Praktična pravila Centralne banke Crne Gore za davanje elektronske usluge povjerenja izrade certifikata za napredni elektronski pečat za učesnike u Platnom sistemu Centralne banke

Podgorica, decembar 2021. godine

Zaštita dokumenta

Sadržaj

1. UVOD

Centralna banka Crne Gore uspostavila je i upravlja infrastrukturom javnih ključeva osnivanjem Certifikacionog tijela Centralne banke Crne Gore za pružanje elektronske usluge povjerenja (u daljem tekstu: CBCG-CA), koje djeluje kao davalac nekvalifikovane elektronske usluge povjerenja za izradu certifikata za upotrebu u okviru zatvorenog okruženja Platnog sistema Centralne banke Crne Gore (u daljem tekstu: PSCB).

Centralna banka Crne Gore (u daljem tekstu: CBCG) kao davalac elektronske usluge povjerenja objavljuje Politiku Centralne banke Crne Gore za davanje elektronske usluge povjerenja izrade certifikata za napredni elektronski pečat za učesnike u platnom sistemu Centralne banke (u daljem tekstu: CBCG – CA Politika ili Politika) i Praktična pravila Centralne banke Crne Gore za davanje elektronske usluge povjerenja izrade certifikata za napredni elektronski pečat za učesnike u platnom sistemu Centralne banke (u daljem tekstu: CBCG-CA Praktična pravila ili Praktična Pravila).

Politika sadrži skup pravila koja ukazuju na primjenljivost certifikata koje opisuje ta politika i koje zakonske, bezbjednosne i tehničke zahtjeve moraju ispunjavati certifikaciona tijela koja izdaju certifikate u skladu sa Politikom.

Ova praktična pravila opisuju kako davalac elektronske usluge povjerenja upravlja svojom uslugom, način na koji ispunjava zakonske, tehničke, organizacione i proceduralne zahtjeve poslovanja.

1.1. Pregled

Politika sadrži opis vrste certifikata koje izdaju CBCG-CA certifikaciona tijela, sadržaj odnosno profile certifikata, primjenljivost certifikata i koje zakonske, bezbjednosne i tehničke zahtjeve moraju ispunjavati CBCG-CA certifikaciona tijela.

Praktična pravila, sadrže uslove upotrebe i opis pravila i postupaka koje realizuje CBCG za pružanje elektronske usluge povjerenja, a koji obuhvata registraciju naručioca, izdavanje, obnovu i opoziv digitalnih certifikata, objavu statusa digitalnih certifikata. Pored navedenog, sadrže i opis tehničkih karakteristika i operativnih postupaka upravljanja IT infrastrukturom koju CBCG koristi za izvođenje i upravljanje elektronskim uslugama povjerenja.

Ova Praktična pravila su dio javnih pravila djelovanja davaoca elektronske usluge povjerenja CBCG-CA koji se objavljuje na internet stranici CBCG.

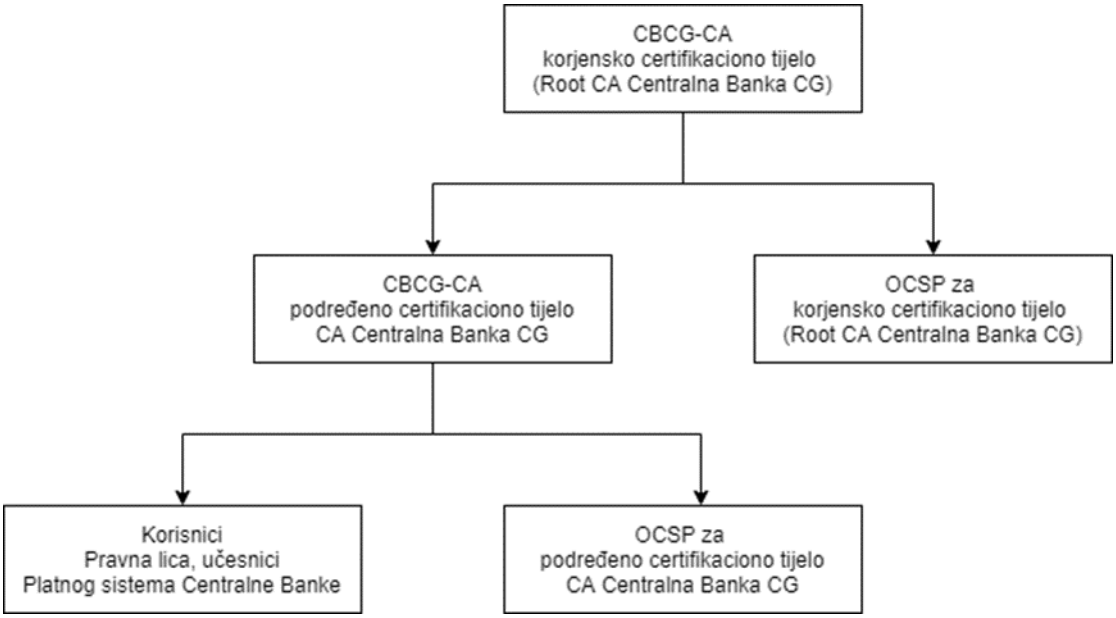
Interni akt kojim se uređuje upravljanje uslugama i informacionom bezbjednošću CBCG je tajni dokument i predstavlja poslovnu tajnu.

Struktura Praktičnih pravila usaglašena je sa standardom RFC 3647 [1]. Određena poglavlja RFC 3647, koja nisu primjenljiva za CBCG-CA, navedena su i sadrže tekst „Nije primjenljivo”.

Sadržina dokumenta CBCG-CA Praktična pravila usaglašena je sa standardima RFC 3647 [1], RFC 5280 [3], EN 319 401 [4] i EN 319 411-1 [2].

Za potrebe izvršenja usluga povjerenja, CBCG ima uspostavljenu sopstvenu infrastrukturu javnih ključeva, CBCG-CA, koja obuhvata i korjensko certifikaciono tijelo i podređeno certifikaciono tijelo.

Na slici 1: Hijerarhija PKI infrastrukture CBCG-CA, prikazana je hijerarhija izdavanja certifikata u okviru certifikacionih tijela davaoca elektronske usluge povjerenja CBCG-CA.



Slika 1: Hijerarhija PKI infrastrukture CBCG-CA

Certifikaciona tijela CBCG-CA imaju jedinstvena imena (engl. Distinguished Name - DN), kao što je navedeno u tabeli u nastavku.

Korjensko certifikaciono tijelo
`CN=Root CA Centralna Banka CG,OI=VATME-02011328,O=Centralna Banka Crne Gore,C=ME`
Podređeno certifikaciono tijelo
`CN=CA Centralna Banka CG,OI= VATME-02011328,O=Centralna Banka Crne Gore,C=ME`

Napomena: Oznaka *OI* u razlikovnim imenima je skraćenica za Organization Identifier (`organizationIdentifier`).

CBCG-CA izdaje digitalne certifikate naručiocima (vidjeti i poglavlje 1.3.3.), koji su učesnici u Platnom sistemu Centralne banke u skladu sa Pravilima rada Platnog sistema Centralne banke Crne Gore.

Praktična pravila definišu sljedeće kategorije digitalnih certifikata koje izdaje CBCG-CA:

- Nekvalifikovani certifikati za:
  - elektronski pečat za upotrebu u okviru PSCB,
  - za servere OCSP,
  - za upravljanje internom infrastrukturom davaoca elektronske usluge povjerenja CBCG-CA.

U sljedećoj tabeli je dat pregled kategorija digitalnih certifikata, naručioca i svrha upotrebe.

Certifikat	Vlasnici	Svrha upotrebe
CBCG PSCB	Učesnici u PSCB	Napredni elektronski pečat, autentifikacija i kriptovanje podataka
CBCG OCSP	Serveri usluge OCSP	OCSP
CBCG PKI	Infrastrukturni certifikat za upravljanje sistemima u okviru CBCG-CA	Digitalni potpis i autentifikacija

Svaka kategorija digitalnih certifikata koja je definisana u ovom dokumentu ima dodijeljen jedinstveni identifikator (OID, Object Identifier) politike u skladu sa kojom je izdata pojedinačna kategorija digitalnih certifikata (vidjeti poglavlje 1.2).

1.2. Naziv dokumenta i identifikacione oznake certifikata

Naziv dokumenta, cr.:	Praktična pravila Centralne banke Crne Gore za davanje elektronske usluge povjerenja izrade certifikata za napredni elektronski pečat za učesnike u Platnom sistemu Centralne banke
Naziv dokumenta, en.:	Certification Practice Statement of the CBCG-CA
Verzija:	v. 1.0
Datum:	17.12.2021.

Svaka kategorija digitalnih certifikata sadrži jedinstveni identifikator (OID), koji je u skladu sa RFC 5280 [3] u svakom izdatom digitalnom certifikatu upisan u polje `id-ce-certificatePolicies`, parametar `policyIdentifier` (vidjeti RFC 5280 [3], poglavlje 4.2.1.4.).

Svi identifikatori (OID) u digitalnim certifikatima imaju prefiks 1.3.6.1.4.1. 34288. Identifikator je registrovan pri međunarodnoj organizaciji IANA (http://www.iana.org/), koja upravlja identifikatorom za prefiks *iso.org.dod.internet.private.enterprise* (1.3.6.1.4.1). OID broj 34288 je kod IANA registrovan na CBCG.

Sljedeći identifikatori (OIDs) dodijeljeni su kategorijama nekvalifikovanih certifikata za napredni elektronski pečat koji se koristi u zatvorenom PSCB:

Nekvalifikovani certifikati	Identifikator (CertPolicyId)
CBCG PSCB produkcija	1.3.6.1.4.1. 34288.(nekvalifikovani certifikati)2.(PSCB)1.(produkcija)1.(verzija)1
CBCG PSCB test	1.3.6.1.4.1. 34288.(nekvalifikovani certifikati)2.(PSCB)1.(test)2.(verzija)1

Sljedeći identifikatori (OIDs) dodijeljeni su kategoriji certifikata za OCSP:

Nekvalifikovani certifikati	Identifikator (CertPolicyId)
CBCG OCSP	1.3.6.1.4.1. 34288.(nekvalifikovani)2.(ocsp)2.(generacija)1.(verzija)1

Sljedeći identifikatori (OIDs) dodijeljeni su digitalnim certifikatima koji se koriste interno za upravljanje infrastrukturom i sistemima u okviru CBCG-CA:

Digitalni certifikat	Identifikator (CertPolicyId)
CBCG PKI	1.3.6.1.4.1. 34288. (nekvalifikovani)2.(pki-interno)3.(generacija)1. {id} Napomena: vrijednost {id} dodijeljuje se interno.

1.3. Učesnici infrastrukture javnih ključeva

1.3.1. Certifikaciona tijela

Certifikaciona tijela koja djeluju u okviru CBCG-CA pružaju uslugu povjerenja u skladu sa ovim praktičnim pravilima, Zakonom o elektronskoj identifikaciji i elektronskom potpisu, kao i odgovarajućim pravilnicima i standardima.

U okviru infrastrukture javnih ključeva koju je CBCG uspostavila za pružanje usluge povjerenja, korjensko certifikaciono tijelo, odnosno korjenski izdavalac certifikata CBCG-CA ima samopotpisani digitalni certifikat koji je izdat u okviru kontrolisanog postupka generisanja kriptografskih ključeva (engl. Root Key Generation Ceremony).

Korjensko certifikaciono tijelo izdaje samo certifikate podređenim certifikacionim tijelima odnosno izdavaocima certifikata CBCG-CA, serveru OCSP i certifikate za upravljanje infrastrukturom i sistemima u okviru CBCG-CA.

Podređena certifikaciona tijela CBCG-CA izdaju certifikate krajnjim korisnicima, učesnicima u PSCB (vidi poglavlje 1.3.3. ovih praktičnih pravila), serveru OCSP i certifikate za upravljanje infrastrukturom i sistemima u okviru CBCG-CA.

CBCG je posebnim aktom uspostavila organizacionu strukturu za pružanje i upravljanje uslugama povjerenja, kroz poslove:

- Komiteta Certifikacionog tijela CBCG za pružanje elektronskih usluga povjerenja (engl. Policy Management Authority – PMA),
- Operativne poslove CBCG-CA - (engl. Operations Authority – OA), i
- Poslove registracije - (engl. Registration Authority – RA).

Lica koja izvršavaju poslove upravljanja radom, operativne poslove i poslove registracije su zaposleni u CBCG.

1.3.2. Poslovi registracije (Registration Authority - RA)

Poslovi registracije u okviru usluge povjerenja su provjera identiteta naručilaca odnosno korisnika certifikata, obrada zahtjeva i odobrenje ili odbijanje zahtjeva za izdavanje, obnovu ili opoziv certifikata.

1.3.3. Naručioci i korisnici digitalnih certifikata

Naručilac digitalnog certifikata je lice koje zahtijeva certifikat u ime pravnog lica, organa vlasti ili u svoje ime kada je naručilac istovremeno i korisnik.

Korisnik certifikata CBCG-CA je pravno lice ili organ vlasti identifikovano kao korisnik privatnog ključa koji je povezan sa javnim ključem sadržanim u digitalnom certifikatu i naveden je u polju Vlasnik (*eng. Subject*) certifikata.

Kada je naručilac istovremeno i korisnik, odgovoran je za sve obaveze u vezi sa korišćenjem certifikata.

1.3.4. Treća lica

Treća lica su CBCG i drugi učesnici u PSCB koji se oslanjaju na certifikate izdate od strane CBCG-CA, bez obzira na to da li su naručilac certifikata ili nijesu.

Za provjeru važenja primljenog certifikata, treća lica moraju provjeriti status na važećoj listi opozvanih certifikata (CRL) ili putem usluge provjere statusa digitalnih certifikata (OCSP).

1.3.5. Ostali učesnici

Nije primjenljivo.

1.4. Svrha upotrebe certifikata

1.4.1. Dozvoljena upotreba certifikata

Digitalni certifikati koje izdaje CBCG-CA mogu se koristiti na način kao što je za pojedinačnu kategoriju certifikata navedeno u sljedećoj tabeli.

Kategorija certifikata	Dozvoljena upotreba
CBCG PSCB	Za napredni elektronski pečat, autentifikaciju i kriptovanje podataka
CBCG OCSP	Za OCSP servise u okviru CBCG-CA
CBCG PKI	Za upravljanje servisa u okviru CBCG-CA

1.4.2. Nedozvoljena upotreba certifikata

Certifikati izdati od strane CBCG-CA mogu se koristiti samo u skladu sa ovim praktičnim pravilima, Politikom i zakonom.

1.5. Upravljanje praktičnim pravilima

1.5.1. Organizacija koja upravlja Praktičnim pravilima

Ovim praktičnim pravilima upravlja CBCG.

1.5.2. Kontakt podaci:

Adresa: Centralna banka Crne Gore
Bulevar Sv. Petra Cetinjskog br. 6
81000 Podgorica
E-mail: cbcg-ca@cbcg.me
Internet: https://www.cbcg.me

1.5.3. Utvrđivanje adekvatnosti i kompatibilnost praktičnih pravila spoljnih CA sa ovim praktičnim pravilima

U vezi sa odgovarajućim odredbama, vidjeti poglavlje 1.5.3. u dokumentu CBCG-CA Politika.

1.5.4. Postupak odobrenja Praktičnih pravila davaoca usluga povjerenja

Praktična pravila, odnosno njegove izmjene i/ili dopune donosi Guverner CBCG. Dokument se objavljuje u elektronskoj verziji, u formi PDF, na internet stranici CBCG.

1.6. Definicije i skraćenice

Pojedini pojmovi korišćeni u ovoj politici imaju sljedeće značenje:

Elektronski pečat	je skup podataka u elektronskom obliku, koji su pridruženi drugim podacima u elektronskom obliku ili su sa njima logički povezani radi obezbjeđenja porijekla i integriteta tih podataka i zasniva se na certifikatu za elektronski pečat.
Napredni elektronski pečat	je elektronski pečat koji ispunjava posebne zahtjeve utvrđene Zakonom o elektronskoj identifikaciji i elektronskom potpisu.
Autor elektronskog pečata	je pravno lice ili organ vlasti koje upotrebljava elektronski pečat korišćenjem podataka za izradu elektronskog pečata.
Podaci za izradu elektronskog pečata	su jedinstveni podaci koje autor elektronskog pečata koristi za izradu elektronskog pečata.
Certifikat za elektronski pečat	je elektronska potvrda koja povezuje podatke za verifikaciju elektronskog pečata sa pravnim licem ili organom vlasti i potvrđuje naziv tog lica ili organa vlasti.
Informacioni sistem	je sistem za transformaciju, slanje, čuvanje i druge obrade podataka u elektronskoj formi.
Certifikat javnog ključa	je javni ključ korisnika, zajedno sa identifikacionim podacima korisnika koji je digitalno potpisan privatnim ključem certifikacionog tijela koje ga je izdalo.
Certifikat	je certifikat javnog ključa odnosno digitalni certifikat.
Certifikaciono tijelo	izdaje digitalne certifikate ili pruža druge usluge u vezi sa digitalnim certifikatima. (engl. Certification Authority, CA)
Izdavalac certifikata	je certifikaciono tijelo.
Elektronska usluga povjerenja	je usluga kojom se omogućava visok nivo pouzdanosti razmjene i obrade podataka u elektronskom obliku, a koja podrazumijeva

	izradu certifikata za napredni elektronski pečat za učesnike u PSCG;
Korjensko certifikaciono tijelo (korjenski izdavalac)	je izdavalac digitalnih certifikata koje u okviru infrastrukture javnih ključeva predstavlja polazište povjerenja (eng. trust point). Korjenski izdavalac se koristi samo za izdavanje digitalnih certifikata podređenim izdavaocima.
Podređeno certifikaciono tijelo (podređeni izdavalac)	je izdavalac digitalnih certifikata kome je digitalnu potvrdu izdao korjenski odnosno nadređeni izdavalac. Podređeni izdavalac izdaje certifikate naručiocima odnosno krajnjim korisnicima ili drugim podređenim izdavaocima.
Nekvalifikovani certifikati	su certifikati koji se ne smatraju kvalifikovanim u skladu sa Zakonom.

Skraćenice:

ASN.1 Abstract Syntax Notation One
CA Certification Authority
PKI Public Key Infrastructure
CRL Lista opozvanih certifikata
OID Object Identifier
SHA Secure Hash Algorithm
URI Uniform Resource Identifier
CN Common Name
DN Distinguished Name
RDN Relative Distinguished NameURL Uniform Resource Locator
HSM Hardware Security Module (Bezbjednosni hardverski modul)
PMA Policy Management Authority
NTP Network time protocolRA Registration Authority (Poslovi registracije)
IPS Intrusion prevention system
DMZ Demilitarized Zone
OCSP Online Certificate Status Protocol
OI Organization Identifier (polje organizationIdentifier u jedinstvenom imenu)
RTGS Real Time Gross Settlement - poravnanje po bruto principu u relanom vremenu
DNS Deffered Net Settlement – poravnanje po neto principu u odloženom vremenu
PSCB Platni sistem Centralne banke Crne Gore

2. OBJAVE I REPOZITORIJUM

2.1. Repozitorijum

CBCG-CA koristi interne i javne repozitorijume.

Javni repozitorijumi su dostupni na sljedećim internet adresama:

Javne internet stranice:	https://www.cbcg.me http://pki.cbcg.me
Direktorijum LDAP	ldap.cbcg.me

2.2. Objavljivanje informacija o certifikatima

CBCG-CA javno objavljuje na javnom repozitorijumu iz tačke 2.1.:

- CBCG-CA Politiku,
- Praktična pravila,
- liste opozvanih certifikata (eng. Certificate Revocation Lists, CRL),
- status certifikata putem protokola OCSP,
- certifikat korjenskog certifikacionog tijela Root CA CBCG,
- certifikat podređenog certifikacionog tijela CBCG-CA,
- ostale javne informacije povezane sa pružanjem usluga povjerenja.

CBCG-CA čini dostupnim ili šalje korisnicima dokumenta za potrebe zatvorenog PSCB i to:

- uputstvo za instalaciju digitalnog certifikata,
- uputstva za sticanje certifikata,
- uputstva za opoziv certifikata,
- uputstva za obnovu certifikata.

2.3. Vrijeme i učestalost objava

Liste opozvanih certifikata se objavljuju nakon izdavanja nove liste kao što je definisano u poglavlju 4.9.7.

Druge informacije objavljuju se čim dođe do promjena ili kada postanu dostupne.

2.4. Pristup podacima u repozitorijumu

U javnim repozitorijumima se objavljuju samo javne informacije koje su dostupne samo za čitanje. Repozitorijumi imaju uspostavljene odgovarajuće tehničke bezbjednosne

mehanizme za zaštitu od neovlašćenih promjena podataka i mehanizme za obezbjeđivanje raspoloživosti podataka.

3. PREPOZNAVANJE I PROVJERA ISTOVJETNOSTI

3.1. Određivanje imena

3.1.1. Vrste imena

Za ime subjekta se u certifikatima koristi ime korisnika, kao što je za pojedinačnu kategoriju certifikata navedeno u nastavku ovog poglavlja. Ovjereno ime subjekta je u certifikatu zapisano u atributima koji su dio cjelokupnog X.501 jedinstvenog imena (angl. Distinguished Name, DN). Pojedinačni atributi jedinstvenog imena su u skladu sa RFC 5280 upisani u formi `UTF8String` ili `PrintableString`.

Certifikat korjenskog certifikacionog tijela ima sljedeće jedinstveno ime:

Atribut jedinstvenog imena	Vrijednost
Country Name (C=), obvezan	ME
Organization Name (O=), obavezan	Centralna Banka Crne Gore
Organization Identifier (organizationIdentifier =), obavezan	VATME-02011328
Common Name (CN=), obavezan	Root CA Centralna Banka CG

Certifikat podređenog certifikacionog tijela ima sljedeće jedinstveno ime:

Atribut jedinstvenog imena	Vrijednost
Country Name (C=), obavezan	ME
Organization Name (O=), obavezan	Centralna Banka Crne Gore
Organization Identifier (organizationIdentifier =), obvezan	VATME-02011328

Common Name (CN=), obavezan	CA Centralna Banka CG

Jedinstveno ime je u certifikatima za upotrebu u PSCB:

Atribut jedinstvenog imena	Vrijednost
Country Name (C=), obvezan	ME
Organization Name (O=), obavezan	Centralna Banka Crne Gore
Organization Identifier (organizationIdentifier =), obavezan	VATME-02011328
Organizational Unit Name (OU=), obavezan	Oznaka sistem u okviru PSCP (RTGS za produkcijsku granu, RTGS-TEST za testnu granu)
Organizational Unit Name (OU=), obavezan	Naziv učesnika u okviru PSCB
Common Name (CN=), obavezan	Oznaka vrste certifikata učesnika u okviru PSCB

Jedinstveno ime je u digitalnim certifikatima za servere OCSP zapisano u sljedećoj formi:

Atribut jedinstvenog imena	Vrijednost
Country Name (C=), obavezan	ME
Organization Name (O=), obavezan	Centralna Banka Crne Gore
Organization Identifier (organizationIdentifier =), obavezan	VATME-02011328
Common Name (CN=), obavezan	Opšti naziv usluge OCSP

Jedinstveno ime u digitalnim certifikatima za upravljanje internom infrastrukturom CBCG-CA, dodjeljuje se interno.

3.1.2. Potreba za smislenosti imena

Jedinstveno ime certifikata čini skup atributa u skladu sa RFC 5280 [3] i EN 319 412 djelovi 1 do 3 [5] [6] [7].

3.1.3. Anonimnost korisnika i korišćenje pseudonima

Nije primjenljivo.

3.1.4. Pravila za interpretaciju različitih oblika imena

Vrste imena i značenje pojedinačnog atributa u jedinstvenom imenu certifikata navedeni su u poglavlju 3.1.1. Jedinstveno ime može sadržati dodatna polja, a koja ne utiču na identifikaciju korisnika certifikata.

Redosljed relativnih imena (RDN) jedinstvenog imena (DN) može se razlikovati od navedenog u poglavlju 3.1.1. i ne utiče na pouzdanost odnosno vjerodostojnost jedinstvenog imena.

U jedinstvenom imenu certifikata su pojedinačna polja zapisana kao ASN.1 `utf8String` ili ASN.1 `printableString`. U slučaju nepredviđenih znakova CBCG-CA zadržava pravo da potraži kombinaciju slova iz kodne tabele ASCII.

3.1.5. Jedinstvenost imena

CBCG-CA za svakog korisnika certifikata određuje jedinstveno ime (DN), koje je u digitalnom certifikatu u skladu sa RFC 5280 [3] upisano u polju `Subject`.

Set atributa u jedinstvenom imenu (DN) certifikata jednolično predstavlja svakog korisnika certifikata. Jedinstvenost imena za pravna lica je obezbijeđena atributom `organizationIdentifier` i atributom `commonName`.

3.1.6. Priznavanje, provjera istovjetnosti i uloga zaštićenih marki

CBCG-CA će nastojati da riješi sporove koji se mogu pojaviti prilikom dodjeljivanja imena (npr. može zahtijevati od naručioca da se sporni dio jedinstvenog imena promijeni tako da ne bude u konfliktu sa već korišćenim razlikovnim imenom).

Naručioci ne smiju zahtijevati izdavanje certifikata na ime koje bi kršilo prava trećih lica (kao na primjer naziv pravnog lica, lično ime, intelektualna prava ili druga prava svojine).

CBCG-CA može, po sopstvenoj procjeni bez obrazloženja, odbaciti zahtjev naručioca ili zahtijevati dodatne dokaze, ako sumnja da se zahtjevom krše prava trećih lica (kao na primjer naziv pravnog lica, lično ime, autorska i druga prava). Ukoliko je potvrda već izdata, CBCG-CA može da je opozove.

3.2. Prva registracija

3.2.1. Metode dokazivanja vlasništva privatnog ključa

Dokaz posjedovanja privatnog ključa je obezbijeđen korišćenjem postupaka na osnovu priznatih standarda, kao što su PKCS#10 (Public Key Cryptographic Standard #10), Certificate Management Protocol (CMP).

3.2.2. Provjera istovjetnosti učesnika u Platnom sistemu

Provjera istovjetnosti učesnika PSCB vrši se u skladu sa Pravilima rada Platnog sistema Centralne banke Crne Gore.

3.2.3. Provjera istovjetnosti za fizička lica u vezi sa učesnicima u PSCG

Provjera fizičkih lica u vezi sa učesnicima u PSCG, odnosno zastupnika učesnika u PSCG, vrši se u skladu sa Pravilima rada Platnog sistema Centralne banke Crne Gore.

3.2.4. Podaci o vlasnicima digitalnih certifikata koji se ne provjeravaju

Svi podaci koji su sadržani u jedinstvenom imenu certifikata, koji su u tabelama u poglavlju 3.1.1. označeni kao "obavezan", moraju biti provjereni kao dio postupka registracije certifikata.

3.2.5. Provjera ovlašćenja

Svi postupci provjere ovlašćenja vrše se kao dio postupka registracije certifikata.

3.2.6. Kriterijumi za međusobno povezivanje

Za odgovarajuće odredbe, vidjeti poglavlje 1.5.3.

3.3. Provjera istovjetnosti pri obnovi certifikata

3.3.1. Provjera istovjetnosti prilikom rutinske obnove digitalnih certifikata

Prilikom rutinske obnove digitalnih certifikata ne radi se ponovna provjera istovjetnosti podataka o podnosiocu, već zahtjev za obnovu digitalnih certifikata podnosi zaposleni koji obavlja poslove registracije učesnika u PSCB, organizacionoj jedinici koja obavlja operativne poslove.

3.3.2. Provjera istovjetnosti pri obnovi certifikata posle opoziva

Prilikom obnove certifikata poslije opoziva ne radi se ponovna provjera istovjetnosti podataka o podnosiocu, već zahtjev za obnovu poslije opoziva podnosi zaposleni koji obavlja poslove registracije učesnika u PSCB, organizacionoj jedinici koja obavlja operativne poslove.

3.4. Provjera istovjetnosti prilikom zahtjeva za opoziv certifikata

Prilikom podnošenja zahtjeva za opoziv radi se ponovna provjera istovjetnosti podataka o podnosiocu.

4. UPRAVLJANJE CERTIFIKATIMA

4.1. Zahtjev za izdavanje certifikata

4.1.1. Ko može zatražiti izdavanje certifikata

Certifikati se izdaju samo učesnicima u PSCB.

Izdavanje certifikata za test sisteme PSCB mogu tražiti lica zadužena za poslove registracije (RA).

Redovnu periodičnu zamjenu certifikata u skladu sa Pravilima rada Platnog sistema Centralne banke Crne Gore mogu tražiti lica zadužena za poslove registracije (RA).

4.1.2. Postupak obrade zahtjeva i odgovornosti

CBCG-CA izdaje certifikat nakon provjere identiteta naručioca i uspješnog završetka procesa registracije, a u skladu sa Pravilima rada Platnog sistema Centralne banke Crne Gore i internim procedurama. Koraci prilikom izdavanja certifikata su:

- Naručilac podnosi potpisani zahtjev za izdavanje certifikata i prilaže dokumentaciju za identifikaciju;
- Naručilac izjavljuje da prihvata CBCG-CA Praktična pravila i uslove korišćenja certifikata;
- Zahtjev za izdavanje certifikata mora biti prihvaćen i odobren od strane zaposlenih CBCG-CA koji vrše poslove registracije;
- Nakon provjere identiteta, zahtjev za izdavanje certifikata CBCG-CA se prosljeđuje zaposlenima koji obavljaju operativne poslove;
- Zaposleni koji obavljaju operativne poslove CBCG-CA kreiraju korisnika sa odgovarajućim profilom certifikata i generišu aktivacione kodove koji se sastoje od korisničkog imena i autorizacionog koda (jednokratna lozinka);
- CBCG-CA generiše certifikate i kodove za preuzimanje.

Certifikati se učesnicima dostavljaju na CD-u, dok se kodovi za preuzimanje dostavljaju u zatvorenoj koverti. Učesnici PSCB preuzimaju CD i kovertu sa kodovima za preuzimanje lično.

Učesnici mogu preuzeti generisane certifikate i sami, putem aplikacije. I u tom slučaju, CBCG-CA kodove za preuzimanje dostavlja u zatvorenoj koverti. Učesnici PSCB lično preuzimaju kovertu sa kodovima za preuzimanje certifikata.

Postupci obrade zahtjeva učesnika PSCB vrše se u skladu sa internim procedurama za rad.

4.2. Obrada zahtjeva za izdavanje certifikata

4.2.1. Postupci identifikacije i autentifikacije

Vidjeti poglavlje 4.1.2.

4.2.2. Odobrenje ili odbijanje zahtjeva za izdavanje certifikata

Zahtjev za izdavanje certifikata CBCG-CA će biti odobren, ako su ispunjeni sljedeći uslovi:

- Naručilac je predao zahtjev za izdavanje certifikata i priložio dokumenta za identifikaciju;
- Podnosilac zahtjeva ima odgovarajuće ovlašćenje, ako djeluje u ime Naručioca;
- Forma za registraciju zajedno sa dokumentima za identifikaciju i autorizaciju je uspješno provjerena;
- Podnosilac zahtjeva je potpisao izjavu da je upoznat sa uslovima izdavanja i korišćenja certifikata navedenim u ovim praktičnim pravilima.

U slučaju da neki od ovih uslova nije ispunjen, ili da postoji opravdana sumnja da naručilac krši pravila ovog dokumenta, ugovor sa korisnikom ili zakon, CBCG-CA će odbiti zahtjev za izdavanje certifikata.

4.2.3. Rok za obradu zahtjeva za izdavanje certifikata

Na rok za obradu zahtjeva za izdavanje certifikata primjenjuju se Pravila rada Platnog sistema Centralne banke Crne Gore.

4.3. Postupak preuzimanja certifikata

4.3.1. Postupak preuzimanja certifikata

CBCG-CA aplikacija za izdavanje certifikata će nakon primanja zahtjeva:

- verifikovati validnost kodova za aktivaciju sadržanih u zahtjevu;
- verifikovati da li korisnik posjeduje privatni ključ povezan sa javnim ključem poslatim za certifikaciju, kako je predviđeno u poglavlju 3.2.1.;
- verifikovati da li je zahtjev za izdavanje certifikata tehnički ispravan;
- izdati traženi certifikat ukoliko su ispunjeni svi uslovi.

Certifikate učesnika PSCB preuzimaju administratori sistema učesnika u PSCB u skladu sa posebnim aktima CBCG ili učesnici PSCB neposredno putem aplikacije.

4.3.2. Obavještenje korisnika o izdavanju certifikata

Lice koje preuzima certifikat će primiti obavještenje o izdavanju certifikata u okviru postupka preuzimanja certifikata (vidjeti poglavlje 4.3.1.).

4.4. Preuzimanje certifikata

Lice koje preuzima certifikat će preuzeti certifikat po okončanju postupka izdavanja certifikata (vidjeti poglavlje 4.3.1.).

4.4.1. Postupak potvrde preuzimanja certifikata

Naručilac odmah nakon preuzimanja, odnosno prije prvog korišćenja certifikata mora provjeriti sadržinu certifikata i vjerodostojnost certifikata na osnovu certifikata certifikacionih tijela i čim je to moguće, bez nepotrebnog odlaganja, obavijestiti CBCG-CA o eventualnim greškama. U suprotnom, podrazumijeva se da su podaci tačni i naručilac preuzima svu odgovornost za tačnost podataka u certifikatu.

O eventualnoj grešci u certifikatu naručilac će, bez odlaganja, obavijestiti davaoca elektronske usluge CBCG-CA na kontakt adresu koja je navedena u poglavlju 1.5.2.

4.4.2. Objava certifikata

CBCG-CA objavljuje certifikate u LDAP direktorijumu koji nije javno dostupan. Pristup je dozvoljen samo sa sistema koji su povezani u PSCB.

4.4.3. Obavještavanje drugih učesnika o izdavanju certifikata

Nije primjenljivo.

4.5. Upotreba ključeva i certifikata

4.5.1. Upotreba ključeva i certifikata od strane korisnika

Naručioci moraju koristiti certifikate u skladu sa zahtjevima navedenim u poglavlju 1.4.

Privatne ključeve mogu da koriste samo vlasnici kojima je bio izdat certifikat pripadajućeg javnog ključa.

Naručioci se moraju starati o bezbjednosti svojih privatnih ključeva i preventivno postupati da spriječe neovlašćenu upotrebu.

4.5.2. Korišćenje certifikata od strane trećih lica

Treća lica moraju da ograniče oslanjanje na certifikate odnosno pripadajuće javne ključeve samo za svrhe upotrebe definisane ovim pravilima.

Treća lica moraju:

- biti upoznata sa zahtjevima iz ovih praktičnih pravila i dosljedno ih uzeti u obzir,

- prije korišćenja, provjeriti status digitalnih certifikata na listi opozvanih certifikata ili usluge OCSP,
- čim je to moguće, bez nepotrebnog odlaganja, obavijestiti CBCG-CA o sumnji ili saznanju zloupotrebe bilo kog certifikata koje je izdao CBCG-CA.

4.6. Obnova certifikata bez promjene ključa

Obnova certifikata bez promjene ključeva nije dozvoljena.

4.7. Obnova digitalnih certifikata

Obnova certifikata je proces u kom CBCG-CA izdaje naručiocu novi certifikat. Novi certifikat sadrži iste identifikacione oznake naručioca kao stari certifikat i novi javni ključ.

4.7.1. Okolnosti obnove digitalnih certifikata

Obnova certifikata se vrši:

- Nakon opoziva certifikata, ako korisnik zahtijeva izdavanje novog;
- Nakon isteka važenja certifikata ili po isteku vremenskog perioda upotrebe privatnog ključa, ako je taj period kraći nego period važenja certifikata;
- Prilikom redovne zamjene certifikata koja se obavlja, po pravilu, jednom godišnje, ili u slučaju kada to zahtijevaju razlozi bezbjednosti, prije isteka roka od jedne godine u skladu sa Pravilima rada Platnog sistema Centralne banke Crne Gore.

4.7.2. Ko može da zahtijeva obnovu certifikata

Obnovu certifikata može zahtijevati naručilac odnosno isto lice koje je bilo podnosilac zahtjeva kod prvog izdavanja certifikata (vidjeti poglavlje 4.1.1.), ili zaposleni CBCG ovlašćen za poslove registracije.

4.7.3. Obrada zahtjeva za obnovu certifikata

Obradu zahtjeva za obnovu certifikata rade ovlašćeni službenici CBCG-CA u skladu sa internim procedurama.

4.7.4. Obavještenje korisnika o izdavanju novog certifikata

Isto kao što je navedeno u poglavlju 4.3.2.

4.7.5. Postupak potvrde preuzimanja novog certifikata

Isto kao što je navedeno u poglavlju 4.4.1.

4.7.6. Objava obnovljenog certifikata

Isto kao što je navedeno u poglavlju 4.4.2.

4.7.7. Obavještavanje drugih korisnika o izdavanju certifikata

Isto kao što je navedeno u poglavlju 4.4.3.

4.8. Izmjena certifikata

Izmjena certifikata je postupak koji omogućava naručiocima da zatraže certifikat sa izmijenjenim identifikacionim podacima. Izmjena certifikata zahtijeva izdavanje novog certifikata za novi javni ključ i izdaje se po istom postupku kao prvo izdavanje.

4.8.1. Okolnosti u kojima se realizuje izmjena certifikata

Naručilac može zahtijevati izmjenu certifikata kada dođe do promjene podataka sadržanih u certifikatu.

4.8.2. Ko može zahtijevati izmjenu certifikata

Izmjenu certifikata može zahtijevati naručilac, odnosno isto lice koje je bilo podnosilac zahtjeva kod prvog izdavanja certifikata (vidjeti poglavlje 4.1.1.).

4.8.3. Obrada zahtjeva za izmjenu certifikata

Isto kao što je navedeno u poglavlju 4.2.

4.8.4. Obavještenje korisniku o izdavanju izmijenjenih certifikata

Isto kao što je navedeno u poglavlju 4.3.2.

4.8.5. Postupak potvrde preuzimanja izmijenjenih certifikata

Isto kao što je navedeno u poglavlju 4.4.1.

4.8.6. Objava izmijenjenih certifikata

Isto kao što je navedeno u poglavlju 4.4.2.

4.8.7. Obavještavanje drugih učesnika o izdavanju izmijenjenih certifikata

Isto kao što je navedeno u poglavlju 4.4.3.

4.9. Prijevremeno (opoziv) i privremeno (suspenzija) ukidanje validnosti i opoziv certifikata

Postupak se koristi za prijevremeno ukidanje (opoziv) ili privremeno ukidanje (suspenziju) važenja certifikata.

Opoziv certifikata znači prijevremeno konačno ukidanje važenja certifikata. Poništenje opoziva nije moguće.

Suspenzija znači privremeno ukidanje važenja certifikata. Certifikat koji je u stanju privremenog ukidanja, može se konačno opozvati ili se poništava privremeno ukidanje.

U oba slučaja, tj. ako je certifikat opozvan ili suspendovan, status certifikata se objavljuje na listi opozvanih certifikata. U slučaju poništenja suspenzije, taj status certifikata se briše sa liste opozvanih certifikata.

4.9.1. Okolnosti opoziva

CBCG-CA će izvršiti opoziv certifikata u sljedećim slučajevima:

- Na zahtjev lica iz tačke 4.9.2;
- Ukoliko CBCG-CA primi obavještenje da je korisnik certifikata preminuo ili izgubio poslovnu sposobnost ili prestao da postoji, odnosno istekao je rok važenja ovlašćenja za potpisivanje ili su se promijenile okolnosti koje utiču na važenje certifikata;
- Kada CBCG-CA utvrdi da je podatak sadržan u certifikatu pogrešan ili je certifikat izdat na osnovu pogrešnih podataka;
- Kada je neki od aktivacionih podataka, kao što su lozinka ili PIN, iskorišćeni za zaštitu privatnog ključa, ugrožen ili za to postoji sumnja;
- Ukoliko CBCG-CA prestane da pruža elektronske usluge povjerenja koje nije preuzeo drugi davalac usluga povjerenja;
- Ukoliko CBCG-CA utvrdi da certifikat nije izdat u skladu sa ovim praktičnim pravilima;
- Ukoliko naručilac ili korisnik certifikata krši odredbe Praktičnih pravila, propisa kojima se reguliše pružanje elektronskih usluga povjerenja ili Pravila rada Platnog sistema Centralne banke Crne Gore, i
- U drugim slučajevima propisanim Zakonom o elektronskoj identifikaciji i elektronskom potpisu.

4.9.2. Ko može zahtijevati opoziv

Opoziv certifikata može zahtijevati:

- naručilac ili korisnik certifikata,
- zaposleni CBCG-CA ili
- nadležni sud ili upravni organ.

4.9.3. Postupci za opoziv

Zahtjev za opoziv se može podnijeti pisanim putem ili u elektronskom obliku potpisan kvalifikovanim elektronskim potpisom. Zahtjev se dostavlja na kontaktnu e-mail adresu u skladu sa tačkom 1.5.2 ovih pravila.

4.9.4. Vrijeme za posredovanje zahtjeva za opoziv

Lice iz tačke 4.9.2 dužno je da bez odlaganja zatraži opoziv certifikata, čim sazna razloge koji zahtijevaju opoziv.

4.9.5. Vrijeme od zahtjeva za opoziv do opoziva

U svim slučajevima će opozvani certifikat biti objavljen na listi opozvanih certifikata najkasnije u roku od 24 časa od trenutka kada CBCG-CA primi zahtjev za opoziv.

4.9.6. Obaveza provjere liste opozvanih certifikata

Treća lica odnosno svaki subjekt koji se oslanja na certifikate koje izdaje CBCG-CA, prije prihvatanja, mora provjeriti status certifikata na posljednjoj važećoj listi opozvanih certifikata ili preko usluge OCSP.

Ukoliko nijedna od važećih lista opozvanih certifikata i servera OCSP nije dostupna zbog greške u sistemu, nefunkcionisanja usluge ili drugog uzroka, korišćenje certifikata mora biti odbijeno.

Treća lica odnosno svaki subjekt koji pristupa listi opozvanih certifikata, mora da provjeri njegovu vjerodostojnost na osnovu certifikata certifikacionog tijela kao i da period validnosti liste opozvanih certifikata nije istekao.

4.9.7. Učestalost objava liste opozvanih certifikata

CBCG-CA ažurira liste opozvanih certifikata najmanje jednom u 24 časa, odnosno najkasnije u roku od 60 minuta, u slučaju opoziva certifikata.

Lista opozvanih certifikata korjenskog certifikacionog tijela ažurira se čim se izvrši opoziv certifikata ili najmanje jednom na svakih 365 dana.

4.9.8. Dozvoljena zakašnjenja redovne provjere statusa certifikata

Nije primjenljivo.

4.9.9. Usluga on-line provjere statusa digitalnih certifikata (OCSP)

OCSP servis obezbjeđuje CBCG-CA. Lokacija servisa je označena sa URL-om uključenim u svakom izdatom certifikatu.

4.9.10. Obaveza redovne provjere statusa certifikata

Kao u poglavlju 4.5.2.

4.9.11. Ostale forme objavljivanja opozvanih certifikata

Nije primjenljivo.

4.9.12. Posebni zahtjevi u pogledu zloupotrebe ključa

Nije primjenljivo.

4.9.13. Okolnosti za privremeno ukidanje validnosti (suspenzija) certifikata

Privremeno ukidanje validnosti (suspenzija) certifikata može se koristiti samo u internim postupcima CBCG-CA.

4.9.14. Ko može zahtijevati suspenzije ili ukidanje suspenzija certifikata

Nije primjenljivo.

4.9.15. Postupci za suspenzije ili ukidanje suspenzija certifikata

Nije primjenljivo.

4.9.16. Ograničenja perioda privremenog ukidanja validnosti

Period privremenog ukidanja validnosti u okviru internih postupaka CBCG-CA nije ograničen.

4.10. Usluge objavljivanja statusa certifikata

4.10.1. Tehničke karakteristike usluge

Status digitalnih certifikata se objavljuje kao lista opozvanih certifikata X.509 Certificate Revocation List (CRL) u skladu sa RFC 5280 [3] i po protokolu OCSP u skladu sa RFC 6960.

Liste opozvanih certifikata su dostupne po protokolu http. Internet adrese lista opozvanih certifikata su u skladu sa RFC 5280 [3] navedene u polju certifikata `cRLDistributionPoints` (X.509 CRL Distribution Points), sadržanom u svakom izdatom certifikatu.

Usluga OCSP je dostupna na internet adresi koja je navedena u polju certifikata `id-pe-authorityInfoAccess:id-ad-ocsp,` sadržanom u svakom izdatom certifikatu.

4.10.2. Raspoloživost usluge pristupa listi opozvanih certifikata

Pristup listi opozvanih certifikata i usluge OCSP dostupan je 24 časa, svih dana u sedmici, tokom cijele godine.

4.10.3. Dodatne mogućnosti

Nije primjenljivo.

4.11. Trajanje ugovornog odnosa sa naručiocem

Ugovorni odnos se završava po isteku ili opozivu posljednjeg certifikata naručioca.

4.12. Sigurnosno kopiranje i otkrivanje privatnog ključa

CBCG-CA ne vrši čuvanje ili sigurnosno kopiranje privatnih ključeva korisnika.

5. FIZIČKA ZAŠTITA, ORGANIZACIONE BEZBJEDNOSNE MJERE I ZAHTJEVI ZA ZAPOSLENE

5.1. Fizička zaštita

Bezbjednosne mjere na nivou fizičkog okruženja su opisane u internim aktima CBCG-CA koja su usklađena sa ISO/IEC 27001. Dokumentacija, odnosno pojedinačni dijelovi mogu biti na raspolaganju za uvid svakom licu koje izrazi interesovanje i dokaže da je njihovo davanje na uvid potrebno.

5.1.1. Lokacija sajta i izgradnja

CBCG-CA funkcioniše u zoni visoke sigurnosti CBCG IT centra koji je lociran u Podgorici.

Sistemske komponente i funkcionisanje CBCG-CA locirani su u fizički zaštićenoj sredini u cilju sprječavanja njihovog neovlašćenog korišćenja, pristupa ili odavanja osjetljivih informacija. Kontrole fizičke bezbjednosti sprovode se konzistentno uz primjenu najboljih praksi u obezbjeđivanju fizičke sigurnosti. Mjere zaštite sadrže:

- Pristup je ograničen na zaposlene CBCG-CA;
- Svi ostali pristupi su pod pratnjom i svaki pristup se loguje;
- Zidovi su od čvrste gradnje;
- Sigurnosne elektronske brave i sistemi pristupa;
- Nadzor 24 sata/7dana sedmično sa obezbjeđenjem na licu mjesta i centralnim video nadzorom.

5.1.2. Fizički pristup

CBCG-CA koristi kombinaciju kartica i elektronske brave. CBCG politika sigurnosti zahtijeva da se ojačana CA područja tretiraju kao "*zone sigurnosti*" i da implementirane kontrole fizičkog pristupa obezbjeđuju dosljedno sprovođenje ove politike.

Sva senzitivna područja unutar zgrade nadzirana su preko CCTV kamera i sve se aktivnosti bilježe lokalno, pod bezbjednim uslovima, i daljinski u stanici za nadzor sigurnosti. Zgrada je zaštićena sigurnosnim sistemima sa alarmom, koji šalju signal lokacijama sa dežurnim licima (zaposlenim ili angažovanim), u slučaju nastanka uslova za aktivaciju alarma.

5.1.3. Napajanje i klimatizacija

CBCG IT Centar opremljen je sa klima uređajima u cilju kontrolisanja toplote i vlažnosti, i svih kritičnih komponenti koje su povezane sa neprekidnim napajanjem (UPS) uređajima, koje isto tako uslovljavaju napajanje.

CBCG-CA konstantno prati sisteme preko monitoring sistema koji automatski šalju upozorenje na lokaciju sa dežurnim zaposlenim ukoliko se pojavi greška.

5.1.4. Izloženosti vodi

CBCG-CA obezbjeđuje da njene CA komponente ne budu izložene nikakvim potencijalnim vodenim, odnosno drugim tečnim opasnostima.

5.1.5. Suprotstavljanje vatri i protivpožarna zaštita

CBCG IT Centar je opremljen detektorima za toplotu i sistemom za gašenje požara, koji je povezan sa glavnim protivpožarnim sistemom objekta i kontrolnom stanicom.

5.1.6. Skladištenje medija

Svi mediji za skladištenje koji sadrže informacije CBCG-CA uključujući i backup trake, uskladišteni su u prostoru CBCG IT Centra koji je otporan na vatru.

Ako se mediji šalju na skladištenje na lokacije van objekta, čuvaju se u zonama zaštićenog ambijenta.

5.1.7. Odlaganje otpada

Papirna dokumenta i magnetski mediji se fizički uništavaju prije odlaganja.

CBCG-CA zadržava sve neservisirane hardverske komponente radi sigurnog odlaganja.

5.1.8. Backupovi van lokacije

CBCG-CA koristi kriptografske kontrole sa visokim stepenom sigurnosti radi osiguranja elektronskog transporta podataka u svrhu backup-a.

Fizički oblici kontrola koji se primjenjuju na lokacijama van objekta obezbjeđuju nivo sigurnosti koji je sličan onom u CBCG-CA primarnom IT centru.

5.2. Organizaciona bezbjednosna mjera

5.2.1. Organizacija CBCG-CA

CBCG-CA ima utvrđenu organizacionu strukturu, podjelu zadataka i ovlašćenja za pristup infrastrukturi i podacima s obzirom na zadatke koje obavlja pojedini zaposleni.

Zaposleni u CBCG-CA obavljaju sljedeće operativne poslove:

Operativna uloga	Odgovornosti
Administratori HSM	Lica zadužena za upravljanje hardverskim sigurnosnim modulima (HSM) i logičnih particija HSM. Obuhvata četiri nivoa zahtjeva: • Administrator HSM • Administrator za bezbjednost logičke particije HSM • Korisnik logičke particije HSM
PKI Administrator bezbjednosti	Lica zadužena za upravljanje podešavanjem aplikacije za izdavanje certifikata i upravljanje digitalnim certifikatima u okviru aplikacije za izdavanje certifikata.
PKI Administrator	Lica zadužena za upravljanje digitalnim certifikatima u okviru aplikacije za izdavanje certifikata.
Administrator bezbjednosnih kopija kriptografskih materijala	Lica zadužena za čuvanje bezbjednosnih kopija kriptografskih ključeva ovjerioca i po potrebi drugih bezbjednosno osjetljivih podataka.
Security Safe Custodian	Lica zadužena za čuvanje osjetljivih materijala (kopije lozinka i sl.) u sigurnosnom sefu.
Sistemski administrator (OS, mrežna oprema i LDAP)	Lica zadužena za upravljanje sistemima IT na kojima funkcionišu sklopovi softvera ovjerioca.
Zaposleni na poslovima registracije	Lica zadužena za prijem zahtjeva za izdavanje certifikata i verifikaciju identiteta korisnika.

5.2.2. Broj lica potrebnih za izvođenje postupka

Dva lica su potrebna za izvršavanje sljedećih zadataka:

- upravljanje hardverskim sigurnosnim modulom (HSM) i ključevima za izradu bezbjednosne kopije HSM-a,
- povraćaj bezbjednosne kopije privatnih ključeva certifikacionog tijela na hardverski sigurnosni modul (HSM) i
- aktiviranje privatnih ključeva certifikacionog tijela na hardverskom sigurnosnom modulu (HSM).

Ostale pojedinačne zadatke u pogledu dodijeljenog operativnog zahtjeva može da izvrši jedno lice.

5.2.3. Provjera identiteta zaposlenih koji obavljaju operativne poslove

Svi zaposleni koji rade na softveru sistema CBCG-CA prilikom prijave na pojedinačni sistem se autentifikuju digitalnim certifikatom ili jakom lozinkom.

5.2.4. Nespojivost zadataka

CBCG-CA obezbjeđuje podjelu dužnosti zaposlenih koji obavljaju operativne poslove i na taj način obezbjeđuje dodjeljivanje zadataka navedenih u poglavlju 5.2.1. različitim licima.

5.3. Zahtjevi za zaposlene CBCG-CA

5.3.1. Kvalifikacije, iskustva i bezbjednosno povjerenje

Zaposleni CBCG ne smiju izvršavati zadatke koji su u sukobu interesa sa njihovim nadležnostima u okviru CBCG-CA.

5.3.2. Provjera adekvatnosti zaposlenih

Nije primjenljivo.

5.3.3. Osposobljavanje zaposlenih

Zaposleni CBCG koji izvršavaju ove poslove moraju da ispunjavaju uslove u pogledu obrazovanja i radnog iskustva posebna stručna znanja koja su potrebna za obavljanje ovih specifičnih zadataka, u skladu sa aktom CBCG.

5.3.4. Učestalost dodatnih edukacija

Zahtjevi za edukaciju zaposlenih se redovno provjeravaju i odobravaju u skladu sa potrebama naročito u slučaju promjena tehnologije i verzija softvera.

5.3.5. Rotacija radnih mjesta

Nije primjenljivo.

5.3.6. Mjere u slučaju postupanja suprotno ovim pravilima

U slučaju postupanja zaposlenih suprotno ovim pravilima, primjenjuju se mjere utvrđene zakonom i posebnim aktima CBCG.

5.3.7. Zahtjevi za angažovana lica

Ako je za izvršavanje određenih zadataka potrebno angažovanje spoljnih izvođača CBCG mora da izvrši provjeru njihove sposobnosti, odnosno obučenosti.

Svi spoljni izvođači moraju da potpišu izjavu o tajnosti.

5.3.8. Dokumentacija za zaposlene koji obavljaju operativne poslove

CBCG stavlja na raspolaganje zaposlenima koji obavljaju operativne poslove interne priručnike, kao i originalnu dokumentaciju softvera i hardvera.

5.4. Postupci prikupljanja i upravljanja logovima za reviziju

CBCG-CA ima uspostavljen stalni nadzor djelovanja svoje infrastrukture u okviru koga se bilježe revizorski tragovi dozvoljene i nedozvoljene upotrebe i pristupa infrastrukturi CBCG-CA.

5.4.1. Vrste bilježenih događaja

CBCG-CA bilježi sljedeće vrste događaja:

- događaji na operativnom sistemu, softveru i hardveru certifikacionog tijela,
- događaji u vezi sa ključevima certifikacionog tijela,
- događaji u vezi s ključevima korisnika i digitalnim certifikatima - izdavanje, preuzimanje, obnova, opoziv,
- događaji u vezi sa bezbjednosnom politikom i upravljanjem informacionim sistemom CBCG-CA i
- događaji u vezi sa bezbjednosnom politikom i upravljanjem komunikacionim sistemom.

Zapis događaja u elektronskoj ili papirnoj formi sadrži datum i vrijeme događaja, i ukoliko je tehnički izvodljivo, i jedinstvenog identifikatora lica koje je izazvalo događaj.

CBCG-CA prikuplja i bilježi u elektronskoj ili papirnoj formi i podatke koji utiču na bezbjednost, a nisu dio komunikaciono-informacionog sistema:

- događaje u vezi sa fizičkim pristupom sistemima CBCG-CA i fizičkom lokacijom;
- kadrovske promjene zaposlenih koji obavljaju operativne poslove CBCG-CA.

5.4.2. Učestalost pregleda logova za reviziju

Zaposleni koji obavljaju operativne poslove CBCG-CA pregledaju dnevnike bilježenih događaja prilikom svakog primljenog upozorenja iz nadzornih sistema. Pregled uključuje:

- pregled zapisa u dnevniku i
- analizu i izvještavanje o relevantnim događajima - rješavanje problema.

Zaposleni koji obavljaju operativne poslove CBCG-CA sprovode redovne preglede bilježenih događaja, i to najmanje jednom godišnje. Redovni pregled uključuje:

- prikupljanje i spajanje dnevnika od posljednjeg redovnog pregleda dnevnika,
- pregled zapisa u dnevniku i izradu izvještaja o relevantnim događajima i
- izradu arhivskih kopija dnevnika.

5.4.3. Period čuvanja revizorskih dnevnika

Revizorski dnevnici softvera za upravljanje digitalnim certifikatima čuvaju se najmanje tri mjeseca na sistemima CBCG-CA i sistemu za čuvanje podataka, kao što je definisano u poglavlju 5.5.2.

Operativni logovi certifikacionog tijela softvera i sistema čuvaju se najmanje mjesec dana na sistemima CBCG-CA i najmanje godinu dana na sistemu za čuvanje podataka.

5.4.4. Zaštita revizorskih dnevnika

Dnevnici se čuvaju u odgovarajućem bezbjednosnom području.

Pristup dnevnicima bilježenih događaja je dozvoljen samo ovlašćenim licima:

- zaposlenima koji obavljaju operativne poslove CBCG-CA u okviru radnih zadataka i
- nadležnim inspekcijskim organima, u skladu sa zakonom.

Za operativne dnevnike na operativnom sistemu i softveru koriste se zaštite koje dozvoljava operativni sistem.

Za revizorske dnevnike softvera za upravljanje digitalnim certifikatima koriste se mehanizmi zaštite integriteta zapisa.

5.4.5. Bezbjednosne kopije revizorskih dnevnika

Bezbjednosna kopija revizorskih dnevnika odnosno tragova sprovodi se u okviru dnevnog bezbjednosnog kopiranja sistema. Kopija operativnih i revizorskih dnevnika čuva se na udaljenoj lokaciji.

5.4.6. Način prikupljanja revizorskih dnevnika

Prikupljanje operativnih i revizorskih dnevnika odnosno tragova na informacionim sistemima izvodi se automatski.

Prikupljanje revizorskih tragova sljedećih događaja izvodi se ručno za:

- Generisanje ključeva i certifikata certifikacionih tijela CBCG-CA;
- Fizički pristup spoljnih izvođača u prostorije CBCG-CA;
- Promjene konfiguracija na informacionim sistemima CBCG-CA;
- Nadgradnje softvera i hardvera;
- Zahvate na održavanju (najavljeni i nenajavljeni) na sistemima CBCG-CA;
- Odstupanja od normalnog djelovanja, utvrđena prilikom pregleda i sistemskih dnevnika;
- Promjene zaposlenih koji obavljaju operativne poslove CBCG-CA;
- Uništavanje informacija i/ili medija.

5.4.7. Obavještavanje lica koje je izazvalo događaj

Lice koje je izazvalo događaj se ne obavještava o događaju.

5.4.8. Ocjena i otklanjanje ranjivosti

CBCG-CA sprovodi ocjenu ranjivosti kao dio postupaka obrade revizorskih dnevnika.

5.5. Arhiviranje podataka

5.5.1. Vrste arhiviranih podataka

CBCG-CA arhivira sljedeće zapise:

- Informacije definisane u poglavlju 5.4.1.;
- Digitalne certifikate i stanje opozvanih certifikata;
- Izvještaje o bezbjednosnim pregledima infrastrukture CBCG-CA.

5.5.2. Vrijeme čuvanja

CBCG-CA čuva revizorske dnevnike najmanje deset godina. Digitalni certifikati i status opoziva se čuvaju trajno.

5.5.3. Zaštita arhiva

Pristup arhivskim podacima CBCG-CA dozvoljen je zaposlenima koji obavljaju operativne poslove CBCG-CA, po potrebi.

5.5.4. Bezbjednosna kopija arhiva

Bezbjednosna kopija arhiva se realizuje u okviru redovnog dnevnog bezbjednosnog kopiranja sistema CBCG-CA. Kopija se čuva na udaljenoj lokaciji. Prenos bezbjednosnih kopija na drugu lokaciju se vrši preko zaštićene elektronske komunikacije i interne računarske mreže.

5.5.5. Zahtjevi za vremensko pečatiranje zapisa

Arhivirani zapisi su vremenski označeni prilikom njihovog nastanka korišćenjem sistemskog sata sistema, na kome je događaj nastao. Sistemski sati svih informacionih sistema su usaglašeni sa pouzdanim spoljašnjim izvorom korišćenjem protokola NTP.

5.5.6. Arhiviranje (unutrašnje/spoljašnje)

Arhiviranje se vrši unutar CBCG-CA.

5.5.7. Postupak za pristup arhivskim podacima i njihova verifikacija

Arhivirani podaci su na raspolaganju za uvid svakoj strani koja izrazi interesovanje i dokaže da je njihovo stavljanje na uvid opravdano.

Mišljenje u vezi opravdanosti zahtjeva za pristup arhivskim podacima, za svaki konkretni slučaj daje CBCGPMA.

Stavljanje na uvid traženih podataka vrši se u skladu sa posebnim propisima CBCG.

5.6. Obnova certifikata certifikacionog tijela

Obnova privatnih ključeva certifikacionih tijela će biti izvršena najmanje pet godina prije isteka certifikata, a po potrebi i ranije. Prilikom obnove privatnih ključeva biće generisan novi par kriptografskih ključeva i novi certifikat certifikacionog tijela.

5.7. Postupci u slučaju ugrožavanja privatnog ključa i plan oporavka

5.7.1. Postupci za reagovanje na bezbjednosne incidente i nepravilnosti

CBCG-CA sprovodi postupke za reagovanje na bezbjednosne incidente i nepravilnosti u skladu sa ISO/IEC 27001.

5.7.2. Uništavanje softvera, hardvera ili podataka

U slučaju kvara hardverske ili softverske opreme, odnosno podataka pri kojima privatni ključ CBCG-CA nije bio uništen, usluge CBCG-CA će biti uspostavljene ponovo u najkraćem mogućem roku. U slučaju uništavanja privatnog ključa CBCG-CA primjenjuje se postupak opisan u poglavlju 5.7.3.

5.7.3. Ugrožavanje privatnog ključa certifikacionog tijela

U slučaju da je privatni ključ certifikacionog tijela ugrožen, CBCG-CA će opozvati sve certifikate koju su trenutno validni.

5.7.4. Plan oporavka u slučaju prirodne ili druge katastrofe

U slučaju prirodne ili druge katastrofe, pri kojoj privatni ključ CBCG-CA nije bio uništen, usluge će biti uspostavljene ponovo u najkraćem mogućem roku. Postupci su detaljnije definisani u povjerljivom dijelu internih pravila djelovanja CBCG-CA.

U slučaju uništenja privatnog ključa CBCG-CA primjenjuje se postupak opisan u poglavlju 5.7.3.

5.8. Prestanak pružanja elektronske usluge povjerenja

U slučaju prestanka pružanja elektronske usluge povjerenja, CBCG će:

- Najmanje tri mjeseca prije planiranog prestanka pružanja usluge, o svojoj namjeri obavijestiti sve trenutne naručioce i organ državne uprave nadležan za poslove elektronske uprave i elektronskog poslovanja;
- Uložiti sve razumne napore da obezbedi nastavak pružanja usluge kod drugog davaoca elektronskih usluga povjerenja. Drugom davaocu usluga povjerenja će

dostaviti kompletnu dokumentaciju u vezi sa uslugama koje je pružalo CBCG-CA. Naručioce i organ državne uprave nadležan za poslove elektronske uprave i elektronskog poslovanja, obavijestiće na koga, kada i pod kojim uslovima će prenijeti pružanje usluga povjerenja;

- U slučaju da ne pronađe drugog davaoca elektronskih usluga povjerenja koji bi preuzeo usluge koje je pružalo CBCG-CA, CBCG-CA će opozvati sve izdate i još validne certifikate i u skladu sa EN 319 411-1, objaviti CRL s valjanošću do "99991231235959Z". Kompletnu dokumentaciju u vezi sa uslugama koje je pružalo CBCG-CA, CBCG će čuvati najmanje deset godina od dana prestanka pružanja elektronske usluge povjerenja;
- U slučaju da ne pronađe drugog davaoca elektronskih usluga povjerenja koji bi preuzeo usluge CBCG-CA i ne bude u mogućnosti da obezbedi objavu CRL i čuvanje dokumentacije u vezi sa uslugama koje pruža CBCG-CA, CBCG-CA će opozvati sve izdate i važeće certifikate i, u skladu sa EN 319 411-1, generisati CRL sa valjanošću do "99991231235959Z". Tako generisani CRL i kompletnu dokumentaciju u vezi sa uslugama koje pruža CCBG-CA, CBCG će dostaviti organu državne uprave nadležnom za poslove elektronske uprave i elektronskog poslovanja.

6. TEHNIČKI BEZBJEDNOSNI ZAHTJEVI

6.1. Generisanje i instalacija para ključeva

6.1.1. Generisanje para ključeva

Privatni kriptografski ključevi certifikacionih tijela u okviru CBCG-CA stvoreni su na hardverskom sigurnosnom modulu (eng. Hardware Security Module, HSM) u okviru kontrolisanog postupka (eng. *Key Generation Ceremony*).

Postupak generisanja kriptografskih ključeva korjenskih izdavaoca izvodi se uz sljedeće kontrole:

- postupak se izvodi uz prisustvo lica koje nije zaposleno u CBCG (svjedok) i
- sačinjava se zapisnik izvođenja postupka koji ovjerava odnosno potvrđuje svjedok.

Postupci generisanja kriptografskih ključeva podređenih izdavaoca su realizovani pomoću sljedećih kontrola:

- postupak obavljaju zaposleni zaduženi za operativne poslove u okviru CBCG-CA uz prisustvo najmanje jednog člana Komiteta Certifikacionog tijela CBCG za pružanje elektronskih usluga povjerenja , koje nema aktivne povjerljive uloge prilikom izvođenja postupka koji potvrđuje da je postupak obavljen kao što je zabilježeno u zapisniku postupka i
- sačinjava se zapisnik izvođenja postupka.

6.1.2. Prenos privatnog ključa korisniku

Privatni ključevi učesnika PSCB se generišu softverskim alatima i dostavljaju korisnicima u obliku arhivske datoteke u skladu sa standardom PKCS#12 [16].

6.1.3. Prenos korisnikovog ključa izdavaocu certifikata

Korisnički javni ključ se prenosi izdavaocu certifikata u okviru postupka izdavanja certifikata. Javni ključ se prenosi u formi PKCS#10.

6.1.4. Dostavljanje javnog ključa certifikacionog tijela trećim licima

Javni ključ certifikacionog tijela se dostavlja trećim licima u obliku certifikata.

6.1.5. Dužina asimetričnih ključeva

Asimetrični ključevi RSA imaju sljedeće dužine:

- korjenski izdavaoci koriste RSA ključeve dužine 3072 bita,
- podređeni izdavaoci koriste RSA ključeve dužine 3072 bita,

- korisnički RSA ključevi imaju dužinu 2048 bita,
- kriptografski ključevi servera OCSP moraju biti RSA dužine najmanje 2048 bita,
- ključevi certifikata za upravljanje internom infrastrukturom davaoca elektronskog usluga povjerenja CBCG-CA moraju biti dužine najmanje 2048 bita.

6.1.6. Parametri za generisanje javnih ključeva i provjeru parametara

Svi parametri kriptografskih ključeva se generišu u okviru kriptografskih modula u kojima se ključevi formiraju.

6.1.7. Namjene upotrebe ključeva (X.509 v3 keyUsage)

CBCG-CA definiše svrhu korišćenja kriptografskih ključeva i certifikata u polju `keyUsage`. Polje `keyUsage` se koristi u skladu sa RFC 5280 [3].

Pored polja `keyUsage` za dodatno definisanje se koristi i polje `extKeyUsage`, u kome se može odrediti svrha upotrebe. Polje `extKeyUsage` se koristi u skladu sa RFC 5280 [3].

Potpisivanje certifikata i liste opozvanih certifikata dozvoljeno je samo sa ključevima certifikacionih tijela. Certifikati certifikacionih tijela imaju `keyUsage` polje, koje sadrži sljedeće svrhe upotrebe:

- keyCertSign
- cRLSign.

Pregled korišćenja polja `keyUsage` je dat u sljedećoj tabeli. Upotreba polja `extKeyUsage` zavisi, odnosno prilagođena je pojedinačnoj aplikaciji (na primjer serveri SSL, OCSP).

Tip certifikata	Polje `keyUsage`	Polje `extKeyUsage`
Certifikaciona tijela	`keyCertSign, cRLSign`	
Certifikat za OCSP	`digitalSignature`	`OCSPSigning`
Certifikat za upravljanje infrastrukture davaoca usluga povjerenja	`digitalSignature i/ili keyEncipherment`	`serverAuth i/ili clientAuth`
Certifikat za napredni elektronski pečat CBCG PSCB	`digitalSignature, keyEncipherment, nonRepudiation`	`cbcgPscbEku*`

Polje `keyUsage` može zavisno od tipa certifikata i dodatne svrhe upotrebe zadržati i druge `keyUsage` oznake u skladu sa RFC 5280.

* Polje extKeyUsage `cbcgPscbEku` ima vrijednosti:

- 1.3.6.1.4.1.4852.13.2.1976.9, za produkcijske sisteme,
- 1.3.6.1.4.1.4852.5.1.1990.1, za test sisteme.

6.2. Zaštita privatnih ključeva i tehničke kontrole kriptografskih modula

6.2.1. Standardi za kriptografski modul

Generisanje ključeva certifikacionog tijela i njihova upotreba izvodi se u hardverskom sigurnosnom kriptografskom modulu, koji ima potvrdu o usaglašenosti sa FIPS 140-2 Level 3.

Generisanje ključeva servera OCSP i njihova upotreba izvodi se u hardverskom sigurnosnom kriptografskom modulu, koji ima potvrdu o usaglašenosti sa FIPS 140-2 Level 3.

6.2.2. Kontrola privatnog ključa sa (n od m) ovlašćenim licima

Kao što je opisano u poglavlju 5.2.2.

6.2.3. Otkrivanje (eng. Escrow) privatnog ključa

CBCG-CA ne podržava otkrivanje privatnog ključa.

6.2.4. Bezbjednosno kopiranje privatnih ključeva

CBCG-CA ne vrši bezbjednosno kopiranje privatnih ključeva korisnika.

6.2.5. Arhiviranje privatnog ključa

Nije primjenljivo.

6.2.6. Prenos privatnog ključa u kriptografski modul i iz njega

Privatni ključevi certifikacionih tijela su stvoreni u hardverskom sigurnosnom modulu (HSM) i mogu biti aktivirani samo unutar hardverskog sigurnosnog modula.

Privatni ključevi servera za OCSP su stvoreni u hardverskom sigurnosnom modulu (HSM) i mogu biti aktivirani samo unutar hardverskog sigurnosnog modula.

6.2.7. Čuvanje privatnog ključa certifikacionih tijela u kriptografskom modulu

CBCG-CA je u okviru kontrolisanog postupka (eng. *Key Generation Ceremony*) napravio bezbjednosnu kopiju privatnih ključeva certifikacionog tijela. Bezbjednosne kopije su zaštićene pametnim karticama i mehanizmima hardverskog kriptografskog modula. Prilikom povraćaja ključa iz bezbjednosne kopije potrebno je odobrenje dva zaposlena koja obavljaju operativne poslove. Odobrenje se izvodi na osnovu autentifikacije pametnom karticom.

6.2.8. Postupak za aktiviranje privatnog ključa

Privatni ključevi certifikacionih tijela za potpisivanje se aktiviraju tokom startovanja aplikacije za izdavanje certifikata što zahtijeva HSM lozinku.

Korisnici moraju koristiti PKI klijentsku aplikaciju ili pametne kartice koje aktiviraju privatne ključeve kao dio procesa prijave tokom kojeg se korisnik autentifikuje pomoću lozinke ili PIN-a.

6.2.9. Postupak za deaktiviranje privatnog ključa

Privatni ključevi certifikacionih tijela deaktiviraju se prilikom zaustavljanja aplikacije za upravljanje certifikatima ili usluge za OCSP.

Deaktiviranje privatnih ključeva korisničkih certifikata je pod kontrolom kriptografskog modula od strane korisnika. Korisnici su dužni da deaktiviraju ključeve čim nijesu pod njihovom kontrolom.

6.2.10. Postupak za uništenje privatnog ključa

CBCG-CA će u slučaju potrebe izvršiti uništenje svih kopija privatnih ključeva svojih usluga u okviru kontrolisanih postupaka.

6.2.11. Nivo sigurnosti kriptografskih modula

Kao što je opisano u poglavlju 6.2.1.

6.3. Ostali aspekti upravljanja parovima ključeva

6.3.1. Arhiviranje javnog ključa

CBCG-CA arhivira javne ključeve svojih usluga (certifikacionih tijela, usluge OCSP) i korisničke javne ključeve odnosno certifikate kao što je opisano u poglavlju 5.5.4.

6.3.2. Period validnosti ključeva i certifikata

Periodi validnosti javnih ključeva i certifikata su:

- javni ključ i certifikat korjenskih certifikacionih tijela: 25 godina i 3 mjeseca,
- javni ključ i certifikat podređenih certifikacionih tijela: 15 godina i 3 mjeseca,
- javni ključ i certifikati korisnika: do 5 godina i
- javni ključ i certifikat servera OCSP: do 5 godina.

6.4. Aktivacioni podaci

6.4.1. Generisanje i instaliranje aktivacionih podataka

Za ključ certifikata koje preuzimaju administratori sistema učesnika PSCB, PIN generiše davalac usluga povjerenja i šalje ga ili predaje korisniku kao dio procesa isporuke certifikata.

Za učesnike PSCB koji sami preuzimaju certifikat, davalac usluga povjerenja generiše kod za preuzimanje certifikata i predaje ih korisniku.

6.4.2. Zaštita aktivacionih podataka

Nije primjenljivo.

6.4.3. Drugi aspekti aktivacionih podataka

Nije primjenljivo.

6.5. Bezbjednosni zahtjevi za računare

6.5.1. Specifični bezbjednosni zahtjevi za računare

Hardver i softver koje koristi CBCG-CA jesu standardni (eng. off-the-shelf) proizvodi koji su dodatno bezbjednosno ojačani po preporukama CIS Benchmarks (https://www.cisecurity.org/cis-benchmarks/).

6.5.2. Nivo bezbjednosne zaštite računara

Operativni sistemi i drugi korišćeni proizvodi su standardni (eng. off-the-shelf) proizvodi.

6.6. Tehnička kontrola životnog ciklusa certifikacionog tijela

6.6.1. Kontrola razvoja sistema

Aplikacije i proizvodi koje koristi CBCG-CA su standardni (*eng. off-the-shelf*) proizvodi.

6.6.2. Upravljanje bezbjednošću

Operativni sistemi na kojima funkcioniše softver CBCG-CA su bezbjednosno ojačani (*eng. hardened*) u skladu sa preporukama najbolje prakse (vidjeti i poglavlje 6.5.).

Mrežni segmenti, u kojima su instalirani serveri davaoca usluga povjerenja, odvojeni su od ostalih mreža. Bezbjednost između mrežnih segmenata je obezbijeđena korišćenjem požarnih pregrada (Firewall) sa IPS funkcionalnošću.

Prije uspostavljanja produkcionog okruženja izvršeno je testiranje bezbjednosti (*eng. vulnerability scan*) sistema CBCG-CA. Testiranje bezbjednosti se izvodi najmanje jednom u tri mjeseca.

6.6.3. Bezbjednosna ocjena (*eng. Security Ratings*) životnog ciklusa

Nije primjenljivo.

6.7. Bezbjednosne kontrole na nivou računarske mreže

Serveri usluga CBCG-CA su postavljeni u DMZ, koji je zaštićen firewall uređajem sa IPS funkcionalnošću. Do servera je dozvoljen samo eksplicitno specifikovan promet.

6.8. Sistemska vremenska oznaka

Datum i vrijeme su dodati svim sistemskim i aplikativnim logovima. Sistemsko vrijeme je sinhronizovano sa više eksternih resursa. Za sinhronizaciju se koristi NTP protokol.

7. PROFIL CERTIFIKATA I LISTA OPOZVANIH CERTIFIKATA

7.1. Profil certifikata

Certifikati koje izdaje CBCG-CA ispunjavaju zahteve ITU-T X.509 [14], RFC 5280 [3] i RFC 6818 [13] standarda, kao i ETSI EN 319 412 Part1 [5], ETSI EN 319 412 Part2 [6] i ETSI EN 319 412 Part3 [7].

7.1.1. Verzija certifikata

Certifikati sadrže sljedeće osnovne oznake:

X.509 oznaka	Opis
Signature	Digitalni potpis certifikacionog tijela
Issuer	Jedinstveno ime certifikacionog tijela
Validity	Period validnosti certifikata
Subject	Jedinstveno ime korisnika certifikata
subjectPublicKeyInformation	Oznaka algoritma ključa
Version	X.509 verzija certifikata
serialNumber	Jedinstveni serijski broj certifikata

7.1.2. Ekstenzije certifikata

Ekstenzije su namijenjene korišćenju dodatnih atributa u X.509 v3 certifikatima. Standardne ekstenzije su definisane u skladu sa RFC 5280, koji dozvoljava i korišćenje sopstvenih ekstenzija za privatne potrebe certifikacionog tijela.

Ekstenzije u certifikatima korjenskih certifikacionih tijela su:

X.509 ekstenzija	Opis
subjectKeyIdentifier	Sažeta vrijednost javnog ključa certifikacionog tijela
keyUsage	Svrha upotrebe javnog ključa kao što je definisano u poglavlju 6.1.7. Polje je obilježeno kao kritično.
basicConstraints	Polje ima vrijednost *true* u certifikatima certifikacionih tijela CBCG-CA. Polje je obilježeno kao kritično.

Ekstenzije u certifikatima potvrdama podređenih certifikacionih tijela su:

X.509 ekstenzija	Opis
authorityKeyIdentifier	Sažeta vrijednost javnog ključa korjenskog certifikacionog tijela

subjectKeyIdentifier	Sažeta vrijednost javnog ključa certifikacionog tijela
keyUsage	Svrha upotrebe javnog ključa kao što je definisano u poglavlju 6.1.7. Polje je obilježeno kao kritično.
certificatePolicies: CertPolicyID CPS URI	 anyPolicy OID { 2 5 29 32 0 } Internet adresa do CBCG-CA Praktičkih pravila
CRLDistributionPoints	Adrese na kojima je objavljena lista opozvanih certifikata.
basicConstraints	Polje ima vrijednost *true* u certifikatima certifikacionih tijela . Polje je obilježeno kao kritično.
authorityInfoAccess	Polje sadrži http adresu servera OCSP

Ekstenzije u korisničkim certifikatima su:

X.509 ekstenzija	Opis
authorityKeyIdentifier	Sažeta vrijednost javnog ključa certifikacionog tijela
subjectKeyIdentifier	Sažeta vrijednost javnog ključa korisnika
keyUsage	Svrha upotrebe javnog ključa kao što je definisano u poglavlju 6.1.7. Polje je obilježeno kao kritično.
extendedKeyUsage	Proširena svrha korišćenja certifikata kao što je definisano u poglavlju 6.1.7.
certificatePolicies: CertPolicyID CPS URI	 Identifikaciona oznaka certifikata u skladu sa poglavljem 1.2. Internet adresa do CBCG-CA Praktičkih pravila
CRLDistributionPoints	Adrese na kojima je objavljena lista opozvanih certifikata.
basicConstraints	Polje nije prisutno ili ima vrijednost *false*. Ako je polje prisutno označeno je kao kritično.
authorityInfoAccess	Polje sadrži http adresu na kojoj je objavljen certifikat certifikacionog tijela i http adresu servera OCSP.

Ekstenzije u certifikatima OCSP u skladu su sa RFC 5280 i RFC 6960.

7.1.3. Identifikacijske oznake (eng. object identifiers) algoritama

Algoritam	Identifikacijska oznaka
RSA Encryption	1.2.840.113549.1.1.1
SHA256 with RSA Encryption	1.2.840.113549.1.1.11

7.1.4. Forme imena

Jedinstvena imena u certifikatima su u skladu sa standardom X.501 i X.509 (vidjeti i poglavlje 3.1.1.).

7.1.5. Ograničenja jedinstvenog imena

Nije primjenljivo.

7.1.6. Identifikacione oznaka certifikate

Svi certifikati izdati naručiocima sadrže identifikacionu oznaku politike u polju `certificatePolicies` (vidjeti i poglavlje 1.2.).

7.1.7. Korišćenje ekstenzije za ograničenja politike certifikata

Nije primjenljivo.

7.1.8. Specifični podaci o politici certifikata (*eng. Policy Qualifiers extension*)

Nije primjenljivo.

7.1.9. Procesiranje oznake kritičnosti ekstenzija u certifikatima

Aplikacije moraju procesirati ekstenzije u certifikatima u skladu sa preporukama RFC 5280 [3].

7.2. Profil liste opozvanih certifikata (CRL)

Liste opozvanih certifikata koje izdaje CBCG-CA ispunjavaju zahteve ITU-T X.509 [14], RFC 5280 [3] i RFC 6818 [13] standarda.

7.2.1. Verzija

Registri opozvanih certifikata sadrže sljedeće osnovna polja:

X.509 polje	Opis
Version	Verzija profila (v2)
Signature	Digitalni potpis certifikacionog tijela

Issuer	Jedinstveno razlikovno ime certifikacionog tijela
thisUpdate	Vrijeme izdavanja CRL
nextUpdate	Vrijeme izdavanja nasljedne CRL
revokedCertificates	Serijski brojevi opozvanih certifikata

7.2.2. Ekstenzije lista opozvanih certifikata

CBCG-CA koristi X.509 Version 2 CRL ekstenzije koje su navedene u sljedećoj tabeli:

X.509 polje	Opis
CRLNumber	Serijski broj CRL
reasonCode	Kod razloga za opoziv: (0) unused (1) keyCompromise (2) cACompromise (3) affiliationChanged (4) superseded (5) cessationOfOperation (6) certificateHold
invalidityDate	Datum i vrijeme opoziva

7.3. Profil OCSP

Profil OCSP poruka (zahtjev/odgovor) usluge OCSP je u skladu sa RFC 6960 [13].

8. PROVJERA USAGLAŠENOSTI I OSTALE FORME KONTROLE

Interna revizija CBCG-CA se vrši u skladu sa odredbama Zakona o Centralnoj banci Crne Gore i Pravilnika o internoj reviziji Centralne banke Crne Gore.

9. OSTALA POSLOVNA I PRAVNA PITANJA

U vezi sa odgovarajućim odredbama, vidjeti poglavlje 9 u dokumentu CBCG-CA Politika.

Reference:

[1] RFC 3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework"

[2] EN 319 411-1 "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements"

[3] RFC 5280 "Internet X.509 Public Key Infrastructure Certificates and Certificate Revocation List (CRL) Profile"

[4] EN 319 401 "General Policy Requirements for Trust Service Providers"

[5] EN 319 412 Part1: "Overview and common data structures"

[6] EN 319 412 Part2: "Certificate profile for certificates issued to natural persons"

[7] EN 319 412 Part3: "Certificate profile for certificates issued to legal persons"

[8] Zakon o elektronskoj identifikaciji i elektronskom potpisu ("Službeni list CG", br. 31/17 i 72/19)

[9] Pravila rada platnog sistema Centralne banke Crne Gore ("Sl. list Crne Gore", br. 48/14 i 57/14)

[10] Pravilnik o mjerama i aktivnostima za zaštitu certifikata za elektronski potpis i elektronski pečat ("Službeni list CG", br. 53/18 i 20/20)

[11] Pravilnik o bližoj sadržini i načinu vođenja evidencije davalaca elektronskih usluga povjerenja i registra kvalifikovanih davalaca elektronskih usluga povjerenja ("Službeni list CG", broj 20/20)

[12] Politika Centralne banke Crne Gore za davanje elektronske usluge povjerenja izrade certifikata za napredni elektronski pečat za učesnike u Platnom sistemu Centralne banke

[13] RFC 6818: Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

[14] ITU-T Recommendation X.509: ISO/IEC9594-8:2008, Information Technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks

[15] RFC 6960: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP

[16] PKCS#12: Personal Information Exchange Syntax Standard