Pošta Crne Gore AD Podgorica
Odbor direktora
Broj: 00010-20260408-1/4
Podgorica,14.04.2026. godine

Projekat:	Javni PKI - Pošta Crne Gore Akcionarsko Društvo Podgorica (u daljem tekstu Pošta Crne Gore AD)
Naziv dokumenta:	**Pravilnik o postupcima izdavanja certifikata i zaštiti sistema (Certification Practice Statement - CPS)**
Verzija:	Verzija 12.0
Datum:	01.04.2026
Autori:	Tatjana Popović, Andreja Vujačić, Ivan Brković, - Pošta Crne Gore AD, Dragomir Stevanović – Axians Crna Gora d.o.o.

Reference:

OSNOVNI ZAKONI

[1] Zakon o elektronskoj identifikaciji i elektronskom potpisu
[2] Zakon o Centralnoj banci Crne Gore („Službeni list CG", br. 40/10, 6/13 i 70/17)
[3] Zakon o platnom prometu ("Službeni list Crne Gore", br. 062/13 od 31.12.2013, 006/14 od 04.02.2014, 111/22 od 07.10.2022, 007/23 od 20.01.2023)

PRAVILNICI I ODLUKE

[1] Pravilnik o bližim uslovima koje mora da ispunjava kvalifikovani davalac elektronskih usluga povjerenja
[2] Pravilnik o načinu ocjenjivanja usaglašenosti kvalifikovanih sredstava za izradu elektronskih potpisa i elektronskih pečata i sadržaju liste certifikovanih kvalifikovanih sredstava za izradu elektronskih potpisa i elektronskih pečata
[3] Pravilnik o mjerama i aktivnostima za zaštitu certifikata za elektronski potpis i elektronski pečat
[4] Pravilnik o sadržini i načinu vođenja evidencije davalaca elektronskih usluga povjerenja i registra kvalifikovanih davalaca elektrosnkih usluga povjerenja
[5] Pravilnik o najnižem iznosu osiguranja rizika od odgovornosti za štete koje nastanu vršenjem elektronskih usluga povjerenja
[6] Pravilnik o načinu sprovođenja verifikacije i načinu vršenja usluge čuvanja kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata
[7] Pravilnik o minimalnim tehničkim standardima i pratećim procedurama u odnosu na koje se određuje stepen sigurnosti sistema elektronske identifikacije
[8] Pravilnik o tehničkim i operativnim zahtjevima koji se odnose na čvor - mjesto priključenja sistema elektronske identifikacije i procesu uspostavljanja okvira za interoperabilnost sistema elektronske identifikacije
[9] Pravilnik o okviru za interoperabilnost sistema elektronske identifikacije
[10] Odluka o obezbjeđivanju pouzdane provjere autentičnosti klijenta i zajedničkim sigurnim otvorenim standardima komunikacije Savjeta Centralne banke Crne Gore

OSTALI ZAKONI

[1] Zakon o zaštiti podataka o ličnosti

STANDARDI

[1] ISO/IEC 27001:2013 – Information technology – Security techinques – Information security management
[2] ISO 9001:2015 - Quality management systems - Requirements
[3] ETSI EN 319 401 V2.2.1. (2018-04) – Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
[4] ETSI EN 319 411-1 V1.2.2. (2018-04) – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
[5] ETSI EN 319 411-2 V2.2.2. (2018-04) – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing

certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates

[6] ETSI EN 319 412-1 V1.1.1. (2016-02) – Electronic Signatures and Infrastructures (ESI);Certificate Profiles; Part 1: Overview and common data structures

[7] ETSI EN 319 412-2 V2.1.1. (2016-02) – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons

[8] ETSI EN 319 412-3 V1.1.1. (2016-02) – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons

[9] ETSI EN 319 412-5 V2.2.1. (2017-11) – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements

[10] ETSI EN 319 403 V 2.2.2 (2015-08) - Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers

[11] ETSI TS 119 312 V1.3.1. (2019-02) – Electronic Signatures and Infrastructures (ESI); Cryptographic Suites

[12] ETSI TS 119 495 V1.6.1 (2022-11) Electronic Signatures and Infrastructures (ESI);Sector Specific Requirements; Certificate Profiles and TSP Policy Requirements for Open Banking

[13] ETSI TS 119 412-1 V1.2.1 (2018-05) - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures

[14] EN 419 211-1:2014 – Protection profiles for secure signature creation device – Part 1: Overview (EN 419211-1:2014)

[15] EN 419 211-2:2013 – Protection profiles for secure signature creation device – Part 2: Device with key generation (EN 419211-2:2013)

[16] EN 419 211-4:2013 – Protection profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted channel to certificate generation application (EN 419211-4:2013)

[17] EN 419 211-5:2013 –Protection profiles for secure signature creation device – Part 5: Extension for device with key generation and trusted channel to signature creation application (EN 419211-5:2013)

[18] NIST FIPS PUB 140-2 (2001) – Security Requirements for Cryptographic Modules

[19] IETF RFC 3647 – Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework

[20] IETF RFC 5280 (2008) – Internet X.509 Public Key Infrastructure; Certificate and Certificate Revocation List (CRL) Profile

[21] IETF RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP (2013)

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.

12. Konačna verzija 8.0 od 10.10.2017 godine
    - Pravilnik usaglašen sa Zakonom o elektronskoj identifikaciji i elektronskom potpisu.

13. Konačna verzija 8.1 od 17.10.2019 godine
    - Pravilnik proširen sa kvalifikovanim certifikatom za uslugu elektronskog vremenskog pečata i kvalifikovanim certifikatom za napredni elektronski pečat za elektronsku fiskalizaciju.
14. Konačna verzija 8.2 od 06.10.2020 godine
    - Pravilnik proširen sa kvalifikovanim certifikatom za napredni elektronski potpis za elektronsku fiskalizaciju.
15. Konačna verzija 9.0 od 11.02.2022 godine
    - Pravilnik proširen sa certifikatom za autentifikaciju krajnjeg korisnika.
    - Pravilnik usaglašen sa Zakonom o elektronskoj identifikaciji i elektronskom potpisu.
16. Konačna verzija 10.0 od 04.12.2023 godine
    - Pravilnik proširen sa certifikatom za OCSP sistem.
    - Pravilnik je dopunjen sa informacijama o sistemu elektronske identifikacije, informacijama o sredstvu elektronske identifikacije visokog stepena sigurnosti, pri čemu je upravljanje sistemom elektronske identifikacije u skladu sa Zakonom o elektronskoj identifikaciji i elektronskom potpisu
17. Konačna verzija 11.0 od 08.02.2024 godine
    - Pravilnik proširen sa certifikatima za PSD2.
    - Napravljene određene korekcije u 1.1 Kratak pregled a vezano za sistem elektronske identifikacije
18. Konačna verzija 12.0 od 01.04.2026 godine
    - Promjena formata podataka koji se upisuju u SerialNumber atribut polja Subject certifikata krajnjeg korisnika
    - Dodavanje novog PostaCG CA atributa

Sadržaj

1. UVOD 12
1.1. Kratak pregled 12
1.2. Naziv dokumenta i identifikacioni podaci 13
1.3. Učesnici infrastrukture javnih ključeva 17
1.3.1. Certifikaciono tijelo (*Certification Authority*) 17
1.3.2. Registraciona tijela (*Registration Authorities*) 18
1.3.3. Naručioci i krajnji korisnici 19
1.3.4. Treća lica (*Relying parties*) 19
1.3.5. Ostali učesnici 19
1.4. Upotreba certifikata 19
1.4.1. Dozvoljena upotreba certifikata 19
1.4.2. Zabranjena upotreba certifikata 20
1.5. Upravljanje pravilnika 20
1.5.1. Tijelo koje upravlja Pravilnikom 20
1.5.2. Kontakt 20
1.5.3. Subjekt koji utvrđuje usaglašenost Pravilnika sa Zakonom 20
1.5.4. Postupci odobravanja Pravilnika 20
1.6. Definicije i skraćenice 20
2. OBJAVE I ODGOVORNOSTI REPOZITORIJUMA 24
2.1. Repozitoriji 24
2.2. Objava informacija o certifikatima 24
2.3. Vrijeme ili frekvencija objava 25
2.4. Kontrole pristupa do repozitorija 25
3. IDENTIFIKACIJA I AUTENTIFIKACIJA 26
3.1. Dodjeljivanje imena 26
3.1.1. Vrste imena 26
3.1.2. Potreba za smislenim imenima 26
3.1.3. Anonimnost krajnjeg korisnika i upotreba pseudonima 26
3.1.4. Pravila za tumačenje različitih vrsta imena 26
3.1.5. Jedinstvenost imena 32
3.1.6. Prepoznavanje, verifikacija i uloga zaštitnih znakova 32
3.2. Inicijalna provjera identiteta 32
3.2.1. Metoda za dokazivanje posjedovanja privatnog ključa 32
3.2.2. Provjera identiteta pravnog lica 32
3.2.3. Provjera identiteta fizičkog lica 33
3.2.4. Podaci o krajnjem korisniku koji se ne provjeravaju 34
3.2.5. Provjera ovlašćenja 34
3.2.6. Kriterijumi za povezivanje 34
3.3. Provjera identiteta kod zahtjeva za obnovu certifikata 34
3.3.1. Provjera identiteta kod rutinske obnove certifikata 34
3.3.2. Provjera identiteta kod zahtjeva za obnovu certifikata poslije opoziva ... 34
3.4. Provjera identiteta kod zahtjeva za opoziv 35
4. Upravljanje certifikatima 36
4.1. Zahtjev za izdavanje certifikata 36
Certifikat za napredni ili kvalifikovani elektronski potpis izdaje se isključivo punoljetnom fizičkom licu. 36
4.1.1. Ko može da zahtijeva izdavanje certifikata 36
4.1.2. Proces obrade zahtjeva i odgovornosti 36
4.2. Procesuiranje zahtjeva za certifikat 37

4.2.1. Postupak identifikacije i autentifikacije 37
4.2.2. Odobravanje ili odbijanje zahtjeva za izdavanje certifikata 37
4.2.3. Vrijeme za obradu zahtjeva 38
4.3. Izdavanje certifikata 38
4.3.1. Postupci CA u fazi izdavanja certifikata 38
4.3.2. Obavještavanje krajnjeg korisnika o izdavanju certifikata od strane CA 38
4.4. Prihvatanje certifikata 39
4.4.1. Postupak potvrde prihvata certifikata od strane krajnjeg korisnika 39
4.4.2. Objava certifikata od strane certifikacionog tijela 39
4.4.3. Obavještavanje ostalih učesnika o izdavanje certifikata 39
4.5. Upotreba para ključeva i certifikata 39
4.5.1. Upotreba privatnog ključa i certifikata sa strane krajnjeg korisnika 39
4.5.2. Upotreba javnog ključa i certifikata sa strane trećih lica 39
4.6. Obnova certifikata bez promjene ključa 40
4.7. Obnova certifikata 40
4.7.1. Okolnosti pod kojima se može obnoviti certifikat 40
4.7.2. Ko može da zahtijeva obnovu certifikata 40
4.7.3. Proces obrade zahtjeva za obnovu certifikata 40
4.7.4. Obavještavanje korisnika o izdavanju obnovljenog certifikata 40
4.7.5. Postupak potvrde prihvatanja obnovljenog certifikata 40
4.7.6. Objava obnovljenog certifikata 40
4.7.7. Obavještavanje ostalih učesnika o izdavanju obnovljenog certifikata 40
4.8. Promjena certifikata 40
4.8.1. Okolnosti pod kojima se može promjeniti certifikat 40
4.8.2. Ko može da zahtijeva promjenu certifikata 41
4.8.3. Proces obrade zahtjeva za promjenu certifikata 41
4.8.4. Obavještavanje krajnjeg korisnika o izdavanju promijenjenog certifikata 41
4.8.5. Postupak potvrde prihvata promijenjenog certifikata 41
4.8.6. Objava promijenjenog certifikata 41
4.8.7. Obavještavanje ostalih učesnika o izdavanju promijenjenog certifikata 41
4.9. Opoziv i suspenzija certifikata 41
4.9.1. Okolnosti pod kojima se vrši opoziv certifikata 41
4.9.2. Ko može da zahtijeva opoziv certifikata 42
4.9.3. Postupak opoziva 42
4.9.4. Vrijeme za predaju zahtjeva za opoziv 42
4.9.5. Vrijeme od zahtjeva za opoziv do opoziva 42
4.9.6. Obaveza provjere registra opozvanih certifikata sa strane trećih lica 43
4.9.7. Frekvencija izdavanja registra opozvanih certifikata (CRL) 43
4.9.8. Dozvoljena zakašnjenja kod objave registra opozvanih certifikata 43
4.9.9. On-line provjera statusa certifikata 43
4.9.10. Zahtjev za on-line provjeru statusa certifikata 43
4.9.11. Ostali oblici objavljivanja statusa certifikata 43
4.9.12. Posebni zahtjevi u slučaju kompromitovanja ključa 43
4.9.13. Okolnosti pod kojima se može izvršiti suspenzija certifikata 43
Ako se činjenice definisane u 4.9.1 Okolnosti pod kojima se vrši opoziv certifikata ne mogu odmah utvrditi na nesumnjiv način, certifikaciono tijelo će bez odlaganja da suspenduje certifikat do utvrdivanja tih činjenica 43
4.9.14. Ko može da traži suspenziju certifikata 43

4.9.15. Postupak suspenzije 43
4.9.16. Ograničenja perioda trajanja suspenzije 44
4.10. Servis objavljivanja statusa certifikata 44
4.10.1. Operativne karakteristike 44
4.10.2. Raspoloživost servisa 44
4.10.3. Dodatne funkcije 44
4.11. Prekid dogovora/ugovora/sporazuma 44
4.12. Deponovanje (escrow) i povratak ključa 44
4.12.1. Pravila upravljanja deponovanja i povratka privatnih ključeva za dešifrovanje 44
4.12.2. Pravila upravljanja enkapsulacije ključa sesija i povratka 45
5. KONTROLA FIZIČKOG PRISTUPA, PROCEDURA I OSOBLJA 46
5.1. Fizička zaštita 46
5.1.1. Lokacija i konstrukcija 46
5.1.2. Kontrola fizičkog pristupa 46
5.1.3. Napajanje i klimatizacija 46
5.1.4. Zaštita od vode 46
5.1.5. Zaštita od vatre 47
5.1.6. Smještanje medija 47
5.1.7. Odlaganje nepotrebnih materijala 47
5.1.8. Smještanje kopija medija na udaljenoj lokaciji 47
5.2. Kontrola procedura 47
5.2.1. Povjerljive uloge osoblja certifikacionog tijela 47
5.2.2. Potreban broj osoba za operativne postupke 48
5.2.3. Identifikacija i autentifikacija osoba za pojedine uloge 49
5.2.4. Povjerljive uloge koje moraju biti odvojene 49
5.3. Kontrola osoblja 49
5.3.1. Kvalifikacije, iskustva i provjere 49
5.3.2. Provjera prethodnih angažovanja 50
5.3.3. Obuka 50
5.3.4. Učestalost ponovnih obuka 50
5.3.5. Učestalost i redosljed rotacije uloga 50
5.3.6. Sankcije za neautorizovane aktivnosti 50
5.3.7. Zahtjevi za osoblje koje radi po ugovoru 50
5.3.8. Dokumentacija za potrebe osoblja 50
5.4. Procedure upravljanja revizijskih dnevnika 50
5.4.1. Događaji koji se bilježe 50
5.4.2. Učestalost procesuiranja dnevnika 51
5.4.3. Vrijeme čuvanja dnevnika 51
5.4.4. Zaštita dnevnika 51
5.4.5. Izrada rezervnih kopija dnevnika 51
5.4.6. Sistem prikupljanja dnevnika 51
5.4.7. Obavještavanje lica koje je izazvalo događaj 52
5.4.8. Procjena ranjivosti sistema 52
5.5. Arhiviranje podataka 52
5.5.1. Podaci koji se arhiviraju 52
5.5.2. Period čuvanja podataka u arhivi 53
5.5.3. Zaštita arhive 53
5.5.4. Procedure arhiviranja 53
5.5.5. Zahtjev za vremenski pečat arhiviranih podataka 53

5.5.6. Sistem arhiviranja (interni ili eksterni) 53
5.5.7. Procedure kontrole pristupa arhiviranim podacima i verifikacija..... 53
5.6. Obnova CA certifikata 53
5.7. Kompromitovanje i oporavak sistema poslije nepredviđenih situacija 53
5.7.1. Procedure kod incidenata ili kompromitovanja 53
5.7.2. Greške u radu sistema, programske opreme ili oštećenja podataka..... 53
5.7.3. Kompromitovanje privatnog ključa 54
5.7.4. Prirodne i druge katastrofe..... 54
5.8. Prestanak rada CA ili RA..... 54
6. TehničkO bezbJEDONOSNE kontrole..... 55
6.1. Generisanje ključeva i instalacija..... 55
6.1.1. Generisanje para ključeva..... 55
6.1.2. Dostavljanje krajnjem korisniku privatnog ključa..... 55
6.1.3. Dostavljanje javnog ključa krajnjeg korisnika davaocu elektronskih usluga povjerenja 55
6.1.4. Dostavljanje javnog ključa davaoca elektronskih usluga povjerenja trećim licima 55
6.1.5. Dužina ključeva 55
6.1.6. Generisanje parametara javnih ključeva 56
6.1.7. Namjena upotrebe ključeva (X.509 keyUsage) 56
6.2. Zaštita privatnog ključa i kontrole kriptografskih modula 57
6.2.1. Standardi i kontrole kriptografskih modula 57
6.2.2. N od M kontrola privatnog ključa..... 57
6.2.3. Deponovanje (key escrow) privatnog ključa 57
6.2.4. Kopija privatnih ključeva..... 57
6.2.5. Arhiviranje privatnih ključeva 57
6.2.6. Prenos privatnog ključa u kriptografski modul..... 57
6.2.7. Čuvanje kriptografskih ključeva na kriptografskom modulu 58
6.2.8. Način aktiviranja privatnog ključa..... 58
6.2.9. Način deaktiviranja privatnog ključa 58
6.2.10. Način uništavanja privatnog ključa..... 58
6.2.11. Nivo sigurnosti kriptografskih modula 58
6.3. Ostali aspekti upravljanja para ključeva 58
6.3.1. Arhiviranje javnog ključa 58
6.3.2. Rok važnosti certifikata i period upotrebe para ključeva..... 58
6.4. Aktivacijski podaci 59
6.4.1. Generisanje i instalacija aktivacijskih podataka 59
6.4.2. Zaštita aktivacijskih podataka..... 59
6.4.3. Ostali aspekti aktivacijskih podataka..... 59
6.5. Bezbjedonosni zahtjevi za računare..... 59
6.5.1. Specifični računarsko tehničko-bezbjedonosni zahtjevi..... 59
6.5.2. Nivo zaštite računara..... 60
6.6. Tehnički nadzor tokom upotrebe sistema 60
6.6.1. Nadzor razvoja sistema..... 60
6.6.2. Upravljanje bezbjednošću..... 60
6.6.3. Nadzor bezbjednosti tokom upotrebe sistema 60
6.7. Nadzor bezbjednosti računarske mreže 60
6.8. Vremenski pečat (Time-stamping) 60
7. CERTIFIKAT, CRL I OCSP PROFILI 61
7.1. Profil certifikata 61

7.1.1. Broj (brojevi) verzija Version number(s) 61
7.1.2. Ekstenzije certifikata 61
7.1.3. Identifikatori Algoritamskih objekata 64
7.1.4. Forme imena 64
7.1.5. Ograničenja za ime 65
7.1.6. Identifikator objekta za politiku davanja usluga povjerenja 65
7.1.7. Korišćenje Politike ograničenja ekstenzija 65
7.1.8. Sintaksa i semantika za kvalifikatore politike 65
7.1.9. Procesuiranje semantike za kritične ekstenzije Politike usluge povjerenja 65
7.2. CRL profil 65
7.2.1. Broj (brojevi) verzija 65
7.2.2. CRL i CRL entry ekstenzije 66
7.3. OCSP profil 66
7.3.1. Broj (brojevi) verzija 66
7.3.2. OCSP ekstenzije 66
8. REVIZIJA usaglašenosti i druge procjene 68
8.1. Učestalost ili okolnosti kada se vrše revizije 68
8.2. Identitet/kvalifikacije revizora 68
8.3. Revizorov odnos prema procjenjivanom subjektu 68
8.4. Oblasti koje pokriva procjenjivanje 68
8.5. Aktivnosti koje se preduzimaju u slučaju nedostatka 68
8.6. Objavljivanje rezultata 68
9. ostall poslovni I pravni aspekti 69
9.1. Cijene 69
9.1.1. Cijene usluga certifikacionog tijela 69
9.1.2. Nadoknade za pristup certifikatu 69
9.1.3. Nadoknade za opoziv ili pristup statusu informacija 69
9.1.4. Nadoknade za ostale servise 69
9.1.5. Politika refundiranja 69
9.2. Finansijska odgovornost 69
9.2.1. Osiguranja ili garancije davaoca elektronske usluge povjerenja 69
9.2.2. Ostala sredstva 69
9.2.3. Osiguranja ili garancije korisnika 69
9.3. Povjerljivost poslovnih informacija 69
9.3.1. Obim povjerljivih informacija 69
9.3.2. Informacije koje ne ulaze u obim povjerljivih informacija 69
9.3.3. Odgovornost za zaštitu povjerljivih informacija 70
9.4. Privatnost ličnih informacija 70
9.4.1. Plan privatnosti 70
9.4.2. Informacija koja se tretira privatnom 70
9.4.3. Informacija koja se ne smatra privatnom 70
9.4.4. Odgovornost za zaštitu privatnih informacija 70
9.4.5. Obavještenje i davanje saglasnosti za korišćenje privatnih informacija 70
9.4.6. Otkrivanje informacije u skladu sa sudskim ili administrativnim procesom 70
9.4.7. Ostale okolnosti kada se mogu otkrivati informacije 70
9.5. Prava na intelektualnu svojinu 70
9.6. Garancije 70
9.6.1. Garancije certifikacionog tijela (CA) 70
9.6.2. Garancije registracionog tijela (RA) 71

9.6.3. Garancije naručioca 71
9.6.4. Garancije trećih lica 71
9.6.5. Garancije ostalih učesnika 71
9.7. Izuzeća garancija 71
9.8. Ograničenja odgovornosti 72
9.8.1. Odgovornost i ograničenje od odgovornosti [PoštaCG-CA] 72
9.8.2. Odgovornost i ograničenje od odgovornosti krajnjih korisnika 72
9.9. Obeštećenja 72
9.10. Rok i prekid 72
9.10.1. Rok 72
9.10.2. Prekid 72
9.10.3. Efekti prekida i preživljavanja 72
9.11. Individualno obavještavanje i komunikacija sa učesnicima 73
9.12. Izmjene 73
9.12.1. Procedura za izmjenu 73
9.12.2. Mehanizmi obavještavanja i vremenski periodi 73
9.12.3. Okolnosti pod kojima se OID mora izmijeniti 73
9.13. Rješavanja u slučaju spora 73
9.14. Primjena zakona 73
9.15. Usaglašenost sa primjenljivim zakonom 73
9.16. Razne odredbe 74
9.16.1. Cjelokupni ugovor 74
9.16.2. Prenos prava 74
9.16.3. Klauzula o valjanosti 74
9.16.4. Izvršenje (nadoknade za pravnog zastupnika i odricanje od prava) 74
9.16.5. Viša sila 74
9.17. Ostale odredbe 74

Na osnovu Zakon o elektronskoj identifikaciji i elektronskom potpisu ("Službeni list Crne Gore", br. 031/17 i 072/19), Odbor direktora Pošte Crne Gore AD na sjednici od 14.04.2026. donio je

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

1. UVOD

1.1. Kratak pregled

Pošta Crne Gore AD upravlja infrastrukturom javnih ključeva [PoštaCG-PKI] za javne potrebe.U okviru [Pošte CG-PKI] za potrebe davanja elektronskih usluga povjerenja uspostavljeno je certifikaciono tijelo sa samo-potpisanim certifikatom (*Single Rooted Certification Authority*) [PoštaCG-CA].
[PoštaCG-CA] je kvalifikovani davalac elektronskih usluga povjerenja i upravlja sistemom elektronske identifikacije.
[PoštaCG-CA] kao davalac elektronskih usluga povjerenja izdaje kvalifikovane certifikate za napredni i kvalifikovani elektronski potpis, kvalifikovane certifikate za napredni i kvalifikovani elektronski pečat i kvalifikovane certifikate za autentifikaciju internet stranica. Pored navedenih kvalifikovanih certifikate izdaje i certifikate za upotrebu na Microsoft infrastrukturi, i certifikate za druge namjene

Infrastruktura javnih ključeva [PoštaCG-PKI] odnosno [PoštaCG-CA] istovremeno predstavlja i sistem elektronske identifikacije (PoštaCG-CA eID sistem), koji izdaje i upravlja sredstvo elektronske identifikacije visokog stepena sigurnosti. Sredstvo elektronske identifikacije koje izdaje [PoštaCG-CA] sadrži certifikat za autentifikaciju izdat na kriptografskom tokenu/kvalifikovanom sredstvu za izradu elektronskog potpisa (QSCD sredstvo).
Krajnji korisnik je vlasnik sredstva elektronske identifikacije. PoštaCG-CA eID sistem razlikuje dva slučaja vezano za krajnjeg korisnika:

- Krajnji korisnik je fizičko lice u kom slučaju sredstvo elektronske identifikacije sadrži certifikat za autentifikaciju fizičkog lica izdat na kriptografskom tokenu/kvalifikovanom sredstvu za izradu elektronskog potpisa (QSCD sredstvo).
- Krajnji korisnik je fizičko lice kod pravnog lica u kom slučaju sredstvo elektronske identifikacije sadrži certifikat za autentifikaciju fizičkog lica kod pravnog lica izdat na kriptografskom tokenu/kvalifikovanom sredstvu za izradu elektronskog potpisa (QSCD sredstvo).

Infrastruktura javnih ključeva [PoštaCG-PKI] odnosno [PoštaCG-CA] istovremeno pruža usluge izdavanja certifikata na osnovu odredbi Zakona o Centralnoj banci Crne Gore („Službeni list CG", br. 40/10, 6/13 i 70/17), Zakona o platnom prometu ("Službeni list Crne Gore", br. 062/13 od 31.12.2013, 006/14 od 04.02.2014, 111/22 od 07.10.2022, 007/23 od 20.01.2023) i Odlukom o obezbjeđivanju pouzdane provjere autentičnosti klijenta i zajedničkim sigurnim otvorenim standardima

komunikacije Savjeta Centralne banke Crne Gore - Član 35 (u daljem tekstu PSD2 certifikati eng. EUropean Payment Services Directive)

[PoštaCG-CA] nudi elektronske usluge povjerenja i usluge sistema elektronske identifikacije zainteresovanim fizičkim ili pravnim licima ili organima vlasti.

Certifikaciono tijelo [PoštaCG-CA] izdaje slijedeće tipove digitalnih certifikata za :

- kvalifikovani certifikat za kvalifikovani elektronski potpis izdat na kvalifikovanom sredstvu za izradu elektronskog potpisa (QSCD sredstvo);
- kvalifikovani certifikat za napredni elektronski potpis;
- kvalifikovani certifikat za povjerljivost izdat na kriptografskom tokenu/ kvalifikovanom sredstvu za izradu elektronskog potpisa (QSCD sredstvo);
- kvalifikovani certifikat za povjerljivost;
- kvalifikovani certifikat za autentifikaciju internet stranica;
- certifikat za Microsoft Windows Domain Controllera (DC) server;
- certifikat za SmartLogon izdat na kriptografskom tokenu/kvalifikovanom sredstvu za izradu elektronskog potpisa (QSCD sredstvo);
- kvalifikovani certifikat za kvalifikovani elektronski pečat izdat na kvalifikovanom sredstvu za izradu elektronskog potpisa (QSCD sredstvo);
- kvalifikovani certifikat za napredni elektronski pečat;
- kvalifikovani certifikat za uslugu elektronskog vremenskog pečata;
- kvalifikovani certifikat za napredni elektronski pečat za elektronsku fiskalizaciju;
- kvalifikovani certifikat za napredni elektronski potpis za elektronsku fiskalizaciju
- kvalifikovani certifikat za OCSP sistem (Online Certifikcate Status Protocol)
- certifikat za autentifikaciju krajnjeg korisnika izdat na kriptografskom tokenu/kvalifikovanom sredstvu za izradu elektronskog potpisa (QSCD sredstvo), čini sredstvo elektronske identifikacije visokog stepena sigurnosti
- Kvalifikovani certifikat za napredni elektronski pečat za PSD2
- Kvalifikovani certifikat za autentifikaciju internet stranica za PSD2

1.2. Naziv dokumenta i identifikacioni podaci

Ovaj dokument nosi naziv „Pravilnik o postupcima izdavanja certifikata i zaštite sistema“ i sadrži opšta pravila pružanja elektronskih usluga povjerenja , pravila upravljanja sistemom elektronske identifikacije, pravila o postupcima izdavanja certifikata i pravila o zaštiti sistema 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 certifikati za kvalifikovani elektronski potpis i za napredni elektronski potpis	
Kvalifikovani certifikat za kvalifikovani elektronski potpis izdat na kvalifikovanom sredstvu za izradu elektronskog potpisa (QSCD sredstvo)	
Opis:	Kvalifikovani certifikat za kvalifikovani elektronski potpis izdat na kvalifikovanom sredstvu za izradu elektronskog potpisa (QSCD sredstvo)

Namjena:	Kvalifikovani elektronski potpis definisan u Zakonu o elektronskoj identifikaciji i elektronskom potpisu član 11. 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 certifikat za napredni elektronski potpis

Opis:	Kvalifikovani certifikat za napredni elektronski potpis
Namjena:	Napredni elektronski potpis definisan u Zakonu o elektronskoj identifikaciji i elektronskom potpisu član 10. 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 certifikat za napredni elektronski potpis za elektronsku fiskalizaciju

Opis:	Kvalifikovani certifikat za napredni elektronski potpis za elektronsku fiskalizaciju
Namjena:	Napredni elektronski potpis definisan u Zakonu o elektronskoj identifikaciji i elektronskom potpisu član 10. i verifikacija identiteta korisnika
Period važenja:	Jedna (1) do pet (5) godina
Identifikaciona oznaka:	1.3.6.1.4.1.36737.1.1.1.3

Kvalifikovani certifikati za povjerljivost

Kvalifikovani certifikat za povjerljivost izdat na kriptografskom tokenu/ kvalifikovanom sredstvu za izradu elektronskog potpisa (QSCD sredstvo)

Opis:	Kvalifikovani certifikat za povjerljivost izdat na kriptografskom tokenu/ kvalifikovanom sredstvu za izradu elektronskog potpisa (QSCD sredstvo) 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

Kvalifikovani certifikat za povjerljivost

Opis:	Kvalifikovani certifikat za povjerljivost sa mogućnošću oporavka istorije privatnih ključeva
Namjena:	Povjerljivost (šifriranje) podataka

Period važenja:	Jedna (1) do pet (5) godina
Identifikaciona oznaka:	1.3.6.1.4.1.36737.1.2.1.2

Kvalifikovani certifikati za autentifikaciju internet stranica

Kvalifikovani certifikat za autentifikaciju internet stranica

Opis:	Kvalifikovani certifikati za autentifikaciju internet stranica
Namjena:	Autentifikacija internet stranica definisana u Zakonu o elektronskoj identifikaciji i elektronskom potpisu član 32 i uspostavljanje SSL/TLS sesije
Period važenja:	Jedna (1) do pet (5) godina
Identifikaciona oznaka:	1.3.6.1.4.1.36737.1.5.1.1

Kvalifikovani certifikat za autentifikaciju internet stranica za PSD2

Opis:	Kvalifikovani certifikati za autentifikaciju internet stranica za PSD2
Namjena:	Autentifikacija internet stranica definisana u Zakonu o elektronskoj identifikaciji i elektronskom potpisu član 32 i uspostavljanje SSL/TLS sesije
Period važenja:	Jedna (1) do pet (5) godina
Identifikaciona oznaka:	1.3.6.1.4.1.36737.1.5.1.2

Certifikat za Microsoft Windows Domain Controllera (DC) server

Certifikat za Microsoft Windows Domain Controllera (DC) server

Opis:	Certifikat za Microsoft Windows Domain Controllera (DC) server
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

Certifikat za SmartLogon izdat na kriptografskom tokenu/ kvalifikovanom sredstvu za izradu elektronskog potpisa (QSCD sredstvo)

Certifikat za SmartLogon izdat na kriptografskom tokenu/ kvalifikovanom sredstvu za izradu elektronskog potpisa (QSCD sredstvo)

Opis:	Certifikat za SmartLogon izdat na kriptografskom tokenu/ kvalifikovanom sredstvu za izradu elektronskog potpisa (QSCD sredstvo)

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

Kvalifikovani certifikati za elektronske pečate i uslugu elektronskog vremenskog pečata

Kvalifikovani certifikat za kvalifikovani elektronski pečat izdat na kvalifikovanom sredstvu za izradu elektronskog potpisa (QSCD sredstvo)

Opis:	Kvalifikovani certifikat za kvalifikovani elektronski pečat izdat na kvalifikovanom sredstvu za izradu elektronskog potpisa (QSCD sredstvo)
Namjena:	Kvalifikovani elektronski pečat definisan u Zakonu o elektronskoj identifikaciji i elektronskom potpisu član 25. stav 3.
Period važenja:	Jedna (1) do pet (5) godina
Identifikaciona oznaka:	1.3.6.1.4.1.36737.1.6.1.1

Kvalifikovani certifikat za napredni elektronski pečat

Opis:	Kvalifikovani certifikat za napredni elektronski pečat
Namjena:	Napredni elektronski pečat definisan u Zakonu o elektronskoj identifikaciji i elektronskom potpisu član 25. stav 2.
Period važenja:	Jedna (1) do pet (5) godina
Identifikaciona oznaka:	1.3.6.1.4.1.36737.1.6.1.2

Kvalifikovani certifikat za uslugu elektronskog vremenskog pečata

Opis:	Kvalifikovani certifikat za uslugu elektronskog vremenskog pečata
Namjena:	Napredni elektronski pečat za izradu elektronskog vremenskog pečata ili kvalifikovanog elektronskog vremenskog pečata u skladu sa Zakonom o elektronskoj identifikaciji i elektronskom potpisu član 26.
Period važenja:	Jedna (1) do pet (5) godina
Identifikaciona oznaka:	1.3.6.1.4.1.36737.1.6.1.3

Kvalifikovani certifikat za napredni elektronski pečat za elektronsku fiskalizaciju

Opis:	Kvalifikovani certifikat za napredni elektronski pečat za elektronsku fiskalizaciju
Namjena:	Napredni elektronski pečat definisan u Zakonu o elektronskoj identifikaciji i elektronskom potpisu član 25.

	stav 2.
Period važenja:	Jedna (1) do pet (5) godina
Identifikaciona oznaka:	1.3.6.1.4.1.36737.1.6.1.4
Kvalifikovani certifikat za OCSP sistem	
Opis:	Kvalifikovani certifikat za OCSP sistem
Namjena:	Napredni elektronski pečat za potpisivanje odgovora OCSP sistema u skladu sa Zakonom o elektronskoj identifikaciji i elektronskom potpisu član 25.
Period važenja:	Jedna (1) do pet (5) godina
Identifikaciona oznaka:	1.3.6.1.4.1.36737.1.6.1.5
Kvalifikovani certifikat za napredni elektronski pečat za PSD2	
Opis:	Kvalifikovani certifikat za napredni elektronski pečat za PSD2
Namjena:	Napredni elektronski pečat definisan u Zakonu o elektronskoj identifikaciji i elektronskom potpisu član 25. stav 2.
Period važenja:	Jedna (1) do pet (5) godina
Identifikaciona oznaka:	1.3.6.1.4.1.36737.1.6.1.6
Certifikat za autentifikaciju krajnjeg korisnika izdat na kriptografskom tokenu/ kvalifikovanom sredstvu za izradu elektronskog potpisa (QSCD sredstvo)	
Opis:	Certifikat za autentifikaciju krajnjeg korisnika izdat na kriptografskom tokenu/ kvalifikovanom sredstvu za izradu elektronskog potpisa (QSCD sredstvo)
Namjena:	Verifikacija identiteta –krajnjeg korisnika
Period važenja:	Jedna (1) do pet (5) godina
Identifikaciona oznaka:	1.3.6.1.4.1.36737.1.7.1.1

1.3. Učesnici infrastrukture javnih ključeva

1.3.1. Certifikaciono tijelo (*Certification Authority*)

Certifikaciono tijelo [PoštaCG-CA] izdaje certifikate u skladu sa Zakonom o elektronskoj identifikaciji i elektronskom potpisu (u daljem tekstu Zakon) 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] PMA (*Policy Management Authority*);
- Izvođenje postupaka upravljanja certifikatima i upravljanje infrastrukturom, privatnih kriptografskih ključeva, servera i programa [PoštaCG-CA] OA (*Operations Authority*);
- Identifikaciju korisnika [PoštaCG-CA] RA (*Registration Authority*).

[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 elektronskih usluga povjerenja (*PKI Disclosure Statement* - PDS);
- PotpisUgovor sa krajnjim korisnikom (*End-User Agreement*)
- Podnošenje Pravilnika na usvajanje Odboru direktora Pošte Crne Gore;
- Predlaže za imenovanje osoblje [PoštaCG-CA] OA na njihove dužnosti;
- Nadzor i reviziju usklađenosti davanja elektronskih usluga povjerenja [PoštaCG-CA] sa ovim Pravilnikom;
- Autorizaciju oporavka i povratka istorije privatnih ključeva za dešifrovanje krajnjih korisnika, koji su bili izdati 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 krajnjih korisnika;
- Potpisivanje i izdavanje X.509 certifikata za povezivanje identiteta krajnjih korisnika sa njihovim javnim kriptografskim ključevima;
- Objavljivanje certifikata u javnom LDAP imeniku;
- Opoziv certifikata na osnovu zahtjeva krajnjih korisnika ili na svoju inicijativu;
- Izdavanje i objavljivanje liste opozvanih certifikata;
- Upravljanje infrastrukturom certifikacionog tijela u skladu sa ovim Pravilnikom;
- Rješavanje sporova između krajnjih korisnika ili 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 krajnjih 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. U situaciji kada RA prikuplja zahtjeve u papirnom obliku, jedna kopija originalnih zahtjeva proslijeđuje se u [PoštaCG-CA]. Način proslijeđivanja može biti ličnom dostavom ili internom poštom. U situaciji

kada RA prikuplja zahtjeva u elektronskom obliku, kreira predmet i isti prosljeđuje u [PoštaCG-CA].

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 prosledjivanje podataka za izdavanje 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 krajnjeg korisnika i za proslijedjivanje podataka za izdavanje certifikata i zahtjeva za promjenu statusa certifikata prema centralnom registracionom tijelu;
  - Uručenje certifikata, predmetnog Ugovora i ostale dokumentacije po uspješnoj verifikaciji identiteta krajnjeg korisnika

1.3.3. Naručioci i krajnji korisnici

[PoštaCG-CA] izdaje certifikate zainteresovanim fizičkim ili pravnim licima ili organima vlasti.

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

Kada se certifikat izda naručiocu koji je pravno lice, tada naručilac daje certifikat na upotrebu krajnjem 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 ili pravna lica ili organe vlasti, 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 krajnjim 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 subjekti koji, na neki način, doprinose ili učestvuju u obezbijedjivanju kvaliteta rada davaoca elektronskih usluga povjerenja i usluga sistema elektronske identifikacije.

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 certifikatu krajnjih korisnika 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 elektronskog potpisa, verifikaciju elektronskog pečata, verifikaciju elektronskog

vremenskog pečata, verifikaciju identiteta internet stranica, verifikaciju identiteta ili funkcije krajnjeg korisnika, identiteta ili funkcije servera 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] moraju da se koriste u skladu sa Zakonom, ovim Pravilnikom i drugim propisima iz ove oblasti.

1.5. Upravljanje pravilnika

1.5.1. Tijelo koje upravlja Pravilnikom

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

1.5.2. Kontakt

Kontaktni podaci za [PoštaCG-CA] su:

Adresa: Pošta Crne Gore AD
Certification Authority PMA
Slobode 1
81000 Podgorica
Crna Gora
E-mail: info@postacg-ca.me, pma@postacg.me
Internet: http://www. postacg-ca.me/

Kontaktni podaci za [PoštaCG-CA] Registracionog tijelo (RA) su:

Adresa: Pošta Crne Gore AD
Certification Authority RA
Slobode 1
81000 Podgorica
Crna Gora
E-mail: info@postacg-ca.me, ra@postacg.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

Autentifikacija: Elektronski postupak koji omogućava potvrđivanje elektronske identifikacije fizičkog ili pravnog lica ili porijekla i integriteta podataka u elektronskom obliku.
Arhiva:_ Specifična baza podataka za čuvanje zapisa za određeni period vremena u cilju bezbjednosti, backup-a ili revizije.
Autor elektronskog pečata: Pravno lice ili organ vlasti koje upotrebljava elektronski pečat korišćenjem podataka za izradu elektronskog pečata;
Asimetrični kriptografski algoritmi: Kriptografski algoritmi koji se koriste za realizaciju tehnologije digitalnog potpisa kojom se obezbjeđuje: autentičnost,

integritet i neporecivost transakcija. Algoritmi se nazivaju asimetričnim zato što se različiti kriptografski ključevi koriste za šifrovanje i za dešifrovanje.

Asimetrični par ključeva (key pair): Privatni ključ i javni ključ, kao matematički par koji se koriste za potrebe rada asimetričnog kriptografskog algoritma, kao što je na primjer RSA algoritam.

Autorizacija: Procedura utvrđivanja prava koje neki autentifikovani korisnik ima za korišćenje odgovarajuće aplikacije ili servisa.

Aplikacija certifikacionog tijela - 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 certifikata i zahtjeva za promjenu statusa certifikata prema aplikaciji certifikacionog tijela,
- kreiranje certifikata na kriptografskom tokenu/QSCD sredstvu ili fajlu za korisnike koji su izabrali ovaj model,
- prosleđivanje registracionog i autentikacionog koda, praznog kriptografskog tokena/QSCD sredstvu ili popunjenog kriptografskog tokena/QSCD sredstvu ili fajla i PIN-a na adresu navedenu u zahtjevu ili lokalnom registracionom tijelu.

Certifikaciono tijelo – pravno, fizičko lice (preduzetnik) ili organ vlasti koje izdaje certifikate ili pruža druge usluge povezane s elektronskim potpisom, uključujući sisteme davalaca elektronskih usluga povjerenja.

Certifikat ili digitalni 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 služe za potpis i elektronsku 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 krajnji korisnik za preuzimanje i rad sa certifikatom.

Korisnik je fizičko, pravno lice ili organ vlasti koje se oslanja da elektronsku identifikaciju ili elektronsku uslugu povjerenja;

Krajnji korisnik je autor elektronskog pečata ili potpisnik ili vlasnik sredstva elektronske identifikacije;

Kriptografski modul – Aplikacija certifikacionog tijela koja omogućava kreiranje certifikata na kriptografskom tokenu ili drugom davaocu kriptografskih usluga.

Kriptografski token – Uređaj na kome se kreiraju podaci za izradu elektronskog potpisa. Kriptografski token može da bude u obliku pametne kartice, ili token uređaja sa integrisanom pametnom karticom.

Kvalifikovano sredstvo za izradu elektronskog potpisa (QSCD sredstvo) - Uređaj na kome se kreiraju podaci za izradu elektronskog potpisa, a koji zadovoljava sve tehničke zahtjeve za kvalifikovanim elektronskim potpisom navedene u Zakonu, podzakonskim aktima i ovim dokumentu. QSCD sredstvo može da bude u obliku

pametne kartice, ili token uređaja sa integrisanom pametnom karticom. Samo sa QSCD sredstvom moguće je formirati kvalifikovani elektronski potpis.

Kvalifikovani certifikat - certifikat koji je izdat od strane certifikacionog tijela za izdavanje kvalifikovanih certifikata i sadrži podatke predviđene zakonom.

Kvalifikovani elektronski potpis - napredni elektronski potpis koji je izrađen pomoću kvalifikovanog sredstva za izradu elektronskog potpisa i zasniva se na kvalifikovanom certifikatu za elektronski potpis.

Lični identifikacioni podaci - obuhvataju skup podataka u elektronskom obliku koji omogućavaju da se utvrdi identitet fizičkog, pravnog lica ili organa vlasti;

Napredni elektronski potpis - elektronski potpis kojim se pouzdano garantuje identitet potpisnika i integritet elektronskog dokumenta, a koji ispunjava uslove propisane Zakonom.

Naručilac - je fizičko, pravno lice ili organ vlasti koje naručuje uslugu od davaoca elektronske usluge povjerenja ili usluge elektronske identifikacije.

Organ vlasti je državni organ, organ državne uprave, organ lokalne samouprave, odnosno lokalne uprave i pravno lice koje vrši javna ovlašćenja.

PIN – šifra koja se koristi za zaštitu pristupa podacima za izradu elektronskog potpisa koji se nalaze na kriptografskom tokenu/QSCD sredstvu.

Podaci za izradu elektronskog potpisa – jedinstveni podaci (kodovi ili privatni kriptografski ključevi), koje potpisnik koristi za izradu elektronskog potpisa;

Podaci za verifikaciju tj. provjeru elektronskog potpisa – podaci koji se koriste za verifikaciju elektronskog potpisa ili elektronskog pečata;

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.

Podaci za izradu elektronskog pečata - jedinstveni podaci koje autor elektronskog pečata koristi za izradu elektronskog pečata;

Certifikat za elektronski pečat - elektronska potvrda koja povezuje podatke za verifikaciju elektronskog pečata sa pravnim licem ili oragnom vlasti i potvrđuje naziv tog pravnog lica ili organa vlasti;

Kvalifikovani certifikat za elektronski pečat - certifikat za elektronski pečat koji izdaje kvalifikovani davalac usluga povjerenja i koji ispunjava posebne uslove propisane zakonom;

Sredstvo za izradu elektronskog pečata - odgovarajuća računarska oprema ili računarski program koji se koristi za izradu elektronskog pečata;

Sredstvo za izradu kvalifikovanog elektronskog pečata - sredstvo za izradu elektronskog pečata koje ispunjava posebne uslove propisane zakonom;

Elektronski vremenski pečat – je skup podataka u elektronskom obliku koji povezuju druge podatke u elektronskom obliku sa određenim vremenom i na taj način dokazuju da su ti podaci postojali u to vrijeme;

Kvalifikovani elektronski vremenski pečat - je elektronski vremenski pečat koji ispunjava posebne zahtjeve, i to:

1) povezuje datum i vrijeme sa podacima tako da se sprječava svaka mogućnost promjene podataka;
2) zasnovan je na preciznom vremenskom izvoru koji je povezan sa koordiniranim univerzalnim vremenom (UTC); i
3) potpisan je naprednim elektronskim potpisom ili pečatiran pomoću naprednog elektronskog pečata kvalifikovanog davaoca usluga povjerenja.

Vremenski pečat – sinonim za Elektronski vremenski pečat

Davalac elektronskih usluga povjerenja – pravno, fizičko lice (preduzetnik) ili organ vlasti koje pruža jednu ili više usluga u skladu sa Zakonom o elektronskoj identifikaciji i elektronskom potpisu .

Kvalifikovani davalac elektronskih usluga povjerenja – pravno, fizičko lice (preduzetnik) ili organ vlasti koje ispunjava zahtjeve propisane Zakonom o elektronskoj identifikaciji i elektronskom potpisu za kvalifikovanog davaoca elektronskih usluga povjerenja za jednu ili više usluga u predmetnom zakonu.

Elektronska identifikacija - je postupak korišćenja identifikacionih podataka u elektronskom obliku koji na jedinstven način predstavljaju fizičko lice, pravno lice ili organ vlasti.

Sistem elektronske identifikacije - je sistem za izdavanje sredstava elektronske identifikacije fizičkim licima, pravnim licima, organima vlasti, odnosno fizičkim licima koja zastupaju pravna lica ili organe vlasti.

Sredstvo elektronske identifikacije - može biti skup podataka, računarska oprema (hardver) ili računarski program (softver) koji sadrže identifikacione podatke u elektronskom obliku ili povezuju fizičko lice, pravno lice ili organ vlasti sa tim podacima, a koji se koriste za autentifikaciju za uslugu u elektronskom obliku.

faktor autentifikacije je faktor za koji je potvrđeno da je povezan sa fizičkim licem, a može pripadati jednoj od sljedećih kategorija: faktor autentifikacije na osnovu vlasništva (faktor autentifikacije za koji subjekt mora dokazati da ga posjeduje), faktor autentifikacije na osnovu znanja (faktor autentifikacije za koji subjekt mora dokazati da ga poznaje), svojstveni faktor autentifikacije (faktor zasnovan na fizičkom obilježju fizičkog lica)

dinamička autentifikacija je elektronski proces u kojem se upotrebljava kriptografija ili druge tehnike, kako bi se na zahtjev zainteresovane strane stvorio elektronski dokaz da subjekt kontroliše ili posjeduje identifikacione podatke, a koji se mijenja sa svakom autentifikacijom između subjekta i sistema koji provjerava identitet subjekta;

NCA (National Competent Authority) je naziv organa koji je pružaocu platnih usluga izdao odobrenje za pružanje platnih usluga

Uloge pružaoca platnih usluga mogu biti:

- vođenje računa - PSP_AI;
- iniciranje plaćanja - PSP_PI;
- pružanje informacija o računu - PSP_AS; i/ili
- izdavanje platnih instrumenata na osnovu platnih kartica - PSP_IC;

Skraćenice:

ARL	Authority 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
PSD2	Payment Services Directive 2
NCA	National Competent Authority
nCAName	NCA Name
nCAId	NCA Id

PSP (eng. Payment Service Provider) Pružalac platnih usluga
PSP_AI (eng. Account Information Service) Pružalac platnih usluga - vođenje računa
PSP_PI (eng. Payment Initiation Service Provider) Pružalac platnih usluga - iniciranje plaćanja
PSP_AS (eng. Account Servicing Payment Service Provider) Pružalac platnih usluga - pružanje informacija o računu
PSP_IC (eng. Payment Service Provider Issuing Card-based payment instruments) Pružalac platnih usluga - izdavanje platnih instrumenata na osnovu platnih kartica

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; http://eid.postacg-ca.me
Javni imenik LDAP: ldap://ldap.postacg-ca.me

Putem OCSP servisa dostupne su informacije o statusu izdatih certifikata koje izdaje PoštaCG CA tijelo.

Adrese OCSP servisa je: http://ocsp.postacg-ca.me/PostaCGCA

U repozitorijumu se ne objavljuju povjerljivi podaci.

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;
- Šablon 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 elektronskih usluga povjerenja i usluga elektronske identifikacije.

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 krajnjeg korisnika koje je definisano u tabeli u odjeljku 3.1.4. Pravila za tumačenje različitih vrsta imena. U certifikatima je ime ili funkcija krajnjeg korisnika, polje Subject, upisano kao jedinstveno ime (Distinguished Name - DN), u obliku X.509 printableString 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 krajnjeg korisnika i ima smislenu vrijednost.

3.1.3. Anonimnost krajnjeg 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 tj. X500 jedinstveno ime) u skladu sa RFC5280 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 za elektronske potpise, povjerljivost i autentifikaciju krajnjeg korisnika:

Atribut jedinstvenog imena	Sadržaj
Country (C =)	Dvoslovna ISO3166-1 oznaka države u kojoj je registrovano sjedište davaoca usluge povjerenja
Organizational Unit (OU =)	Fizičko lice
Common Name (CN=)	Ime i prezime krajnjeg korisnika
Serial Number (serialNumber =)	- Osmocifreni jedinstveni identifikator krajnjeg korisnika definisan članom 4. Uredbe o načinu određivanja identifikacionog broja potpisnika kvalifikovanog certifikata za elektronski potpis Ministarstva unutrašnih poslova Crne Gore sa prefiksom „PNOME–“ ili - Broj lične karte krajnjeg korisnika izdat od nadležnog organa sa prefiksom „IDCME–“ ili - Broj pasoša krajnjeg korisnika izdat od nadležnog organa sa prefiksom „PAS + dvoslovna oznaka države–“. Dvoslovna oznaka države mora biti u skladu sa međunarodnim standardom ISO 3166-1 ili. - Jedinstveni serijski broj koji određuje davalac usluge povjerenja i u formatu: CA:PCG-xx...x (x – broj od 0 do 9).
givenName	Ime krajnjeg korisnika

Surname	Prezime krajnjeg korisnika

* Atribut "Common Name" može da sadrži i dodatne informacije kao na primjer akademsku titulu krajnjeg korisnika.

Oblik za fizičko lice kod pravnog lica za elektronske potpise, povjerljivost i autentifikaciju krajnjeg korisnika:

Atribut jedinstvenog imena	Sadržaj
Country (C =)	Dvoslovna ISO3166-1 oznaka države u kojoj je registrovano sjedište davaoca usluge povjerenja
Organizational Unit (OU =)	Pravno lice
OrganizationName (O =)	Registrovani puni ili skraćeni naziv pravnog lica
organizationIdentifier	Registrovani poreski identifikacioni broj (PIB) pravnog lica u formatu „VATDvoslovna ISO3166-1 oznaka države u kojoj je registrovano sjedište pravnog lica -PIB“
Common Name (CN=)	Ime i prezime krajnjeg korisnika*
Serial Number (serialNumber =)	- Osmocifreni jedinstveni identifikator krajnjeg korisnika definisan članom 4. Uredbe o načinu određivanja identifikacionog broja potpisnika kvalifikovanog certifikata za elektronski potpis Ministarstva unutrašnih poslova Crne Gore sa prefiksom „PNOME–“ ili - Broj lične karte krajnjeg korisnika izdat od nadležnog organa sa prefiksom „IDCME–“ ili - Broj pasoša krajnjeg korisnika izdat od nadležnog organa sa prefiksom „PAS + dvoslovna oznaka države–“. Dvoslovna oznaka države mora biti u skladu sa međunarodnim standardom ISO 3166-1 ili. - Jedinstveni serijski broj koji određuje davalac usluge povjerenja i u formatu: CA:PCG-xx...x (x – broj od 0 do 9).
givenName	Ime krajnjeg korisnika
Surname	Prezime krajnjeg korisnika

* Atribut "Common Name" može da sadrži i dodatne informacije kao na primjer akademsku titulu krajnjeg korisnika.

Oblik za pravno lice za elektronske pečate:

Atribut jedinstvenog imena	Sadržaj
Country (C =)	Dvoslovna ISO3166-1 oznaka države u kojoj je registrovano sjedište davaoca usluge povjerenja
Organizational Unit (OU =)	Pravno lice
OrganizationName (O =)	Registrovani puni ili skraćeni naziv pravnog lica

organizationIdentifier	Registrovani poreski identifikacioni broj (PIB) pravnog lica u formatu „VATDvoslovna ISO3166-1 oznaka države u kojoj je registrovano sjedište pravnog lica -PIB“
Common Name (CN=)	Puni ili skraćeni naziv pravnog lica
Serial Number (serialNumber =)	Jedinstveni serijski broj koji određuje davalac usluge povjerenja i u formatu: CA:PCG-xx...x (x – broj od 0 do 9).

* Navedeni atributi sadrže punu identifikaciju subjekta. Jedinstveno ime može da sadrži i dodatne atribute na primjer dodatni "Organizational Unit (OU =)" za potrebe pojedinog subjekta.

Oblik za pravno lice za napredne elektronske pečate za PSD2:

Atribut jedinstvenog imena	Sadržaj
Country (C =)	Dvoslovna ISO3166-1 oznaka države u kojoj je registrovano sjedište davaoca usluge povjerenja
Organizational Unit (OU =)	Pravno lice
OrganizationName (O =)	Registrovani puni ili skraćeni naziv pravnog lica
organizationIdentifier	Autorizacijski broj pravnog lica u formatu koji je u skladu sa: ETSI TS 119 495 [12] Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Certificate Profiles and TSP Policy Requirements for Open Banking Poglavlje 5.2.1 Authorization Number or other recognized identifier for Open Banking
Common Name (CN=)	Puni ili skraćeni naziv pravnog lica
Serial Number (serialNumber =)	Jedinstveni serijski broj koji određuje davalac usluge povjerenja i u formatu: CA:PCG-xx...x (x – broj od 0 do 9).

* Navedeni atributi sadrže punu identifikaciju subjekta. Jedinstveno ime može da sadrži i dodatne atribute na primjer dodatni "Organizational Unit (OU =)" za potrebe pojedinog subjekta.

Oblik za autentifikaciju internet stranica za pravna lica:

Atribut jedinstvenog imena	Sadržaj
Country (C =)	Dvoslovna ISO3166-1 oznaka države u kojoj je registrovano sjedište davaoca usluge povjerenja
Organizational Unit (OU =)*	Pravno lice

OrganizationName (O =)	Registrovani puni ili skraćeni naziv pravnog lica
organizationIdentifier	Registrovani poreski identifikacioni broj (PIB) pravnog lica u formatu „VATDvoslovna ISO3166-1 oznaka države u kojoj je registrovano sjedište pravnog lica -PIB“ (polje nije obavezno)
State (St) =	Engleski naziv države u kojoj je registrovano sjedište pravnog lica
Lokacija (L) =	Naziv grada u kome je registrovano sjedište pravnog lica
Jurisdiction of Incorporation (jurisdictionCountryName) =	Dvoslovna ISO3166-1 oznaka države nadležne za registraciju pravnog lica
Tip organizacije (businessCategory)	Sadrži jednu od sledećih vrijednosti: "Private Organization", "Government Entity", "Business Entity", ili "Non-Commercial Entity"
Common Name (CN=)	Puno domensko ime servera (eng. Fully Qualified Domain Name, FQDN)
Serial Number (serialNumber =)**	Registrovani matični broj pravnog lica

* Navedeni atributi sadrže punu identifikaciju subjekta. Jedinstveno ime može da sadrži i dodatne atribute na primjer dodatni "Organizational Unit (OU =)" za potrebe pojedinog subjekta.

** Za vladine institucije koje ne posjeduju Registrovani matični broj pravnog lica ili raspoložive podatke o datumu kreiranja koji se mogu verifikovati, [PoštaCG-CA] će unijeti vrijednost "Government".

Oblik za autentifikaciju internet stranica za pravna lica PSD2:

Atribut jedinstvenog imena	Sadržaj
Country (C =)	Dvoslovna ISO3166-1 oznaka države u kojoj je registrovano sjedište davaoca usluge povjerenja
Organizational Unit (OU =)*	Pravno lice
OrganizationName (O =)	Registrovani puni ili skraćeni naziv pravnog lica
organizationIdentifier	Autorizacijski broj pravnog lica u formatu koji je u skladu sa: ETSI TS 119 495 [12] Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Certificate Profiles and TSP Policy Requirements for Open Banking Poglavlje 5.2.1 Authorization Number or other recognized identifier for Open Banking
State (St) =	Engleski naziv države u kojoj je registrovano sjedište pravnog lica

Lokacija (L) =	Naziv grada u kome je registrovano sjedište pravnog lica
Jurisdiction of Incorporation (jurisdictionCountryName) =	Dvoslovna ISO3166-1 oznaka države nadležne za registraciju pravnog lica
Tip organizacije (businessCategory)	Sadrži jednu od sledećih vrijednosti: "Private Organization", "Government Entity", "Business Entity", ili "Non-Commercial Entity"
Common Name (CN=)	Puno domensko ime servera (eng. Fully Qualified Domain Name, FQDN)
Serial Number (serialNumber =)**	Registrovani matični broj pravnog lica

* Navedeni atributi sadrže punu identifikaciju subjekta. Jedinstveno ime može da sadrži i dodatne atribute na primjer dodatni "Organizational Unit (OU =)" za potrebe pojedinog subjekta.

** Za vladine institucije koje ne posjeduju Registrovani matični broj pravnog lica ili raspoložive podatke o datumu kreiranja koji se mogu verifikovati, [PoštaCG-CA] će unijeti vrijednost "Government".

Oblik za fizičko lice kod pravnog lica za SmartLogon:

Atribut jedinstvenog imena	Sadržaj
Country (C =)	Dvoslovna ISO3166-1 oznaka države u kojoj je registrovano sjedište davaoca usluge povjerenja
Organizational Unit (OU =)	Pravno lice
OrganizationName (O =)	Registrovani puni ili skraćeni naziv pravnog lica
organizationIdentifier	Registrovani poreski identifikacioni broj (PIB) pravnog lica u formatu „VATDvoslovna ISO3166-1 oznaka države u kojoj je registrovano sjedište pravnog lica -PIB“
Common Name (CN=)	Ime i prezime ili funkcija korisnika

Serial Number (serialNumber =)	- Osmocifreni jedinstveni identifikator krajnjeg korisnika definisan članom 4. Uredbe o načinu određivanja identifikacionog broja potpisnika kvalifikovanog certifikata za elektronski potpis Ministarstva unutrašnih poslova Crne Gore sa prefiksom „PNOME–“ ili - Broj lične karte krajnjeg korisnika izdat od nadležnog organa sa prefiksom „IDCME–“ ili - Broj pasoša krajnjeg korisnika izdat od nadležnog organa sa prefiksom „PAS + dvoslovna oznaka države–“. Dvoslovna oznaka države mora biti u skladu sa međunarodnim standardom ISO 3166-1 ili. - Jedinstveni serijski broj koji određuje davalac usluge povjerenja i u formatu: CA:PCG-xx...x (x – broj od 0 do 9).

Oblik za Microsoft Windows Domain Controllera (DC) servere:

Atribut jedinstvenog imena	Sadržaj
Country (C =)	Dvoslovna ISO3166-1 oznaka države u kojoj je registrovano sjedište davaoca usluge povjerenja
Organizational Unit (OU =)	Pravno lice
OrganizationName (O =)	Registrovani puni ili skraćeni naziv pravnog lica
organizationIdentifier	Registrovani poreski identifikacioni broj (PIB) pravnog lica u formatu „VATDvoslovna ISO3166-1 oznaka države u kojoj je registrovano sjedište pravnog lica -PIB“
Common Name (CN=)	DC server hostname sa domenom (FQDN)

Oblik za pravno lice za kvalifikovane certifikate za uslugu elektronskog vremenskog pečata:

Atribut jedinstvenog imena	Sadržaj
Country (C =)	Dvoslovna ISO3166-1 oznaka države u kojoj je registrovano sjedište davaoca usluge povjerenja
Organizational Unit (OU =)	Pravno lice
OrganizationName (O =)	Registrovani puni ili skraćeni naziv pravnog lica
organizationIdentifier	Registrovani poreski identifikacioni broj (PIB) pravnog lica u formatu „VATDvoslovna ISO3166-1 oznaka države u kojoj je registrovano sjedište pravnog lica -PIB“
Common Name (CN=)	Puni ili skraćeni naziv pravnog lica

Serial Number (serialNumber =)	Jedinstveni serijski broj koji određuje davalac usluge povjerenja i u formatu: CA:PCG-xx...x (x – broj od 0 do 9).

* Navedeni atributi sadrže punu identifikaciju subjekta. Jedinstveno ime može da sadrži i dodatne atribute na primjer dodatni "Organizational Unit (OU =)" za potrebe pojedinog subjekta.

U certifikatima su imena krajnjih 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 krajnjem 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 ili sredstva elektronske identifikacije i dogovoriti se da se traženo ime u certifikatu promijeni tako da se razlikuje od imena u certifikatu već izdatom drugom krajnjem 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 klijent aplikacije krajnjeg korisnika 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];
- Zvaničnih dokumenata koja mogu biti i u elektronskom obliku a koji pružaju dokaz o identitetu pravnog lica, a za koja se mora napraviti provjera tačnosti podataka putem online servisa ukoliko nisu dostavljeni u originalu ili ovjerenoj kopiji – 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.

- Na osnovu validnih podataka za izradu elektronskog potpisa ili sredstva elektronske identifikacije visokog nivoa povjerenja koji su izdati od strane kvalifikovanog davaoca elektronskih usluga povjerenja.
- Za izdavanje PSD2 certifikata pravno lice u okviru zahtjeva za izdavanje PSD2 certifikata mora da unese sve atribute neophodne za izdavanje PSD2 certifikata, a koji su dodijeljeni od strane NCA.

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 certifikata.

Predaju dokumentacije za izdavanje certifikata osim lica na čije ime glasi zahtjev i ovlašćenje za izdavanje/obnovu 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 certifikat za strano pravno lice izdaje za potrebe rada sa pravnim licem iz Crne Gore koje daje predmetnu izjavu / potvrdu;
- zvaničnih dokumenata koja mogu biti i u elektronskom obliku a 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 certifikat;
- zahtjev i ovlašćenje (shodno odjeljku 3.2.2. Provjera identiteta pravnog lica).

[PoštaCG-CA] RA čuva 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 ili vlasnici sredstva elektronske identifikacije koje izdaje [PoštaCG-CA] će biti identifikovani licem u lice ili na osnovu validnih podataka za izradu elektronskog potpisa ili sredstva elektronske identifikacije visokog nivoa povjerenja koji su izdati od strane kvalifikovanog davaoca elektronskih usluga povjerenja.
Pojedinci koji se identifikuju licem u lice moraju da se identifikuju koristeći jedan od slijedećih dokumenata koje je izdala država:

- Lična karta
- Pasoš

Prilikom identifikacije licem u lice krajnji korisnik mora da posjeduje važeći identifikacioni dokument sa fotografijom (važeća lična karta ili pasoš) i upoređivanjem fotografije sa krajnjim korisnikom, utvrđeno da fizičko lice odgovara prijavljenom identitetu,

3.2.4. Podaci o krajnjem korisniku koji se ne provjeravaju

[PoštaCG-CA] ne provjerava podatke koji se ne nalaze na identifikacionom dokumentu (npr. E-mail adresa). Krajnji korisnik je odgovoran za tačnost podataka unesenih na Zahtjevu i Ovlašćenju, a koji se ne nalaze na identifikacionom dokumentu.

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. Naziv pravnog lica koje će biti uključeno u certifikat mora biti identično Registrovanom punom ili skraćenom nazivu 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. Verifikacija identiteta krajnjeg korisnika se izvede na osnovu validnih podataka za izradu elektronskog potpisa ili sredstva elektronske identifikacije visokog nivoa povjerenja koji su izdati od strane kvalifikovanog davaoca elektronskih usluga povjerenja.
Identifikacija krajnjeg 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 elektronski popunjenog zahtjeva od strane krajnjeg korisnika koji zahtijeva obnovu certifikata, sa tim da je identitet korisnika verifikovan upotrebom validnih podataka za izradu elektronskog potpisa ili sredstva elektronske identifikacije visokog nivoa povjerenja koji su izdati od strane kvalifikovanog davaoca elektronskih usluga povjerenja.
Elektronski popunjen zahtjev mora biti u propisanim formatima definisanim na Repozitoriju.

3.3.2. Provjera identiteta kod zahtjeva za obnovu certifikata poslije opoziva

Provjera identiteta krajnjeg 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

Krajnji korisnik koji želi da opozove certifikat, šalje elektronski potpisan zahtjev za opoziv registracionom tijelu sa validnim podacima za izradu elektronskog potpisa krajnjeg korisnika koji zahtijeva opoziv certifikata ili se lično identifikuje kao u odjeljku 3.2.3. Provjera identiteta fizičkog lica.

U slučaju da pravno lice traži opoziv certifikata, provjera identiteta se vrši na način opisan u odjeljku 3.2.2. Provjera identiteta pravnog lica.

4. UPRAVLJANJE CERTIFIKATIMA

4.1. Zahtjev za izdavanje certifikata

Certifikat za napredni ili kvalifikovani elektronski potpis izdaje se isključivo punoljetnom fizičkom licu.

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 krajnjim 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 krajnji korisnik preuzima sam

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

- Krajnji korisnik podnese potpisan zahtjev za izdavanje certifikata sa pratećom dokumentacijom kao što je opisano u 3.2. Inicijalna provjera identiteta;
- Krajnji korisnik prihvata [PoštaCG-CA] CPS uslove potpisivanjem ugovora (End-User Agreement);
-
- Identitet krajnjeg korisnika se provjeri kao što je opisano u 3.2. Inicijalna provjera identiteta

- 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 krajnjeg 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 krajnjem korisniku u tehničkom postupku preuzimanja certifikata;
- Kodove za aktiviranje certifikata koje krajnji korisnik preuzima sam je potrebno poslati krajnjem korisniku koji je tražio izdavanje certifikata:
  - referentni broj šalje CRA elektronskim putem na e-mail adresu koju je krajnji korisnik naveo na obrascu zahtjeva za izdavanje certifikata;
  - autorizacijski kod se može dostaviti na različite načine:
    - on je odštampan i zatvoren u kovertu. CRA isporučuje kovertu preporučeno putem pošte ili je krajnji korisnik preuzima lično u LRA kancelariji.
    - CRA šalje kod drugim komunikacionim kanalom uključujući i slanje na email adresu

Krajnji 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 ili fajlu

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

- Krajnji korisnik podnese potpisan zahtjev za izdavanje certifikata sa pratećom dokumentacijom kao što je opisano u 3.2. Inicijalna provjera identiteta;
- 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 krajnjeg 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 PKI Administratoru u tehničkom postupku preuzimanja certifikata;
- Kriptografski token/QSCD sredstvo i PIN za zaštitu kriptografskog tokena/QSCD sredstava na koji je preuzet certifikat, ili fajl i lozinku za zaštitu fajla na koji je preuzet certifikat, je potrebno poslati krajnjem korisniku koji je tražio izdavanje certifikata:
  - Kriptografski token/QSCD sredstvo ili fajl CRA isporučuje u koverti preporučeno putem pošte/Post Express-om ili je krajnji korisnik preuzima lično u LRA kancelariji;
  - PIN za zaštitu kriptografskog tokena/QSCD sredstva na koji je preuzet certifikat, ili lozinka za zaštitu fajla na koji je preuzet certifikat, je odštampan i zatvoren u kovertu. CRA isporučuje preporučeno putem pošte/Post Express-om ili je krajnji korisnik preuzima lično u LRA kancelariji.
- Identitet krajnjeg korisnika se provjeri kao što je opisano u 3.2. Inicijalna provjera identiteta
- Krajnji korisnik prihvata [PoštaCG-CA] CPS uslove potpisivanjem ugovora (End-User Agreement);

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 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;
- Verifikacija identiteta krajnjeg korisnika i po potrebi ovlašćenja je uspješna;
- Podnosilac zahtjeva je potpisom ugovora 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 krajnjim 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 ili nakon prijema zahtjeva u elektronskom obliku, tj. Obavezno se u dijelu inicijalne obrade mora obaviti provjera popunjenosti podataka na obrascu zahtjeva za izdavanje certifikata, i kompletnosti dostavljene dokumentacije

.

[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 kompletnog zahtjeva sa svom propisanom dokumentacijom.

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 krajnji 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 certifikat može preuzeti samo lice na čije ime isti glasi (samo lično).

Ne predvidja se mogućnost preuzimanje certifikata uz ovlašćenje drugog lica.

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

4.3.2. Obavještavanje krajnjeg korisnika o izdavanju certifikata od strane CA

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

4.4. Prihvatanje certifikata

4.4.1. Postupak potvrde prihvata certifikata od strane krajnjeg korisnika

Krajnji korisnik će primiti sve potrebne certifikate u toku on-line procesa preuzimanja certifikata (vidi odjeljak 4.3). Dodatna potvrda prihvatanja certifikata nije potrebna.
U slučaju neuspješnog preuzimanja certifikata, mora krajnji korisnik o problemu obavijestiti [PoštaCG] RA (vidi RA kontakt informacije u odjeljku 1.5.2 Kontakt).
U slučaju certifikata izdatog na kriptografskom tokenu/QSCD sredstvu ili fajlu, krajnji korisnik potpisom korisničkog ugovora (End User Agreement) potvrđuje preuzimanje istog.
Ukoliko se naknadno utvrdi da u certifikatu postoje pogrešni podaci, krajnji 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 za elektronski potpis (postavljen bit (0) *digitalSignature* za elektronski potpis i bit (1) *nonRepudiation* za ne-poricanje) neće biti objavljeni.

4.4.3. Obavještavanje ostalih učesnika o izdavanje certifikata

[PoštaCG-CA] će obavijestiti NCA, ako NCA objavi način na koji se obavještenje može dostaviti.
[PoštaCG-CA] neće obavijestiti nijednog drugog učesnika.

4.5. Upotreba para ključeva i certifikata

4.5.1. Upotreba privatnog ključa i certifikata sa strane krajnjeg 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.
Krajnji 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. Krajnji 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] ili OCSP servis;
- 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 krajnjem korisniku novi certifikat. Novi certifikat sadrži iste identifikacione podatke o krajnjem korisniku kao stari certifikat i novi javni ključ krajnjeg korisnika.

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 krajnjeg 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 krajnjeg 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 krajnjim korisnicima da zahtijevaju promjenu podataka sadržanih u certifikatu. Promjena certifikata traži obnovu certifikata i obrađuje se kao početni zahtjev za izdavanje certifikata.

4.8.1. Okolnosti pod kojima se može promjeniti certifikat

Krajnji korisnik može zahtijevati promjenu certifikata kada se promijeni bilo koji od identifikacionih podataka (npr. ime, prezime, ...).

4.8.2. Ko može da zahtijeva promjenu certifikata

Promjenu certifikata mogu tražiti krajnji 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 izdavanje certifikata.

4.8.4. Obavještavanje krajnjeg korisnika o izdavanju promijenjenog certifikata

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

4.8.5. Postupak potvrde prihvata promijenjenog certifikata

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

- opoziv certifikata zahtijeva krajnji korisnik ili njegov ovlašćeni zastupnik;
- ako certifikaciono tijelo utvrdi da je podatak u certifikatu pogrešan ili je certifikat izdat na osnovu pogrešnih podataka;
- ako certifikaciono tijelo primi obavještenje da je krajnji korisnik ili pravno, odnosno fizičko lice u čije ime potpisuje izgubilo poslovnu sposobnost, umrlo ili je prestalo da postoji, odnosno istekao rok važenja ovlašcenja za potpisivanje ili su se promijenile činjenice koje utiču na važenje certifikata;
- ako certifikaciono tijelo utvrdi da su podaci za izradu elektronskog potpisa ili informacioni sistem krajnjeg korisnika ugroženi na način koji utiče na pouzdanost i bezbjednost izrade elektronskog potpisa ili kad treće lice te podatke koristi na neprimjeren način;
- ako certifikaciono tijelo utvrdi da su podaci za provjeru elektronskog potpisa ili informacioni sistem davaoca elektronskih usluga povjerenja ugroženi na način koji utiče na bezbjednost i pouzdanost certifikata;
- ako certifikaciono tijelo prestaje sa radom ili mu je rad zabranjen, a izdatim certifikatima nije istekao rok važenja, osim ako elektronske usluge povjerenja ne prenese na drugog davaoca tih usluga;
- istekne rok važenja certifikata;
- ako certifikaciono tijelo primi sudsku odluku ili upravni akt koji se odnose na važenje certifikata

- postoje drugi pravni razlozi predviđeni internim aktima iz člana 37 stav 4 Zakona o elektronskoj identifikaciji i elektronskom potpisu, i drugim propisima koji regulišu ovu oblast
- ako certifikaciono tijelo utvrdi da krajnji korisnik krši odredbe [PoštaCG-CA] Pravilnika;

[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 krajnjeg korisnika ;
- na službeni zahtjev od strane suda, nadležnog organa državne uprave, odnosno pravnog lica kod kojeg je krajnji korisnik zaposlen u trenutku podnošenja zahtjeva za opoziv certifikata;
- U slučaju PSD2 certifikata na službeni zahtjev od strane NCA;
- na zahtjev davaoca elektronskih usluga povjerenja 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 kranjeg korisnika ili ovlašćenog predstavnika pravnog lica na potpisanom i ovjerenom obrascu poslatom poštom, lično u [PoštaCG-CA] LRA kancelariji ili u elektronskom obliku, elektronski 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.
Certifikaciono tijelo objavljuje listu opozvanih certifikata na svojoj internet stranici.
Opoziv certifikata obavezno sadrži datum i vrijeme donošenja, a proizvodi dejstvo od trenutka unošenja u evidenciju suspendovanih i opozvanih certifikata.
Certifikaciono tijelo će da obavijesti krajnjeg korisnika o opozivu certifikata, u roku od 24 časa od primljenog zahtjeva ili obavještenja, odnosno nastanka okolnosti zbog koje se certifikat opoziva.

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 listi suspendovanih i opozvanih certifikata (CRL) najkasnije u periodu od dva radna 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 elektronskog 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 72 sata.

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

Certifikaciono tijelo podržava online provjeru statusa opozvanosti izdatih certifikata putem OCSP servisa čiji je rad usaglašen s dokumentom IETF RFC 6960.

Informacija o statusu opozvanosti certifikata korišćenjem OCSP servisa dostupna je u realnom vremenu.

Adresa OCSP servisa zavisi od pripadajućeg CA tijela za koje OCSP servis daje odgovore o statusu, a upisuje se u ekstenziji Authority Information Access svakog certifikata kojeg izdaje PoštaCG CA tijelo.

4.9.10.Zahtjev za on-line provjeru statusa certifikata

Za korišćenje OCSP servisa treće lica treba da imaju aplikaciju koja može da koristi OCSP servis upotrebom GET ili POST HTTP metode.

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 krajnjeg korisnika.

4.9.13.Okolnosti pod kojima se može izvršiti suspenzija certifikata

Ako se činjenice definisane u 4.9.1 Okolnosti pod kojima se vrši opoziv certifikata ne mogu odmah utvrditi na nesumnjiv način, certifikaciono tijelo će bez odlaganja da suspenduje certifikat do utvrdivanja tih činjenica.

4.9.14.Ko može da traži suspenziju certifikata

Certifikaciono tijelo.

4.9.15.Postupak suspenzije

Autorizovano lice [PoštaCG-CA] CRA vrši suspenziju koristeći odgovarajuće aplikacije, i definisane interne procedure.
Suspenzija certifikata obavezno sadrži datum i vrijeme donošenja, a proizvodi dejstvo od trenutka unošenja u evidenciju suspendovanih i opozvanih certifikata.
Certifikaciono tijelo će da obavijesti krajnjeg korisnika o suspenziji certifikata, u roku od 24 časa od primljenog zahtjeva ili obavještenja, odnosno nastanka okolnosti zbog koje se certifikat suspenduje.

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*) i OCSP servis. 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. Adresa OCSP servisa zavisi od certifikacionog tijela za koje OCSP odgovara o statusu certifikata, a upisuje se u ekstenziji Authority Information Access svih certifikata koje izdaje pripadajuće certifikaciono tijelo.

Preporuka trećim licima je da za provjeru statusa certifikata koriste OCSP servis i da se provjera statusa pristupom CRL koristi kao alternativna metoda provjere u slučaju nedostupnosti OCSP servisa ili u slučaju da aplikacija trećih lica podržava provjeru statusa certifikata samo putem CRL.

4.10.2.Raspoloživost servisa

[PoštaCG-CA] garantuje dostupnost servisa za objavljivanje CRL i OCSP 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 krajnjeg 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 krajnji korisnik nije više u radnom odnosu).
[PoštaCG-CA] čuva dokumentaciju u vezi krajnjih korisnika, certifikata i statusa certifikata u skladu sa zakonima Crne Gore.
U slučaju da krajnji korisnik prekine ugovor prije isteka važenja certifikata, [PoštaCG-CA] će opozvati 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 certifikata koji se koriste za elektronski 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 krajnji korisnik, ili pravno lice koje je zahtijevalo početno izdavanje certifikata. Identitet krajnjeg 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 elektronskih usluga povjerenja;
- 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 krajnjeg korisnika i nadležni organ uprave, najmanje tri mjeseca prije dana predviđenog za raskid ugovora.

[PoštaCG-CA] dužan je, za krajnje korisnika kojima je izdao certifikate, da obezbijedi nastavak obavljanja elektronskih usluga povjerenja kod drugog davaoca usluga i da mu dostavi svu dokumentaciju u vezi sa obavljenim elektronskim uslugama povjerenja.

Ako [PoštaCG-CA] ne obezbijedi nastavak obavljanja elektronskih usluga povjerenja 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*).
Par kriptografskih ključeva za potpisivanje i verifikovanje potpisa se generiše na strani krajnjeg korisnika u korisničkoj aplikaciji, odnosno na kriptografskom tokenu/QSCD sredstvu. Kriptografski ključ za kvalifikovani elektronski potpis se nikada ne smješta na hardverskoj ili softverskoj opremi [PoštaCG] certifikacionog tijela.
Kod certifikata koji se upravljaju koristeći PKIX-CMP protokol, par kriptografskih ključeva za šifrovanje i dešifrovanje krajnjeg korisnika generiše [PoštaCG] certifikaciono tijelo i drži njegovu kopiju u šifrovanom obliku u svojoj bazi.

6.1.2. Dostavljanje krajnjem 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 krajnjeg korisnika po PKIX-CMP protokolu. Referentni broj i autorizacioni kod koje krajnji korisnik dobija radi preuzimanja kriptografskih ključeva obezbjeđuje sigurnost prenosa kriptografskih ključeva.
Uručenje privatnog ključa krajnjem korisniku za certifikate izdate na kriptografskom tokenu/QSCD sredstvu ili u fajlu vrši se njegovim uručivanjem u prostorijama lokalnog registracionog tijela ili lično na adresu navedenu u zahtjevu.
Privatni kriptografski ključ za potpisivanje koji generiše korisnička aplikacija nije potrebno dostavljati krajnjem korisniku.

6.1.3. Dostavljanje javnog ključa krajnjeg korisnika davaocu elektronskih usluga povjerenja

Javni kriptografski ključ za verifikovanje potpisa krajnjeg korisnika 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 elektronskih usluga povjerenja 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 certifikate krajnjih korisnika koji se upravljaju sa PKIX-CMP protokolom javni ključ 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 namjene upotrebe:

Tip certifikata	X.509 keyUsage (bit)
kvalifikovani certifikati za elektronske potpise	digitalSignature (0), nonRepudiation (1)
kvalifikovani certifikati za elektronske pečate	digitalSignature (0), nonRepudiation (1)
kvalifikovani certifikati za povjerljivost	keyEncipherment (2)
kvalifikovani certifikat za autentifikaciju internet stranica	digitalSignature (0), keyEncipherment (2)
certifikat za Microsoft Domain Controller server	digitalSignature (0), keyEncipherment (2)
certifikat za SmartLogon	digitalSignature (0), keyEncipherment (2)
Kvalifikovani certifikat za uslugu elektronskog vremenskog pečata	digitalSignature (0), nonRepudiation (1)
certifikat za autentifikaciju krajnjeg korisnika	digitalSignature (0), keyEncipherment (2)
kvalifikovani certifikat za OCSP	digitalSignature (0), nonRepudiation (1)

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

Tip certifikata	X.509 ExtendedKeyUsage
certifikat za autentifikaciju internet stranica	Server Authentication Client Authentication
Kvalifikovani certifikat za uslugu elektronskog vremenskog pečata	timeStamping
certifikat za Microsoft Domain Controller server	Server Authentication Client Authentication
certifikat za SmartLogon	Client Authentication Smart Card Logon
certifikat za autentifikaciju krajnjeg korisnika	Client Authentication

kvalifikovani certifikat za OCSP	OCSP Signing

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+.
QSCD sredstvo zadovoljava standarde CC EAL 5+/PP QSCD.
Privatni ključ krajnjeg korisnika je zaštićen fizičkim i logičkim kontrolama računara krajnjeg korisnika. Krajnji korisnik je obavezan osigurati zaštitu privatnog ključa tako da se minimalizuje mogućnost otkrivanja privatnog ključa. Preporuka [PoštaCG-CA] je da krajnji korisnici koriste kriptografske tokene koji zadovoljavaju sigurnosne standarde najmanje FIPS 140-2 Level 2 ili QSCD sredstvo koje zadovoljavaju sigurnosne standarde najmanje CC EAL 5+, 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 krajnjih 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 krajnjih korisnika za dešifrovanje, koji se generišu u kriptografskom modulu aplikacije certifikacionog tijela, se prenesu u kriptografski modul krajnjeg korisnika koristeći PKIX-CMP protokol.
Za privatne ključeve krajnjeg korisnika za kvalifikovani elektronski potpis/pečat nema posebnih zahtjeva pošto se generišu u QSCD sredstvu.

Za privatne ključeve krajnjih korisnika za napredni elektronski potpis/pečat nema posebnih zahtjeva.
Za privatne ključeve krajnjih korisnika za potpis/pečat koji se generišu u kriptografskom modulu na strani krajnjih korisnika nema posebnih zahtjeva.

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.
Privatni kriptografski ključevi krajnjeg korisnika se aktiviraju poslije uspješne autentifikacije krajnjeg 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 krajnji 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 krajnjeg korisnika se uništava ukoliko ga korisnik obriše sa kriptografskog tokena/QSCD sredstva ili se kriptografski token/QSCD sredstvi fizički ošteti ili krajnji korisnik obriše fajl u kome se nalaze i privatni ključevi.

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 ključeve krajnjeg korisnika, 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.
- Ključevi krajnjih korisnika:
  - Javni ključ za autentifikaciju: 1 do 5 godina
  - Javni ključ za verifikovanje potpisa: 1 do 5 godina.
  - Privatni ključ za potpisivanje: 1 do 5 godina.
  - Javni ključ za šifrovanje: 1 do 5 godina.
  - 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 certifikata. Brojevi i kodovi su jedinstveni i generišu se u aplikaciji certifikacionog tijela primjenom odgovarajućeg algoritma.
Krajnji korisnici upotrebljavaju lozinke za aktivaciju privatnih kriptografskih ključeva. Za certifikate koji se generišu na kriptografskom tokenu/QSCD sredstvu ili fajlu 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. Krajnji korisnik može promijeniti lozinku na kriptografskom tokenu/QSCD sredstvu.
Za certifikate koje generišu krajnji korisnici lično, svaki krajnji korisnik smišlja svoju lozinku. U slučaju da krajnji 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 krajnjem korisniku različitim komunikacionim kanalima. Referentni broj se šalje elektronskom poštom, dok se autorizacioni kod može dostaviti na više načina: putem preporučene pošiljke sa povratnicom sa tim da se u preporučenoj pošiljci nalazi i prazan kriptografski token, ili putem preporučene pošiljke sa povratnicom ili drugim komunikacionim kanalima,. U slučaju dostave putem preporučene pošiljke koriste sePost Express dostave sa obaveznim ličnim prijemom ili ga preuzima krajnji korisnik lično u prostorijama lokalnog registracionog tijela. Preporučena pošiljka može da sadrži i povratnu dokumentaciju (Ugovor o izdavanju i korišćenu digitalnog certifikata, ...)

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 krajnjeg korisnika i arhiviranje revizijskih podataka;
- Revizijske beleške 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)

Definisano Pravilnikom o postupcima izrade kvalifikovanih elektronskih vremenskih pečata [PoštaCG-QTSA]

(QTSA Practice Statement)

7. CERTIFIKAT, CRL I OCSP PROFILI

7.1. Profil certifikata

7.1.1. 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. Algoritam potpisa je RSA-SHA256.
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

7.1.2. 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 hash polja *Subject Public Key Info* kvalifikovanog elektronskog certifikata korisnika.
Key Usage	Namjena (keyUsage) javnog kriptografskog ključa korisnika kvalifikovanog elektronskog certifikata kao što je navedeno u 6.1.7 Polje je u svim certifikatima označeno kao kritično.
Extended Key Usage	Proširena namjena (ExtendedKeyUsage) javnog kriptografskog ključa korisnika kvalifikovanog elektronskog certifikata kao što je navedeno u 6.1.7. Polje je u certifikatima za uslugu elektronskog vremenskog pečata označeno kao kritično.
Certificate Policies	Identifikacija politike i adrese Web strane na kojoj se nalaze ova praktična pravila.
Issuer Alternative Name	Alternativno ime certifikacionog tijela koji sadrži naziv, poreski identifikacioni broj* i oznaku države u kojoj je davalac usluga registrovan. * poreski identifikacioni broj je isti kao matični broj

Subject Alternative Name	Alternativno ime krajnjeg korisnika certifikata. U ovom polju može da se navede adresa elektronske pošte krajnjeg korisnika certifikata ako je adresa elektronske pošte navedena u zahtjevu ili ugovoru, web server hostname (FQDN) i/ili TCP/IP adresa, drugi jedinstveni identifikator krajnjeg korisnika certifikata (Permanent Identifier), ili neki drugi podatak koji je važan krajnjem korisniku certifikata. Vrijednost atributa Permanent Identifier (OID: 1.3.6.1.5.5.7.8.3) je u slijedećem obliku: - Osmocifreni jedinstveni identifikator krajnjeg korisnika definisan članom 4. Uredbe o načinu određivanja identifikacionog broja potpisnika kvalifikovanog certifikata za elektronski potpis Ministarstva unutrašnih poslova Crne Gore sa prefiksom „PNOME–“ Ili - Broj lične karte krajnjeg korisnika izdat od nadležnog organa sa prefiksom „IDCME–“ Ili - Broj pasoša krajnjeg korisnika izdat od nadležnog organa sa prefiksom „PAS + dvoslovna oznaka države–“. Dvoslovna oznaka države mora biti u skladu sa međunarodnim standardom ISO 3166-1.
CRL Distribution Points	Lokacija na kojoj se nalaze registri opozvanih certifikata.
Qualified Certificate Statements	Oznaka da je certifikat izdat kao kvalifikovani elektronski certifikat (*OID*: 1.3.6.1.5.5.7.1.3), koja sadrži oznake u skladu sa tehničkim standardom ETSI EN 319 412-5 ili ETSI TS 119 495 [12]. Sadržaj oznaka pojedinog tipa certifikata naveden je u 7.1.2.1.
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")
Authority Information Access (authorityInfoAccess)	Informacije o Lokaciji na kojoj je dostupan certifikat na kojem se zasniva napredni elektronski potpis certifikacionog tijela (polje id-ad-calssuers) i adresa OCSP servisa (polj id-ad-ocsp).

7.1.2.1. Polje Qualified Certificate Statements (qCStatements)

Polje *qCStatements* (1.3.6.1.5.5.7.1.3) sadrži oznake u skladu sa tehničkim standardom ETSI EN 319 412-5 ili ETSI TS 119 495 [12] za PSD2 certificate

Kvalifikovani certifikati za elektronske potpise

Polje *qCStatements* u Kvalifikovanom certifikatu za kvalifikovani elektronski potpis izdat na pametnoj kartici sadrži oznake:

- id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)
- id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)
- QCstatement QcType (0.4.0.1862.1.6)

  - id-etsi-qct-esign (0.4.0.1862.1.6.1)
- id-etsi-qcs-QcPDS (0.4.0.1862.1.5)

Polje *qCStatements* u Kvalifikovanom certifikatu za napredni elektronski potpis sadrži oznake:

- id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)
- QCstatement QcType (0.4.0.1862.1.6)
  - id-etsi-qct-esign (0.4.0.1862.1.6.1)
- id-etsi-qcs-QcPDS (0.4.0.1862.1.5)

Kvalifikovani certifikati za elektronske pečate

Polje *qCStatements* u Kvalifikovanom certifikatu za kvalifikovani elektronski pečat izdat na pametnoj kartici sadrži oznake:

- id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)
- id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)
- QCstatement QcType (0.4.0.1862.1.6)
  - id-etsi-qct-eseal (0.4.0.1862.1.6.2)
- id-etsi-qcs-QcPDS (0.4.0.1862.1.5)

Polje *qCStatements* u Kvalifikovanom certifikatu za napredni elektronski pečat sadrži oznake:

- id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)
- QCstatement QcType (0.4.0.1862.1.6)
  - id-etsi-qct-eseal (0.4.0.1862.1.6.2)
- id-etsi-qcs-QcPDS (0.4.0.1862.1.5)

Kvalifikovani certifikati za elektronske pečate za PSD2

Polje *qCStatements* u Kvalifikovanom certifikatu za napredni elektronski pečat za PSD2 sadrži oznake:

- id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)
- QCstatement QcType (0.4.0.1862.1.6)
  - id-etsi-qct-eseal (0.4.0.1862.1.6.2)
- id-etsi-qcs-QcPDS (0.4.0.1862.1.5)
- id-etsi-psd2-qcStatement (0.4.0.19495.2)
  - rolesOfPSP (jedna ili više vrijednosti iz PSP_AS, PSP_PI, PSP_AI, PSP_IC)
  - nCAName
  - nCAId

Kvalifikovani certifikati za autentifikaciju internet stranica

Polje *qCStatements* u Kvalifikovanom certifikatu za autentifikaciju internet stranica sadrži oznake:

- id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)

- QCstatement QcType (0.4.0.1862.1.6)
  - id-etsi-qct-web (0.4.0.1862.1.6.3)
- id-etsi-qcs-QcPDS (0.4.0.1862.1.5)

Kvalifikovani certifikati za autentifikaciju internet stranica za PSD2

Polje *qCStatements* u Kvalifikovanom certifikatu za autentifikaciju internet stranica za PSD2 sadrži oznake:

- id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)
- QCstatement QcType (0.4.0.1862.1.6)
  - id-etsi-qct-web (0.4.0.1862.1.6.3)
- id-etsi-qcs-QcPDS (0.4.0.1862.1.5)
- id-etsi-psd2-qcStatement (0.4.0.19495.2)
  - rolesOfPSP (jedna ili više vrijednosti iz PSP_AS, PSP_PI, PSP_AI, PSP_IC)
  - nCAName

nCAId**Kvalifikovani certifikati za uslugu elektronskog vremenskog pečata**

Polje qCStatements u kvalifikovanom certifikatu za napredni elektronski pečat koji se koristi za uslugu kvalifikovanog elektronskog vremenskog pečata sadrži oznake:

- id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)
- QCstatement QcType (0.4.0.1862.1.6)
  - id-etsi-qct-eseal (0.4.0.1862.1.6.2)
- id-etsi-qcs-QcPDS (0.4.0.1862.1.5)

Kvalifikovani certifikati za OCSP servis

Polje *qCStatements* u Kvalifikovanom certifikatu za OCSP servis sadrži oznake:

- id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)
- QCstatement QcType (0.4.0.1862.1.6)
  - id-etsi-qct-eseal (0.4.0.1862.1.6.2)
- id-etsi-qcs-QcPDS (0.4.0.1862.1.5)

7.1.3. Identifikatori Algoritamskih objekata

Algoritam	Identifikacijska oznaka
RSA Encryption	1.2.840.113549. 1.1.1
RSA with SHA-1signature	1.2.840.113549.1.1.5
SHA256 with RSA Encryption	1.2.840.113549.1.1.11

7.1.4. Forme imena

Certifikati izdati od strane [PoštaCG-CA] sadrže kompletno X.500 jedinstveno ime izdavača certifikata i krajnjih 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.

7.1.4.1. PostaCG CA atributi

PostaCG CA atributi	Identifikacijska oznaka
Ime oca ili majke	Ime oca ili majke krajnjeg korisnika OID: 1.3.6.1.4.1.36737.2.1 Oblik: UTF8String
Datum rođenja	Datum rođenja krajnjeg korisnika OID: 1.3.6.1.4.1.36737.2.2 Oblik: IA5String, DD.MM.YYYY (DD.MM.GGGG)
Adresa	Adresa prebivališta odnosno boravišta krajnjeg korisnika OID: 1.3.6.1.4.1.36737.2.3 Oblik: UTF8String
Grad	Grad prebivališta odnosno boravišta krajnjeg korisnika OID: 1.3.6.1.4.1.36737.2.4 Oblik: UTF8String
CA SB krajnjeg korisnika	Jedinstveni serijski broj koji generiše PostaCG-CA sistem za krajnjeg korisnika OID: 1.3.6.1.4.1.36737.2.5 Oblik: UTF8String, Format CA:PCG-xx...x (x – broj od 0 do 9).

7.1.5. 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.

7.1.6. Identifikator objekta za politiku davanja usluga povjerenja

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

7.1.7. Korišćenje Politike ograničenja ekstenzija

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

7.1.8. Sintaksa i semantika za kvalifikatore politike

Ne koriste se

7.1.9. Procesuiranje semantike za kritične ekstenzije Politike usluge povjerenja

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

7.2. CRL profil

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

7.2.2. 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 Info certifikata certifikacionog tijela.
CRL Number	Redni broj liste opozvanih certifikata.
Issuing Distribution Point	Lokacija na kojoj se nalazi parcijalna lista 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.

7.3. OCSP profil

Profil odgovora OCSP servisa usaglašen je s dokumentom IETF RFC 6960.

7.3.1. Broj (brojevi) verzija

Profil odgovora OCSP servisa u skladu je sa verzijom 1 prema dokumentu IETF RFC 6960.

7.3.2. OCSP ekstenzije

Ekstenzije odgovora OCSP servisa prikazane su u tabeli 7.2.

Ekstenzije	***Vrijednost***
Nonce	Vrijednost Nonce iz zahtjeva za status certifikata.
Extended Revoked Definition	Kod razloga opoziva certifikata (*Reason code*)
Archive Cutoff	CSS-6.3.10-10 [CONDITIONAL]: If OCSP is provided, the OCSP responder should use the ArchiveCutOff extension as specified in IETF RFC 6960 [i.9], with the archiveCutOff date set to the CA's certificate "notBefore" time and date value. CSS-6.3.10-03 [CONDITIONAL]: If CRLs are provided, the TSP should not remove from the CRL revoked certificates after they have expired.

Tabela 7.2. Ekstenzije odgovora OCSP servisa

*

8. REVIZIJA USAGLAŠENOSTI I DRUGE PROCJENE

8.1. Učestalost ili okolnosti kada se vrše revizije

Nadležni organ vrši reviziju rada [PostaCG] CA u skladu sa Zakonom o elektronskoj identifikaciji i 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.

8.2. 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.

8.3. Revizorov odnos prema procjenjivanom subjektu

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

8.4. Oblasti koje pokriva procjenjivanje

Revizor će ocijeniti usklađenost između:

- ❖ Ovog Pravilnika i Zakona o elektronskoj identifikaciji i elektronskom potpisu
- ❖ Ovog Pravilnika i implementiranih CA servisa i procedura

8.5. 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.

8.6. Objavljivanje rezultata

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

9. OSTALI POSLOVNI I PRAVNI ASPEKTI

9.1. Cijene

9.1.1. Cijene usluga certifikacionog tijela

[PoštaCG-CA] naplaćuje davanje elektronskih usluga povjerenja i elektronske identifikacije. Cijene ovih usluga biće objavljene na javnoj web stranici definisanoj u odjeljku 2 OBJAVE I ODGOVORNOSTI REPOZITORIJUMA.

9.1.2. Nadoknade za pristup certifikatu

Ne naplaćuje se.

9.1.3. Nadoknade za opoziv ili pristup statusu informacija

Ne naplaćuje se.

9.1.4. Nadoknade za ostale servise

Pogledati odjeljak 9.1.1. Cijene usluga certifikacionog tijela.

9.1.5. Politika refundiranja

Troškovi se ne refundiraju.

9.2. Finansijska odgovornost

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

9.2.1. Osiguranja ili garancije davaoca elektronske usluge povjerenja

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

9.2.2. Ostala sredstva

Nije primjenljivo.

9.2.3. Osiguranja ili garancije korisnika

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

9.3. Povjerljivost poslovnih informacija

9.3.1. Obim povjerljivih informacija

Sve informacije koje se prikupljaju, generišu, prenose i održavaju od strane [PoštaCG-CA], smatraće se povjerljivim, osim informacija opisanih u odjeljku 9.3.2. Informacije koje ne ulaze u obim povjerljivih informacija, ne smatraju se povjerljivim.

9.3.2. 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.

9.3.3. 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.

9.4. Privatnost ličnih informacija

9.4.1. 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.

9.4.2. Informacija koja se tretira privatnom

Definisano u odjeljku 9.4.1. Plan privatnosti.

9.4.3. Informacija koja se ne smatra privatnom

Definisano u odjeljku 9.3.2. Informacije koje ne ulaze u obim povjerljivih informacija.

9.4.4. Odgovornost za zaštitu privatnih informacija

Kao što je definisano u odjeljku 9.3.3. Odgovornost za zaštitu povjerljivih informacija.

9.4.5. 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*).

9.4.6. 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.

9.4.7. Ostale okolnosti kada se mogu otkrivati informacije

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

9.5. Prava na intelektualnu svojinu

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

9.6. Garancije

9.6.1. Garancije certifikacionog tijela (CA)

[PoštaCG-CA] garantuje da pruža elektronske usluge povjerenja i elektronske identifikacije, 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) i osigurati rad OCSP servisa;
- Da će osigurati da njeni RA-ovi budu svjesni odredbi koje se na njih odnose u ovom Pravilniku.

9.6.2. 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.

9.6.3. 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].

9.6.4. 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].

9.6.5. 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.

9.7. 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 ili OCSP servisu, 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.

9.8. Ograničenja odgovornosti

9.8.1. Odgovornost i ograničenje od odgovornosti [PoštaCG-CA]

[PoštaCG-CA] je dužna da na propisan način izdaje 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.

9.8.2. Odgovornost i ograničenje od odgovornosti krajnjih korisnika

Krajnji korisnik je odgovoran za štetu koja je nastala njegovom krivicom.
Krajnji korisnik nije odgovoran za štetu ako dokaže da je postupao u skladu sa ovim Pravilnikom i propisima iz ove oblasti kao i ugovorom zaključenim sa [PoštaCG-CA].

9.9. 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.

9.10. Rok i prekid

9.10.1. Rok

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

9.10.2. Prekid

Važnost [PoštaCG-CA] Pravilnika nije vremenski ograničena.

9.10.3. 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 9.12.2. Mehanizmi obavještavanja

i vremenski periodi, kao i treća lica preko javne web stranice a na način definisan u odjeljku 2.1 Repozitorijumi.

9.11. 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.

9.12. Izmjene

9.12.1. 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.

9.12.2. 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.

9.12.3. 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.

9.13. 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.

9.14. 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.

9.15. 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.

9.16. Razne odredbe

9.16.1. Cjelokupni ugovor

Ovaj Pravilnik [PoštaCG-CA] i ugovor sa naručiocem obuhvataju sve elemente koji definišu odnos između [PoštaCG-CA] i naručioca certifikata.

9.16.2. 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.

9.16.3. 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).

9.16.4. Izvršenje (nadoknade za pravnog zastupnika i odricanje od prava)

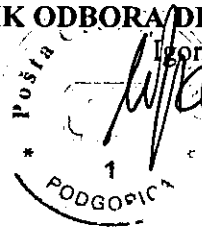
Nema odredbi.

9.16.5. 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.

9.17. Ostale odredbe

Danom stupanja na snagu ovog Pravilnika prestaje da važi Pravilnik o postupcima izdavanja certifikata i zaštiti sistema (Certification Practice Statement - CPS) broj 00010-20240223-1/4-2 od 28.02.2024. godine.

Ovaj Pravilnik stupa na snagu danom usvajanja od strane Odbora direktora .

PREDSJEDNIK ODBORA DIREKTORA
Igor Bulatović