisnik ili ovlašćeni predstavnik pravnog lica koji je tražio izdavanje prvog certifikata;
- ako certifikaciono tijelo sazna da je korisnik umro ili je izgubio svoje poslovne sposobnosti ili je pravno lice prestalo postojati ili ako su se stvorile okolnosti koje imaju značajan efekat na valjanost certifikata;
- kada neka informacija sadržana u certifikatu postaje netačna ili se sumnja da je netačna;

- kada je kompromitovan privatni ključ povezan s certifikatom ili se sumnja da je bio kompromitovan;
- kada je kompromitovan bilo koji podatak za aktiviranje privatnog ključa, kao što su lozinke ili PIN;
- ako certifikaciono tijelo utvrdi da certifikat nije izdat ispravno ili u skladu s [PoštaCG] CA Pravilnikom;
- korisnik krši odredbe [PoštaCG] CA Pravilnika;
- iz drugih razloga koji su utvrđeni Zakonom o elektronskom potpisu i drugim propisima koji regulišu ovu oblast.

[PoštaCG] CA Policy Management Authority može opozvati [PoštaCG] CA certifikat, kada to smatra potrebnim.

4.9.2. Ko može da zahtijeva opoziv certifikata

Opoziv certifikata može biti zatražen:

- od strane korisnika certifikata;
- na službeni zahtjev od strane suda, nadležnog organa državne uprave, odnosno pravnog lica kod kojeg je potpisnik zaposlen u trenutku podnošenja zahtjeva za opoziv certifikata;
- na zahtjev davaoca usluga certifikovanja u slučajevima neispunjavanja tehničkih uslova, odnosno ako se pri upotrebi elektronskog potpisa ne postupa na propisani način.

4.9.3. Postupak opoziva

Zahtjev za opoziv certifikata može biti podnesen od strane korisnika ili ovlašćenog predstavnika pravnog lica na potpisanom i ovjerenom obrascu poslatom poštom, lično u [PoštaCG] CA LRA kancelariji ili u elektronskom obliku, digitalno potpisanim sa privatnim ključem koji je predmet zahtjeva za opoziv u skladu sa propisanim formatima definisanim na Repozitoriju, koji se šalje na e-mail adresu [PoštaCG] CA RA navedenu u odjeljku 1.5.2. Kontakt.

Identifikacija podnosioca zahtjeva za opoziv se radi kao što je definisano u odjeljku 3.4 Provjera identiteta kod zahtjeva za opoziv.

4.9.4. Vrijeme za predaju zahtjeva za opoziv

Subjekt koji je postao svjestan okolnosti koje zahtijevaju opoziv certifikata mora zatražiti opoziv što je prije moguće i bez nepotrebnog odgađanja.

4.9.5. Vrijeme od zahtjeva za opoziv do opoziva

U svim slučajevima opoziva certifikata certifikaciono tijelo će objaviti opoziv u evidenciji opozvanih certifikata (CRL) najkasnije slijedećeg radnog dana od trenutka kad je [PoštaCG] CA RA primio valjan zahtjev za opoziv.

4.9.6. Obaveza provjere registra opozvanih certifikata sa strane trećih lica

Treća lica su dužna provjeriti [PoštaCG] CA CRL prije korišćenja bilo kojeg certifikata izdatog od strane [PoštaCG] CA. Ako se ne može utvrditi status certifikata, zbog otkaza sistema ili gubitka servisa, treća strana ne smije prihvatiti certifikat.

Treća lica koja pristupaju CRL treba da provjere kredibilitet i integritet CRL, provjerom digitalnog potpisa koristeći [PoštaCG] CA certifikat, kao i da period važenja CRL nije istekao.

4.9.7. Frekvencija izdavanja registra opozvanih certifikata (CRL)

[PoštaCG] CA izdaje CRL odmah posle izvođenja opoziva bilo kojeg certifikata, odnosno najmanje jednom u 24 sata sa razdobljem važenja CRL 48 sati.

4.9.8. Dozvoljena zakašnjenja kod objave registra opozvanih certifikata

Nema uslova. (vidi odjeljak 4.9.7)

4.9.9. On-line provjera statusa certifikata

Ne koristi se.

4.9.10. Zahtjev za on-line provjeru statusa certifikata

Ne koristi se.

4.9.11. Ostali oblici objavljivanja statusa certifikata

Ne koristi se.

4.9.12. Posebni zahtjevi u slučaju kompromitovanja ključa

Nema posebnih zahtjeva u slučaju kompromitovanja privatnog ključa korisnika.

4.9.13. Okolnosti pod kojima se može izvršiti suspenzija certifikata

Ne koristi se.

4.9.14. Ko može da traži suspenziju certifikata

Ne koristi se.

4.9.15. Postupak suspenzije

Ne koristi se.

4.9.16. Ograničenja perioda trajanja suspenzije

Ne koristi se.

4.10. Servis objavljivanja statusa certifikata

4.10.1. Operativne karakteristike

Certifikaciono tijelo objavljuje status certifikata koristeći X.509 liste opozvanih certifikata (*X.509 Certificate Revocation List - CRL*). CRL je objavljen putem LDAP imenika i web stranice. Tačne lokacije (LDAP i HTTP adrese) objavljene su korišćenjem X.509 CRL Distribution Points ekstenzije koja se nalazi u svim izdatim certifikatima.

4.10.2. Raspoloživost servisa

[PoštaCG] CA garantuje dostupnost servisa za objavljivanje CRL 24 sata/7 dana nedeljno, uz maksimalne neplanirane prekide rada najviše deset (10) dana u godini.

U slučaju planiranih prekida servisa informacija o vremenu i planiranom periodu prekida servisa biće objavljena na javnim web stranicama kao što je definisano u 2 OBJAVE I ODGOVORNOSTI REPOZITORIJUMA.

4.10.3. Dodatne funkcije

Nije primjenjivo.

4.11. Prekid dogovora/ugovora/sporazuma

Ugovor o korišćenju certifikata završava nakon isteka vremenskog perioda važenja izdatog certifikata, opoziva poslednjeg certifikata korisnika ili obavještenja ovlašćenog predstavnika pravnog lica koje je tražilo izdavanje certifikata. Pravno lice koje je tražilo izdavanje certifikata je dužno obavijestiti [PoštaCG] CA o postojanju okolnosti zbog kojih certifikat više nije potreban (na primer korisnik nije više u radnom odnosu).

[PoštaCG] CA čuva dokumentaciju u vezi korisnika, certifikata i statusa certifikata u skladu sa zakonima Crne Gore.

U slučaju da korisnik prekine ugovor prije isteka važenja certifikata, [PoštaCG] CA će opozvati korisnikove certifikate izdate po prekinutom ugovoru.

4.12. Deponovanje (escrow) i povratak ključa

Deponovanje (escrow) privatnog ključa u okviru [PoštaCG] CA infrastrukture nije dozvoljeno.

4.12.1. Pravila upravljanja deponovanja i povratka privatnih ključeva za dešifrovanje

[PoštaCG] CA nikada ne čuva kopije privatnih ključeva korisnika kvalifikovanih certifikata koji se koriste za digitalni potpis ili autentifikaciju.

Povratak istorije privatnog ključa za dešifrovanje je podržan samo za [PoštaCG] CA certifikate koji imaju postavljen bit *keyEncypherment* i za koje se radi kopija privatnog ključa kao što je definisano u 1.2. Naziv dokumenta i identifikacioni podaci.

Povratak istorije privatnih ključeva za dešifrovanje može tražiti korisnik, ili pravno lice koje je zahtijevalo početno izdavanje certifikata. Identitet korisnika je potvrđen kao što je definisano u odjeljku 3.2. Inicijalna provjera identiteta.

Povratak istorije privatnih ključeva se obavlja na isti način kao obnova certifikata.

Povratak istorije privatnih ključeva mora biti na aplikaciji certifikacionog tijela uvijek ovlašćen od strane dva [PoštaCG] CA OA administratora sa odgovarajućim dozvolama.

4.12.2. Pravila upravljanja enkapsulacije ključa sesija i povratka

Nije primjenljivo.

5. KONTROLA FIZIČKOG PRISTUPA, PROCEDURA I OSOBLJA

5.1. Fizička zaštita

5.1.1. Lokacija i konstrukcija

Najvažnija oprema [PoštaCG] CA certifikacionog tijela se nalazi u posebnoj i zaštićenoj prostoriji, lociranoj u zgradi Pošte Crne Gore.
Kontrola fizičkog pristupa certifikacionom tijelu je implementirana u skladu sa zakonom i propisima iz ove oblasti, i to na slijedeći način:

- Pristup bez pratnje je ograničen na operativno osoblje [PoštaCG] CA certifikacionog tijela;
- Pristup sa pratnjom ovlašćenog lica se zahtijeva za sva lica osim operativnog osoblja [PoštaCG] CA;
- Pristup se može sprovoditi isključivo uz prisustvo najmanje dva ovlašćena lica koja imaju pravo pristupa informacionom sistemu davaoca usluga certifikovanja;
- Svaki pristup prostorijama je elektronski zabilježen i unijet u elektronski dnevnik za pristup prostorijama. Elektronski dnevnici se pregledaju najmanje jedanput nedeljno;
- Pristup zbog održavanja sistema mora biti unaprijed najavljen osim u slučaju hitne intervencije operativnog osoblja [PoštaCG] CA;
- Za vrijeme prisustva lica za održavanje vrši se stalni video nadzor;
- Svaki pristup prostoriji certifikacionog tijela se evidentira u poseban dnevnik navodeći ime i prezime, datum i vrijeme pristupa i razlog pristupa;
- Na svim ulazima u prostorije certifikacionog tijela su postavljeni elektronski sistemi za kontrolu pristupa i nadzor;
- Zgrada u kojoj se nalazi oprema certifikacionog tijela je 24 sata/7 dana pod kontrolom stražara ili video nadzorom i alarmnim sistemom.

5.1.2. Kontrola fizičkog pristupa

[PoštaCG] CA certifikaciono tijelo koristi za kontrolu fizičkog pristupa elektronske brave sa elektronskom karticom ili čitačem otiska prsta.
Sve sigurnosno osjetljive prostorije [PoštaCG] CA certifikacionog tijela su nadgledane 24 sata/7 dana nedeljno:

- video nadzorom tj. senzorima koji su povezani sa centralnim uređajem sistema u portirnici,
- sistemom protivprovalne zaštite na nivou poslovne zgrade Pošte Crne Gore tj. senzorima koji su povezani sa policijom i sistemom obavještavanja na mobilni telefon rukovodioca službe za osiguranje i protivpožarnu zaštitu.

5.1.3. Napajanje i klimatizacija

Sigurnosno osjetljive prostorije [PoštaCG] CA su opremljene dvostrukim klima uređajima za održavanje temperature. Sistemi za nadzor stalno prate njihov rad i šalju alarm na minimalno dva mobilna telefona članova operativnog osoblja [PoštaCG] CA u slučaju kvara ili odstupanja od normalnih vrijednosti.
Sve kritične komponente su vezane na sistem za neprekidno napajanje (UPS) .

5.1.4. Zaštita od vode

Unutar prostorija certifikacionog tijela nema vodovodnih instalacija. U blizini zgrade u kojoj se nalazi certifikaciono tijelo nema riječnih tokova, a prostorija je smještena na drugom spratu.

5.1.5. Zaštita od vatre

Kompletan prostor je zaštićen sistemom za otkrivanje i automatsku dojavu požara tj. senzorima koji su povezani sa centralnim uređajem sistema u portirnici i sistemom obavještavanja na mobilni telefon rukovodioca službe za osiguranje i protivpožarnu zaštitu.

5.1.6. Smještanje medija

Svi mediji na kojima se nalaze podaci certifikacionog tijela, uključujući rezervne kopije sistema, su smješteni u sefu otpornom na vatru u prostorijama certifikacionog tijela.
Mediji poslati na udaljenu lokaciju se čuvaju u sefu u poslovnoj banci.

5.1.7. Odlaganje nepotrebnih materijala

Nepotrebna papirna dokumentacija i računarski mediji za smeštaj podataka se fizički uništavaju prije odlaganja na otpad. Svi podaci sa nepotrebnih medija koji se koriste za smeštaj podataka kao što su kriptografski ključevi, podaci za aktiviranje ili datoteke biće nepovratno obrisani prije nego što se iznesu iz prostorija certifikacionog tijela ili prije uništenja.

5.1.8. Smještanje kopija medija na udaljenoj lokaciji

[PoštaCG] CA koristi bezbjednu udaljenu lokaciju za smještaj medija sa podacima. Mediji se smještaju u udaljenu bezbjednu zonu zaštićenu od spoljnih uticaja i sa kontrolom pristupa, koja ima uporediv nivo zaštite sa bezbjednom zonom na primarnoj [PoštaCG] CA lokaciji.

5.2. Kontrola procedura

5.2.1. Povjerljive uloge osoblja certifikacionog tijela

Zavisno od njihove uloge, [PoštaCG] CA osoblje može imati korisnički nalog na: serverima certifikacionog tijela, aplikaciji certifikacionog tijela ili na oba. Aplikacija certifikacionog tijela koju koristi [PoštaCG] CA ima implementiranu podjelu ovlašćenja između pouzdanih uloga koje se dodjeljuju osoblju u skladu s njihovim obavezama.
Aplikacija certifikacionog tijela koristi brojne povjerljive uloge, koje se dodjeljuju osoblju u zavisnosti od njihovih dužnosti. Privilegije određenih naloga na operativnim sistemima računara i naloga u aplikacijama, ograničavaju pristup osoblju certifikacionog tijela na radnje koje su im potrebne u obavljanju njihovih dužnosti.
Razdvajanje dužnosti povjerljivih uloga na aplikaciji certifikacionog tijela se osigurava različitim nivoima fizičke kontrole i kontrole pristupa na operativnom sistemu.
Povjerljive uloge osoblja certifikacionog tijela su:

- PKI Master User
- PKI Security Officer
- PKI Administrator
- Referent registracionog tijela

PKI *Master User* ima neophodne privilegije da:

- Izvrši konfiguraciju hardvera i softvera certifikacionog tijela;
- Upravlja hardverom i softverom certifikacionog tijela uključujući i obnovu ključeva samog certifikacionog tijela;
- Izvrši inicijalnu konfiguraciju aplikacija certifikacionog tijela i upravlja istim;
- Startuje i zaustavi servise aplikacija certifikacionog tijela;
- Kreira početne PKI *Security Officer* naloge;
- Obnovi PKI *Security Officer* naloge;
- Obnovi administrativne servise certifikacionog tijela;
- Izvrši kreiranje rezervnih kopija, obnovu i ponovno šifrovanje baze podataka aplikacije certifikacionog tijela.

PKI *Security Officer* ima neophodne privilegije da:

- Upravlja nalozima ostalih PKI *Security Officer*-a, PKI *Administrator*-a;
- Upravlja nalozima korisnika;
- Postavlja i mijenja pravila bezbjednosti certifikacionog tijela;
- Vrši međusobnu certifikaciju certifikacionog tijela sa drugim certifikacionim tijelima (*cross certification)*;
- Pregleda elektronske dnevnike;
- Postavlja početnu firewall konfiguraciju i nadgleda tekuće održavanje;
- Upravlja profilima certifikata;
- Sastavlja izvještaje.

PKI *Administrator* ima neophodne privilegije da:

- Organizuje i vrše prikupljanje, kontrolu i unos korisničkih zahtjeva dobijenih od LRA;
- Organizuje slanje i uručenje enkripcionih tokena ili neophodnih podataka za kreiranje certifikata;
- Obavlja komunikaciju sa podnosiocima zahtjeva u slučaju potrebe;
- Odobrava korisničke zahtjeve;
- Upravlja korisničkim nalozima;
- Upravlja oporavkom kriptografskih ključeva korisnika certifikata;
- Upravlja certifikatima;
- Sastavlja izvještaje.

Referenti registracionog tijela su ovlašćeni od strane certifikacionog tijela da:

- Primaju i registruju zahtjeve za izdavanje kvalifikovanog elektronskog certifikata;
- Primaju i registruju zahtjeve za promjenu statusa kvalifikovanog elektronskog certifikata;
- Provjeravaju identitet korisnika;
- Šalju centralnom registracionom tijelu dokumentaciju i podatke o korisnicima kvalifikovanih elektronskih certifikata;

5.2.2. Potreban broj osoba za operativne postupke

Dvije (2) PKI *Master User* autorizacije su potrebne da bi se izvršili slijedeći poslovi:

- Ponovno šifrovanje baze podataka;
- Obnova kriptografskog ključa certifikacionog tijela;
- Promjena lozinke PKI *Master User*-a i lozinke certifikacionog tijela;
- Ponovno podešavanje broja autorizacija za PKI *Security Officer*-e na jednu autorizaciju;
- Obnavljanje certifikata PKI *Security Officer*-a;
- Promjena hash algoritma za certifikate;
- Promjena SEP algoritma za šifrovanje;
- Podešavanje automatske prijave za servise certifikacionog tijela;
- Onemogućavanje višestruke PKI *Master User* autorizacije;

Dvije (2) PKI *Security Officer* autorizacije su potrebne da bi se izvršili slijedeći poslovi:

- Podešavanje roka važnosti certifikata;
- Međusobna certifikacija sa drugim certifikacionim tijelima;
- Podešavanje ili promjena administrativne politike na osnovu PMA naloga;
- Podešavanje ili promjena korisničke politike na osnovu PMA naloga;
- Kreiranje, promjena ili brisanje naloga sa ulogom PKI *Security Officer na osnovu PMA naloga*;

Dve (2) PKI *Administrator* autorizacije su potrebne da bi se izvršile slijedeće operacije:

- Oporavak korisničkih naloga i povratak istorije privatnog ključa za dekripciju.

Jedna osoba može da obavlja sve ostale poslove koji nisu navedeni u ovom odjeljku, uključujući i poslove referenta lokalnog registracionog tijela.

5.2.3. Identifikacija i autentifikacija osoba za pojedine uloge

Osoblje certifikacionog tijela sa povjerljivim ulogama je podvrgnuto sigurnosnoj provjeri prije nego su imenovani da rade kao članovi [PoštaCG] CA osoblja.

Svaki pojedinac sa povjerljivom ulogom se kod prijave na aplikaciju certifikacionog tijela identifikuje digitalnim certifikatom ili korisničkim imenom i lozinkom. Zajedničko korišćenje naloga ili certifikata između osoblja certifikacionog tijela je zabranjeno. Osoblje je ograničeno na aktivnosti koje su autorizovane za datu ulogu kroz kontrole koje postavlja aplikacija, operativni sistem i procedure certifikacionog tijela.

5.2.4. Povjerljive uloge koje moraju biti odvojene

U cilju održavanja razdvajanje dužnosti, prava prijave na sisteme certifikacionog tijela moraju biti u skladu sa matricom prikazanom u slijedećoj tabeli:

[PoštaCG] CA Uloga	Korisnički nalog na operativnom sistemu	Korisnički nalog na aplikaciji CA	Uloga na aplikaciji CA
PKI Master User	Ne	Ne	Master User
PKI Security Officer	Ne	Da	Security Officer
PKI Administrator	Ne	Da	Administrator
Referent registracionog tijela	Ne	Da	End User
Administrator Direktorijuma	Da	Ne	Nema uloge
Administrator Operativnog Sistema	Da	Ne	Nema uloge

5.3. Kontrola osoblja

5.3.1. Kvalifikacije, iskustva i provjere

Osoblje certifikacionog tijela su stalno zaposleni ili zaposleni na određeno vrijeme. Oni su angažovani na poslovima certifikacionog tijela i adekvatno osposobljeni za izvršavanje radnih dužnosti.

Referenti lokalnog registracionog tijela su stalno zaposleni ili zaposleni na određeno vrijeme. Obaveze referenata lokalnog registracionog tijela se po pravilu ne smatraju cjelodnevnim angažovanjem. Referenti lokalnog registracionog tijela su adekvatno osposobljeni za izvršavanje radnih dužnosti.

Osoblje certifikacionog tijela i referenti registracionog tijela se obavezuju da ne smiju da objavljuju ili saopštavaju povjerljive informacije vezane za bezbjednost certifikacionog tijela ili informacije o korisnicima.

Osoblju certifikacionog tijela i referentima lokalnog registracionog tijela se ne dodjeljuju poslovi izvan djelokruga poslova za koje su angažovani u certifikacionom tijelu ili registracionom tijelu, a koji bi mogli dovesti do sukoba interesa sa ovim poslovima.

Korisnici su, na osnovu ugovora, upoznati sa bezbjedonosnim pravilima koja je potrebno da primenjuju u cilju zaštite njihovih računara i uređaja za šifrovanje, kao i sa politikom po kojoj su njihovi certifikati izdati.

5.3.2. Provjera prethodnih angažovanja

[PoštaCG] CA radi provjeru osoblja prema trenutno uspostavljenoj praksi u Pošti Crne Gore u skladu sa zakonom i propisima iz ove oblasti.

5.3.3. Obuka

[PoštaCG] CA obezbjeđuje obuku svom osoblju i referentima registracionih tijela.

Za osoblje certifikacionog tijela, obuka uključuje postupke zaštite sistema i podataka, obuku specifičnu za njihove uloge i odgovornosti, obuku za korišćenje aplikacije certifikacionog tijela i obuku za preduzimanje postupaka na oporavku sistema od štete i procedure kontinuiteta rada.

Za referente registracionog tijela, obuka uključuje postupke zaštite sistema i podataka i obuku specifičnu za njihove uloge i odgovornosti.

5.3.4. Učestalost ponovnih obuka

Osoblje certifikacionog tijela pohađa obuke kad su imenovani na funkciju i po potrebi, kada se vrše promjene tehničkih sredstava (hardvera i softvera) certifikacionog tijela i načina obavljanja djelatnosti. Plan obrazovanja osoblja [PoštaCG] CA se redovno revidira i prilagođava potrebama zbog promjena u okviru sistema PKI.

5.3.5. Učestalost i redosljed rotacije uloga

Nije primjenjeno.

5.3.6. Sankcije za neautorizovane aktivnosti

U slučaju izvršene ili sumnje na izvršene neautorizovane aktivnosti od strane osobe koja izvršava obaveze u vezi sa radom certifikacionog tijela ili registracionog tijela, [PoštaCG] CA će onemogućiti njen dalji pristup sistemima i aplikaciji certifikacionog tijela i opozvati sve certifikate koji su joj izdati.

Izvršene neautorizovane aktivnosti se prijavljuju nadležnoj službi u Pošti Crne Gore u skladu sa internim pravilima.

5.3.7. Zahtjevi za osoblje koje radi po ugovoru

U slučaju da se dodijeli povjerljiva uloga osobi koja nije u sistemu Pošte Crne Gore, za nju važe isti uslovi kao za stalno osoblje [PoštaCG] CA. Svi koji rade na ovaj način su obavezni potpisati sporazum o tajnosti (*non-disclosure agreement*).

5.3.8. Dokumentacija za potrebe osoblja

[PoštaCG] CA osoblje ima pristup dokumentaciji sistema certifikacionog tijela, uključujući hardver, softver, dokumentaciju aplikacije certifikacionog tijela, operativne procedure, procedure u slučaju požara, procedure kontrole pristupa i ovom Pravilniku.

5.4. Procedure upravljanja revizijskih dnevnika

5.4.1. Događaji koji se bilježe

U elektronske dnevnike zapisuju se slijedeće vrste događaja:

- događaji u vezi sa korisničkim kriptografskim ključevima i certifikatima: izdavanje, preuzimanje, opoziv, suspenzija, obnova i arhiviranje,
- događaji u vezi sa kriptografskim ključevima aplikacije certifikacionog tijela,
- događaji u certifikacionom tijelu, registracionom tijelu, tehničkim sredstvima (hardveru i softveru),
- događaji u vezi sa administracijom, kreiranjem rezervnih kopija, sigurnosnom politikom i korišćenjem aplikacije certifikacionog tijela, registracionog tijela i javnog imenika,
- događaji u vezi sa fizičkim pristupom sistemu certifikacionog tijela.

5.4.2. Učestalost procesuiranja dnevnika

Administratori certifikacionog tijela pregledaju elektronske dnevnike jedanput nedeljno. Pod pregledom se podrazumjeva:

- prikupljanje svih elektronskih dnevnika od poslednjeg pregleda,
- pregled zapisa u elektronskim dnevnicima,
- analiza i kreiranje izvještaja o relevantnim događajima, razrješavanje problema ili prijava problema odgovornoj osobi certifikacionog tijela koja preduzima dalje korake u cilju rješavanja problema.

5.4.3. Vrijeme čuvanja dnevnika

Kopije elektronskih dnevnika se čuvaju najmanje dva mjeseca na sistemima i najmanje sedam godina na arhivskom mediju na sigurnoj udaljenoj lokaciji.

5.4.4. Zaštita dnevnika

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

Za elektronske dnevnike operativnog sistema se upotrebljavaju zaštite koje omogućava sam operativni sistem.

Elektronski dnevnici aplikacija certifikacionog tijela su zaštićeni tehnologijom kriptografije javnih kriptografskih ključeva.

5.4.5. Izrada rezervnih kopija dnevnika

Elektronski dnevnici se snimaju na odgovarajućim medijima u okviru redovne procedure izrade rezervnih kopija. Za kreiranje rezervnih kopija zaduženi su ovlašćeni administratori. Rezervne kopije elektronskih dnevnika se čuvaju na primarnoj lokaciji certifikacionog tijela i na drugoj udaljenoj lokaciji u zaštićenom prostoru. Na udaljenu lokaciju se rezervne kopije prenose jednom nedjeljno.

5.4.6. Sistem prikupljanja dnevnika

Podaci za elektronske dnevnike se prikupljaju automatski i ručno kao što je prikazano u slijedećoj tabeli.

Događaji koji se zapisuju u elektronske dnevnike	Način prikupljanja podataka	Odgovorna osoba ili sistem
Događaji povezani sa korisnicima certifikacionog tijela	automatsko	aplikacija certifikacionog tijela
Događaji povezani sa kriptografskim ključevima certifikacionog tijela	automatsko	aplikacija certifikacionog tijela
Događaji na aplikaciji javnog imenika	automatsko	aplikacija certifikacionog tijela, aplikacija javnog imenika
Događaji na operativnom sistemu	automatsko	operativni sistem
Događaji na računarskoj mreži	automatsko	ruteri, operativni sistem
Kreiranje rezervnih kopija i obnova baze korisnika certifikacionog tijela	automatsko	aplikacija certifikacionog tijela, operativni sistem
Kreiranje rezervnih kopija i obnova logova, konfiguracije certifikacionog tijela	automatsko	aplikacija certifikacionog tijela, operativni sistem
Kreiranje rezervnih kopija i obnova javnog imenika	automatsko	aplikacija javnog imenika, operativni sistem
Fizički pristup do certifikacionog tijela	ručno, automatsko	osoblje certifikacionog tijela, sistem za kontrolu pristupa
Promene konfiguracije i hardvera na sistemu	ručno	osoblje certifikacionog tijela
Održavanje rada na sistemu i prostoru	ručno	osoblje certifikacionog tijela
Kadrovske promene	ručno	osoblje certifikacionog tijela
Poništavanje za to predviđenih podataka	ručno	osoblje certifikacionog tijela

5.4.7. Obavještavanje lica koje je izazvalo događaj

Lice koje je izazvalo događaj se ne obavještava.

5.4.8. Procjena ranjivosti sistema

Procjena ranjivosti se vrši u sklopu pregleda elektronskih dnevnika.

5.5. Arhiviranje podataka

5.5.1. Podaci koji se arhiviraju

[PoštaCG] CA arhivira slijedeće podatke:

- elektronske dnevnike iz odjeljka 5.4,
- ugovore sa korisnicima i dokumentaciju korisnika,
- zahtjeve za opozivima certifikata i prijave kompromitovanja kriptografskih ključeva,
- certifikate, registre opozvanih certifikata, politike i procedure rada certifikacionog tijela,
- privatne kriptografske ključeve korisnika za dešifrovanje podataka.

5.5.2. Period čuvanja podataka u arhivi

[PoštaCG] CA čuva:

- Elektronske dnevnike, najmanje sedam godina;
- Certifikate, registre opozvanih certifikata i privatne kriptografske ključeve, najmanje trideset godina;
- Ugovore sa korisnicima, dokumentacije korisnika i korespodenciju trećih lica sa [PoštaCG] CA, najmanje deset godina.

5.5.3. Zaštita arhive

Arhiva, prethodno navedena, se čuva na lokaciji certifikacionog tijela i na drugoj udaljenoj lokaciji. Na drugoj udaljenoj lokaciji se čuva dio arhive u elektronskoj formi. Arhiva je zaštićena sa odgovarajućim sigurnosnim mehanizmima. Pristup arhivama je dozvoljen samo ovlašćenim osobama.

5.5.4. Procedure arhiviranja

Arhivski materijal u elektronskoj formi se čuva na udaljenoj lokaciji u prostorijama sa fizičkim i sigurnosnim kontrolama uporedivim sa kontrolama na primarnoj lokaciji certifikacionog tijela.

5.5.5. Zahtjev za vremenski pečat arhiviranih podataka

Arhivirani podaci nose vremensku oznaku koju dodaje operativni sistem na kojem su bili kreirani. Vremenska oznaka nije kriptografski vremenski pečat.

5.5.6. Sistem arhiviranja (interni ili eksterni)

[PoštaCG] CA koristi interni sistem za izradu rezervnih i arhivskih kopija.

5.5.7. Procedure kontrole pristupa arhiviranim podacima i verifikacija

Pristup arhiviranim podacima je dozvoljen samo ovlašćenim predstavnicima [PoštaCG] CA na osnovu potrebe po znanju (*need-to-know*) ili u skladu sa važećim zakonom i propisima iz ove oblasti.

5.6. Obnova CA certifikata

Zamjena [PoštaCG] CA ključa i obnova certifikata će se izvršiti po isteku 70% perioda važenja certifikata ili ranije. Poslije zamjene certifikata [PoštaCG] CA će objaviti novi certifikat na javnim web stranicama i u direktorijumu LDAP.

5.7. Kompromitovanje i oporavak sistema poslije nepredviđenih situacija

5.7.1. Procedure kod incidenata ili kompromitovanja

[PoštaCG] CA ima implementirane procedure reagovanja na bezbjedonosne incidente i kvarove u skladu sa pozitivnim zakonskim propisima.

5.7.2. Greške u radu sistema, programske opreme ili oštećenja podataka

[PoštaCG] CA ima uspostavljen plan oporavka od nepredviđenih katastrofa, koji pokriva oporavak poslovanja nakon kvara računarskih resursa, softvera i podataka.

5.7.3. Kompromitovanje privatnog ključa

[PoštaCG] CA će u slučaju kompromitovanja svog privatnog kriptografskog ključa opozvati sve izdate certifikate i ponovo izdati sve certifikate korisnika važeće u momentu kompromitovanja ključa certifikacionog tijela.

5.7.4. Prirodne i druge katastrofe

U slučaju prirodnih i drugih katastrofa [PoštaCG] CA će obnoviti poslovanje certifikacionog tijela u najkraćem mogućem roku koristeći podatke sa rezervnih kopija sistema.

5.8. Prestanak rada CA ili RA

U slučaju da [PoštaCG] CA, zbog mogućeg stečaja ili potrebe, odnosno namjere prestanka poslovanja, ima namjeru da prestane sa radom, dužan je o tome obavijestiti svakog potpisnika i nadležni organ uprave, najmanje tri mjeseca prije dana predviđenog za raskid ugovora.

[PoštaCG] CA dužan je, za potpisnike kojima je izdao certifikate, da obezbijedi nastavak obavljanja usluga certifikovanja kod drugog davaoca usluga i da mu dostavi svu dokumentaciju u vezi sa obavljenim uslugama certifikovanja.

Ako [PoštaCG] CA ne obezbijedi nastavak obavljanja usluga kod drugog davaoca ovih usluga, dužan je opozvati sve izdate certifikate i o tome odmah, a najkasnije u roku od 48 sati, obavijestiti nadležni organ uprave i dostaviti mu svu dokumentaciju u vezi sa obavljenim uslugama.

[PoštaCG] CA mora osigurati raspoloživost liste opozvanih certifikata (CRL) za razdoblje šest mjeseci posle opoziva svih certifikata.

[PoštaCG] CA mora osigurati da će se arhivirani podaci zadržati najmanje trideset godina od zadnjeg dana rada.

6. TehničkO bezbJEDONOSNE kontrole

6.1. Generisanje ključeva i instalacija

6.1.1. Generisanje para ključeva

Par kriptografskih ključeva [PoštaCG] certifikacionog tijela za potpisivanje je generisan prilikom instaliranja aplikacije certifikacionog tijela i tokom procedure generisanja (*Root Key Generation Ceremony*) po precizno definisanoj proceduri. U toku generisanja para kriptografskih ključeva za potpisivanje koristi se zaštita koja važi za prostorije [PoštaCG] certifikacionog tijela iz odjeljku 5.1, višestruka autentifikacija ovlašćenih osoba i hardverski kriptografski modul (*Hardware Security Module - HSM*).
Korisnikov par kriptografskih ključeva za potpisivanje i verifikovanje potpisa se generiše na strani korisnika u korisničkoj aplikaciji, odnosno na smart kartici. Kriptografski ključ za potpisivanje se nikada ne smješta na hardverskoj ili softverskoj opremi [PoštaCG] certifikacionog tijela.
Kod certifikata koji se upravljaju koristeći PKIX-CMP protokol, korisnikov par kriptografskih ključeva za šifrovanje i dešifrovanje generiše [PoštaCG] certifikaciono tijelo i drži njegovu kopiju u šifriranom obliku u svojoj bazi.

6.1.2. Dostavljanje korisniku privatnog ključa

Kod certifikata koji se upravljaju koristeći PKIX-CMP protokol privatni kriptografski ključ za dešifrovanje podataka generiše aplikacija certifikacionog tijela i prenosi se do korisnika po PKIX-CMP protokolu. Referentni broj i autorizacioni kod koje korisnik dobija radi preuzimanja kriptografskih ključeva obezbjeđuje sigurnost prenosa kriptografskih ključeva.
Uručenje privatnog ključa korisniku za certifikate izdate na kriptografskom tokenu vrši se njegovim uručivanjem u prostorijama lokalnog registracionog tijela ili lično na adresu navedenu u zahtjevu.
Privatni kriptografski ključ za potpisivanje generiše korisnička aplikacija tako da ga nije potrebno dostavljati korisniku.

6.1.3. Dostavljanje javnog ključa korisnika davaocu usluge certifikovanja

Korisnikov javni kriptografski ključ za verifikovanje potpisa se dostavlja [PoštaCG] certifikacionom tijelu po PKIX-CMP, Netscape SPKC ili PKCS#10 protokolu.
Kriptografski ključ certifikata koji se upravlja koristeći PKIX-CMP protokol generiše aplikacija certifikacionog tijela tako da nije potrebno dostavljati javni ključ za šifrovanje.

6.1.4. Dostavljanje javnog ključa davaoca usluge certifikovanja trećim licima

Javni ključ za verifikaciju potpisa [PoštaCG] certifikacionog tijela se dostavlja zainteresovanim stranama u okviru [PoštaCG] CA certifikata u PKCS#7 ili X.509 obliku. U X.509 obliku isti je objavljen i u Repozitoriju.
Za korisničke certifikate koji se upravljaju sa PKIX-CMP protokolom javni ključ korisnika je objavljen u okviru certifikata u X.509 obliku u Repozitorijumu.

6.1.5. Dužina ključeva

Kriptografski ključevi koje [PoštaCG] CA koristi za potpisivanje certifikata su RSA ključevi dužine najmanje 3072 bita.
Korisničke aplikacije moraju generisati asimetrične ključeve RSA minimalne dužine 2048 bita.

6.1.6. Generisanje parametara javnih ključeva

[PoštaCG] CA ne generiše DSA ključeve.

6.1.7. Namjena upotrebe ključeva (X.509 keyUsage)

Za potpisivanje certifikata i liste opozvanih certifikata (CRL) upotrebljava se isključivo privatni kriptografski ključ aplikacije certifikacionog tijela.
Certifikat javnog ključa certifikacionog tijela ima postavljene *keyUsage* bitove za *keyCertSign* i *cRLSign.*
U certifikatima koje izdaje [PoštaCG] CA su slijedeće X.509 keyUsage oznake namene upotrebe:

Tip certifikata	X.509 keyUsage (bit)
kvalifikovani digitalni certifikat izdat na pametnoj kartici	digitalSignature (0), nonRepudiation (1)
kvalifikovani digitalni certifikati	digitalSignature (0), nonRepudiation (1)
kvalifikovani digitalni certifikat za povjerljivost izdat na pametnoj kartici	keyEncipherment (2)
kvalifikovan digitalni certifikat za povjerljivost	keyEncipherment (2)
digitalni certifikat za SSL server	digitalSignature (0), keyEncipherment (2)
digitalni certifikat za DC server	digitalSignature (0), keyEncipherment (2)
digitalni certifikat za SmartLogon	digitalSignature (0), keyEncipherment (2)

U slijedećim certifikatima koje izdaje [PoštaCG] CA su X.509 ExtendedKeyUsage oznake namjene upotrebe:

Tip certifikata	X.509 ExtendedKeyUsage
digitalni certifikat za SSL server	ServerAuth
digitalni certifikat za DC server	Server Authentication Client Authentication

digitalni certifikat za SmartLogon	Client Authentication Smart Card Logon

6.2. Zaštita privatnog ključa i kontrole kriptografskih modula

6.2.1. Standardi i kontrole kriptografskih modula

Sve operacije za generisanje [PoštaCG] CA kriptografskih ključeva i potpisivanja certifikata vrše se na hardverskom kriptografskom modulu koji zadovoljava sigurnosne standarde nivoa FIPS 140-2 Level 3.
Kriptografski token zadovoljava standarde FIPS 140-2 Level 2 ili više ili EAL 4+.
Privatni ključ korisnika je zaštićen fizičkim i logičkim kontrolama korisnikovog računara. Korisnik je obavezan osigurati zaštitu privatnog ključa tako da se minimalizuje mogućnost otkrivanja privatnog ključa. Preporuka [PoštaCG] CA je da korisnici koriste kriptografske tokene koji zadovoljavaju sigurnosne standarde najmanje FIPS 140-2 Level 2 ili druge verifikovane do najmanje uporedivog nivoa.

6.2.2. N od M kontrola privatnog ključa

Definisano u odjeljku 5.2.2. Potreban broj osoba za operativne postupke.

6.2.3. Deponovanje (key escrow) privatnog ključa

[PoštaCG] CA ne dozvoljava deponovanje privatnog ključa.

6.2.4. Kopija privatnih ključeva

Aplikacija [PoštaCG] certifikacionog tijela čuva šifrovane kopije ključeva korisnika koji se upravljaju PKIX-CMP protokolom za potrebe oporavka i povratka istorije ključeva. Aplikacija [PoštaCG] certifikacionog tijela takođe čuva šifrovanu kopiju svog privatnog ključa za potpisivanje certifikata.
Aplikacija [PoštaCG] certifikacionog tijela radi rezervnu kopiju baze najmanje jednom dnevno. Rezervna kopija baze aplikacije certifikacionog tijela se kopira na rezervne medije u okviru izrade redovne rezervne kopije sistema.
Korisnički kriptografski ključevi koji se upravljaju koristeći PKCS#10 ili Netscape SPKC protokol se ne čuvaju na strani aplikacije [PoštaCG] certifikacionog tijela.

6.2.5. Arhiviranje privatnih ključeva

Privatni ključevi se arhiviraju u skladu sa odjeljkom 5.5.4. Procedure arhiviranja.

6.2.6. Prenos privatnog ključa u kriptografski modul

Privatni ključ za potpisivanje [PoštaCG] certifikacionog tijela se generiše unutar hardverskog kriptografskog modula. Privatni ključ za potpisivanje [PoštaCG] certifikacionog tijela nikad se ne pojavljuje van hardverskog kriptografskog modula u čitljivom obliku.
Privatni ključevi korisnika za dešifrovanje, koji se generišu u kriptografskom modulu aplikacije certifikacionog tijela, se prenesu u korisnikov kriptografski modul koristeći PKIX-CMP protokol.
Za privatne ključeve korisnika za potpisivanje nema posebnih zahtjeva pošto se generišu u kriptografskom modulu na strani korisnika.

6.2.7. Čuvanje kriptografskih ključeva na kriptografskom modulu

Privatni ključ certifikacionog tijela za potpisivanje se koristi samo na hardverskom kriptografskom modulu (HSM). Rezervna kopija privatnog ključa certifikacionog tijela za potpisivanje se čuva za potrebe oporavka sistema u šifrovanom obliku na serveru aplikacije certifikacionog tijela. Privatni ključ certifikacionog tijela je zaštićen master ključem i uvijek se šifruje i dešifruje unutar HSM. Master ključ za šifrirovanje/dešifrovanje se čuva na pametnim karticama.

6.2.8. Način aktiviranja privatnog ključa

Privatni kriptografski ključ aplikacije certifikacionog tijela za potpisivanje se aktivira posle startovanja aplikacije certifikacionog tijela. Za aktiviranje je potrebna smart kartica za pristup hardverskom kriptografskom modulu, kao i lozinka korisnika sa PKI Master ulogom.
Korisnički privatni kriptografski ključevi se aktiviraju poslije uspješne autentifikacije korisnika sa lozinkom u korisničkoj aplikaciji.

6.2.9. Način deaktiviranja privatnog ključa

Privatni kriptografski ključ aplikacije certifikacionog tijela za potpisivanje se deaktivira sa zaustavljanjem aplikacije certifikacionog tijela.
Korisničke aplikacije moraju da deaktiviraju privatni kriptografski ključ kada se korisnik odjavi sa sistema, ili deaktivira (*plug out*) kriptografski token.

6.2.10. Način uništavanja privatnog ključa

Prilikom zaustavljanja aplikacije certifikacionog tijela poništavaju se svi kriptografski ključevi koji se nalaze u radnoj memoriji HSM.
Preporuka je da korisničke aplikacije prebrišu privatne kriptografske ključeve iz radne memorije računara prije nego što ponovo dodijele memoriju. Takođe se preporučuje da prebrišu sav prostor na disku koji se koristi za privatne kriptografske ključeve, prije nego što se taj prostor na disku dodijeli operativnom sistemu.
Privatni kriptografski ključ korisnika se uništava ukoliko ga korisnik obriše sa kriptografskog tokena ili se kriptografski token fizički ošteti.

6.2.11. Nivo sigurnosti kriptografskih modula

Kao što je definisano u odjeljku 6.2.1. Standardi i kontrole kriptografskih modula.

6.3. Ostali aspekti upravljanja para ključeva

6.3.1. Arhiviranje javnog ključa

Certifikaciono tijelo arhivira javni kriptografski ključ aplikacije certifikacionog tijela i javne korisničke ključeve, kao što je opisano u odjeljku 5.5.4. Procedure arhiviranja.

6.3.2. Rok važnosti certifikata i period upotrebe para ključeva

Rok važnosti javnih i privatnih kriptografskih ključeva [PoštaCG] certifikacionog tijela je:

- Javni ključ certifikacionog tijela za verifikovanje potpisa: 20 godina.
- Privatni ključ certifikacionog tijela za potpisivanje: 14 godina.
- Korisnički ključevi za certifikate:
  - Korisnički javni ključ za autentifikaciju: 1 do 5 godina
  - Korisnički javni ključ za verifikovanje potpisa: 1 do 5 godina.
  - Korisnički privatni ključ za potpisivanje: 1 do 5 godina.
  - Korisnički javni ključ za šifrovanje: 1 do 5 godina.
  - Korisnički privatni ključ za dešifrovanje: rok važnosti nije ograničen.

6.4. Aktivacijski podaci

6.4.1. Generisanje i instalacija aktivacijskih podataka

Referentni brojevi (*reference numbers*) i autorizacioni kodovi (*authorization codes*) su podaci za preuzimanje korisničkih certifikata. Brojevi i kodovi su jedinstveni i generišu se u aplikaciji certifikacionog tijela primjenom odgovarajućeg algoritma.

Korisnici upotrebljavaju lozinke za aktivaciju privatnih kriptografskih ključeva. Za certifikate koji se generišu na kriptografskom tokenu u okviru certifikacionog tijela, lozinku generiše generator lozinke, poslije čega se ona stavlja u zaštićenu kovertu i dostavlja korisniku poštanskim tokovima na adresu navedenu u zahtjevu. Lozinka ima osam ili više karaktera. Korisnik je obavezan da promijeni lozinku kada prvi put upotrijebi kriptogtrafski token.

Za certifikate koje generišu korisnici lično, svaki korisnik smišlja svoju lozinku. U slučaju da korisnik koristi korisničku aplikaciju koju mu je dodijelilo certifikaciono tijelo, mora izabrati lozinku u skladu sa politikom aplikacije certifikacionog tijela.

Lozinke se ne čuvaju u aplikaciji certifikacionog tijela.

6.4.2. Zaštita aktivacijskih podataka

Referentni brojevi i autorizacioni kodovi se generišu u aplikaciji certifikacionog tijela i smještaju se u šifrovanu bazu podataka. Autorizacioni kodovi se pod nadzorom osoblja certifikacionog tijela štampaju na neprovidne koverte.

Referentni broj i autorizacioni kod se dostavljaju korisniku različitim komunikacionim kanalima. Referentni broj se šalje korisniku elektronskom poštom, dok se autorizacioni kod zajedno sa praznim kriptografskim tokenom dostavlja korisniku putem preporučene pošiljke sa povratnicom, Post Express dostave sa obaveznim ličnim prijemom ili ga preuzima korisnik lično u prostorijama lokalnog registracionog tijela.

6.4.3. Ostali aspekti aktivacijskih podataka

Nije primenljivo.

6.5. Bezbjedonosni zahtjevi za računare

6.5.1. Specifični računarsko tehničko-bezbjedonosni zahtjevi

[PoštaCG] CA ima na računarima i aplikacijama implementirane tehničke bezbjedonosne kontrole, uključujući:

- Kontrolu prijave u aplikaciju certifikacionog tijela na nivou pojedinih uloga;
- Razdvajanje dužnosti između uloga na aplikaciji certifikacionog tijela;
- Šifrirane komunikacije između aplikacije certifikacionog tijela i korisničkih klijent aplikacija;
- Šifrirane baze podataka certifikacionog tijela;
- Arhiviranje istorije ključeva certifikacionog tijela i korisnika i arhiviranje revizijskih podataka;
- Revizijske belleške događaja u vezi bezbjednosti.

6.5.2. Nivo zaštite računara

Aplikacija certifikacionog tijela ima ocjenu sigurnosti nivoa EAL4+ augmented.

Operativni sistemi računara certifikacionog tijela i drugi proizvodi koji se koriste su komercijalni proizvodi.

6.6. Tehnički nadzor tokom upotrebe sistema

6.6.1. Nadzor razvoja sistema

Sve aplikacije i proizvodi koje koristi certifikaciono tijelo su komercijalni proizvodi.

6.6.2. Upravljanje bezbjednošću

[PoštaCG] CA ima uspostavljano upravljanje problema, promjena i konfiguracija za hardverske i softverske komponente sistema certifikacionog tijela u skladu sa pozitivnim zakonskim propisima.

6.6.3. Nadzor bezbjednosti tokom upotrebe sistema

[PoštaCG] certifikaciono tijelo sprovodi sva testiranje prije implementacije u kontrolisanom okruženju.

6.7. Nadzor bezbjednosti računarske mreže

Računarsku mrežu certifikacionog tijela čine povezani mrežni segmenti, na kojima se nalaze serveri i radne stanice. Segmenti su međusobno povezani firewall-ovima. Računarska mreža certifikacionog tijela je preko firewall-a povezana sa Internetom. Bezbjedonosna pravila na firewall-ovima dozvoljavaju saobraćaj samo protokolima koji su neophodno potrebni za pristup servisima certifikacionog tijela.

6.8. Vremenski pečat (Time-stamping)
Nije primijenjeno.

CERTIFIKAT, CRL I OCSP PROFILI

6.9. Profil certifikata

6.9.1. Broj (brojevi) verzija Version number(s)

[PoštaCG] CA izdaje X.509 v3 certifikate u skladu sa RFC 3280. Koriste se slijedeća X.509 osnovna polja:

X509 ekstenzija	Opis
signature	Elektronski potpis kvalifikovanog elektronskog certifikata privatnim kriptografskim ključem aplikacije certifikacionog tijela.
issuer	Jedinstveno ime certifikacionog tijela
Valid From	Datum i vrijeme početka važenja kvalifikovanog elektronskog certifikata
Valid To	Datum i vrijeme prestanka važenja kvalifikacionog elektronskog certifikata.
subject	Jedinstveno ime korisnika certifikata
subjectPublicKeyInformation	Javni kriptografski ključ korisnika certifikata, dužina javnog ključa i naziv algoritma javnog ključa
version	Verzija X.509 certifikata, verzija 3 (2)
serialNumber	Jedinstveni serijski broj certifikata

6.9.2. Ekstenzije certifikata

Koriste se slijedeće ekstenzije certifikata:

Naziv polja-ekstenzije	**Opis polja -ekstenzije**
Authority Key Identifier	Identifikator javnog kriptografskog ključa certifikacionog tijela koji se računa kao SHA -1 hash polja Subject Public Key Info certifikata certifikacionog tijela.
Subject Key Identifier	Identifikator javnog kriptografskog ključa korisnika certifikata koji se računa kao SHA -1 hash polja *Subject Public Key Info* kvalifikovanog elektronskog certifikata korisnika.
Key Usage	Namjena javnog kriptografskog ključa korisnika kvalifikovanog elektronskog certifikata.
Private Key Usage Period	Rok važnosti privatnog kriptografskog ključa korisnika, koji je par javnom kriptografskom ključu iz kvalifikovanog elektronskog certifikata.
Certificate Policies	Identifikacija politike certifikacije i adrese Web strane na kojoj se nalazi ova praktična pravila.
Subject Alternative Name	Alternativno ime korisnika kvalifikovanog elektronskog certifikata. U ovom polju može da se navede adresa elektronske pošte korisnika certifikata, ako je adresa elektronske pošte navedena u ugovoru ili SSL server hostname (FQDN)
Basic Constraints	Oznaka koja ukazuje da je certifikat korisnički i ona sadrži "*Subject Type=End Entity*".
CRL Distribution Points	Lokacija na kojoj se nalaze registri opozvanih certifikata.
Entrust Vers Info	Verzija aplikacije certifikacionog tijela (*OID*: 1.2.840.113533.7.65.0).
Qualified Certificate Statements	Oznaka da je certifikat izdat kao kvalifikovani elektronski certifikat (*OID*: 1.3.6.1.5.5.7.1.3), koja sadrži objekat *id-etsi-qcs-QcCompliance* (*OID*: 0.4.0.1862.1.1) i ako je certifikat izdat na kartici dodatno objekat *id-etsi-qcs-QcSSCD* (*OID*: 0.4.0.1862.1.4).
Domain Controller	Oznaka da je certifikat izdat za Microsoft Domain Controller (OID= 1.3.6.1.4.1.311.20.2,n,o,BMPString,"DomainController")

6.9.3. 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

6.9.4. Forme imena

Certifikati izdati od strane [PoštaCG] CA sadrže kompletno X.500 jedinstveno ime izdavača certifikata i korisnika certifikata u slijedećim poljima: issuer name (CA ime) i subject name. Jedinstvena imena su tekstualna polja u X.501 printable, teletex ili UTF8 formatu.

6.9.5. Ograničenja za ime

Specijalni znaci čije korišćenje u imenima nije dozvoljeno su: ? (upitnik), - (*backslash*), # (taraba), $ (dolar), % (procenat), = (jednako), + (plus), | (uspravna crta), ; (tačka-zarez), < (manje), > (veće) i , (zarez). Iste je potrebno izostaviti ili zamijeniti drugim znacima.

6.9.6. Identifikator objekta za politiku certifikovanja

Svi certifikati izdati od strane CA sadrže OID politike certifikovanja na osnovu koje je izdat certifikat. OID za svaku politiku certifikovanja definisan je u odjeljku 1.2. Naziv dokumenta i identifikacioni podaci

6.9.7. Korišćenje Politike ograničenja ekstenzija

[PoštaCG] CA koristi *policyConstraints* ekstenziju samo u među-certifikatima (cross-certificates), ukoliko su u upotrebi.

6.9.8. Sintaksa i semantika za kvalifikatore politike

Ne koriste se

6.9.9. Procesuiranje semantike za kritične ekstenzije Politike Certifikovanja

PKI klijentske aplikacije moraju procesuirati ekstenzije označene kao kritične u saglasnosti sa RFC 3280.

6.10. CRL profil

6.10.1. Broj (brojevi) verzija

CA izdaje X.509 v2 format CRLs koristeći višestruke distribucijske tačke u okviru sopstvenog LDAP direktorijuma i http web servera.

Koriste se slijedeća osnovna X.509 polja :

Naziv polja	**Opis polja**
Version	Verzija X.509 registra opozvanih certifikata
Signature Algorithm	Hash algoritam i asimetrični kriptografski algoritam korišćen za potpisivanje registra opozvanih certifikata od strane aplikacije certifikacionog tijela..
Issuer	Jedinstveno ime certifikacionog tijela
Effective Date (This Update)	Datum i vrijeme izdavanja registra opozvanih certifikata
Next Update	Datum i vrijeme slijedećih izdavanja registra opozvanih certifikata.
Revoked Certificates	Spisak serijskih brojeva opozvanih certifikata i datuma i vremena njihovog opozivanja.
Signature	Elektronski potpis registra opozvanih certifikata privatnim kriptografskim ključem aplikacije certifikacionog tijela.

6.10.2. CRL i CRL entry ekstenzije

***Naziv polja* - ekstenzije**	**Opis polja- ekstenzije**
Authority Key Identifier	Identifikator javnog kriptografskog ključa certifikacionog tijela koji se računa kao SHA-1 hash polja *Subject Public Key Infocertifikata certifikacionog tijela.*
CRL Number	Redni broj registra opozvanih certifikata.
Issuing Distribution Point	Lokacija na kojoj se nalazi parcijalni registar opozvanih certifikata.
reasonCode	Razlog opoziva certifikata.
Invalidity Date	Datum kompromitovanja ili sumnje u kompromitovanje privatnog kriptografskog ključa ili datum kada je kvalifikovani elektronski certifikat na neki drugi način prestao da bude važeći.

6.11. OCSP profil

6.11.1. Broj (brojevi) verzija

Nije podržano.

6.11.2. OCSP ekstenzije

Nije podržano.

7. REVIZIJA usaglašenosti i druge procjene

7.1. Učestalost ili okolnosti kada se vrše revizije

Nadležni organ vrši reviziju rada [PostaCG] CA u skladu sa Zakonom o elektronskom potpisu i drugim propisima iz ove oblasti.
[PoštaCG] CA Policy Management Authority (PMA) je tijelo odgovorno za organizovanje interne revizije i drugih procjena, kao i organizacije koja će iste da obavi. PMA će inicirati provjere jednom godišnje uz pomoć revizora, koji mogu biti interni ili eksterni. Ova se provjera može proširiti i na CA ovlašćenu Agenciju za Registraciju.
Moguće je izvršiti i više od jedne interne revizije godišnje ukoliko je to zahtijevano od strane PMA ili je to posljedica nezadovoljavajućih rezultata prethodne revizije.

7.2. Identitet/kvalifikacije revizora

Interni revizor će biti iz Pošte Crne Gore, sa odgovarajućim IT znanjem i revizorskim iskustvom.
Nezavisni eksterni revizor će biti angažovan od strane kompetentne stručne kompanije što je u saglasnosti sa odgovarajućim nacionalnim i internacionalnim standardima i kodeksima prakse.
Interni ili eksterni revizor mora ispunjavati slijedeće kriterijume:

- Značajno iskustvo u primjeni PKI i kriptografskih tehnologija;
- Iskustvo u radu sa aplikacijom certifikacionog tijela;
- Iskustvo u sprovođenju certifikacionih aktivnosti ili revizijama sistema informacionih tehnologija.

7.3. Revizorov odnos prema procjenjivanom subjektu

Interni ili eksterni revizor treba da je oslobođen od konflikata interesa i da je nezavistan od CA.

7.4. Oblasti koje pokriva procjenjivanje

Revizor će ocijeniti usklađenost između:

- ❖ Ovog Pravilnika i Zakona o elektronskom potpisu i podzakonskih akata
- ❖ Ovog Pravilnika i implementiranih CA servisa i procedura

7.5. Aktivnosti koje se preduzimaju u slučaju nedostatka

[PoštaCG] CA PMA će preduzeti odgovarajuće radnje u cilju rješavanja bilo kakvih nedostataka ili identifikovanih neusklađenosti koje su rezultat revizije, unutar dogovorenog vremenskog okvira u zavisnosti od ozbiljnosti rizika.

7.6. Objavljivanje rezultata

Rezultati revizije se dostavljaju [PoštaCG] CA Policy Management Authority.

8. ostalI poslovni I pravni aspekti

8.1. Cijene

8.1.1. Cijene usluga certifikacionog tijela

[PoštaCG] CA naplaćuje usluge certifikovanja. Cijene ovih usluga biće objavljene na javnoj web stranici definisanoj u odjeljku 2 OBJAVE I ODGOVORNOSTI REPOZITORIJUMA.

8.1.2. Nadoknade za pristup certifikatu

Ne naplaćuje se.

8.1.3. Nadoknade za opoziv ili pristup statusu informacija

Ne naplaćuje se.

8.1.4. Nadoknade za ostale servise

Pogledati odjeljak 9.1.1. Cijene usluga certifikacionog tijela.

8.1.5. Politika refundiranja

Troškovi se ne refundiraju.

8.2. Finansijska odgovornost

[PoštaCG] CA snosi finansijsku odgovornost za obavljanje svoje djelatnosti u skladu sa važećim propisima Crne Gore.

8.2.1. Osiguranja ili garancije davaoca usluge certifikovanja

[PoštaCG] CA je dužno da obezbijedi osiguranja od rizika od odgovornosti za štete koje mogu nastati pružanjem usluga certifikovanja u skladu sa zakonom i propisima iz ove oblasti.

8.2.2. Ostala sredstva

Nije primjenljivo.

8.2.3. Osiguranja ili garancije korisnika

Naručioci i povezana lica isključivo su odgovorni da obezbijede adekvatno osiguranje ili garanciju pokrivenosti osiguranjem za korišćenje certifikata u okviru njihovih servisa ili aplikacija.

8.3. Povjerljivost poslovnih informacija

8.3.1. Obim povjerljivih informacija

Sve informacije koje se prikupljaju, generišu, prenose i održavaju od strane [PoštaCG] CA, smatraće se povjerljivim, osim informacija opisanih u odjeljku 8.3.2. Informacije koje ne ulaze u obim povjerljivih informacija, koje se ne smatraju povjerljivim.

8.3.2. Informacije koje ne ulaze u obim povjerljivih informacija

Informacije koje se objavljuju kao dio certifikata, CRL, Pravilnika ili druge informacije koje se objavljuju u javnom repozitorijumu certifikacionog tijela, neće se smatrati povjerljivim.

8.3.3. Odgovornost za zaštitu povjerljivih informacija

[PoštaCG] CA je odgovoran za zaštitu povjerljivih informacija u skladu sa Zakonom o zaštiti podataka o ličnosti i pozitivnim propisima Crne Gore.

8.4. Privatnost ličnih informacija

8.4.1. Plan privatnosti

Bilo koji lični podatak koji obezbjeđuje CA držaće se u skladu sa zahtjevima postavljenim u Zakonu o zaštiti podataka o ličnosti. Davanje gore navedenih informacija može se vršiti jedino u saglasnosti sa Zakonom o zaštiti podataka o ličnosti.

8.4.2. Informacija koja se tretira privatnom

Definisano u odjeljku 8.4.1. Plan privatnosti.

8.4.3. Informacija koja se ne smatra privatnom

Definisano u odjeljku 8.3.2. Informacije koje ne ulaze u obim povjerljivih informacija.

8.4.4. Odgovornost za zaštitu privatnih informacija

Kao što je definisano u odjeljku 8.3.3. Odgovornost za zaštitu povjerljivih informacija.

8.4.5. Obavještenje i davanje saglasnosti za korišćenje privatnih informacija

[PoštaCG] CA će koristiti privatnu informaciju isključivo u svrhe za koje je Naručilac dao saglasnost u toku procesa registracije. Smatra se da je Naručilac dao saglasnost potpisivanjem ugovara sa krajnjim korisnikom (*End User Agreement*).

8.4.6. Otkrivanje informacije u skladu sa sudskim ili administrativnim procesom

Povjerljiva informacija može jedino biti objavljena ili predata od strane [PoštaCG] CA zakonom ovlašćenim službenicima u skladu sa važećim propisima Crne Gore.

8.4.7. Ostale okolnosti kada se mogu otkrivati informacije

[PoštaCG] CA će otkriti privatnu informaciju samo u slučajevima kada dobije pismenu saglasnost od Naručioca.

8.5. Prava na intelektualnu svojinu

Sva prava intelektualne svojine [PoštaCG] CA uključujući zaštitne znake ostaju isključivo vlasništvo [PoštaCG] CA.

8.6. Garancije

8.6.1. Garancije certifikacionog tijela (CA)

[PoštaCG] CA garantuje da izdaje certifikate, izvršava ostale procedure vezane za upravljanje certifikatima i upravlja infrastrukturom certifikacionog tijela u skladu sa ovim Pravilnikom i propisima iz ove oblasti. [PoštaCG] CA odgovara za usklađenost sa procedurama opisanim u ovom Pravilniku i propisama iz ove oblasti, čak i u slučaju kada pojedinu funkciju certifikacionog tijela preuzmu pod-ugovarači.

Generalno, [PoštaCG] CA garantuje:

- Da su informacije o naručiocu i certifikacionom tijelu koje izdaje certifikat, a koje su sadržane u certifikatima tačne;
- Da će provjeriti identitet naručioca prije izdavanja certifikata;
- Da će osigurati tačnost i integritet informacija objavljenih u LDAP direktorijumu ili drugim repozitorijumima;
- Da će obezbijedi pristup jednom on-line javnom direktorijumu;
- Da će izdati certifikate naručiocima čiji su zahtjevi prihvaćeni u skladu sa ovim Pravilnikom;
- Da će opozovati certifikate koje je izdao, nakon prijema validnog zahtjeva da to učini ili u skladu sa ovim pravilnikom;
- Da će izdati i objaviti Liste opozvanih certifikata (CRLs);
- Da će osigurati da njeni RA-ovi budu svjesni odredbi koje se na njih odnose u ovom Pravilniku.

8.6.2. Garancije registracionog tijela (RA)

RA garantuje za tačnost i potpunost informacija koje provjeravaju njeni referenti. Detaljne obaveze RA definisane su u relevantnim odjeljcima ovog Pravilnika.

8.6.3. Garancije naručioca

Prihvatanjem certifikata koji je izdao [PoštaCG] CA, naručilac garantuje da:

- Čuva svoje privatne ključeve;
- Čuva svoju lozinku za zaštitu kriptografskih modula u kojem drži svoj privatni ključ;
- Odmah obavijesti certifikaciono tijelo, o bilo kakvoj netačnosti ili promjenama u informacijama sadržanim u certifikatu;
- Koristi svoje certifikate u skladu sa zakonskim odredbama i za odobrene namjene koje su opisane u sekciji 1.4 Upotreba certifikata;
- Odmah obavijesti certifikaciono tijelo, ako je kompromitovan privatni ključ povezan s certifikatom ili se sumnja da je bio kompromitovan;
- Odmah obavijesti certifikaciono tijelo o bilo kojoj sumnjivoj ili poznatoj zloupotrebi bilo kojeg certifikata koji je izdat od strane [PoštaCG] CA.

8.6.4. Garancije trećih lica

Prije oslanjanja na certifikat koji je izdao [PoštaCG] CA, obaveza je trećih lica da:

- Budu svjesna ograničenja certifikata i odgovornosti [PoštaCG] CA kako je detaljno opisano u ovom Pravilniku;
- Ograniče oslanjanje na certifikate koje je izdao [PoštaCG] CA za odgovarajuće upotrebe kako je detaljno objašnjeno u odjeljku 1.4 Upotreba certifikata;
- Da se preko provjere statusa certifikata na validnim listama opozvanih certifikata (CRLs) uvjeri da certifikat nije opozvan;
- Odmah obavijesti [PoštaCG] CA o bilo kojoj sumnjivoj ili poznatoj zloupotrebi bilo kojeg certifikata koji je izdat od strane [PoštaCG] CA.

8.6.5. Garancije ostalih učesnika

Bilo koji drugi učesnici obavezni su da koriste certifikate i ponašaju se u skladu sa ovim Pravilnikom i važećim propisima iz ove oblasti.

8.7. Izuzeća garancija

Osim garancija navedenih u ovom Pravilniku i povezanim ugovorima, i onim što je do najvišeg stepena dozvoljeno zakonom, [PoštaCG] CA isključuje bilo koje garancije, uslove ili predstavljanja (izraženih, podrazumijevanih u štampanom ili pisanom obliku), uključujući bilo koje garancije za mogućnost trgovine ili korišćenja za određenu upotrebu. [PoštaCG] CA naročito isključuje:

- bilo koju odgovornost za štetu koja može da se pojavi od momenta kada [PoštaCG] CA primi validan zahtjev za opoziv certifikata, do momenta objave informacije o opozivu istog na CRL, u skladu sa odjeljkom 4.9.5. Vrijeme od zahtjeva za opoziv do opoziva,
- bilo kakvu garanciju tačnosti ili pouzdanosti bilo koje informacije sadržane u certifikatima koju nije dostavila [PoštaCG] CA,
- odgovornost za predstavljanje informacija sadržanih u certifikatu,
- bilo kakvu garanciju organima vlasti ili garanciju statusa bilo koje osobe koja koristi certifikat [PoštaCG] CA,
- bilo koju odgovornost za stvari van kontrole [PoštaCG] CA uključujući raspoloživost ili rad Interneta, ili telekomunikacija ili drugih infrastruktura ili RA sistema, uključujući opremu i programe,
- bilo koju odgovornost za štete koje su nastale kao rezultat događaja više sile kako je detaljno opisano u odjeljku 9.16.5. Viša sila.

8.8. Ograničenja odgovornosti

8.8.1. Odgovornost i ograničenje od odgovornosti [PoštaCG] CA

[PoštaCG] CA je dužna da na propisan način izdaje kvalifikovane elektronske certifikate i odgovorna je za štetu pričinjenu licu koje se pouzdalo u taj certifikat, u skladu sa ovim Pravilnikom i propisima iz ove oblasti kao i ugovorom zaključenim između [PoštaCG] CA i korisnika.

8.8.2. Odgovornost i ograničenje od odgovornosti korisnika kvalifikovanog certifikata

Korisnik je odgovoran za štetu koja je nastala njegovom krivicom.

Korisnik nije odgovoran za štetu ako dokaže da je postupao u skladu sa ovim Pravilnikom i propisima iz ove oblasti kao i ugovorom zaključenim između [PoštaCG] CA i korisnika.

8.9. Obeštećenja

Svaka stranka za sebe snosi isključivu odgovornost za nadoknađivanje štete drugim strankama za pretrpljene gubitke ili štetu koja je nastala kao rezultat neovlašćenog korišćenja certifikata ili ne postupanja u skladu sa ovim Pravilnikom i propisima iz ove oblasti.

8.10. Rok i prekid

8.10.1. Rok

[PoštaCG] CA Pravilnik i drugi dokumenti stupaju na snagu nakon njihovog usvajanja.

8.10.2. Prekid

Važnost [PoštaCG] CA Pravilnika nije vremenski ograničena.

8.10.3. Efekti prekida i preživljavanja

Nakon prestanka važenja Pravilnika, kao rezultata objavljivanja novog, certifikat će se koristiti u skladu sa ovim Pravilnikom koji je bio validan na dan izdavanja certifikata. U slučaju promjena okolnosti do nivoa kada ovo nije moguće, [PoštaCG] CA će obavijestiti naručioce na način definisan u odjeljku 8.12.2. Mehanizmi obavještavanja i vremenski periodi, kao i treća lica preko javne web stranice a na način definisan u odjeljku 2.1 Repozitorijumi.

8.11. Individualno obavještavanje i komunikacija sa učesnicima
[PoštaCG] CA nakon usvajanja distribuira ovaj Pravilnik i njegove izmjene kao i druge važeće akte/dokumenate) preko njegove web stranice. Pogledati takođe odjeljak 9.12.2. Mehanizmi obavještavanja i vremenski periodi.

8.12. Izmjene
8.12.1. Procedura za izmjenu
[PoštaCG] CA osoblje može svoje primjedbe slati direktno [PoštaCG] CA PMA u pisanom ili e-mail obliku, na adrese definisane u odjeljku 1.5.2. Kontakt.

8.12.2. Mehanizmi obavještavanja i vremenski periodi
[PoštaCG] CA PMA može odlučiti da ne obavještava pretplatnike i treća lica u slučaju izmjena sa malim ili nikakvim uticajem. [PoštaCG] CA PMA u potpunosti odlučuje o tome da li izmjene imaju bilo kakav uticaj na pretplatnike i treća lica, na sopstvenu odgovornost.
Sve izmjene u ovom Pravilniku biće objavljene na način koji je definisan u odjeljku 2 OBJAVE I ODGOVORNOSTI REPOZITORIJUMA.
[PoštaCG] CA će obavjestiti korisnike o promjenama koje imaju materijalnog uticaja na njih, putem e-maila i na javnoj web stranici definisanoj u odjeljku 2 OBJAVE I ODGOVORNOSTI REPOZITORIJUMA.

8.12.3. Okolnosti pod kojima se OID mora izmijeniti
OID certifikata definisanih u ovom pravilniku će biti promijenjen u slučaju kada promjene imaju materijalni uticaj na naručioce i treća lica.

8.13. Rješavanja u slučaju spora
Svi sporovi u vezi certifikata izdatih od strane [PoštaCG] CA se moraju dostaviti na adresu naznačenu u odjeljku 1.5.2. Kontakt. Sporove treba, ako je moguće, rješavati pregovorima. Ukoliko se ne postigne razrješenje nesporazuma putem pregovora, rješenje će se potražiti kod nadležnog suda u Crnoj Gori.

8.14. Primjena zakona
Ovaj Pravilnik, kao i odnosi između [PoštaCG] CA i RA, naručioca, korisnika certifikata i trećih lica predmet su i biće tumačeni u skladu sa pozitivnim propisima Crne Gore.
8.15. Usaglašenost sa primjenljivim zakonom
Ovaj pravilnik usaglašen je sa:
- Zakonom o zaštiti podataka o ličnosti,
- Zakonom o elektronskom potpisu,
- i drugim propisima iz ove oblasti.

8.16. Razne odredbe
8.16.1. Cjelokupni ugovor
Ovaj Pravilnik [PoštaCG] CA i ugovor sa naručiocem obuhvataju sve elemente koji definišu odnos između [PoštaCG] CA i naručioca certifikata.

8.16.2. Prenos prava
Naručiocima certifikata nije dozvoljeno da prava i obaveze koji proističu iz ovog pravilnika i ugovora sa naručiocem u cjelosti ili parcijalno prenesu na treća lica po bilo kom osnovu.

8.16.3. Klauzula o valjanosti
Nevaljanost jednog ili više djelova ovog dokumenta, neće imati uticaj na valjanost ostalih odredbi, pod uslovom da nemaju uticaj na materijalne odredbe (povjerenje u certifikat i upotrebu certifikata).

8.16.4. Izvršenje (nadoknade za pravnog zastupnika i odricanje od prava)
Nema odredbi.

8.16.5. Viša sila
Višu silu predstavljaju vanredne okolnosti i nepredvidljive situacije kao što su prirodne katastrofe, terorizam, nedostatak napajanja ili prekid telekomunikacionih veza, požar, nepredvidljivi incidenti kao što su virusi ili napadi sa ciljem onemogućavanja servisa, greške u kriptografskim algoritmima i sl.
[PoštaCG] CA ili druge stranke neće biti odgovorne za bilo kakvu štetu koja je nastala usljed događaja koji su rezultat više sile.

8.17. Ostale odredbe
Danom stupanja na snagu ovog Pravilnika prestaje da važi Pravilnik o postupcima izdavanja certifikata i zaštiti sistema certifikovanja (Certification Practice Statement - CPS) broj 00010-4369/7-11 od 26.06.2012. god.

Ovaj pravilnik stupa na snagu osmog dana od dana objavljivanja u Službenom poštanskom glasniku.

PREDSJEDNIK
ODBORA DIREKTORA
Prof. dr Igor Radusinović

Pošta Crne Gore AD Podgorica
Odbor direktora
Broj: 00010-15142/11
Podgorica,28.12.2016.godine

Na osnovu člana 28 i 30 Statuta Pošte Crne Gore AD Podgorica, Odbor direktora Pošte je na sjednici održanoj dana 28.12.2016. godine, donio

O D L U K U
o usvajanju Pravilnika o poslovnoj tajni Pošte Crne Gore AD Podgorica

Član 1
Usvaja se Pravilnik o poslovnoj tajni Pošte Crne Gore AD Podgorica, u tekstu koji čini sastavni dio ove Odluke.

Član 2
Za realizaciju ove Odluke zadužuje se Izvršni direktor.

Član 3
Odluka stupa na snagu danom donošenja.

PREDSJEDNIK
Prof. dr Igor Radusinović

Pošta Crne Gore AD Podgorica
Odbor direktora
Broj: 00010-15142/11-1
Podgorica,28.12.2016.godine

Na osnovu člana 2 i 6 Zakona o tajnosti podataka ("Službeni list Crne Gore", br. 014/08 od 29.02.2008, 076/09 od 18.11.2009, 041/10 od 23.07.2010, 040/11 od 08.08.2011, 038/12 od 19.07.2012, 044/12 od 09.08.2012, 014/13 od 15.03.2013, 018/14 od 11.04.2014, 048/15 od 21.08.2015) i člana 28 Statuta Pošte Crne Gore AD Podgorica ("Službeni list Crne Gore", br. 061/11 od 23.12.2011, 012/13 od 01.03.2013), Odbor direktora Pošte Crne Gore AD Podgorica na sjednici održanoj dana 28.12.2016. godine donio je

P R A V I L N I K
o poslovnoj tajni

Član 1
(1) Ovim Pravilnikom uređuje se pojam poslovne tajne, kao i mjere i postupci za utvrđivanje, upotrebu i zaštitu podataka koji predstavljaju poslovnu tajnu Pošte Crne Gore AD Podgorica (u daljem tekstu: Pošte), a čijim bi saopštavanjem neovlašćenim osobama mogle nastupiti štetne posljedice u poslovanju, državnim interesima ili poslovnom ugledu Pošte.
(2) Ovaj Pravilnik ne primjenjuje se na podatke o ličnosti, odnosno na druge tajne i povjerljive podatke koji ne predstavljaju poslovnu tajnu, a koji se štite na način propisan posebnim zakonima i drugim propisima te opšim aktima Pošte.

Član 2
Pojedini pojmovi u smislu ovog Pravilnika imaju sljedeće značenje:

- podatak je dokument, odnosno svaki napisani, umnoženi, nacrtani, slikovni, štampani, snimljeni, fotografisani, magnetni, optički, elektronički ili bilo koji drugi zapis podatka, saznanje, mjera, postupak, predmet, usmeno saopštenje ili informacija, koja s obzirom na svoj sadržaj ima važnost povjerljivosti i cjelovitosti za Poštu;
- dokumenta su sva pisana akta (dopisi, tablice, grafikoni, nacrti, crteži i slično);
- predmeti su makete, modeli, uzorci, fotografije, filmovi, mikrofilmovi i drugi zapisi koji su svjetlosno, zvukovno, mašinski, ručno ili na drugi način zabilježeni na određenoj podlozi;
- mjere i postupci su sve vrste naloga, uputstava, saopštenja i drugih preduzetih radnji službenih lica;
- spoljni saradnici su pravna i fizička lica koje se s Poštom nalaze u ugovornom ili drugom pravnom odnosu.

Član 3

(1) Poslovnu tajnu predstavljaju podaci koji su kao poslovna tajna određeni zakonom, drugim propisom ili opštim aktom Pošte, a koji predstavljaju proizvodnu tajnu, rezultate istraživačkog rada, te druge podatke zbog čijeg bi saopštavanja neovlašćenom licu mogle nastupiti štetne posljedice za državne ili interese Pošte.
(2) Saglasno odredbi stava 1. ovog člana, poslovnu tajnu predstavljaju posebno:

- podaci o sastavu sigurnosnih, zaštitnih i odbrambenih mjera,
- podaci o izumu i tehničkom unaprijeđenju,
- podaci koji čine posebna znanja ili dostignuća u poslovanju bitna za odvijanje tehničko-tehnološkog postupka,
- podaci o zaradama i drugim primanjima zaposlenih,
- ostali podaci koji su ovim aktom utvrđeni za poslovnu tajnu.

Član 4

(1) Ne može se odrediti da se svi podaci koji se odnose na poslovanje Društva smatraju poslovnom tajnom niti se za poslovnu tajnu mogu utvrditi podaci čije saopštavanje nije protivno interesima Pošte.
(2) Poslovnom tajnom ne mogu se odrediti podaci koji su od značenja za poslovno povezivanje pravnih lica niti podaci koji se odnose na zaštićeno tehničko unaprijeđenje, otkriće ili pronalazak.

Član 5

(1) Kao tajna čuvaju se i:

- podaci koje je Pošta kao poslovnu tajnu saznala od drugih pravnih lica,
- podaci koji se odnose na poslove koje Pošta obavlja za potrebe Vojske Crne Gore, Ministarstva unutrašnjih poslova Crne Gore ili drugih javnih institucija, ako su označeni odgovarajućim stepenom tajnosti,
- dokumentacija u postupcima javne nabavke koja je saglasno posebnim propisima označena tajnom,
- podaci koji su zakonom, drugim propisom ili opštim aktom donesenim na osnovu zakona utvrđeni tajnim podacima od posebnog državnog značaja.

(2) Kad je to iz razloga obavljanja poslova Pošte nužno, podatke iz stava 1. ovog člana može drugim osobama saopštiti samo Odbor direktora ili osoba ovlašćena od Odbora direktora i to:

- uz prethodnu pisanu saglasnost pravnog lica koja je saglasno svom opštem aktu odredila da se ti podaci smatraju poslovnom tajnom,
- uz prethodnu pisanu suglasnost zainteresovanog pravnog ili fizičkog lica ako su u pitanju podaci iz postupaka javne nabavke .

(3) U zahtjevu kojim se traži saglasnost iz stava 2. ovog člana mora se navesti:

- koji su podaci u pitanju,
- kome se podaci saopštavaju,
- koja je osoba ovlašćena da da to saopštenje,
- razlozi zbog kojih je saopštavanje nužno,
- način na koji će se podaci saopštiti, odnosno koristiti.

Član 6

Podatke o izumu ostvarenom na radu ili u vezi s radom, zaposleni je dužan čuvati kao poslovnu tajnu i ne smije ih saopštiti trećoj osobi bez odobrenja Odbora direktora.

Član 7

(1) Podaci koji predstavljaju poslovnu tajnu ne smiju se saopštavati niti činiti dostupnim neovlašćenim osobama, ako posebnim zakonom nije drugačije određeno.
(2) Poslovnu tajnu dužni su čuvati svi zaposleni Pošte , članovi Odbora direktora, kao i spoljni saradnici koji na bilo koji način saznaju za podatak koji predstavlja poslovnu tajnu.
(3) Čuvanje poslovne tajne podrazumijeva njeno direktno čuvanje te preduzimanje zaštitnih mjera i aktivnosti radi onemogućavanja drugih osoba da neovlašćeno saznaju ili dođu u posjed podataka koji predstavljaju poslovnu tajnu.
(4) Obaveza čuvanja poslovne tajne traje i nakon prestanka radnog odnosa u Pošti, prestanka članstva u tijelima Pošte, odnosno nakon prestanka ugovornog ili drugog pravnog odnosa s Poštom u trajanju od 5 godina.

Član 8

Podaci koji se smatraju poslovnom tajnom mogu se saopštiti zaposlenima u Pošti kojima su ti podaci nužni za obavljanje poslova, a drugim pravnim ili fizičkim licima ako je to neophodno za izvršavanje ugovornih obaveza ili im se podaci mogu ili moraju saopštiti na osnovu zakona ili drugih propisa.

Član 9

Odbor direktora određuje osobu koja je osim Odbora direktora ovlašćena za uvid u poslovne tajne, njihovo čuvanje, te odlučivanje o tome koji se zaposleni u Pošti mogu ovlastiti za čuvanje i postupanje s podacima koji predstavljaju poslovnu tajnu, odnosno kojim se trećim licima poslovna tajna može saopštiti ili dati na uvid.

Član 10

(1) U obradi podataka koji predstavljaju poslovnu tajnu zaposleni se moraju pridržavati odredaba ovog Pravilnika, a na zahtjev Odbora direktora ili osobe ovlašćene od Odbora direktora obavezni su potpisati i izjavu o čuvanju tajnosti podataka.
(2) Izjavom iz stava 1. ovog člana zaposleni se obavezuje da podatke koji predstavljaju poslovnu tajnu neće iznositi ili ih na drugi način učiniti dostupnim trećim osobama kao i da će preduzeti sve mjere za zaštitu tajnosti podataka.

Član 11

Zaposleni su dužni upozoriti sve ovlašćene spoljne saradnike, koji će prilikom izvršenja nekog posebnog ugovora ili na neki drugi način saznati za poslovnu tajnu, da su obavezni čuvati poslovnu tajnu i da je ne smiju saopštavati niti činiti dostupnom neovlašćenim licima.

Član 12

(1) Ne smatra se povredom čuvanja poslovne tajne saopštavanje podataka koji se smatraju poslovnom tajnom ako se to saopštavanje obavlja fizičkim ili pravnim licima kojima se takvi podaci mogu ili moraju saopštavati:

1. na osnovu zakona i drugih propisa,
2. na osnovu ovlašćenja koje proizilazi iz dužnosti koju obavljaju, položaja na kome se nalaze ili radnog mjesta na kojem su zaposleni.

(2) Ne smatra se povredom čuvanja poslovne tajne saopštavanje podataka koji se smatraju poslovnom tajnom na sjednicama Odbora direktora te na stručnim sastancima ako je takvo saopštavanje nužno za obavljanje poslova.
(3) Ovlašćena osoba koja na sjednici ili sastanku saopštava podatke koji se smatraju poslovnom tajnom, dužna je upozoriti prisutne da se ti podaci smatraju poslovnom tajnom, a prisutni su dužni da ono što tom prilikom saznaju čuvaju kao poslovnu tajnu.

Član 13

Podatke koji se smatraju poslovnom tajnom trećim licima na njihov pisani zahtjev može saopštiti Odbor direktora ili osoba ovlašćena od Odbora direktora.

Član 14

(1) O saopštavanju trećim licima podataka koji predstavljaju poslovnu tajnu vodi se evidencija koja sadrži:

- podatke o imenu, prezimenu i funkciji lica, odnosno nazivu tijela kojem su saopšteni tajni podaci,
- informaciju o tome koji su podaci saopšteni i u kojem obimu,
- informaciju o datumu kada su podaci saopšteni,
- informaciju o svrsi za koju su podaci saopšteni.

(2) Evidencija iz stava 1. ovog člana vodi se na jednom mjestu u organizacionoj jedinici u čijem je djelokrugu nastao podatak koji predstavlja poslovnu tajnu.

Član 15

Umnožavanje, prepisivanje i izrada izvoda dokumenata i drugih podataka koji predstavljaju poslovnu tajnu može se obavljati samo uz pisano odobrenje Odbora direktora ili osobe ovlašćene od Odbora direktora.

Član 16

(1) Na svaki dokument koji predstavlja poslovnu tajnu stavlja se oznaka „poslovna tajna“.
(2) Oznaka iz stava 1. ovog člana unosi se u obrazac dokumenta odmah prilikom njegove izrade i to u gornjem desnom uglu svake stranice poslovnog dokumenta, otiskom ili mašinski, odnosno u obliku naljepnica ako se radi o predmetima koji se moraju označiti, a nisu dokument.
(3) Uz oznaku iz stava 1. ovog člana navodi se:

- zavodni broj predmeta,
- oznaka da li je riječ o originalu ili kopiji dokumenta,
- broj primjeraka,
- ukupan broj stranica dokumenta.

(4) Svaki dokument iz stava 1. ovog člana mora imati na svakoj stranici označen broj stranice i ukupan broj stranica dokumenta.
(5) Svi prilozi dokumenta iz stava 1. ovog člana moraju biti označeni na jednak način kao i dokument.
(6) Na prednjoj strani omota spisa u kojem su sadržani dokumenti i drugi podaci koji predstavljaju poslovnu tajnu, otiskom pečata na vidljivom mjestu stavlja se natpis „poslovna tajna“.

Član 17

Zaposleni koji rade na sastavljanju, prepisivanju i umnožavanju dokumenata i drugih podataka koji predstavljaju poslovnu tajnu dužni su uništiti primjerke neuspješnog umnožavanja dokumenta kao i druge materijale koji bi mogli otkriti sadržaj dokumenta koji je sastavljan ili umnožavan.

Član 18

(1) Dokumenti i drugi podaci koji predstavljaju poslovnu tajnu prilikom otpremanja moraju biti naslovljeni na tačno određenog primaoca po imenu i prezimenu, funkciji te nazivu organizacione cjeline.
(2) Dokumenti i drugi podaci koji predstavljaju poslovnu tajnu otpremaju se primaocu isključivo u zatvorenom omotu nezavisno o tome da li se otpremaju primaocu u drugoj organizacionoj cjelini Pošte ili primaocu izvan Pošte.
(3) Na omotnici u kojoj se otpremaju dokumenti i drugi podaci koji predstavljaju poslovnu tajnu, u lijevom gornjem uglu upisuje se zavodni broj dokumenta i stavlja se otisak službenog pečata, a u desnom uglu omotnice upisuje se oznaka „poslovna tajna“ , kao i oznaka „lično otvoriti“. Omotnica se zatvara ljepljivom trakom, a preko ruba lijepljenja stavlja se otisak službenog pečata.

Član 19

(1) Svaka organizaciona cjelina Pošte (Regionalni centri pošta, Poštansko-logistički centar i Sektori u Direkciji Pošte) u čijem je djelokrugu nastao dokument ili drugi podatak koji predstavlja poslovnu tajnu dužna je voditi evidenciju u koju se upisuju dokumenti koji predstavljaju poslovnu tajnu i u kojoj se evidentira kretanje tih dokumenata tako da je u svakom trenutku poznato gdje se i kod koje osobe nalazi dokument ili drugi podatak koji predstavlja poslovnu tajnu.
(2) U evidenciju iz stava 1. ovog člana unose se podaci o svim osobama koje su dokument dobile na uvid, odnosno na upotrebu, podatak o tome da li je i u koliko primjeraka izvršeno umnožavanje te po potrebi i drugi važni podaci o kretanju tog dokumenta.
(3) Organizaciona cjelina Pošte koja je primila dokument iz stava 1. ovog člana dužna je pratiti kretanje tog dokumenta za sve vrijeme dok se dokument nalazi u toj organizacionoj cjelini.
(4) Za sprovođenje obaveza iz stava 1, 2. i 3. ovog člana odgovorni su rukovodioci Regionalnih centara pošta, rukovodioc Poštansko-logističkog centra i rukovodioci Sektora u Direkciji Pošte.

Član 20

(1) Sva dokumenti i drugi podaci koji predstavljaju poslovnu tajnu čuvaju se odvojeno od ostalih dokumenata u zaključanim ormarima ili sefovima i evidentiraju se u posebnoj evidenciji prema broju i datumu.
(2) Evidencija iz stava 1. ovog člana vodi se u organizacionoj jedinici u čijem je djelokrugu nastao dokument, odnosno drugi podatak koji predstavlja poslovnu tajnu, a za vođenje evidencije odgovoran je rukovodioc te organizacione jedinice.
(3) Centralna evidencija u koju se upisuju sva dokumenta i drugi podaci koji predstavljaju poslovnu tajnu vodi se u Direkciji Pošte.

Član 21

(1) U slučaju otkrivanja ili nestanka dokumenata ili drugih podataka koji predstavljaju poslovnu tajnu, zaposleni su dužni da bez odlaganja obavijeste Izvršnog direktora i Odbor direktora koji će odmah poduzeti potrebne mjere za otklanjanje mogućih štetnih posljedica i pokrenuti postupak za utvrđivanje okolnosti pod kojima je došlo do otkrivanja, odnosno nestanka tajnih dokumenata ili podataka.
(2) O otkrivenim ili nestalim dokumentima i drugim podacima koji predstavljaju poslovnu tajnu vodi se posebna evidencija.
(3) Evidencija iz stava 2. ovog člana vodi se u Direkciji Pošte.

Član 22

(1) Dokumenta i drugi podaci koji predstavljaju poslovnu tajnu zaposleni ne smije čuvati/ snimati na lokalnom disku personalnog ili laptop, odnosno smart phone/tablet računara već isključivo na dodijeljenom mrežnom direktorijumu.
(2) Zaposleni ne smije računarsku opremu koju koristi, a kojom je moguće pristupiti podacima koji predstavljaju poslovnu tajnu, ostaviti bez nadzora u okruženju u kojem je moguć pristup i korištenje opreme od strane neovlašćenih osoba, a ako se to ne može izbjeći, oprema mora biti isključena ili programski zaključana.

Član 23

(1) Podaci koji predstavljaju poslovnu tajnu ne smiju se razmjenjivati putem elektronske pošte, osim u slučaju kad je odgovarajućim metodama kripto zaštite osigurana od moguće zloupotrebe.

(2) U slučaju iz stava 1. ovog člana, za razmjenu podataka koji predstavljaju poslovnu tajnu zabranjeno je koristiti privatne sisteme za razmjenu elektronske pošte već se smije koristiti isključivo službeni sistem za razmjenu elektronske pošte.

Član 24

(1) Spisi u kojima se nalaze podaci koji predstavljaju poslovnu tajnu arhiviraju se na način da se stavljaju u posebne omote koji se zatvaraju ljepljivom trakom tako da je onemogućen uvid u sadržaj spisa bez fizičkog uništavanja omota.

(2) Na omot se stavlja potpis zaposlenog koji je izvršio pakovanje i rukovodioc organizacione jedinice, sa naznačenim datumom i pečatom organizacione jedinice koja arhivira spis.
(3) Pristup arhiviranim spisima koji predstavljaju poslovnu tajnu ima samo zaposleni kojega je za to ovlastio Odbor direktora ili osoba ovlašćena od Odbora direktora.
(4) Svako postupanje sa spisom u kojemu se nalaze podaci koji predstavljaju poslovnu tajnu, zaposleni iz stava 3. ovog člana dužan je evidentirati u evidenciji za arhiviranje spisa koji predstavljaju poslovnu tajnu.

Član 25

Obaveza čuvanja poslovne tajne traje dok Odbor direktora ne odredi da je prestala potreba za čuvanjem tajnosti.

Član 26

(1) Postupanje protivno odredbama ovog Pravilnika predstavlja težu povredu radne obaveze zbog koje se zaposlenom može otkazati ugovor o radu na način i pod uslovima koje propisuju Zakon o radu i Kolektivni ugovor Pošte Crne Gore AD Podgorica.
(2) Neovlašćeno saopštavanje, ustupanje ili na drugi način činjenje drugom dostupnim podataka koji predstavljaju poslovnu tajnu krivično je djelo, saglasno Krivičnog zakonika Crne Gore.

Član 27

Odbor direktora će u roku od 30 dana od dana stupanja na snagu ovog Pravilnika odrediti odgovorno lice iz člana 9. ovog Pravilnika.

Član 28

Ovlašćuje se nadležni sektor da uz prethodnu suglasnost Odbora direktora utvrdi izgled i sadržaj evidencija iz ovog Pravilnika.

Član 29

Pravilnik o organizaciji i sistematizaciji Pošte Crne Gore AD Podgorica usaglasiće se sa ovim Pravilnikom u roku od 6 mjeseci od dana stupanja na snagu ovog Pravilnika.

Član 30

Ovaj Pravilnik stupa na snagu osmog dana od dana objavljivanja u Službenom poštanskom glasniku, a objaviće se i na oglasnim tablama Pošte.

PREDSJEDNIK
Prof. dr Igor Radusinović

Izdavač: Pošta Crne Gore AD Podgorica; Glavni i odgovorni urednik:
Urednik: Uredništvo i administracija: Podgorica, Slobode broj 1
Telefon: 020/ 403-959, žiro računi: 510-109-04; 520-872100-59
Internet: http://www.postacg.me/glasnik.php ; E-mail: spg@postacg.me