

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

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

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

Zaštita dokumenta

Sva prava zadržana. Nije dozvoljena reprodukcija sadržaja u cjelosti ili djelimično ni na koji način i ni na kakvom mediju bez pisanog odobrenja autora. Kršenje se sankcioniše u skladu sa propisima kojima se uređuju autorska prava, krivičnim i drugim važećim zakonodavstvom.

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

Sadržaj

1.	UVOD	6
1.1.	Pregled	6
1.2.	Naziv dokumenta i identifikacijske oznake certifikata	8
1.3.	Učesnici infrastrukture javnih ključeva	9
1.3.1.	Certifikaciona tijela	9
1.3.2.	Poslovi registracije (Registration Authority - RA)	10
1.3.3.	Naručioci i korisnici digitalnih certifikata	10
1.3.4.	Treća lica	11
1.3.5.	Ostali učesnici	11
1.4.	Svrha upotrebe certifikata	11
1.4.1.	Dozvoljena upotreba certifikata	11
1.4.2.	Nedozvoljena upotreba certifikata	11
1.5.	Upravljanje dokumentom	11
1.5.1.	Organizacija koja upravlja ovim dokumentom	11
1.5.2.	Kontakt podaci	11
1.5.3.	Utvrđivanje adekvatnosti i kompatibilnost praktičnih pravila spoljnih CA sa Praktičnim pravilima	12
1.5.4.	Postupak odobrenja Politike	12
1.6.	Definicije i skraćenice	12
2.	OBJAVE I REPOZITORIJUM	15
2.1.	Repozitorijum	15
2.2.	Objave informacija o certifikatima	15
2.3.	Vrijeme i učestalost objava	15
2.4.	Pristup podacima u repozitorijumu	15
3.	PREPOZNAVANJE I PROVJERA ISTOVJETNOSTI	17
4.	UPRAVLJANJE CERTIFIKATIMA	18
5.	FIZIČKA ZAŠTITA I ORGANIZACIONE BEZBJEDNOSNE MJERE I ZAHTJEVI ZA ZAPOSLENE	19
6.	TEHNIČKI BEZBJEDNOSNI zahtjevi	20
7.	PROFIL CERTIFIKATA I LISTA OPOZVANIH CERTIFIKATA	21
7.1.	Profil certifikata	21
7.2.	Profil liste opozvanih certifikata (CRL)	21
7.3.	Profil OCSP	21
8.	PROVJERA USAGLAŠENOSTI I OSTALE FORME KONTROLE	22
9.	OSTALA POSLOVNA I PRAVNA PITANJA	23
9.1.	Cjenovnik	23
9.1.1.	Cijena izdavanja i upravljanja certifikatima	23

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

9.1.2.	Cijena pristupa certifikatima u javnom imeniku.....	23
9.1.3.	Cijena pristupa listi opozvanih certifikata	23
9.1.4.	Cijena ostalih usluga	23
9.1.5.	Pravo povraćaja.....	23
9.2.	Osiguranje od odgovornosti	23
9.3.	Povjerljivost informacija.....	23
9.3.1.	Obim povjerljivih informacija	23
9.3.2.	Informacije van obima povjerljivih informacija	23
9.3.3.	Odgovornost za obezbjeđivanje povjerljivosti informacija	24
9.4.	Zaštita podataka o ličnosti	24
9.4.1.	Plan obezbjeđivanja zaštite podataka o ličnosti.....	24
9.4.2.	Obim zaštićenih podataka o ličnosti	24
9.4.3.	Podaci o ličnosti koji se ne smatraju povjerljivim	24
9.4.4.	Odgovornost za zaštitu podataka o ličnosti	24
9.4.5.	Pristanak za korišćenje podataka o ličnosti	24
9.4.6.	Prosljeđivanje podataka o ličnosti u sudskim i upravnim postupcima	24
9.5.	Zaštita intelektualne svojine	24
9.6.	Odgovornost i garancije	25
9.6.1.	Odgovornost i garancije davaoca usluga povjerenja.....	25
9.6.2.	Odgovornost i garancije zaposlenih koji obavljaju poslove registracije	25
9.6.3.	Odgovornost i garancije korisnika certifikata.....	25
9.6.4.	Odgovornost i garancije trećih lica	26
9.6.5.	Odgovornost i garancije drugih učesnika	26
9.7.	Isključenje odgovornosti	26
9.8.	Ograničenja odgovornosti.....	27
9.9.	Naknada štete	27
9.10.	Početak i prestanak važenja	27
9.10.1.	Početak važenja.....	27
9.10.2.	Prestanak važenja.....	27
9.10.3.	Učinak i posljedice prestanka važenja	27
9.11.	Obavještenje i komunikacija sa učesnicima	28
9.12.	Promjene dokumenta	28
9.12.1.	Postupak pripreme izmjena i dopuna	28
9.12.2.	Postupak obavještanja	28
9.12.3.	Promjene koje zahtijevaju novu identifikacionu oznaku politike.....	28
9.13.	Rješavanje sporova	28
9.14.	Regulativa	29
9.15.	Usaglašenost sa regulativom.....	29

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

9.16. Opšte odredbe	29
9.16.1. Ostali obavezujući dokumenti.....	29
9.16.2. Prenos prava i obaveza.....	29
9.16.3. Posljedice ništavosti odredaba ove Politike i Praktičnih pravila	29
9.16.4. Ostvarivanje povraćaja troškova u slučaju sporova.....	29
9.16.5. Viša sila.....	29
9.17. Ostale odredbe	30

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).

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: 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: Praktična pravila).

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

Praktična pravila opisuju kako davalac elektronske usluge povjerenja upravlja svojom uslugom. Za elektronsku uslugu povjerenja koju nudi davalac, Praktična pravila opisuju način na koji ispunjava zakonske, tehničke, organizacione i proceduralne zahtjeve poslovanja.

1.1. Pregled

Ovaj dokument opisuje Politiku kojom upravlja CBCG.

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.

Politika je dio javnih pravila djelovanja davaoca elektronske usluge povjerenja CBCG-CA. Povjerljivi dio internih pravila djelovanja davaoca elektronske usluge povjerenja CBCG-CA predstavlja interni poslovnik za upravljanje uslugama i informacionom bezbjednošću CBCG.

Struktura Politike je usaglašena sa standardom RFC 3647 [1]. Određena poglavlja RFC 3647, koja nijesu primjenljiva za CBCG-CA su izostavljena ili navedena ali sadrže tekst „Nije primjenljivo”.

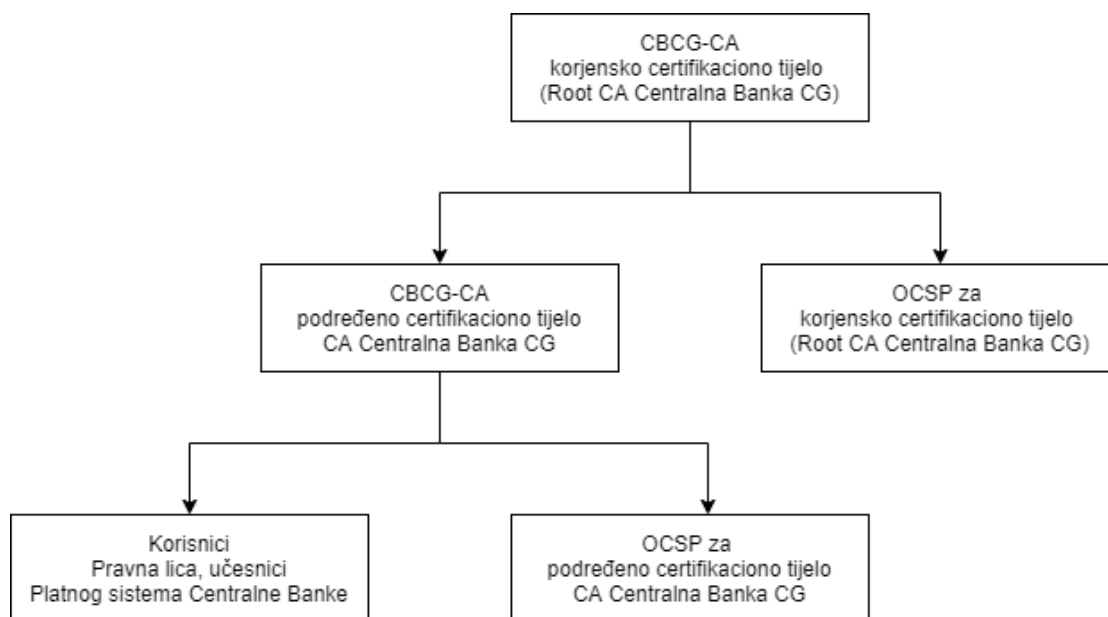
Sadržaj Politike usaglašen je sa standardima: RFC 3647 [1], RFC 5280 [3], EN 319 401 [4] i EN 319 411-1 [2].

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

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

Na Slika 1: Hijerarhija PKI infrastrukture CBCG-CA, prikazana je hijerarhija izdavanja certifikata u okviru certifikacionih tijela CBCG-CA:

- CBCG-CA korjensko certifikaciono tijelo koje izdaje certifikate CBCG-CA podređenom certifikacionom tijelu i za server usluge OCSP;
- CBCG-CA podređeno certifikaciono tijelo koje izdaje certifikate korisnicima i za server usluge OCSP.



Slika 1: Hijerarhija PKI infrastrukture CBCG-CA

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

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 skraćena za Organization Identifier (organizationIdentifier).

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

CBCG-CA izdaje digitalne certifikate naručiocima (vidjeti i poglavlje 1.3.3.), koji su učesnici u PSCB u skladu sa Pravilima rada Platnog sistema Centralne banke Crne Gore [9].

Politika definiše sljedeće kategorije digitalnih certifikata koje izdaje CBCG-CA:

- Nekvalifikovane certifikate 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 Politici 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 identifikacijske oznake certifikata

Naziv dokumenta, cr.: Politika 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.: Certificate policy of the CBCG-CA

Verzija: v. 1.0

Datum: 15.12.2021.

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

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

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 kategorijama 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} dodjeljuje se interno.

1.3. Učesnici infrastrukture javnih ključeva

1.3.1. Certifikaciona tijela

Certifikaciona tijela koja djeluju u okviru CBCG-CA, pružaju usluge povjerenja u skladu sa Politikom i Zakonom o elektronskoj identifikaciji i elektronskom potpisu i odgovarajućim pravilnicima i standardima.

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

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

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 PSCB (vidi 1.3.3.), 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 CBCG.

1.3.1.1. Komitet Certifikacionog tijela CBCG za pružanje elektronskih usluga povjerenja (Policy Management Authority - PMA)

Komitet Certifikacionog tijela CBCG za pružanje elektronskih usluga povjerenja, njegovi zadaci i ciljevi, utvrđeni su posebnom odlukom.

1.3.1.2. Operativni poslovi (Operations Authority - OA)

Operativni poslovi CBCG – CA su definisani posebnom odlukom.

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.

Poslove registracije obavljaju zaposleni CBCG.

1.3.3. Naručioци 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 u zatvorenom okruženju PSCB
CBCG OCSP	Za OCSP servise u okviru CBCG-CA
CBCG PKI	Za upravljanje servisa u okviru CBCG-CA

1.4.2. Nedoželjena upotreba certifikata

Certifikati izdati od strane CBCG-CA mogu se koristiti samo u skladu sa Politikom, Praktičnim pravilima i zakonom (vidjeti poglavlje 9.14.).

1.5. Upravljanje dokumentom

1.5.1. Organizacija koja upravlja ovim dokumentom

Politikom 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 Praktičnim pravilima

CBCG-CA ne radi međusobno priznavanje na nivou davaoca usluga povjerenja.

1.5.4. Postupak odobrenja Politike

Politiku, odnosno njene izmjene i/ili dopune, donosi Guverner. Ova politika 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.

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

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:

CA	Certification Authority
PKI	Public Key Infrastructure
CRL	Lista opozvanih certifikata
OID	Object Identifier
CN	Common Name
DN	Distinguished Name
PMA	Policy Management Authority
RA	Registration Authority (Poslovi registracije)
OCSP	Online Certificate Status Protocol
OI	Organization Identifier (polje <code>organizationIdentifier</code> u jedinstvenom imenu)

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

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. Objave informacija o certifikatima

CBCG-CA javno objavljuje:

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

CBCG-CA čini dostupnim ili šalje korisnicima dokumente 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

Lista opozvanih certifikata se ažurira na način kako je definisano u poglavlju 4.9.7. Praktičnih pravila. Sve ostale informacije se objavljuju čim dođe do promjena ili kada postanu dostupne.

2.4. Pristup podacima u repozitorijumu

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

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

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

3. PREPOZNAVANJE I PROVJERA ISTOVJETNOSTI

Prepoznavanje i provjera istovjetnosti za certifikate koje izdaje CBCG-CA sprovodi se u skladu sa ovom politikom, Praktičnim pravilima, Pravilima rada Platnog sistema Centralne banke Crne Gore, Zakonom o elektronskoj identifikaciji i elektronskom potpisu Crne Gore [7], ostalim propisima (vidjeti poglavlje 9.14 ove politike) i relevantnim standardima (EN 319 411-1 [2]).

Način na koji se sprovodi prepoznavanje i provjera istovjetnosti za certifikate koje izdaje CBCG-CA opisan je u Praktičnim pravilima.

4. UPRAVLJANJE CERTIFIKATIMA

Upravljanje certifikatima koje izdaje CBCG-CA sprovodi se u skladu sa ovom politikom, Praktičnim pravilima, Pravilima rada Platnog sistema Centralne banke Crne Gore, Zakonom o elektronskoj identifikaciji i elektronskom potpisu Crne Gore [7], ostalim propisima (vidjeti poglavlje 9.14 ove politike) i relevantnim standardima (EN 319 411-1 [2]).

Način upravljanja certifikatima koje izdaje CBCG-CA opisan je u Praktičnim pravilima.

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

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

Fizička zaštita i organizacione bezbjednosne mjere za certifikate koje izdaje CBCG-CA sprovodi se u skladu sa ovom politikom, Praktičnim pravilima, Pravilima rada Platnog sistema Centralne banke Crne Gore, Zakonom o elektronskoj identifikaciji i elektronskom potpisu Crne Gore [7], ostalim propisima (vidjeti poglavlje 9.14 ove politike) i relevantnim standardima (EN 319 411-1 [2]).

Fizička zaštita i organizacione bezbjednosne mjere za certifikate koje izdaje CBCG-CA opisani su u Praktičnim pravilima.

6. TEHNIČKI BEZBJEDNOSNI ZAHTJEVI

CBCG-CA sprovodi tehničke bezbjednosne kontrole koje ispunjavaju zahtjeve u skladu sa ovom politikom, Praktičnim pravilima, Pravilima rada Platnog sistema Centralne banke Crne Gore, Zakonom o elektronskoj identifikaciji i elektronskom potpisu Crne Gore [7], ostalim propisima (vidjeti poglavlje 9.14. ove politike) i relevantnim standardima (EN 319 411-1 [2]).

Naručioci, korisnici i treća lica moraju da koriste pouzdane računare i softver.

Tehničke bezbjednosne mjere koje sprovodi CBCG-CA opisane su u Praktičnim pravilima.

7. PROFIL CERTIFIKATA I LISTA OPOZVANIH CERTIFIKATA

7.1. Profil certifikata

Certifikati koje izdaje CBCG-CA ispunjavaju zahtjeve 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]. Odstupanja su opisana, kada je potrebno, u Praktičkim pravilima.

Profili certifikata opisani su u Praktičnim pravilima.

7.2. Profil liste opozvanih certifikata (CRL)

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

Profili liste opozvanih certifikata opisani su u Praktičnim pravilima.

7.3. Profil OCSP

Profil OCSP poruka (zahtjev/odgovor) usluge OCSP je u skladu sa RFC 6960 [16].

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

8. PROVJERA USAGLAŠENOSTI I OSTALE FORME KONTROLE

Način sprovođenja provjere usaglašenosti i ostalih formi kontrole opisan je u
Praktičnim pravilima.

9. OSTALA POSLOVNA I PRAVNA PITANJA

9.1. Cjenovnik

9.1.1. Cijena izdavanja i upravljanja certifikatima

Nije primjenljivo.

9.1.2. Cijena pristupa certifikatima u javnom imeniku

Nije primjenljivo.

9.1.3. Cijena pristupa listi opozvanih certifikata

Provjera statusa certifikata putem liste opozvanih certifikata ili usluge OCSP je besplatna za sve naručioce, korisnike i treća lica.

9.1.4. Cijena ostalih usluga

Nije primjenljivo.

9.1.5. Pravo povraćaja

Nije primjenljivo.

9.2. Osiguranje od odgovornosti

Nije primjenljivo.

9.3. Povjerljivost informacija

9.3.1. Obim povjerljivih informacija

Poslovnom tajnom se smatra podatak ili informacija koja je kao takva označena u skladu sa zakonom ili aktom CBCG.

Poslovnom tajnom se smatraju i podaci ili informacije koji nijesu označeni kao poslovna tajna ukoliko bi njihovim objavljivanjem mogla nastati šteta za CBCG ili bio narušen ugled CBCG.

9.3.2. Informacije van obima povjerljivih informacija

Informacije koje su objavljene u certifikatima i CRL ili druge informacije u javnim repozitorijumima CBCG-CA, ne smatraju se povjerljivim.

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

9.3.3. Odgovornost za obezbjeđivanje povjerljivosti informacija

CBCG-CA je odgovoran za zaštitu povjerljivih informacija, u skladu sa zakonom i Pravilnikom o tajnosti.

9.4. Zaštita podataka o ličnosti

9.4.1. Plan obezbjeđivanja zaštite podataka o ličnosti

U pružanju elektronske usluge povjerenja CBCG-CA vrši prikupljanje podataka o ličnosti u skladu sa zakonom i opštim aktom CBCG kojim se uređuje zaštita podataka o ličnosti.

9.4.2. Obim zaštićenih podataka o ličnosti

Sve informacije o korisniku certifikata ili naručiocu, koje nijesu objavljene u certifikatu, smatraju se povjerljivim.

9.4.3. Podaci o ličnosti koji se ne smatraju povjerljivim

Podaci o ličnosti sadržani u certifikatu, CRL ili druge informacije objavljene u javnim repozitorijumima CBCG-CA ne smatraju se povjerljivim.

9.4.4. Odgovornost za zaštitu podataka o ličnosti

CBCG-CA je odgovoran za zaštitu podataka o ličnosti u skladu sa zakonom i propisima kojima se uređuje zaštita podataka o ličnosti.

9.4.5. Pristanak za korišćenje podataka o ličnosti

Naručilac će se prije izdavanja certifikata upoznati sa podacima koji će biti sadržani u certifikatu.

Naručilac se davanjem saglasnosti sa uslovima korišćenja certifikata slaže i sa svrhom njihove upotrebe.

9.4.6. Prosljeđivanje podataka o ličnosti u sudskim i upravnim postupcima

Povjerljive informacije mogu se učiniti dostupnim sudu i drugim nadležnim organima u skladu sa zakonom i propisom CBCG.

9.5. Zaštita intelektualne svojine

CBCG je vlasnik svih intelektualnih prava na certifikatima i pripadajućoj dokumentaciji.

Naručilac ima, za period trajanja ugovora sa CBCG kao davaocem elektronski usluga povjerenja, pravo na upotrebu certifikata i pripadajuće dokumentacije u skladu sa ovom politikom.

9.6. Odgovornost i garancije

9.6.1. Odgovornost i garancije davaoca usluga povjerenja

CBCG-CA izdaje certifikate i preduzima druge aktivnosti povezane sa upravljanjem certifikatima i infrastrukturom CBCG-CA u skladu sa zakonom, ovom politikom i Praktičnim pravilima.

CBCG-CA:

- Obezbjeđuje da su podaci o korisniku u certifikatu identični dostavljenim;
- Provjerava identitet podnosioca zahtjeva prije izdavanja certifikata;
- Obezbjeđuje tačnost i sveobuhvatnost informacija objavljenih u javnim repozitorijumima;
- Izdaje certifikate naručiocima u skladu sa ovom politikom i Praktičnim pravilima;
- Opoziva certifikate nakon prijema zahtjeva ili iz drugih razloga u skladu sa ovom politikom i Praktičnim pravilima;
- Redovno izdaje i objavljuje listu opozvanih certifikata;
- Obezbjeđuje pristup listi opozvanih certifikata i usluge OCSP;
- Obezbjeđuje da su zaposleni i spoljni izvođači upoznati sa odredbama ove politike i Praktičnih pravila.

9.6.2. Odgovornost i garancije zaposlenih koji obavljaju poslove registracije

Zaposleni koji obavljaju poslove registracije su odgovorni za potpunost informacija o naručiocima na odobrenim obrascima za prijavu i identičnost podataka sa podacima na dostavljenom dokumentu. Detaljnije obaveze navedene su u relevantnim djelovima ove politike, Praktičnih pravila i ako je primjenjivo, u ugovoru sa spoljnjim izvođačem.

9.6.3. Odgovornost i garancije korisnika certifikata

Pored ispunjavanja obaveza koje proističu iz ove politike i Praktičnih pravila, naručilac mora:

- Obezbijediti povjerljivost svojih privatnih kriptografskih ključeva i poštovati sve mjere da se spriječi gubitak, objelodanjivanje, promjena ili neovlašćena upotreba;
- Pažljivo zaštititi kod (lozinku, PIN) za aktiviranje privatnih ključeva;

- Odmah obavijestiti CBCG-CA u slučaju bilo kakvih nepravilnosti ili u slučaju promjene podataka sadržanih u certifikatu;
- Isključivo koristiti svoje kriptografske ključeve i pripadajuću digitalnu potvrdu za svrhe navedene u poglavlju 1.4. Praktičnih pravila;
- U slučaju ugrožavanja ili sumnje na ugrožavanje privatnog ključa, odmah obavijestiti CBCG-CA i opozvati pripadajuću digitalnu potvrdu;
- U slučaju zloupotrebe ili sumnje u zloupotrebu bilo koje potvrde koju je izdao CBCG-CA, o tome odmah obavijestiti CBCG-CA.

9.6.4. Odgovornost i garancije trećih lica

Treća lica moraju, prije nego što se oslone na certifikate CBCG-CA, obavezno provjeriti validnost i status certifikata. Pored toga moraju:

- Biti svjesni svrhe upotrebe i ograničenja upotrebe pojedinačnog certifikata i ograničenja odgovornosti CBCG-CA, kao što je opisano u ovoj politici i Praktičnim pravilima;
- Ograničiti upotrebu certifikata isključivo na svrhe navedene u poglavlju 1.4. Praktičnih pravila;
- Prije svakog prihvatanja provjeriti da certifikat nije bio opozvan;
- U slučaju zloupotrebe ili sumnje na zloupotrebu bilo koje potvrde koju je izdao CBCG-CA, o tome odmah obavijestiti CBCG-CA.

9.6.5. Odgovornost i garancije drugih učesnika

Nije primjenljivo.

9.7. Isključenje odgovornosti

Osim za slučajeve iz tačke 9.6.1. CBCG-CA ne odgovara za štetu, bilo da se radi o običnoj šteti, izmakloj koristi ili nematerijalnoj šteti, koja proističe iz ili u vezi sa korišćenjem certifikata davaoca usluga povjerenja CBCG-CA i sa njima povezanih ključeva.

CBCG-CA naročito isključuje:

- Svaku odgovornost, ako je potvrda izdata kao rezultat greške, nevjerodostojnosti podataka prosljeđenih od strane naručioca ili drugih radnji naručilaca odnosno korisnika ili bilo kog drugog fizičkog ili pravnog lica;
- Svaku odgovornost ako je certifikat korišćen po isteku perioda validnosti;
- Svaku odgovornost ako je certifikat korišćen nakon opoziva i objavljen na listi opozvanih certifikata;
- Svaku odgovornost za eventualnu štetu koja može nastati od trenutka kada CBCG-CA primi važeći zahtjev za opoziv do trenutka objave informacija o

opozivu na listi opozvanih certifikata u skladu sa poglavljem 4.9.5. Praktičnih pravila;

- Svaku odgovornost ako je privatni ključ naručioca/korisnika objelodanjen ili postoji sumnja da je bio objelodanjen;
- Svaku odgovornost, ako je certifikat korišćen u druge svrhe nego što je dozvoljeno u ovoj politici i Praktičnim pravilima, ili u suprotnosti sa zakonom;
- Svaku odgovornost, ako naručilac, korisnik ili treće lice nije postupalo u skladu sa ovom politikom i Praktičnim pravilima ili eventualnim drugim ugovorom;
- Svaku odgovornost, ako je nastala šteta zbog greške u djelovanju hardverske ili softverske opreme naručioca/korisnika ili trećeg lica;
- Odgovornost za štetu koja bi nastala zbog više sile kao što je opisano u poglavlju 9.16.5. ove politike.

9.8. Ograničenja odgovornosti

CBCG-CA ne odgovara za štetu koja bi nastala prilikom upotrebe certifikata zbog postupanja suprotno odredbama ove politike i Praktičnih pravila od strane naručioca, korisnika ili trećih lica.

CBCG-CA ne odgovara za bilo koju štetu nastalu u vezi sa izdavanjem ili korišćenjem certifikata, osim ako je šteta rezultat namjere ili grube nepažnje njenih zaposlenih, u kom slučaju se primjenjuju odredbe Zakona o obligacionim odnosima o odgovornosti privrednog društva i drugih pravnih lica prema trećem.

9.9. Naknada štete

Svaka stranka snosi odgovornost za štetu koju pretrpi CBCG-CA, a koja je posljedica nepravilne upotrebe certifikata, ili ako ne postupa u skladu sa zakonom, Politikom i Praktičnim pravilima.

9.10. Početak i prestanak važenja

9.10.1. Početak važenja

Politika stupa na snagu danom donošenja, a u skladu sa posebnom odlukom.

9.10.2. Prestanak važenja

Važenje ove politike nije vremenski ograničeno.

9.10.3. Učinak i posljedice prestanka važenja

U slučaju prestanka važenja Politike ili Praktičnih pravila zbog donošenja novih, a koji sadrži nove oznake u polju `certificatePolicies`, svi subjekti koriste postojeće

certifikate u skladu sa odredbama Praktičnih pravila i Politike, po kojoj su bili izdati. U slučaju da zbog izmijenjenih okolnosti to više ne bude moguće, CBCG-CA će prilikom donošenja nove verzije Praktičnih pravila ili ove politike o tome obavijestiti naručioce.

U slučaju kada nova verzija Praktičnih pravila ili ove politike sadrži jednake identifikacione oznake u polju `certificatePolicies`, svi subjekti koriste postojeće certifikate u skladu sa odredbama nove verzije Praktičnih pravila i ove politike.

9.11. Obavještenje i komunikacija sa učesnicima

CBCG-CA objavljuje ovu politiku i Praktična pravila na internet stranici, na adresi navedenoj u poglavlju 2.1.

9.12. Promjene dokumenta

9.12.1. Postupak pripreme izmjena i dopuna

Komitet Certifikacionog tijela CBCG za pružanje elektronskih usluga povjerenja razmatra nacрте izmjena i dopuna Praktičnih pravila i Politike, dostavljenih od zaposlenih koji obavljaju operativne poslove CBCG-CA. Nakon izvršenog usaglašavanja prijedlozi dokumenata se dostavljaju Guverneru na usvajanje.

9.12.2. Postupak obavješćavanja

CBCG-CA će preko elektronske pošte obavijestiti naručioca o promjenama koje imaju materijalni uticaj na naručioce ili treće strane.

Ako procijeni CBCG-CA može odlučiti, da ne obavijesti naručioce i treće strane u slučaju promjena koje nemaju materijalni uticaj na korišćenje certifikata. U tom slučaju promjene će se objaviti u rokovima definisanim u poglavlju 2.3, samo na internet stranici na adresi navedenoj u poglavlju 2.1.

9.12.3. Promjene koje zahtijevaju novu identifikacionu oznaku politike

Identifikaciona oznaka politike certifikata sadržana u polju `certificatePolicies`, biće promijenjena samo u slučaju promjena koje imaju materijalni uticaj na naručioce ili treće strane.

9.13. Rješavanje sporova

Nastali sporovi, ako je to moguće, biće riješeni sporazumno, a ukoliko se sporazum ne postigne utvrđuje se nadležnost suda u Podgorici.

9.14. Regulativa

CBCG-CA u pružanju elektronske usluge povjerenja djeluje u skladu sa:

- propisima kojima se uređuje elektronska identifikacija i elektronski potpis,
- propisima kojima se uređuje zaštita podataka o ličnosti i
- drugim propisima koji se odnose na oblast koja je predmet ove politike i Praktičnih pravila.

9.15. Usaglašenost sa regulativom

CBCG-CA postupa u skladu sa propisima navedenim u poglavlju 9.14. ove politike.

9.16. Opšte odredbe

9.16.1. Ostali obavezujući dokumenti

Nije primjenljivo.

9.16.2. Prenos prava i obaveza

Naručilac ili korisnik certifikata ne smije ni u jednom slučaju prenijeti prava i obaveze korišćenja certifikata djelimično ili u cjelosti na treća lica.

9.16.3. Posljedice ništavosti odredaba ove Politike i Praktičnih pravila

Ništavost jednog ili više djelova ove politike ili Praktičnih pravila ne utiče na važenje drugih odredaba, ako nemaju uticaj na stepen povjerenja u certifikat i korišćenje certifikata.

9.16.4. Ostvarivanje povraćaja troškova u slučaju sporova

Nije primjenljivo.

9.16.5. Viša sila

Viša sila je budući i neizvjestan događaj, koji se nije mogao predvidjeti ni izbjeći, niti su na njega strane u poslovnom odnosu mogle uticati.

CBCG, naručilac, odnosno korisnik certifikata i treća lica ne mogu biti odgovorni za štetu koja je nastala uslijed događaja kao rezultat više sile.

Ukoliko je zbog više sile privremeno onemogućeno izvršenje neke obaveze prema ovoj politici ili ugovoru, rok za izvršenje se srazmjerno produžava.

9.17. Ostale odredbe

Nije primjenljivo

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 Crne Gore ("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)

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

- [12] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites"
- [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] Praktična pravila Centralne banke Crne Gore za davanje elektronske usluge povjerenja izrade certifikata za napredni elektronski pečat za učesnike u Platnom sistemu Centralne banke
- [16] RFC 6960: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP