Pružalac usluga od poverenja Halcom A.D. Beograd (HALCOM BG CA)

Politika pružanja usluge

za izdavanje kvalifikovanih elektronskih sertifikata za elektronski potpis pravnih lica

CPName: HALCOM BG CA PL e-signature

CPOID: 1.3.6.1.4.1.5939.10.1.5

Dokument važi od:
12.07.2019.

Pregled prethodnih izdanja:

Izdanje	Broj dokumenata i priloga	Opis izmene	Autor	Datum poslednje izmene
1	79-6-4/10	Početno izdanje	Ana Stojaković	01.10.2010.
2	79-9-2/10	Izmena PUK KOD	Ana Stojaković	01.08.2014.
3	79-10-7/17	Novi podređeni/intermediate sertifikati	Ana Teodosić	16.08.2017.
4	79-12-2/18	Nova CA struktura i usaglašavanje sa novim zakonom	Ana Graovac	19.10.2018.
5	79-12-33/19	Izmena profila korisničkih sertifikata – dodavanje AR ID BROJA u CN	Ana Graovac	05.07.2019

Sadržaj

1.UVOD

(1) HALCOM BG CA za implementaciju svojih usluga u oblasti elektronskog potpisivanja i drugih usluga koristi najsigurnije tehnologije, uključujući korišćenje bezbednih prenosioca podataka. Ova politika je javni deo internih pravila HALCOM BG CA za kvalifikovane elektronske sertifikate za fizička lica, koja se identifikuju kao ovlašćena lica pravnog lica.

(2) HALCOM BG CA izdaje kvalifikovane elektronske sertifikate i druge usluge od poverenja u skladu sa važećim zakonom i podzakonskim aktima Republike Srbije, uredbom eIDAS, ETSI tehničkim zahtevima, standardom IETF RFC, standardom ISO/IEC i drugim srodnim standardima.

1.1. PREGLED

(1) Ova politika uređuje namenu, delovanje i metodologiju upravljanja kvalifikovanim elektronskim sertifikatima, kao i zahteve bezbednosti koje mora ispunjavati pružalac usluga od poverenja HALCOM BG CA, vlasnici kvalifikovanih elektronskih sertifikata, treća lica koji se uzdaju u te sertifikate, te odgovornost svih pomenutih lica.

(2) Pružalac usluga od poverenja HALCOM BG CA izdaje kvalifikovane sertifikate za elektronski potpis. HALCOM BG CA deluje u okviru Halcom a.d. Beograd.

(3) HALCOM BG CA izdaje dva kvalifikovana elektronska sertifikata (dva para asimetričnih ključeva) sa obaveznim korišćenjem bezbednosnog nosioca (smart kartice).

(4) Sve odredbe ove politike vezane za delovanje HALCOM BG CA su propisno i detaljno opisane u dokumentu Opšta pravila rada (CPS) i podrobnije utvrđene u odredbama internih pravila rada pružaoca usluga od poverenja koja predstavljaju dokumente poverljive prirode i koji definišu infrastrukturu, odredbe u vezi sa zaposlenim u HALCOM BG CA (nadležnosti, zadaci, ovlašćenja i zahtevani uslovi pojedinih zaposlenih), fizičku bezbednost (pristup prostorijama, upravljanje hardverskom i programskom opremom), programsku zaštitu (zaštitni softver, zaštitne kopije, …) i interni nadzor (kontrola fizičkih pristupa, ovlašćenja, …).

(5) HALCOM BG CA izdaje kvalifikovane elektronske sertifikate i druge usluge od poverenja u skladu sa važećim zakonom i podzakonskim aktima Republike Srbije, uredbom eIDAS, ETSI tehničkim zahtevima, standardom IETF RFC, standardom ISO/IEC i drugim srodnim standardima.

(6) Listu registracionih tela i operatera (RA – Registration Authority) koji omogućuju podnošenje zahteva za dobijanje kvalifikovanih elektronskih sertifikata za pravna lica od HALCOM BG CA, Halcom a.d. Beograd objavljuje na svojoj web stranici.

1.2. IDENTIFIKACIONI PODACI POLITIKE PRUŽANJA USLUGA OD POVERENJA

(1) Identifikaciona oznaka ove politike HALCOM BG CA je:

CPName: HALCOM BG CA PL e-signature

CPOID: 1.3.6.1.4.1.5939.10.1.5

(2) U svakom kvalifikovanom elektronskom sertifikatu izdatom od strane HALCOM BG CA se u Certificate Policy ekstenziji navodi gore pomenuti CPOID, pogledati poglavlje 7.1.2.

1.3. SUBJEKTI

1.3.1 PRUŽALAC USLUGA OD POVERENJA HALCOM BG CA

Pružalac usluga od poverenja HALCOM BG CA je pružalac usluga od poverenja koji izdaje i upravlja kvalifikovanim elektronskim sertifikatima za elektronsko potpisivanje i druge usluge. Pružalac usluga od poverenja HALCOM BG CA posluje u okviru Halcom a.d. Beograd.

1.3.2 REGISTRACIONA TELA HALCOM BG CA

(1) Registraciono telo (RA) HALCOM BG CA vrši sledeće aktivnosti za potrebe pružaoca usluga od poverenja:
   1. provera identitet fizičkih lica, pravnih lica, ovlašćenih lica pravnog lica i drugih, relevantnih podataka,
   2. prijem zahteva za dobijanje sertifikata,
   3. prijem zahteva za opozivanje/povlačenje sertifikata,
   4. izdavanje potrebne dokumentacije vlasnicima, odnosno budućim vlasnicima, kvalifikovanih elektronskih sertifikata,
   5. prosleđivanje zahteva i ostalih podataka sigurnim putem do HALCOM BG CA pružaoca usluga od poverenja,
   6. proveravaju identitet fizičkih lica i prijem zahteva za izdavanje sertifikata za sertifikate pružaoca usluga od poverenja HALCOM BG CA (vidi poglavlje 4.3.1).

(2) HALCOM BG CA kao pružalac usluga od poverenja, pored svog RA može ovlastiti druge organizacije u poslovnom i javnom sektoru. Svaku takvu organizaciju pružalac usluga od poverenja HALCOM BG CA ugovorom obavezuje za ispunjavanje strogih bezbednosnih uslova u skladu sa važećim evropskim, i nacionalnim propisima te međunarodnim, evropskim i nacionalnim standardima i preporukama, kao i internim pravilima HALCOM BG CA.

(3) Pružalac usluga od poverenja HALCOM BG CA ima široku uspostavljenu geografsku mrežu RA (registracionih tela), što budućim vlasnicima omogućuje jednostavnu prijavu u blizini sedišta datog pravnog ili fizičkog lica.

(4) Detaljan opis poslova i nadležnosti registracionih tela definisan je posebnim dokumentom, kao i ugovorom između registracionih tela i HALCOM BG CA.

1.3.3 NARUČIOCI I VLASNICI SERTIFIKATA

(1) Vlasnici kvalifikovanih elektronskih sertifikata, koji su ovlašćena fizička lica pravnog lica, koriste svoje podatke (par asimetričnih ključeva), dodeljene od strane pružaoca usluga od poverenja, za elektronsko potpisivanje.

(2) Vlasnik sertifikata je pravno lice, čije je ovlašćeno lice nosilac sertifikata.

Usluga	Izdavalac	Naručilac	Vlasnik
Sertifikati za pravne subjekte (e-potpis)	Halcom BG CA PL e-signature	Pravno lice	Fizičko lice

1.3.4 TREĆE STRANE

(1) Treće strane su entiteti, kao na primer fizička lica (pojedinci) i/ili pravna lica (kompanije), koja prihvataju sertifikate i verifikuju elektronski potpis određenih elektronskih dokumenata koji su potpisani od strane korisnika HALCOM BG CA, kao i

koja vrše validaciju kvalifikovanih elektronskih sertifikata izdatih od strane HALCOM BG CA.

(2) Treće strane moraju se ponašati u skladu sa uputstvima pružaoca usluga od poverenja HALCOM BG CA i moraju redovno proveravati validnost sertifikata, svrhu korišćenja sertifikata, kao i period važenja. Detaljnije obaveze i odgovornosti trećih strana su navedene u poglavlju 4.5.2. i 9.6.4.

(3) Treća lica nisu nužno i vlasnici kvalifikovanih elektronskih sertifikata HALCOM BG CA ili kvalifikovanih elektronskih sertifikata drugih pružaoca usluga od poverenja.

1.4. UPOTREBA KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA

HALCOM BG CA upravlja (izdaje i overava, opoziva, obnavlja, čuva, objavljuje) kvalifikovanim elektronskim sertifikatima za elektronsko potpisivanje. Sertifikati su namenjeni fizičkim licima koji se identifikuju kao pripadnici pravnih lica.

1.4.1 PRIHVATLJIVO KORIŠĆENJE KVALIFIKOVANIH ELEKTROSNKIH SERTIFIKATA

(1) Kvalifikovani elektronski sertifikati su namenjeni kvalifikovanom elektronskom potpisivanju jednostranih ili međusobnih komunikacija vlasnika sertifikata te korišćenju u različitim aplikacijama i za različite namene koje se pojave na tržištu.

(2) Kvalifikovani elektronski sertifikati ili ključevi se između ostalog mogu koristiti za:

1) identifikaciju vlasnika sertifikata (ovlašćenog lica pravnog subjekta),
2) dokazivanje identiteta vlasnika sertifikata (ovlašćenog lica pravnog subjekta),
3) potpisivanje dokumenata u elektronskom obliku i njihovu verifikaciju,

(3) šifrovanje i dešifrovanje dokumenata u elektronskom obliku. Kvalifikovan elektronski potpis može da se koristi u aplikacijama kao što su na primer:

1) elektronsko odnosno mobilno bankarstvo,
2) aplikacije e-uprave ili m-uprave,
3) potpisivanje elektronskih ili mobilnih formulara,
4) bezbedno poslovanje sa organima i organizacijama javnog sektora te ostalim pravnim ili fizičkim licima,
5) ostale aplikacije odnosno usluge u kojima se zahteva korišćenje kvalifikovanog elektronskog sertifikata,
6) kontrola pristupa.

1.4.2 NEDOZVOLJENA UPOTREBA

(1) Zabranjeno je korišćenje kvalifikovanih elektronskih sertifikata, izdatih u skladu sa ovom politikom u suprotnosti sa odredbama same politike pružanja usluge, opštih pravila rada (CPS),važećih propisa ili izvan opsega dozvoljenog korišćenja, određenog u prethodnom poglavlju.

(2) Kvalifikovani elektronski sertifikati izdati od strane HALCOM BG CA nisu namenjeni daljoj prodaji.

1.5. UPRAVLJANJE DOKUMENTIMA

1.5.1 ORGANIZACIJA ADMINISTRACIJE DOKUMENATA

(1) Ovim CP dokumentom, kao i ostalim opštim i internim pravilima rada, upravlja pružalac usluga od poverenja HALCOM BG CA.

(2) Naziv organizacije **Halcom a.d. Beograd**
Beogradska 39

11000 BEOGRAD

Srbija

1.5.2 OVLAŠĆENE KONTAKT OSOBE

(1) Za sva pitanja vezana za ovaj CP dokument, možete kontaktirati ovlašćena lica koja su dostupna na dole navedenoj adresi i dole navedenim telefonskim brojevima.

(2) Kontakt:

Halcom A.D. Beograd
Aleksandar Spremić

Beogradska 39
11000 Beograd
Srbija
Tel.: (+381) 11 33 06 500
Fax: (+381) 11 33 48 994

Mail: ca@halcom.rs

http://www. halcom.rs/

1.5.3 ODGOVORNO LICE ZA USKLAĐENOST OVE POLITIKE

Za usklađenosti poslovanja HALCOM BG CA kao pružaoca usluga od poverenja sa ovim CP dokumentom su, u skladu sa svojim nadležnostima, odgovorna ovlašćena lica definisana u poglavlju 1.5.2.

1.5.4 PROCEDURA ODOBRAVANJA CP DOKUMENTA

(1) Svaki predlog novog izmenjenog CP dokumenta se razmatra sa tehnološkog i pravnog aspekta u cilju garantovanja zakonitosti, bezbednosti i kvaliteta. Nakon toga, novi CP dokument se potvrđuje od strane direktora Halcom a.d. Beograd.

(2) Pružalac usluga od poverenja može izdati ispravke kako je navedeno za svaku odredbu u poglavlju 9.12.

1.6. SKRAĆENICE I DEFINICIJE

1.6.1 SKRAĆENICE

CA	Pružalac usluga od poverenja, koji izdaje sertifikate (*engl.: Certification Authority* ili *Certification Agency).*
CPName	Ime politike rada pružaoca usluga od poverenja (*engl.: Certification Policy Name*), jednoznačno povezan sa međunarodno jedinstvenim brojem politike pružanja usluge CPOID (*engl.: Certification Policy Object Identifier*).
CPOID	Međunarodni broj koji jednoznačno definiše politiku (*engl.: Certification Policy Object IDentifier*).
CRL	*Certificate Revocation List* – registar opozvanih kvalifikovanih elektronskih sertifikata
DN	Jedinstveno ime (*engl.: Distinguished Name).*
CP	Politika pružaoca usluge od poverenja (engl. Certificate Policy). Politika koja uređuje svrhu, rad i metodologiju upravljanja uslugama, odgovornosti i sigurnosnih zahteva, koje mora ispuniti pružalac usluga od poverenja, vlasnici sertifikata (korisnici usluga) i treća lica, koja se oslanjaju na ove sertifikate/usluge
CPS	CPS (engl. Certification Practice Statement) predstavlja opšte uslove za pružanje usluge i opšta pravila pružaoca usluga od poverenja.
LDAP	*Lightweight Directory Access Protocol* je protokol koji omogućava pristup sertifikatima i registru opozvanih sertifikata CRL koje izdaje pružalac usluga od poverenja a specificiran prema IETF (*Internet Engineering Task Force*) preporuci IETF RFC 3494.
S/MIME	*Secure Multipurpose Internet Mail Extensions*
AR ID BROJ	Identifikacioni broj korisnika u AR Registru pružaoca usluga od poverenja
SSL	*Secure Sockets Layer*
TLS	*Transport Layer Security*
PKI	*Public Key Infrastructure* je infrastruktura javnih ključeva
HSM	Hardware Security Module je bezbedni kriptografski uređaj za skladištenje i upravljanje ključevima pružaoca usluge od poverenja.
QSCD	*Qualified Signature Creation Device je bezbedni kriptografski uređaj za kreiranje kvalifikovanih elektronskih potpisa (npr. HSM, smart kartica, USB ključ itd.)*

1.6.2 IZRAZI

Pružalac usluga od poverenja	Fizičko ili pravno lice, koje izdaje sertifikate ili obavlja druge usluge od poverenja (engl.: Trust Service provider – TSP).
Lista sertifikata	Lista sertifikata po preporuci X.500, gde se sertifikati čuvaju u skladu sa preporukom X.509 ver. 3 , do kojih je moguće pristupiti po protokolu LDAP.
Identifikacija	Identifikacija predstavlja postupak identifikacije fizičkog i/ili pravnog lica u fizičkom ili elektronskom obliku, koji jednoznačno identifikuju fizičko lice, pravno lice ili fizičko lice kao predstavnika pravnog lica.
Registraciono telo	Služba ili osoba, koja vrši prijem zahteva za izdavanje/opoziv sertifikata, potvrđuje identitet vlasnika sertifikata u ime pružaoca usluga od poverenja (engl.: Registration Authority – RA).
Jedinstveno ime	Jednoznačno ime u kvalifikovanom elektronskom sertifikatu (DN – Distinguished Name) koje nedvosmisleno i jednoznačno definiše datog korisnika u strukturi spiska sertifikata pružaoca usluga od poverenja.

2. ODGOVORNOST ZA PUBLIKACIJE I REPOZITORIJUME

2.1. LISTA DOKUMENATA

(1) Pružalac usluga od poverenja HALCOM BG CA javno objavljuje sve informacije koje se odnose na rad pružaoca usluga od poverenja, obaveštenja korisnicima i trećim licima, kao i ostale važne dokumente, na web stranicama Halcom a.d. Beograd, http://www.halcom.rs.

(2) Dokumenti koji su javno dostupni na web stranicama su:

1. cenovnik,
2. politika korišćenja usluga od poverenja (CP),
3. opšta pravila rada pružaoca usluga od poverenja (CPS),
4. obrasce za naručivanje i druge ugovore o uslugama pružaoca usluga od poverenja,
5. uputstva za bezbedno korišćenje kvalifikovanih elektronskih sertifikata,
6. informacije o važećem zakonodavstvu vezano za rad pružaoca usluga od poverenja,
7. ostale informacije vezane u vezi sa radom HALCOM BG CA.

(3) Međutim javno nisu dostupni dokumenti koji predstavljaju interna pravila pružaoca usluga od poverenja HALCOM BG CA.

2.2. REGISTAR SERTIFIKATA

(1) Nove politike objavljuju se u skladu sa navodima u poglavlju 9.10.

(2) Svi sertifikati pružaoca usluga od poverenja su zasnovani na standardu X.509 i

objavljeni su u centralnom direktorijumu na serveru ldap.halcom.rs, kojim rukovodi HALCOM BG CA. Javno dostupan je samo deo direktorijuma u kome su opozvani sertifikati.

(3) Opozvani sertifikati se odmah objavljuju u registru opozvanih sertifikata (detaljnije u delu 4.9.8.), dok se druge javno dostupne informacije i dokumenti objavljuju po potrebi.

(4) Pristup direktorijumu izdatih sertifikata je omogućen samo ovlašćenim osobama, koji proveravaju veći broj izdatih sertifikata.

2.3. UČESTANOST OBJAVLJIVANJA

(1) CPS ili nove politike se objavljuju najkasnije narednog dana nakon prihvatanja.
(2) HALCOM BG CA obezbeđuje da se sertifikati objavljuju u centralnom direktorijumu odmah (najviše 5 sekundi) nakon njihovog izdavanja.
(3) Registar opozvanih sertifikata se osvežava odmah (najviše 5 sekundi) nakon opoziva sertifikata u javnom registru. Nakon nekoliko minuta, osvežava se i web stranica sa listom opozvanih sertifikata.

(4) Javno dostupne informacije i dokumenti (osim gore navedenog) objavljuju se po potrebi.

2.4. UPRAVLJANJE PRISTUPU DO LISTE DOKUMENATA

(1) Registar izdatih kvalifikovanih elektronskih sertifikata je dostupan na serveru ldap.halcom.rs, TCP port 389 u skladu sa LDAP protokolom. Javno dostupan je samo deo registra, registar opozvanih sertifikata.

(2) Odgovarajućim tehničkim uslovima (mašinska i programska oprema) HALCOM BG CA garantuje kontrole koje sprečavaju neovlašćeno dodavanje, menjanje ili brisanje podataka u registru kvalifikovanih elektronskih sertifikata.

3. IDENTIFIKACIJA I PROVERA KORISNIKA

3.1. DODELA IMENA

Jedinstvena imena koje sadrži kvalifikovani elektronski sertifikat nedvosmisleno i jednoznačno definišu vlasnika kvalifikovanih elektronskih sertifikata osim ako se, ovim dokumentom ili sadržajem kvalifikovanog elektronskog sertifikata, drugačije zahteva.

3.1.1 TIPOVI IMENA

(1) U skladu sa IETF RFC 5280 svaki kvalifikovani elektronski sertifikat sadrži podatke o vlasniku i izdavaocu kvalifikovanog elektronskog sertifikata u obliku jedinstvenog imena. Jedinstveno ime je formirano u skladu sa IETF RFC 5280 i standardom X.501.

(2) Pružalac usluga od poverenja je u izdatom sertifikatu naveden u polju Izdavalac, engl. *Issuer*. Osnovni podaci o vlasniku koje sadrži jedinstveno ime vlasnika kvalifikovanog elektronskog sertifikata nalaze se u izdatom sertifikatu navedeni u polju Nosilac engl. *Subject*.

(3) Jedinstveni serijski broj korisnika u okviru pružaoca usluga od poverenja koji se takođe sadrži u jedinstvenom imenu određuje izdavalac HALCOM BG CA. (više u poglavlju 3.1.5.)

Sertifikati pružaoca usluge od poverenja HALCOM BG CA:

Vrsta sertifikata	Naziv polja	Jedinstveno ime
Kvalifikovani elektronski sertifikat pružaoca usluga od poverenja HALCOM BG CA	Izdavalac engl. Issuer	CN = Halcom BG Root CA 2.5.4.97 = VATRS-102193722 2.5.4.97 = MB:RS-17419722 O = Halcom a.d. Beograd C = RS
Intermediate/podređeni sertifikati za pravno lice	Izdavalac engl. Issuer	CN = Halcom BG Root CA 2.5.4.97 = VATRS-102193722 2.5.4.97 = MB:RS-17419722 O = Halcom a.d. Beograd C = RS
	Korisnik eng. Subject	CN = Halcom BG CA PL e-signature 2.5.4.97 = VATRS-102193722 2.5.4.97 = MB:RS-17419722 O = Halcom a.d. Beograd C = RS
Kvalifikovani elektronski sertifikat za pravna lica	Izdavalac engl. Issuer	CN = Halcom BG CA PL e-signature 2.5.4.97 = VATRS-102193722 2.5.4.97 = MB:RS-17419722 O = Halcom a.d. Beograd C = RS
	Korisnik eng. Subject	E=<elektronska pošta> SERIALNUMBER = PNORS-<JMBG> ili SERIALNUMBER = PAS<oznaka države>-<broj pasoša> ili SERIALNUMBER = IDCRS-<broj lične karte> i SERIALNUMBER = CA:RS-<AR ID BROJ> G = <ime> SN = <prezime> CN = <ime i prezime AR ID BROJ> 2.5.4.97 = VATRS-<poreski ident. broj> 2.5.4.97 = MB:RS-<matični broj> O = <naziv pravnog lica> C = RS

3.1.2 ZAHTEVI ZA KREIRANJE JEDINSTVENOG IMENA

(1) Oznaka pravnog lica, koja je u skladu sa odredbama u poglavlju 3.1.1, uključena u

jedinstveno ime mora ispunjavati sledeće uslove:

- mora biti jedinstveno registrovano u poslovnom ili drugom službenom registru,
- mora biti jednoznačno povezan sa pravnim licem,
- maksimalna dužina može biti četrdeset dva (42) karaktera.

(2) Halcom CA zadržava pravo da odbije firmu, naziv ili šifru privrednog subjekta, ako utvrdi:

- da je neprikladan ili uvredljiv,
- da je zabluda trećim stranama ili već pripada drugom pravnom ili fizičkom licu,
- da je u suprotnosti sa važećim propisima.

3.1.3 ANONIMNI KORISNICI I KORIŠĆENJE PSEUDONIMA

HALCOM BG CA ne izdaje anonimne sertifikate korisnicima.

3.1.4 PRAVILA ZA INTERPRETACIJU RAZLIČITIH FORMI IMENA

(1) Podaci o vlasniku kvalifikovanog elektronskog sertifikata u jedinstvenom imenu sadrže slova srpske abecede, dok se preostali znakovi transformišu prema donjim pravilima:

Znak	Transformacija
Ü	Ue
Ö	Oe
Ø	Oe
ß	Ss
Ñ	N
Ŕ	Rz

(2) Odgovarajućom kombinacijom slova pružalac usluga od poverenja obezbeđuje korišćenje ostalih nepredvidivih znakova.

3.1.5 JEDINSTVENOST IMENA

Jedinstvena imena su jedinstvena za svaki izdati sertifikat i nedvosmisleno i jedinstveno identifikuju pojedinca u strukturi sertifikata.

3.1.6 ZAŠTIĆENA IMENA ILI ROBNE MARKE

(1) Vlasnici kvalifikovanih elektronskih sertifikata ne smeju da zahtevaju imena koja pripadaju nekome drugome čime bi se kršila prava trećih lica.

(2) Eventualne sporove rešavaju isključivo oštećena strana i vlasnik kvalifikovanog elektronskog sertifikata.

(3) Odgovornost za upotrebu imena ili zaštićenih robnih marki je na strani pravnog lica. Pružalac usluga od poverenja HALCOM BG CA nije u obavezi da proverava i/ili obaveštava vlasnika ili pravno lice.

3.2. PROVERA IDENTITETA BUDUĆEG VLASNIKA SERTIFIKATA PRI PRVOM IZDAVANJU SERTIFIKATA

Budući vlasnik kvalifikovanog elektronskog sertifikata mora da zahteva kvalifikovani elektronski sertifikat u ime korisnika u okviru pravnog lica, kao ovlašćeno lice odgovarajućeg pravnog lica. Registraciono telo proverava i potvrđuje identitet budućeg vlasnika kvalifikovanog elektronskog sertifikata.

3.2.1 METOD ZA POSEDOVANJE PROVATNOG KLJUČA

Posedovanje privatnog ključa koji pripada javnom ključu u sertifikatu garantovano je sigurnosnim procedurama pre i kada se sertifikat prihvati standardom PKCS#10.

3.2.2 PROVERA IDENTITETA ORGANIZACIJE

(1) Podaci o pravnom licu dati su u jedinstvenom imenu (pogledati poglavlje 3.1.1 i 3.1.2).

(2) Za budućeg vlasnika sertifikata pravnog lica garantuje zakonski zastupnik pravnog lica svojim potpisom na dokumentaciji za izdavanje sertifikata.

(3) HALCOM BG CA sa odgovarajućim službama i službenim evidencijama proverava ispravnost podataka pravnog lica i identitet zakonskog zastupnika.

(4) HALCOM BG CA, proverava identitet zakonskog zastupnika pravnog lica i podatke o pravnom licu na zvaničnoj web adresi registrovanih pravnih lica.

3.2.3 PROVERA IDENTITETA POJEDINCA

(1) Proveravanje identiteta vlasnika kvalifikovanih sertifikata izvršava operater registracionog tela HALCOM BG CA tako što proveri lične podatke o vlasniku na osnovu ličnog identifikacionog dokumenta, a po potrebi i u odgovarajućim registrima.

(2) Pružalac usluga od poverenja HALCOM BG CA verifikuje lične podatke vlasnika sertifikata u odgovarajućim registrima, osim ako drugačije nije predviđeno zakonom.

3.2.4 NEPROVERENI PODACI U SERTIFIKATU

HALCOM BG CA ne proverava tačnost i rad e-pošte vlasnika sertifikata.

3.2.5 PROVERA IDENTITETA ZAPOSLENIH ZA DOBIJANJE SERTIFIKATA

(1) Zakonski zastupnik pravnog lica svojim potpisom na dokumentaciji za dobijanje sertifikata garantuje da želi za pravno lice i određeno fizičko lice koje je zaposleno ili obavlja poslove ovog pravnog lica naručiti odgovarajući sertifikat.

(2) Ovlašćeno lice pravnog lica potpisom na dokumentima za izdavanje kvalifikovanog elektronskog sertifikata garantuje da je neosporno ovlastio buduće vlasnike sertifikata u okviru pravnog lica. Identitet korisnika, budućeg vlasnika proverava ovlašćeno lice HALCOM BG CA. Pravno lice se kao poslodavac vlasnika sertifikata obavezuje, da će ispunjavati sve odredbe ovog CP dokumenta i važeće propise.

3.2.6 MEĐUSOBNO PRIZNAVANJE

(1) Pružalac usluga od poverenja HALCOM BG CA nije dužan ugovorno sarađivati ili garantovati za ostale pružaoce usluga od poverenja čak iako drugi pružalac usluga od poverenja ima status akreditovanog pružaoca usluga od poverenja za izdavanje kvalifikovanih elektronskih sertifikata.

(2) Pružalac usluga od poverenja HALCOM BG CA obezbeđuje da će ispoštovati međusobnu saradnju sa drugim pružaocima usluga od poverenja isključivo nakon potpisivanja pismenog ugovora sa drugim pružaocima usluga od poverenja koji moraju da ispune nivo sigurnosnih zahteva koje su uporedive ili više od onih koje propisuje HALCOM BG CA.

(3) Ovlašćena lica pružaoca usluga od poverenja HALCOM BG CA proveravaju opšta i interna pravila drugog pružaoca usluga od poverenja, kao i njegovo ispunjavanje sigurnosnih zahteva, ukoliko nema spoljne i nezavisne ocene usklađenosti drugog pružaoca usluge od poverenja.

(4) Troškove potrebne infrastrukture koju zahteva HALCOM BG CA za međusobno priznavanje pokriva drugi pružalac usluga od poverenja, osim ukoliko nije ugovorom dogovoreno drugačije.

3.3. IDENTIFIKACIJA I PROVERA ZAHTEVA ZA OBNAVLJANJE KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA

3.3.1 IDENTIFIKACIJA VLASNIKA SERTIFIKATA PRILIKOM OBNAVLJANJA SERTIFIKATA

Provera identiteta vlasnika sertifikata prilikom obnove sertifikata proverava vrši:

- operater registracionog tela kvalifikovanog pružaoca usluga od poverenja HALCOM BG CA, kao kod prvobitnog izdavanja.

3.3.2 IDENTIFIKACIJA I PROVERA ZA OBNAVLJANJE SERTIFIKATA NAKON OPOZIVA

Provera identiteta vlasnika je u skladu sa odredbama u poglavlju 3.2.3.

3.4. IDENTIFIKACIJA I PROVERA ZAHTEVA ZA OPOZIV KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA

(1) Zahtev za opoziv kvalifikovanog elektronskog sertifikata pravno lice ili vlasnik kvalifikovanog sertifikata predaje:

- lično registracionom telu gde ovlašćena lica registracionog tela provere identitet podnosioca zahteva,
- elektronski, gde zahtev mora biti digitalno potpisan sa kvalifikovanim sertifikatom, čime se prikazuje identitet podnosioca zahteva,
- u slučaju da vlasnik kvalifikovanog elektronskog sertifikata putem telefona, elektronske pošte ili FAX-a zahteva opoziv sertifikata, pružalac usluga od poverenja HALCOM BG CA prvo suspenduje sertifikat. Tek na osnovu prijema overenog pismenog zahteva za opoziv sertifikata, koji vlasnik lično dostavi registracionom telu, faktički se sprovodi sam opoziv sertifikata.

(2) Detaljan postupak opoziva: poglavlje 4.9.3.

4. UPRAVLJANJE SERTIFIKATIMA

4.1. ZAHTEV ZA DOBIJANJE KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA

4.1.1 KO MOŽE DA DOBIJE KVALIFIKOVANI ELEKTRONSKI SERTIFIKAT

Budući vlasnici kvalifikovanih elektronskih sertifikata koji se izdaju u skladu sa ovim CP dokumentom su fizička lica koja predstavljaju ovlašćena lica odgovarajućih pravnih lica.

Za dobijanje kvalifikovanog elektronskog sertifikata moraju biti ispunjeni sledeći uslovi:

- popunjen i dostavljen obrazac narudžbenice ili ugovor u HALCOM BG CA ili RA,
- finansijske obaveze,
- obaveze identifikacije.

4.1.2 PROCES DOSTAVLJANJA ZAHTEVA ZA IZDAVANJE KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA (ENROLLMENT) I ODGOVORNOSTI

Kvalifikovani elektronski sertifikat za ovlašćeno lice pravnog lica:

1) Kvalifikovani elektronski sertifikat se izdaje na osnovu pravilno ispunjene i potpisane narudžbenice za izdavanje kvalifikovanog elektronskog sertifikata (u daljem tekstu narudžbenica) od strane zakonskog zastupnika pravnog lica i budućeg vlasnika sertifikata. Narudžbenica se predaje registracionom telu (RA) HALCOM BG CA. Narudžbenice za izdavanje kvalifikovanog elektronskog sertifikata dostupne su kako kod registracionih tela (RA) HALCOM BG CA tako i na web stranici HALCOM BG CA.
2) Svojim potpisom zakonski zastupnik pravnog lica ovlašćuje osobu pravnog lica (vlasnika sertifikata), da u ime i za račun pravnog lica potpiše narudžbenicu za obnovu postojećeg sertifikata ili izdavanje novog u skladu sa važećim politikama i cenovnikom kvalifikovanog pružaoca usluga od poverenja HALCOM BG CA, pod uslovom da se valjanost elektronskog potpisa može proveriti.
3) Budući vlasnik kvalifikovanog elektronskog sertifikata predaje narudžbenicu/molbu u pismenom obliku.
4) Pre izdavanja narudžbenice, HALCOM BG CA je u obavezi da upozna budućeg vlasnika, kao i pravno lice sa ovim CP dokumentom kao i sa ostalim informacijama o elektronskom potpisivanju i operativnom radu HALCOM BG CA.
5) HALCOM BG CA zadržava pravo da negativno reši molbu korisnika za izdavanje kvalifikovanog elektronskog sertifikata ako je u suprotnosti sa važećim propisima Republike Srbije ili Evropske Unije.

4.2. PROCESIRANJE ZAHTEVA ZA DOBIJANJE KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA

4.2.1 PROVERAVANJE IDENTITETA KORISNIKA

(1) Ovlašćeno lice registracionog tela HALCOM BG CA proverava identitet budućeg vlasnika. Budući vlasnik mora da dokaže svoj identitet važećim ličnim dokumentom sa fotografijom, ličnim prisustvom prilikom preuzimanja sertifikata u registracionom telu, odnosno ovlašćenom kuriru kurirske službe pružaoca usluge od poverenja. Pod ličnim identifikacionim dokumentom smatraju se važeća lična karta i pasoš.

(2) Ovlašćena lica registracionog tela ili pružaoca usluga od poverenja i kurirska služba dužni su da provere identitet vlasnika sertifikata, odnosno sve one podatke koji su navedeni u narudžbenici a dostupni su u službenim evidencijama odnosno u drugim službeno važećim dokumentima.

(3) Ovlašćena lica registracionog tela proveravaju ispunjene molbe/narudžbenice, kao i dopunsku originalnu dokumentaciju koja se zahteva i prosleđuju je pružaocu usluga od poverenja HALCOM BG CA.

4.2.2 POTVRĐIVANJE ILI ODBIJANJE ZAHTEVA ZA DOBIJANJE KVALIFIKOVANOG SERTIFIKATA KORISNIKA

(1) Nakon provere identiteta, HALCOM BG CA ili RA potvrđuju ili odbijaju zahtev za izdavanje kvalifikovanih elektronskih sertifikata. Takvo potvrđivanje ili odbijanje neophodno je da bude obrazloženo lično ili e-mailom podnosiocu ili bilo kojoj drugoj strani ako je u suprotnosti sa poslovnim i etičkim standardima za koje se zalaže HALCOM BG CA.

(2) Nakon potvrđivanja zahteva za izdavanje kvalifikovanih elektronskih sertifikata, RA šalje zahtev za izdavanje kvalifikovanih elektronskih sertifikata do HALCOM BG CA pružaoca usluga od poverenja.

4.2.3 POTREBNO VREME ZA PROCESIRANJE ZAHTEVA KORISNIKA

HALCOM BG CA se po osnovu odobrenog zahteva za izdavanje kvalifikovanog elektronskog sertifikata i izmirenih finansijskih obaveza obavezuje da najkasnije u roku od pet (5) dana izda kvalifikovani elektronski sertifikat i pošalje ga odvojeno registracionom telu koje dalje distribuira sertifikate do budućih vlasnika, odnosno direktno fizičkom licu kome se sertifikat izdaje.

4.3. IZDAVANJE KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA

4.3.1 POSTUPAK IZDAVANJA KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA HALCOM BG CA

(1) Proizvodni postupak za izdavanje kvalifikovanih elektronskih sertifikata sastoji se iz jasno odvojenih koraka (ili funkcija), sa odvojenim podsistemima:

- Napredni kvalifikovani sertifikati:

1. predpersonalizacija bezbednosnog nosioca (generisanje ključeva na smart kartici/USB ključu i PIN/PUK koda),
2. obrada zahteva za izdavanje kvalifikovanog elektronskog sertifikata,
3. priprema kvalifikovanih elektronskih sertifikata,
4. personalizacija smart kartice/USB ključa (izdavanje i upis sertifikata, štampanje podataka vlasnika na smart kartici/USB ključu),
5. štampanje lične lozinke (PIN/PUK koda),
6. isporuka kvalifikovanog elektronskog sertifikata i lične lozinke (PIN/PUK koda).

(2) Kvalifikovani elektronski sertifikat na bezbednom mediju i odgovarajuća lična lozinka (PIN/PUK kod) se do registracionog tela ili samog fizičkog lica dostavlja u dva različita dana u dve odvojene pošiljke ili istog dana odvojenim kurirskim službama ili se vlasniku isporučuje lično na šalterima RA.

(3) Pre distribucije sertifikata (PIN/PUK kod) vlasnik sertifikata se obaveštava putem maila o predstojećoj isporuci.

(4) Naručilac i vlasnik po pravilu nisu ista osoba kao HALCOM BG CA ili registraciono telo HALCOM BG CA. Ako registraciono telo HALCOM BG CA naručuje sertifikate za sebe ili za svoje zaposlene, HALCOM BG CA dodatno proverava takve zahteve i osobe.

(5) Ako HALCOM BG CA naručuje sertifikat za sebe ili za ovlašćena lica, izdaju takvih sertifikata dodatno proverava ovlašćeno lice za unutrašnju kontrolu ili ovlašćeno lice za regulativnu skladnost.

(6) Svi opisani postupci zasnovani su tako da ih ne može izvesti samostalno jedna osoba.

4.3.2 OBAVEŠTENJE VLASNIKU O IZDAVANJU SERTIFIKATA

Opisano u prethodnom poglavlju.

4.4. PREUZIMANJE KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA

4.4.1 SPROVOĐENJE PROCESA PREUZIMANJA KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA

(1) Postupak preuzimanja naprednih sertifikata:

preuzimanje kvalifikovanih elektronskih sertifikata se vrši tako što budući vlasnik primi kvalifikovani elektronski sertifikat na bezbednom mediju i odgovarajuću ličnu lozinku (PIN/PUK kod) lično na šalterima HALCOM BG CA, odnosno na navedenoj adresi od strane ovlašćenog kurira odvojenim pošiljkama (pogledati poglavlje 4.3.1).

(2) Vlasnik sertifikata ili pravno lice mora odmah proveriti ispravnost podataka po prijemu sertifikata i u slučaju mogućih grešaka ili problema, odmah obavestiti HALCOM BG CA.

4.4.2 OBJAVLJIVANJE KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA OD STRANE CA

Postupak je opisan u poglavlju 2.

4.4.3 OBAVEŠTENJE TREĆIH STRANA O IZDATOM SERTIFIKATU

Pružalac usluga od poverenja ne obaveštava druga preduzeća, odnosno organizacija, o izdavanju sertifikata.

4.5. OBAVEZE I ODGOVORNOSTI KORISNIKA SERTIFIKATA

4.5.1 OBAVEZE VLASNIKA SERTIFIKATA

(1) Vlasnik ili budući vlasnik sertifikata dužan je:

- da se upozna i postupa u skladu sa politikom, pre izdavanja sertifikata,
- da se pridržava politike i drugih važećih propisa,
- nakon prijema sertifikata ili aktiviranja sertifikata proveri podatke na sertifikatu, i da za bilo kakve greške ili probleme obavesti HALCOM BG CA ili zatraži opoziv sertifikata,
- prati i poštuje sva obaveštenja HALCOM BG CA,
- prema obaveštenjima, ažurira potreban hardver ili softver za siguran rad sa sertifikatima,
- da odmah obavesti HALCOM BG CA o svim promenama vezano za sertifikat,

- da zatraži opoziv sertifikata ako privatni ključ ugrožen na način koji pogađa pouzdanost upotrebe ili ako postoji rizik od zloupotrebe,
- koristi sertifikat za svrhu koja je naznačena u sertifikatu (videti poglavlje 7.1) i način koji je u skladu sa politikom HALCOM BG CA.

(2) Vlasnik ili budući vlasnik takođe je dužan da zaštiti privatni ključ:

- pažljivo zaštiti podatke za preuzimanje ili aktivaciju sertifikata od neovlašćenih lica,
- drži privatni ključ i sertifikat na način koji obezbeđuje čuvanje privatnosti u skladu sa obaveštenjima i preporukama HALCOM BG CA,
- zaštiti privatni ključ i sve druge poverljive podatke sa odgovarajućom lozinkom u skladu sa preporukom HALCOM BG CA ili na način da samo vlasnik sertifikata ima pristup,
- pažljivo zaštiti lozinke za pristup poverljivim podacima ili privatnom ključu,
- nakon isteka ili opoziva sertifikata postupa u skladu sa obaveštenjima HALCOM BG CA.

4.5.2 OBAVEZE I ODGOVORNOSTI TREĆIH STRANA

(1) Treća strana koja prihvata sertifikate mora:

- rukovati i koristiti sertifikate u skladu sa politikama i drugim pravilima i propisima,
- pažljivo ispitati sve rizike i odgovornosti za korišćenje sertifikata i odrediti politiku za način rukovanja,
- obavestiti HALCOM BG CA ako utvrdi da je privatni ključ ugrožen na način koji utiče na pouzdanost ili ako postoji opasnost od zloupotrebe ili ako su se informacije date u sertifikatu promenile,
- se osloniti na sertifikat samo za svrhu koja je navedena u sertifikatu (pogledati poglavlje 6.1.7) i na način definisan politikom,
- u trenutku korišćenja sertifikata proveriti da sertifikat nije u registru opozvanih sertifikata,
- u trenutku korišćenja sertifikata, proveriti da je elektronski potpis stvoren tokom perioda važenja i sa odgovarajućom svrhom sertifikata,
- u trenutku korišćenja sertifikata, proveriti da je potpis sertifikata HALCOM BG CA, koji je objavljen u ovoj politici i na web stranici Halcom-a,
- poštovati sve odredbe HALCOM BG CA koje su zaključene prilikom sporazuma o upotrebi sertifikata.

(2) Treće strane moraju proveriti validnost potpisa i druge kriptografske operacije koje koriste softver i hardver i da potvrde sve navedene zahteve za sigurnu upotrebu sertifikata.

4.6. OBNAVLJANJE KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA

(1) Obnova kvalifikovanih elektronskih sertifikata moguća je samo na osnovu zahteva vlasnika.

(2) Po isteku važnosti naprednog kvalifikovanog sertifikata nosilac ima pravo da ponovo podnese zahtev za sertifikat.

(3) Postupak podnošenja zahteva za obnovu kvalifikovanih elektronskih sertifikata isti je kao i kod prvobitnog izdavanja.

4.6.1 USLOVI ZA OBNAVLJANJE KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA

Pre isteka validnosti kvalifikovanog elektronskog sertifikata, dostavljanjem zahteva za obnovu kvalifikovanih elektronskih sertifikata, vlasnici kvalifikovanih elektronskih sertifikata obezbeđuju kontinuitet korišćenja kvalifikovanih elektronskih sertifikata. Zahtev za ponovno izdavanje je moguće uložiti i nakon isteka validnosti kvalifikovanih elektronskih sertifikata.

4.6.2 KO MOŽE ZAHTEVATI OBNAVLJANJE KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA

Samo vlasnik kvalifikovanog elektronskog sertifikata može da traži ponovno izdavanje kvalifikovanog elektronskog sertifikata.

4.6.3 PROCESIRANJE ZAHTEVA ZA OBNOVU KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA

(1) Ponovno izdavanje kvalifikovanog elektronskog sertifikata zahteva korisnik dostavljanjem propisane dokumentacije za obnovu kvalifikovanog elektronskog sertifikata registracionom telu HALCOM BG CA.
(2) Postupak garantuje da je pravno lice koje uloži zahtev za obnovu kvalifikovanog elektronskog sertifikata doista vlasnik kvalifikovanog elektronskog sertifikata.
(3) Pružalac usluga od poverenja obnavlja kvalifikovani elektronski sertifikat, tj. procesira dostavljeni zahtev i dostavlja obnovljeni kvalifikovani elektronski sertifikat korisniku.

(4) Provera korisnika u cilju obnove kvalifikovanog elektronskog sertifikata vrši se na isti način kao i provera pri izdavanju kvalifikovanog elektronskog sertifikata prvi put.

4.6.4 OBAVEŠTENJE KORISNIKA DA MU JE IZDAT OBNOVLJENI KVALIFIKOVANI ELEKTRONSKI SERTIFIKAT

Pogledati poglavlje 4.3.2.

4.6.5 SPROVOĐENJE PROCESA PREUZIMANJA OBNOVLJENOG KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA

Pogledati poglavlje 4.4.1.

4.6.6 OBJAVLJIVANJE OBNOVLJENOG KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA OD STRANE CA

Postupak je objašnjen u poglavlju 2.

4.6.7 OBAVEŠTENJE TREĆIH STRANA OD STRANE HALCOM BG CA O OBNOVI DATOG KVALIFIKOVANOG ELEKTRONSOG SERTIFIKATA

Pružalac usluga od poverenja o izdavanju pojedinačnih kvalifikovanih elektronskih sertifikata vlasnicima ne obaveštava preduzeća i druge organizacije.

4.7 REGENERACIJA PARA KLJUČEVA I KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA KORISNIKA

4.7.1 USLOVI ZA REGENERACIJU PARA KLJUČEVA KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA

Ovo poglavlje nije primenljivo u okviru ovih CP.

4.7.2 KO MOŽE ZAHTEVATI REGENERACIJU KLJUČEVA

Ovo poglavlje nije primenljivo u okviru ovih CP.

4.7.3 PROCESIRANJE ZAHTEVA ZA REGENERECIJU KLJUČEVA I SERTIFIKATA

Ovo poglavlje nije primenljivo u okviru ovih CP.

4.7.4 OBAVEŠTENJE KORISNIKA DA MU JE IZDAT NOVI KVALIFIKOVANI ELEKTRONSKI SERTIFIKAT

Ovo poglavlje nije primenljivo u okviru ovih CP.

4.7.5 SPROVOĐENJE PROCESA PRIHVATANJA NOVOG KVALIFIKOVANOD ELEKTRONSKOG SERTIFIKATA

Ovo poglavlje nije primenljivo u okviru ovih CP.

4.7.6 OBJAVLJIVANJE NOVOG KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA OD STRANE CA

Ovo poglavlje nije primenljivo u okviru ovih CP.

4.7.7 OBAVEŠTAVANJE DRUGIH ENTITETA OD STRANE CA O IZDAVANJU NOVOG KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA

Ovo poglavlje nije primenljivo u okviru ovih CP.

4.8 PROMENA KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA KORISNIKA

(1) U slučaju promena podataka koji utiču na ispravnost jedinstvenog imena ili drugih podataka u sertifikatu, sertifikat je potrebno opozvati.

(2) Za dobijanje novog sertifikata potrebno je ponoviti postupak za izdavanje novog sertifikata koji je naveden u poglavlju 4.1.

4.8.1 USLOVI ZA PROMENU KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA KORISNIKA

Ovo poglavlje nije primenljivo u okviru ovih CP.

4.8.2 KO MOŽE ZAHTEVATI PROMENU KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA

Ovo poglavlje nije primenljivo u okviru ovih CP.

4.8.3 PROCESIRANJE ZAHTEVA ZA PROMENU KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA

Ovo poglavlje nije primenljivo u okviru ovih CP.

4.8.4 OBAVEŠTENJE KORISNIKA DA MU JE IZDAT PROMENJENI KVALIFIKOVANI ELEKTRONSKI SERTIFIKAT

Ovo poglavlje nije primenljivo u okviru ovih CP.

4.8.5 SPROVOĐENJE PROCESA PRIHVATANJA NOVOG PROMENJENOG KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA

Ovo poglavlje nije primenljivo u okviru ovih CP.

4.8.6 OBJAVLJIVANJE NOVOG PROMENJENOG KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA OD STRANE CA

Ovo poglavlje nije primenljivo u okviru ovih CP.

4.8.7 OBAVEŠTENJE DRUGIH ENTITETA OD STRANE CA O IZDAVANJU NOVOG PROMENJENOG KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA

Ovo poglavlje nije primenljivo u okviru ovih CP.

4.9. OPOZIV I SUSPENZIJA KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA

(1) Opoziv kvalifikovanog elektronskog sertifikata vlasnik ili zakonski zastupnik može da zahteva bilo kada, ali svakako mora da ga zahteva u slučaju:

1. promene jedinstvenog imena (DN),
2. kada pravno lice ili vlasnik sertifikata promeni ključne ili lične podatke, povezane sa sertifikatom (ime ili prezime, naziv poslovnog imena, ili drugo),
3. kada se ustanovi ili sumnja da je došlo do pronevere ili zloupotrebe privatnog ključa za elektronsko potpisivanje,
4. gubitka poslovne sposobnosti, prestanka ili zabrane rada.

(2) Pružalac usluga od poverenja HALCOM BG CA može da opozove kvalifikovani elektronski sertifikat bez zahteva vlasnika u slučajevima navedenim u prvom paragrafu ili na osnovu zahteva nadležnog suda ili drugog državnog nadležnog organa.

(3) Opoziv sertifikata je moguće uraditi 24h dnevno. Tačno uputstvo za opoziv sertifikata nalazi se na web stranici HALCOM BG CA.

(4) HALCOM BG CA će na osnovu pravilnog zahteva za opoziv sertifikata, isti opozvati u roku od četiri (4) sata. U slučaju nepredviđenih okolnosti HALCOM BG CA može opozvati sertifikat najkasnije osam (8) sati nakon prijema tačnog zahteva. Opozvani kvalifikovani elektronski sertifikat će biti označen u registru opozvanih sertifikata (CRL) prilikom izdavanja prve sledeće CRL liste. Ukoliko nije bilo opoziva sertifikata CRL lista će biti izdata najmanje na svaka dvadeset četiri sata (24). U slučaju da vlasnik kvalifikovanog elektronskog sertifikata isporuči pružaocu usluga od poverenja HALCOM BG CA nepravilan zahtev za opoziv, biće mu poslato upozorenje o nepravilnom zahtevu za opoziv sertifikata i biće upoznat sa uputstvima za dostavljanje pravilnog zahteva za opoziv.

4.9.1 RAZLOZI ZA OPOZIV KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA

(1) Opoziv sertifikata mora tražiti pravno lice ili vlasnik sertifikata u slučaju:

- ako je privatni ključ vlasnika sertifikata ugrožen na način koji utiče na pouzdanost upotrebe,
- ako postoji rizik od zloupotrebe privatnog ključa ili sertifikata vlasnika,
- ako se promene ili su netačni podaci na sertifikatu.

(2) Pružalac usluga od poverenja HALCOM BG CA će opozvati sertifikat bez zahteva vlasnika odmah, ako dođe do saznanja da:

- podaci u sertifikatu nisu ispravni ili je sertifikat izdat na osnovu netačnih podataka,

- je došlo do greške u verifikaciji podataka u RA,
- da su se promenile okolnosti koje utiču na ispravnost sertifikata,
- je došlo do neispunjavanja obaveza vlasnika sertifikata,
- nisu izmirene finansijske obaveze u vezi sa sertifikatom,
- da je ugrožena infrastruktura pružaoca usluga od poverenja na način koji utiče na pouzdanost upotrebe,
- je privatni ključ vlasnika sertifikata ugrožen na način koji utiče na pouzdanost upotrebe,
- HALCOM BG CA prestane da izdaje sertifikate ili da mu se zabrani rad sa sertifikatima a drugi pružalac usluga od poverenja ne preuzme njegove aktivnosti,
- da je opoziv naređen od strane nadležnog suda, prekršajnog ili drugog državnog organa.

(3) Vlasnik sertifikata može zahtevati ponovno kreiranje PIN koda za napredne sertifikate, u slučaju da su podaci zaboravljeni. Pod krivičnom odgovornošću garantuje da nema mogućnosti da privatni ključ bude ugrožen na način koji utiče na pouzdanost upotrebe i da ne postoji rizik od zloupotrebe privatnog ključa ili sertifikata.

4.9.2 KO MOŽE ZAHTEVATI OPOZIV KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA kvalifikovanih elektronskih sertifikata

Opoziv kvalifikovanog elektronskog sertifikata može da zahteva:

- ovlašćeno lice pružaoca usluga od poverenja HALCOM BG CA,
- zakoniti zastupnik pravnog lica,
- vlasnik kvalifikovanih elektronskih sertifikata,
- nadležni sud ili,
- nadležni državni organ.

4.9.3 PROCEDURA PODNOŠENJA ZAHTEVA ZA OPOZIV KVALIFIKOVANIH ELEKTRONSKIH

(1) Opoziv može da zahteva zakoniti zastupnik pravnog lica ili vlasnik sertifikata:

- lično u radno vreme registracionog tela,
- elektronski, 24 sata na dan, svih dana u godini.

(2) Ako se opoziv zahteva:

- lično - potrebno je ispuniti odgovarajući zahtev za opoziv kvalifikovanog elektronskog sertifikata i predati ga registracionom telu,
- elektronski - vlasnik sertifikata mora da dostavi pružaocu usluga od poverenja HALCOM BG CA elektronski potpisan zahtev za opoziv,
- telefonom ili elektronskom poštom zahteva opoziv sertifikata - na osnovu te poruke pružalac usluga od poverenja privremeno suspenduje sertifikat, a po prijemu odgovarajućeg svojeručno potpisanog zahteva za opoziv kvalifikovanog elektronskog sertifikata pružalac usluga od poverenja opoziva sertifikat.

(3) O datumu i vremenu opoziva, o podnosiocu zahteva za opoziv, kao i o uzrocima opoziva,

vlasnik sertifikata mora da bude obavešten.

(4) Sudovi i administrativni organi koji takođe mogu da zahtevaju opoziv kvalifikovanih elektronskih sertifikata, taj proces izvršavaju u skladu sa propisanim procedurama.

(5) Odredbe koje se odnose na opoziv primenjuju se i na procedure u vezi sa ponovnim generisanjem PIN kodova za napredne sertifikate.

4.9.4 VREME ZA IZDAVANJE ZAHTEVA ZA OPOZIVOM KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA

Opoziv sertifikata potrebno je zahtevati odmah, ako postoji mogućnost zloupotrebe, nepouzdanosti ili u hitnim slučajevima. U drugim slučajevima, opoziv se može tražiti prvog radnog dana u vremenu rada registracionog tela (pogledati sledeće poglavlje).

4.9.5 VREME ZA KOJE CA MORA DA PROCESIRA ZAHTEV ZA OPOZIV KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA

(1) Pružalac usluga od poverenja HALCOM BG CA je u obavezi da nakon prijema validnog zahteva za opoziv kvalifikovanih elektronskih sertifikata:

- u roku od četiri (4) sata opozove kvalifikovani elektronski sertifikat u slučaju sumnje na zloupotrebu,
- inače, prvog radnog dana nakon prijema zahteva za opoziv.

(2) Po opozivu, sertifikat se upisuje u listu opozvanih sertifikata odmah (najviše 5 sekundi).

4.9.6 ZAHTEVI ZA TREĆE STRANE U VEZI PROVERE STATUSA KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA

Pre korišćenja kvalifikovanih elektronskih sertifikata izdatih od pružaoca usluga od poverenja HALCOM BG CA, treća lica koja se pouzdaju u dati kvalifikovani elektronski sertifikat moraju da provere najnoviji objavljeni registar opozvanih kvalifikovanih elektronskih sertifikata (CRL).

4.9.7 FREKVENCIJA IZDAVANJA REGISTRA OPPOZVANIH SERTIFIKATA SERTIFIKATA (CRL)

Registar opozvanih kvalifikovanih elektronskih sertifikata se ažurira/obnavlja (za pristup CRL pogledati poglavlje 7.2.3):

- nakon svakog opoziva sertifikata,
- jedanput dnevno, ako nije bilo novih zahteva ili promena u registru, 24 sata nakon poslednje obnove CRL.

4.9.8 VREME OBJAVE REGISTRA OPOZVANIH SERTIFIKATA (CRL)

(1) Objavljivanje novog registra opozvanih sertifikata vrši se:

- u registru opozvanih sertifikata na serveru ldap://ldap.halcom.rs odmah (najviše za 5 sekundi),
- a na web stranici http://domina.halcom.rs/crls sa zakašnjenjem od najviše deset (10) minuta

(2) Pružalac usluga od poverenja HALCOM BG CA pruža maksimalnu dostupnost svojih usluga svakog dana u godini, bez uzimanja u obzir nepredviđenih okolnosti. U slučaju

nepredviđenih okolnosti HALCOM BG CA u registar opozvanih sertifikata može upisati sertifikat najkasnije za 8 (osam) sati. HALCOM BG CA, u slučaju nepredviđene okolnosti kao rezultat više sile ili vanrednih događaja, objaviće registar opozvanih sertifikata najkasnije 24 sata od poslednjeg važećeg registra.

4.9.9 RASPOLOŽIVOST PROCEDURE „ON LINE" PROVERE STATUSA KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA

Podržan je protokol provere sertifikata (OCSP) u skladu sa evropskim i međunarodnim standardima i preporukama (pogledati poglavlje 7.3).

4.9.10 ZAHTEVI „ON LINE" PROVERE STATUSA KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA

Treće strane moraju pre upotrebe proveriti status sertifikata, da nije opozvan.

4.9.11 RASPOLOŽIVOST DRUGIH FORMI OBJAVLJIVANJA STATUSA KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA

Ovo poglavlje nije primenljivo u okviru ovih CP.

4.9.12 SPECIJALNI ZAHTEVI U ODNOSU NA KOMPROMITACIJU PRIVATNOG KLJUČA

Ovo poglavlje nije primenljivo u okviru ovih CP.

4.9.13 USLOVI ZA SUSPENZIJU KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA

(1) U slučaju da vlasnik sertifikata telefonski, elektronski ili FAX-om dostavi zahtev za opoziv sertifikata, isti se do prijema originalnog zahteva u pisanom obliku privremeno suspenduje.

(2) U slučaju da vlasnik sertifikata, druga ili treća lica, državni ili drugi odgovarajući organi odnosno samo pružalac usluga od poverenja, izraze sumnju da se u vezi sa sertifikatom postupa suprotno ovim pravilima, odnosno suprotno važećim propisima, taj se kvalifikovani elektronski sertifikat privremeno suspenduje.

4.9.14 KO MOŽE ZAHTEVATI SUSPENZIJU KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA

Pogledati poglavlje 4.9.13.

4.9.15 PROCEDURA ZAHTEVA ZA SUSPENZIJOM KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA

Pogledati poglavlje 4.9.13.

4.9.16 OGRANIČENJE PRERIODA SUSPENZIJE KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA

Pogledati poglavlje 4.9.13.

4.10 SERVISI PROVERE KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA

4.10.1 PRISTUP ZA PROVERE

(1) Registar opozvanih kvalifikovanih elektronskih sertifikata je javno objavljen na serveru ldap://ldap.halcom.rs/ putem LDAP protokola i na http://domina.halcom.rs/crls putem HTTP protokola.

(2) On-line provera statusa sertifikata je dostupna na linku http://ocsp.halcom.rs .

(3) Detalji o objavljivanju i načinu pristupa nalaze se u poglavljima 7.2 i 7.3.

4.10.2 RASPOLOŽIVOST SERVISA

(1) Provera statusa sertifikata raspoloživa je 24 sata na dan, svih dana u godini.

(2) Pružalac usluga od poverenja HALCOM BG CA pruža maksimalnu dostupnost svojih usluga svakog dana u godini, bez uzimanja u obzir nepredviđenih okolnosti. U slučaju nepredviđenih okolnosti HALCOM BG CA u registar opozvanih sertifikata može upisati sertifikat najkasnije za 8 (osam) sati. HALCOM BG CA, u slučaju nepredviđene okolnosti kao rezultat više sile ili vanrednih događaja, objaviće registar opozvanih sertifikata najkasnije 24 sata od poslednjeg važećeg registra.

4.10.3 DRUGE INFORMACIJE ZA PROVERAVANJE STATUSA

Ovo poglavlje nije primenljivo u okviru ovih CP.

4.11 PRESTANAK KORIŠĆENJA KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA

Odnos vlasnika i pružaoca usluga od poverenja se prekida ako:

- vlasnikov kvalifikovani elektronski sertifikat istekne, a on ga ne obnovi,
- je kvalifikovani elektronski sertifikat opozvan, a vlasnik ne podnese zahtev za novi.

4.12 OTKRIVANJE KOPIJE KLJUČEVA ZA DEŠIFROVANJE

4.12.1 RAZLOZI ZA OTKRIVANJE KOPIJE PRIVATNOG KLJUČA

Ovo poglavlje nije primenljivo u okviru ovih CP.

4.12.2 KO MOŽE ZAHTEVATI KOPIJU KLJUČEVA

Ovo poglavlje nije primenljivo u okviru ovih CP.

4.12.3 POSTUPAK ZA TRAŽENJE KOPIJE KLJUČEVA

Ovo poglavlje nije primenljivo u okviru ovih CP.

5. UPRAVNE, OPERATIVNE I FIZIČKE i BEZBEDNOSNE KONTROLE

(1) HALCOM BG CA planira i izvodi sve bezbednosne mere u skladu sa standardima ISO/IEC 27001, Common Criteria EAL4+ ili FIPS PUB 140-2 level 3 i sa tehničkim zahtevima ETSI.

(2) Oprema pružaoca usluga od poverenja HALCOM BG CA je postavljena u posebnim, odvojenim prostorijama i osigurana sistemom fizičkog i protiv-provalnog tehničkog obezbeđenja na više nivoa. Oprema je osigurana od neovlašćenog pristupa. Oprema je takođe obezbeđena i zaštićena protivpožarnim sistemom, sistemom protiv izliva vode, sistemom ventilacije i sistemom kontinualnog napajanja u više nivoa.

(3) Pružalac usluga od poverenja HALCOM BG CA čuva rezervne i distributivne medijume tako da se u najvećoj meri sprečava gubitak, upad ili neovlašćena upotreba ili promena sačuvanih informacija. Kako za obnovu podataka tako i za arhiviranje važnih informacija obezbeđene su rezervne kopije koje su sačuvane na drugom mestu od onoga gde se drži programska oprema za upravljanje kvalifikovanih elektronskih sertifikata, u cilju obezbeđenja kontinuiteta poslovanja u slučajevima kada se iz nekih razloga unište podaci na osnovnoj lokaciji.

(4) Detaljan opis infrastrukture pružaoca usluga od poverenja HALCOM BG CA, operativni

rad, postupci upravljanja infrastrukturom, kao i nadzor vezan za politiku bezbednosti operativnog rada, definisani su u internim pravilima rada pružaoca usluga od poverenja.

5.1.FIZIČKE BEZBEDNOSNE KONTROLE

(1) Oprema pružaoca usluga od poverenja je obezbeđena sistemima fizičkog i elektronskog obezbeđenja na više nivoa.

(2) Obezbeđenje infrastrukture pružaoca usluga od poverenja realizuje se u skladu sa preporukama struke za najviši nivo obezbeđenja.

(3) Celokupan opis infrastrukture pružaoca usluga od poverenja, primenjene procedure i obezbeđenje infrastrukture definisani su internim pravilima pružaoca usluga od poverenja.

5.1.1 LOKACIJA I ZGRADA PRUŽAOCA USLUGA OD POVERENJA

(1) Oprema pružaoca usluga od poverenja HALCOM BG CA je postavljena u posebnim, bezbednim i odvojenim prostorijama.

(2) Osigurana je sistemom fizičkog i elektronskog obezbeđenja na više nivoa.

(3) Detaljne odredbe nalaze se u internim pravilima pružaoca usluga od poverenja HALCOM BG CA.

5.1.2 FIZIČKI PRISTUP

(1) Pristup infrastrukturi pružaoca usluga od poverenja omogućen je samo ovlašćenim licima pružaoca usluga od poverenja u skladu sa njihovim zadacima i ovlašćenjima, pogledati poglavlju 5.2.1.

(2) Svi pristupi obezbeđeni su u skladu sa postojećim zakonodavstvom i preporukama.

(3) Detaljne odredbe fizičke kontrole bezbednosti nalaze se u internim pravilima pružaoca usluga od poverenja HALCOM BG CA.

5.1.3 ELEKTRIČNO NAPAJANJE I KLIMATIZACIJA

(1) U okviru infrastrukture pružaoca usluga od poverenja obezbeđeno je kontinualno napajanje i odgovarajući klimatski sistemi.

(2) Svi detalji o električnom napajanju i klimatizaciji se nalaze u internim pravilima rada pružaoca usluga od poverenja HALCOM BG CA.

5.1.4 ZAŠTITA OD POPLAVA

(1) Infrastruktura pružaoca usluga od poverenja HALCOM BG CA nije izložena opasnosti od poplava osim u slučaju više sile.

(2) Svi detalji se nalaze u internim pravilima rada pružaoca usluga od poverenja HALCOM BG CA.

5.1.5 PREVENCIJA I ZAŠTITA OD POŽARA

(1) Prostorije pružaoca usluga od poverenja su osigurane od mogućih izbijanja požara.

(2) Svi detalji o prevencije i protivpožarnoj zaštiti se nalaze u internim pravilima rada pružaoca usluga od poverenja HALCOM BG CA.

5.1.6 MEDIJUMI ZA ČUVANJE PODATAKA

(1) Nosioci podataka, na papiru ili u elektronskom obliku, bezbedno se čuvaju u zaštićenim prostorijama/objektima.

(2) Bezbedne kopije programske opreme i šifrovanih baza pružaoca usluga od poverenja HALCOM BG CA redovno se obnavljaju i čuvaju u dve odvojene i fizički obezbeđene prostorije na različitim lokacijama.

5.1.7 ODLAGANJE OTPADA

(1) HALCOM BG CA obezbeđuje sigurno uklanjanje i uništavanje dokumenata u fizičkom/papirnom i elektronskom obliku.

(2) Uklanjanje otpadaka izvodi specijalna komisija u skladu sa internim pravilima pružaoca usluga od poverenja HALCOM BG CA.

(3) Svi detalji o odlaganju smeća se nalaze u internim pravilima rada pružaoca usluga od poverenja HALCOM BG CA.

5.1.8 ČUVANJE NA UDALJENOJ LOKACIJI

Pogledati poglavlje 5.1.6.

5.2. ORGANIZACIONA STRUKTURA PRUŽAOCA USLUGA OD POVERENJA

5.2.1 ORGANIZACIONE GRUPE

(1) Operativni, organizaciono i profesionalno funkcionisanje pružaoca usluga od poverenja HALCOM BG CA rukovodi Sistem administrator koji je odgovoran za upravljanje procedurama HALCOM BG CA.

(2) Ovlašćenim licima pružaoca usluga od poverenja HALCOM BG CA smatraju se:

- zaposleni kod pružaoca usluga od poverenja HALCOM BG CA i
- zaposleni u registracionim telima.

(3) Zaposleni u HALCOM BG CA su raspoređeni u četiri organizacione jedinice koje pokrivaju područja sledećeg sadržaja:

- upravljanje informacionim sistemom,
- upravljanje kvalifikovanim elektronskim sertifikatima,
- bezbednost i kontrola,
- regulativna jedinica.

Organizaciona jedinica	Uloga	Opis osnovnih zadataka	Broj osoba
Upravljanje informacionim sistemom	Glavni sistem administrator	• Priprema početne konfiguracije sistema, • inicijalno podešavanje parametara novih podređenih pružalaca usluga od poverenja, • podešavanje početne konfiguracije mreže, • priprema medija za ponovno pokretanje sistema u slučaju katastrofe, • bezbedno skladištenje i distribucija	2

		kopija i nadogradnja na odvojenoj lokaciji.	
	Sistem administrator	• Upravljajte procedurama izdavanja sertifikata, • pomoć podređenim pružalaocima usluga od poverenja, • ovlašćenje potčinjenih pružalaca usluga poverenja, • pristup protokolu potpisivanje sertifikata, • bezbedno skladištenje i distribucija kopija i nadogradnja na odvojenoj lokaciju.	2
Upravljanje kvalifikovanim elektronskim sertifikatima	Sistem operater	• Priprema sistemskih kopija, nadogradnja i obnova softvera, bezbedno skladištite i distribuiranje kopija, i nadogradnje • administrativne funkcije vezane za održavanje • izvođenje arhiviranja zahtevanih sistemskih zapisa • dnevni pregled sistema, • štampanje PIN kodova.	2
	Operater za autorizaciju	• Potvrđivanje izdavanja sertifikata i aktiviranje lozinki.	2
	Administrator za elektronske sertifikate	• Predpersonalizacija pametnih kartica • priprema sertifikata (obrada potpisanih zahteva za sertifikate), • personalizacija (kreiranje sertifikata, upisivanje na sigurnom nosiocu, štampanje podataka vlasnika na sigurnom mediju), • distribucija sertifikata.	2
	Administrator za PIN kodove	• Distribucija PIN kodova.	2
	Službenik za prijave	• Identifikacija vlasnika ili budućeg vlasnika sertifikata, • prihvatanje dokumenata za izdavanje i opoziv sertifikata.	2

	Službenik za opoziv	• Prprema zahteva za opoziv, • opoziv sertifikata.	2
Bezbednost i kontrola	Glavni administrator bezbednosti	• Određivanje sigurnosnih pravila i praćenje njihovog poštovanja, • pregled dokumentacije sistema i kontrolnih evidencija za praćenje rada, • lična saradnja i pomoć u godišnjem popisu dokumentacije podređenih pružalaca usluga od poverenja.	2
	Sistem evidentičar	• Kontrola bezbednosnih pravila i njihovog poštovanja, • kontrola sistemske dokumentacije i kontrolnih evidencija za praćenje rada.	2
Pravno administrativno	Poverenik za privatnost	• Samostalno i nezavisno usmeravanje, zaštita privatnosti i zaštita ličnih podataka, • stručna pomoć menadžmentu i zaposlenima u operativnoj primeni mera za poštovanje privatnosti.	1
	Poverenik za regulativu i usklađenost	• Obezbjeđivanje usklađenosti sa važećim evropskim i domaćim propisima, međunarodnim standardima i preporukama, • stručna pomoć menadžmentu i zaposlenima u operativnoj primeni mera za i regulatornu usklađenost.	1

5.2.2 BROJ OSOBA ZA POJEDINAČNE ZADATKE

(1) Operativne radne uloge planirane su tako da u najvećoj mogućoj meri sprečavaju mogućnost zloupotreba i podeljene su na pojedinačne, međusobno odvojene organizacione jedinice:

Organizaciona jedinica: Upravljanje informacionim sistemom

Uloga: Glavni sistem administrator

Broj osoba: 2

Zadaci:

- priprema početne konfiguracije sistema,
- inicijalno podešavanje parametara novih podređenih pružalaca usluga od poverenja,
- podešavanje početne konfiguracije mreže,
- priprema medija za ponovno pokretanje sistema u slučaju katastrofe,
- bezbedno skladištenje i distribucija kopija i nadogradnja na odvojenoj lokaciji.

Organizaciona jedinica: Upravljanje informacionim sistemom

Uloga: Sistem administrator

Broj osoba: 2

Zadaci:

- upravljajte procedurama izdavanja sertifikata,• pomoć podređenim pružalaocima usluga od poverenja,
- ovlašćenje potčinjenih pružalaca usluga poverenja,
- pristup protokolu potpisivanje sertifikata,
- bezbedno skladištenje i distribucija kopija i nadogradnja na odvojenoj lokaciju.

Organizaciona jedinica: Upravljanje kvalifikovanim elektronskim sertifikatima

Uloga: Sistem operater

Broj osoba: 2

Zadaci:

- priprema sistemskih kopija, nadogradnja i obnova softvera, bezbedno skladištite i distribuiranje kopija i nadogradnje,
- administrativne funkcije vezane za održavanje,
- izvođenje arhiviranja zahtevanih sistemskih zapisa,
- dnevni pregled sistema,
- štampanje PIN kodova.

Organizaciona jedinica: Upravljanje kvalifikovanim elektronskim sertifikatima

Uloga: Operater za autorizaciju

Broj osoba: 2

Zadaci:

- potvrđivanje izdavanja sertifikata i aktiviranje lozinki.

Organizaciona jedinica: Upravljanje kvalifikovanim elektronskim sertifikatima

Uloga: Administrator za sertifikate

Broj osoba: 2

Zadaci:

- predpersonalizacija pametnih kartica,
- priprema sertifikata (obrada potpisanih zahteva za sertifikate),
- personalizacija (kreiranje sertifikata, upisivanje na sigurnom nosiocu, štampanje podataka vlasnika na sigurnom mediju),
- distribucija sertifikata.

Organizaciona jedinica: Upravljanje kvalifikovanim elektronskim sertifikatima

Uloga: Administrator za PIN/PUK kodove

Broj osoba: 2

Zadaci:

- distribucija PIN kodova .

Organizaciona jedinica: Upravljanje kvalifikovanim elektronskim sertifikatima

Uloga: Službenik za prijavu

Broj osoba: 2

Zadaci:

- identifikacija vlasnika ili budućeg vlasnika sertifikata,
- prihvatanje dokumenata za izdavanje i opoziv sertifikata.

Organizaciona jedinica: Upravljanje kvalifikovanim elektronskim sertifikatima

Uloga: Službenik za opoziv

Broj osoba: 2

Zadaci:

- priprema zahteva za opoziv,
- opoziv sertifikata.

Organizaciona jedinica: Bezbednost i kontrola

Uloga: Glavni administrator bezbednosti

Broj osoba: 2

Zadaci:

- određivanje sigurnosnih pravila i praćenje njihovog poštovanja,
- pregled dokumentacije sistema i kontrolnih evidencija za praćenje rada,
- lična saradnja i pomoć u godišnjem popisu dokumentacije podređenih pružalaca usluga od poverenja.

Organizaciona jedinica: Bezbednost i kontrola

Uloga: Sistem evidentičar

Broj osoba: 2

Zadaci:

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 330 6500, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 6619, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

- kontrola bezbednosnih pravila i njihovog poštovanja,
- kontrola sistemske dokumentacije i kontrolnih evidencija za praćenje rada.

Organizaciona jedinica: Pravno administrativna

Uloga: Poverenik za privatnost

Broj osoba: 1

Zadaci:

- samostalno i nezavisno usmeravanje, zaštita privatnosti i zaštita ličnih podataka,
- stručna pomoć menadžmentu i zaposlenima u operativnoj primeni mera za poštovanje privatnosti.

Organizaciona jedinica: Pravno administrativna

Uloga: Poverenik za regulativu i usklađenost

Broj osoba: 1

Zadaci:

- obezbjeđivanje usklađenosti sa važećim evropskim i domaćim propisima, međunarodnim standardima i preporukama,
- stručna pomoć menadžmentu i zaposlenima u operativnoj primeni mera za i regulatornu usklađenost.

(2) Naveden je minimalan broj zaposlenih za pojedinačne uloge.

5.2.3 IDENTIFIKACIJA I PROVERA ZA SVAKU ULOGU

Dokazivanje identiteta i prava pristupa za izvršavanje pojedinačnih zadataka u skladu sa ulogama pojedinačnih organizacionih jedinica, kao i za izvršavanje zadataka registracionog tela, osigurano je bezbednosnim mehanizmima i kontrolnim postupcima u skladu sa internim pravilima pružaoca usluga od poverenja HALCOM BG CA.

5.2.4 ULOGE KOJE ZAHTEVAJU RAZDVAJANJE DUŽNOSTI

U internim pravilima rada pružaoca usluga od poverenja HALCOM BG CA, svakoj od prethodno navedenih uloga veoma je tačno određeno sa kojom od uloga definisani zadaci u njihovoj odgovornosti mogu ili ne mogu da budu kompatibilni. Za neke od zadataka, neophodno je prisustvo barem dva ovlašćena lica. U slučaju nepredviđenog odsustva određenih zaposlenih, njihove uloge preuzimaju drugi zaposleni, ako to prema internim pravilima nije nekompatibilno.

5.3 KADROVSKE BEZBEDNOSNE KONTROLE

(1) Operativni, organizacioni i profesionalni rad pružaoca usluga od poverenja HALCOM BG CA kontroliše sistem evidentičar koji ne radi posao upravljanja sertifikatima.

(2) Sistem evidentičar nadgleda rad HALCOM BG CA. Sistem evidentičar u slučaju otkrivanja manjkavosti, određuje odgovarajuće mere za eliminisanje tih manjkavosti, koje je HALCOM BG CA dužan izvesti, dok sistem evidentičar nadgleda izvođenje određenih mera.

5.3.1 KVALIFIKACIJA I ISKUSTVO

HALCOM BG CA zapošljava pouzdane i stručno osposobljene zaposlene za koje se zahteva potvrda da nisu kažnjavani za bilo kakvo kriminalno delo. Svi zaposleni se redovno usavršavaju i stiču dodatna znanja vezana za svoje stručno područje.

5.3.2 PROVERA ZAPOSLENIH

Zaposleni pružaoca usluga od poverenja moraju ispuniti zahteve važećih propisa i tehničkih standarda kao i preporuke odgovarajućih kvalifikacija i iskustva.

5.3.3 DODATNE OBUKE ZAPOSLENIH

HALCOM BG CA pružalac usluga od poverenja obezbeđuje obuku za svoje zaposlene u cilju realizacije zadataka svih navedenih organizacionih grupa i zadataka registracionih tela.

5.3.4 UČESTANOST I ZAHTEVI PONOVNE OBUKE

Godišnje ažuriranje obuke izvršava se u cilju uspostave kontinuiteta i ažurnosti znanja zaposlenih, kao i odgovarajućih procedura.

5.3.5 FREKVENCIJA I SEKVENCA ROTACIJE POSLOVA

Ovo poglavlje nije primenljivo u okviru ovih CP.

5.3.6 KAZNENE MERE U ODNOSU NA ZAPOSLENE ZA NEAUTORIZOVANE AKTIVNOSTI

Sankcije se, u slučajevima neovlašćenog ili nemarnog izvođenja zadataka, za ovlašćena lica pružaoca usluga od poverenja, sprovode u skladu sa validnim propisima i internim pravilnikom o disciplinskoj i odštetnoj odgovornosti zaposlenog.

5.3.7 ZAHTEVI ZA NEZAVISNA LICA POD UGOVOROM

Nezavisna lica pod ugovorom su subjekti istih procedura zaštite privatnosti i uslova poverljivosti kao i zaposleni u okviru HALCOM BG CA.

5.3.8 DOKUMENTACIJA KOJA SE DOSTAVLJA ZAPOSLENIMA

HALCOM BG CA čini dostupnom svu neophodnu dokumentaciju zaposlenima koja je u skladu sa njihovim dužnostima i zadacima.

5.4 PROVERE BEZBEDNOSTI SISTEMA

5.4.1 VRSTE EVIDENCIJA

(1) Pružalac usluga od poverenja HALCOM BG CA redovno proverava i evidentira sve što značajno utiče na:

- sigurnost infrastrukture,
- nesmetano delovanje svih sigurnosnih sistema,
- kao i da li je u međuvremenu došlo do upada ili pokušaja upada neovlašćenih lica do opreme ili podataka.

(2) Detaljni podaci o tome dati su u internim pravilima rada pružaoca usluga od poverenja HALCOM BG CA.

5.4.2 FREKVENCIJA PROVERAVANJA EVIDENCIJA

Pružalac usluga od poverenja HALCOM BG CA sprovodi sigurnosne preglede svoje infrastrukture, odnosno dnevnika, jednom dnevno.

5.4.3 PERIOD ČUVANJA AUDIT LOGOVA

Logovi se čuvaju najmanje deset (10) godina nakon njihove pojave, osim ako nije određen duži rok zakonom.

5.4.4 ZAŠTITA AUDIT LOGOVA

(1) HALCOM BG CA implementira mehanizme zaštite audit logova od modifikacije i brisanja tako da niko ne može izvršiti pomenute operacije.

(2) Postupak zaštite audit logova precizno je definisan u internim pravilima HALCOM BG CA.

5.4.5 PROCEDURE BACK UP-A AUDIT LOGOVA

(1) Sigurnosne kopije dnevnika/logova se izrađuju na dnevnoj bazi.

(2) Detalji su dati u internim pravilima rada pružaoca usluga od poverenja HALCOM BG CA.

5.4.6 SISTEM SAKUPLJANJA AUDIT LOGOVA

(1) Podaci se za potrebe dnevnika sakupljaju bilo automatski, bilo ručno, u zavisnosti od vrste podataka.

(2) Detalji o sistemu sakupljanja audit logova propisani su u internim pravilima rada HALCOM BG CA.

5.4.7 OBAVEŠTAVANJE SUBJEKTA KOJI JE PROUZROKOVAO DOGAĐAJ

Subjekat koji je prouzrokovao određeni audit događaj se ne obaveštava o samoj audit aktivnosti.

5.4.8 PROCENA RANJIVOSTI SISTEMA

(1) Analiza dnevnika i nadzor nad sprovođenjem svih postupaka redovno se sprovode od strane ovlašćenih lica pružaoca usluga od poverenja ili automatski, odgovarajućim sigurnosnim mehanizmima na svoj računarsko-komunikacionoj opremi koja je u nadležnosti pružaoca usluga od poverenja.

(2) Ocena ranjivosti se sprovodi na osnovu analize dnevnika.

(3) Detalji procene ranjivosti sistema dati su u internim pravilima rada pružaoca usluga od poverenja HALCOM BG CA.

(4) Analiza konfiguracija sistema i njihova usaglašenost sa internim politikama redovno se sprovodi, najmanje četiri puta godišnje.

5.5 ARHIVIRANJE ZAPISA

5.5.1 TIPOVI ARHIVSKIH ZAPISA

Pružalac usluga od poverenja HALCOM BG CA, u skladu sa odredbama važećih propisa, čuva sledeće podatke/dokumente/arhivsku građu/registratorski materijal:

- dnevnike,
- zapisnike,

- sva dokazna sredstva o izvršenoj proveri identiteta vlasnika sertifikata,
- sve zahteve za dobijanje sertifikata,
- kvalifikovane elektronske sertifikate i registre opozvanih sertifikata,
- politike rada,
- CPS,
- objave i obaveštenja pružaoca usluga od poverenja HALCOM BG CA i
- druge dokumente u skladu sa važećim propisima.

5.5.2 PERIOD ČUVANJA ARHIVE

(1) Podaci se čuvaju u skladu sa zakonskim odredbama.

(2) Dugoročno uskladišteni podaci koji se odnose na ključeve i sertifikate čuvaju se najmanje deset(10) godina nakon isteka sertifikata na koje se odnosi informacija, ako posebnim zakonom nije određen duži rok.

(3) Ostali dugoročno uskladišteni podaci se čuvaju najmanje deset (10) godina nakon njihovog nastanka, pod uslovom da poseban zakon ne predviđa duži rok.

5.5.3 ZAŠTITA ARHIVE

(1) Podaci koji se čuvaju dugotrajno čuvaju se bezbedno.

(2) Detaljne odredbe dugotrajnog čuvanja definišu se u internim pravilima rada HALCOM BG CA a u skladu sa važećim propisima, standardima i preporukama.

5.5.4 PROCEDURA BACK UP-A ARHIVE

(1) Kopija dugotrajno čuvanih podataka čuva se bezbedno.

(2) Detaljne odredbe dugotrajnog čuvanja kopija podataka definišu se u internim pravilima rada pružaoca usluga od poverenja HALCOM BG CA, a u skladu sa važećim propisima, standardima i preporukama.

5.5.5 ZAHTEVI ZA VREMENSKIM PEČATOM ZAPISA

Ovo poglavlje nije primenljivo u okviru ovih CP.

5.5.6 SISTEM SKUPLJANJA ZAPISA

(1) Podaci se sakupljaju na način koji je u skladu sa vrstom dokumenta.

(2) Detaljne odredbe načina sakupljanja podataka definišu se u internim pravilima rada HALCOM BG CA a u skladu sa važećim propisima, standardima i preporukama.

5.5.7 PROCEDURE ZA DOBIJANJE I VERIFIKACIJU INFORMACIJA IZ ARHIVE

(1) Pristup dugotrajno čuvanim podacima omogućen je samo ovlašćenim licima.

(2) Detaljne odredbe u vezi pristupa dugotrajno čuvanim podacima definišu se u internim pravilima rada pružaoca usluga od poverenja HALCOM BG CA a u skladu sa važećim propisima, standardima i preporukama.

5.6 IZMENA KLJUČEVA PRUŽAOCA USLUGA OD POVERENJA

U slučaju novo izdatog sopstvenog kvalifikovanog elektronskog sertifikata pružaoca usluga od poverenja HALCOM BG CA, isti se odmah objavljuje na web stranicama pružaoca usluga od poverenja HALCOM BG CA.

5.7 KOMPROMITACIJA I OPORAVAK U SLUČAJU KATASTROFE

5.7.1 PROCEDURE ZA POSTUPANJE U INCIDENTNIM I KOMPROMITUJUĆIM SITUACIJAMA

U internim pravilima rada, HALCOM BG CA dokumentuje procedure koje treba izvršiti pri rešavanju incidenata, kao i izveštavanje u vezi eventualne kompromitacije ključeva.

5.7.2 RAČUNARSKI RESURSI, SOFTVER ILI PODACI KOJI SU OŠTEĆENI

Detaljne odredbe se definišu u internim pravilima rada pružaoca usluga od poverenja HALCOM BG CA a u skladu sa važećim propisima, standardima i preporukama.

5.7.3 PROCEDURE KOJE SE SPROVODE KOD KOMPROMITACIJE PRIVATNOG KLJUČA KORISNIKA

Detaljne odredbe se definišu u internim pravilima rada pružaoca usluga od poverenja HALCOM BG CA a u skladu sa važećim propisima, standardima i preporukama.

5.7.4 PLAN POSLOVANJA NAKON KATASTROFE

Detaljne odredbe se definišu u internim pravilima rada pružaoca usluga od poverenja HALCOM BG CA a u skladu sa važećim propisima, standardima i preporukama.

5.8 ZAVRŠETAK RADA CA ili RA

(1) Pre nego što prekine svoje aktivnosti pružanja usluga od poverenja, HALCOM BG CA:

- Obezbeđuje svojim korisnicima koji imaju validne sertifikate obaveštenje o nameri da prestane sa pružanjem usluga od poverenja, tj. da prestane da izvršava aktivnosti u svojstvu CA.
- Povlači sve sertifikate koji su još uvek validni (tj. one koji nisu povučeni i nije im istekao rok važnosti), nakon obaveštenja, a bez zahteva za saglasnošću korisnika.
- Blagovremeno obaveštava o povlačenju kvalifikovanih elektronskih sertifikata sve korisnike na koje se to odnosi (vlasnike sertifikata, treća lica koja se pouzdaju u sertifikate i odgovarajuće državne organe). Korisnike sa kojima ima posebne ugovore obaveštava individualno a sve ostale putem internet stranice.
- Čini razumne mere u cilju zaštite zapisa koje čuva u skladu sa ovim CP dokumentom.
- Ukoliko je to moguće, obezbeđuje odgovarajuće mere obezbeđenja sukcesije u smislu ponovnog izdavana kvalifikovanih elektronskih sertifikata od strane drugog CA tela koje je sukcesor – nastavljač izdavanja kvalifikovanih elektronskih sertifikata datog CA – i koje poštuje ekvivalentne CP i CPS dokumente.
- Odredi odgovarajuće telo da preuzme vođenje CRL listi
- Odredi odgovarajuće telo da preuzme vođenje dokumentaciju (zahteve, dnevnike, opozive)
- Opoziva ovlašćenja Registracionih tela.
- Uništava svoje privatne ključeve.

(2) Detaljne odredbe i ažuran plan se definišu u internim pravilima rada pružaoca usluga od poverenja HALCOM BG CA a u skladu sa važećim propisima, standardima i preporukama.

6. TEHNIČKE BEZBEDNOSNE KONTROLE

6.1 GENERISANJE I INSTALACIJA ASIMETRIČNOG KLJUČA

6.1.1 PROCES GENERISANJA ASIMETRIČNOG PARA KLJUČA HALCOM BG CA PRUŽAOCA USLUGA OD POVERENJA

(1) Asimetrični par ključeva pružaoca usluga od poverenja HALCOM BG CA za elektronsko potpisivanje sertifikata i verifikaciju potpisa generiše se prema najvišim sigurnosnim standardima u sigurnom okruženju pružaoca usluga od poverenja HALCOM BG CA.

(2) Za korisnike, vlasnike sertifikata, pružalac usluga od poverenja HALCOM BG CA generiše sledeće asimetrične ključeve i sertifikate:

Tip sertifikata	Ključ	Ključ se generiše
Root i intermediate/podređeni sertifikati	Par ključeva	Na HSM (eng. Hardware Security Module), u sigurnom okruženju pružaoca usluga od poverenja.
Napredni sertifikat	Dva para ključeva	Na sigurnom medijumu, (eng. QSCD) kod pružaoca usluga od poverenjua.

6.1.2 ISPORUKA PRIVATNOG KLJUČA KORISNKU

Način prenosa privatnih ključeva je dat u sledećoj tabeli:

Tip sertifikata	Ključ	Isporuka
Root i intermediate/podređeni sertifikati	Privatni ključ	Nema isporuke
Napredni sertifikat	Privatni ključ	Prenos sigurnosnog medijuma (nosioca) preporučeno poštom

6.1.3 DOSTAVA JAVNOG KLJUČA IZDAVAOCU KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA

Za napredne sertifikate, ključevi se generišu na sigurnom nosiocu u bezbednom okruženju pružaoca usluga od poverenja HALCOM BG CA.

6.1.4 DOSTAVA JAVNOG KLJUČA IZDAVAOCA KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA TREĆIM STRANAMA elektronskih sertifikata trećim stranama

Kvalifikovani elektronski sertifikat sa javnim ključem pružaoca usluga od poverenja HALCOM BG CA vlasnicima kvalifikovanih elektronskih sertifikata, odnosno trećim licima, dostupan je:

- putem web stranice pružaoca usluga od poverenja,
- u javnom registru ldap://ldap.halcom.rs po protokolu LDAP (pogledaj poglavlje 2.3),
- u obliku PEM na adresi http://domina.hacom.rs/crls, pri čemu se dodatno mora proveriti autentičnost sertifikata.

6.1.5 DUŽINA ASIMETRIČNIH KLJUČEVA

Sertifikat	Dužina ključa prema RSA [bit]

Sertifikat pružaoca usluga od poverenja HALCOM BG CA (root)	Najmanje 2048
Intermediate (podređeni) sertifikat pružaoca usluga od poverenja HALCOM BG CA	Najmanje 2048
Kvalifikovani sertifikati za korisnike – pravna lica	Najmanje 2048

6.1.6 GENERISANJE KRIPTOGRAFSKIH PARAMETARA I PROVERA KVALITETA

Kvalitet parametara asimetričnog para ključa pružaoca usluga od poverenja HALCOM BG CA garantovan je od strane proizvođača programske opreme, HSM (Hardware Security Module), koji koristi kvalitetne i sertifikovane hardverske generatore slučajnih brojeva (engl. *random number generator*).

6.1.7 MOGUĆE ''KEY USAGE'' OPCIJE – SVRHA KLJUČEVA I SERTIFIKATA

(1) Namena upotrebe asimetričnih ključeva, odnosno kvalifikovanih elektronskih sertifikata, u skladu je sa *X.509 v3* standardom i definisana je u odgovarajućoj ekstenziji kvalifikovanih elektronskih sertifikata: *korišćenje ključa* (engl. *keyUsage)* i *prošireno korišćenje ključa* (engl. *extended keyUsage).*

(2) Elektronsko potpisivanje kvalifikovanih elektronskih sertifikata i registra opozvanih kvalifikovanih elektronskih sertifikata vrši se privatnim ključem HALCOM BG CA, dok se za verifikaciju pomenutih potpisa koristi javni ključ iz kvalifikovanog elektronskog sertifikata HALCOM BG CA. U tom smislu, *keyUsage* ekstenzija u sertifikatu pružaoca usluga od poverenja sadrži odgovarajuće vrednosti.

(3) Profili kvalifikovanih elektronskih sertifikata koje izdaje pružalac usluga od poverenja HALCOM BG CA navedeni su u poglavlju 7.1.

6.2 ZAŠTITA PRIVATNOG KLJUČA I TEHNIČKE KONTROLE KRIPTOGRAFSKOG MODULA

6.2.1 STANDARDI I KONTROLE KRIPTOGRAFSKOG HARDVERSKOG MODULA

Privatni ključ pružaoca usluga od poverenja HALCOM BG CA zaštićen je kriptografskim modulom koji je sertifikovan u skladu sa FIPS PUB 140-2 nivo 3 ili Common Criteria EAL4+.

6.2.2 KONTROLA PRIVATNOG KLJUČA OD STRANE OVLAŠĆENIH OSOBA

Odredbe vezane za pristup privatnom ključu HALCOM BG CA definisane su u internim pravilima rada pružaoca usluga od poverenja HALCOM BG CA.

6.2.3 OTKRIVANJE KOPIJE PRIVATNOG KLJUČA

Odredbe vezane za pristup privatnom ključu pružaoca usluga od poverenja HALCOM BG CA u skladu je sa važećim propisima i Opštim pravilima poslovanja kao i internim pravilima poslovanja pružaoca usluga od poverenja HALCOM BG CA.

6.2.4 BACKUP KLJUČEVA HALCOM BG CA PRUŽAOCA USLUGA OD POVERENJA

Odredbe vezane za kopiranje privatnog ključa pružaoca usluga od poverenja HALCOM BG CA u skladu je sa važećim propisima i Opštim pravilima poslovanja kao i internim pravilima poslovanja pružaoca usluga od poverenja HALCOM BG CA.

6.2.5 ARHIVIRANJE PRIVATNOG KLJUČA

(1) Kopije privatnih ključeva HALCOM BG CA mogu se kopirati i čuvati samo do strane ovlašćenih osoba pružaoca usluga od poverenja HALCOM BG CA. Sigurne kopije privatnih ključeva čuvaju se sa istim nivoom zaštite kao i ključevi koji su u upotrebi.

(2) Precizniji uslovi kopiranja privatnih ključeva pružaoca usluga od poverenja HALCOM BG CA u skladu je sa važećim propisima i Opštim pravilima poslovanja kao i internim pravilima poslovanja pružaoca usluga od poverenja HALCOM BG CA.

6.2.6 TRANSFER PRIVATNOG KLJUČA NA HARDVERSKI KRIPTOGRAFSKI MODUL

(1) Privatni par ključeva pružaoca usluga od poverenja se generiše u HSM uređaju. Detaljnije odredbe vezane za prenos privatnog ključa HALCOM BG CA definisane su u internim pravilima rada pružaoca usluga od poverenja HALCOM BG CA.

(2) Privatni par ključeva za vlasnike sertifikata se generišu u smart kartici/USB ključu i ne mogu se pročitati sa smart kartice/USB ključa, kao takvi se naknadno dostavljaju vlasniku sertifikata.

6.2.7 ČUVANJE PRIVATNOG KLJUČA NA HARDVERSKOM KRIPTOGRAFSKOM MODULU

(1) Privatni ključ pružaoca usluga od poverenja HALCOM BG CA se čuva u kriptografskom modulu, koje je sertifikovan u skladu sa FIPS PUB 140-2 nivo 3 i/ili Common Criteria EAL4+.

(2) Privatni ključevi korisnika:

- napredni sertifikati se generišu i čuvaju na bezbednom medijumu.

6.2.8 METODA AKTIVACIJE PRIVATNOG KLJUČA

(1) Postupak aktivacije privatnog ključa HALCOM BG CA i procedura distribuirane odgovornosti u vezi tog postupka definisane su u internim pravilima rada pružaoca usluga od poverenja.

(2) HALCOM BG CA preporučuje upotrebu programskog okruženja, koji prilikom odjave ili nakon isteka nekog vremena, onemogući pristup njihovom privatnom ključu bez unosa odgovarajuće lozinke.

6.2.9 METODA DEAKTIVIRANJA PRIVATNOG KLJUČA

Postupak za deaktivaciju/uništavanje privatnog ključa pružaoca usluga od poverenja HALCOM BG CA vrši se bezbednim načinom u skladu sa odredbama internih pravila rada HALCOM BG CA.

6.2.10 METODA UNIŠTAVANJA PRIVATNOG KLJUČA

(1) Postupak za uništenje privatnog ključa pružaoca usluga od poverenja HALCOM BG CA vrši se bezbednim načinom u skladu sa odredbama internih pravila rada HALCOM BG CA i uputstva proizvođača bezbednog kriptografskog uređaja. Privatni ključ se uništava na takav način da ga nije moguće ponovo koristiti.

(2) Uništenje privatnih ključeva korisnika, je u nadležnosti vlasnika sertifikata. Mogu koristiti odgovarajuće aplikacije za sigurno brisanje sertifikata.

6.2.11 KARAKTERISTIKE KRIPTOGRAFSKIH HARDVERSKIH MODULA

Bezbedni kriptografski uređaji odgovaraju standardima navedenim u poglavlju 6.2.1.

6.3 NEKI DRUGI ASPEKTI URPAVLJANJA PAROM KLJUČEVA

6.3.1 ARHIVIRANJE JAVNOG KLJUČA

Pružalac usluga od poverenja HALCOM BG CA arhivira svoj javni ključ, kao i javne ključeve vlasnika kvalifikovanog elektronskog sertifikata, kao što je navedeno u poglavlju 5.5.

6.3.2 PERIOD VALIDNOSTI KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA I PRIVATNOG KLJUČA

(1) U dole navedenoj tabeli su data vremena važenja privatnih i javnih ključeva pružaoca usluga od poverenja HALCOM BG CA i ovlašćenih korisnika pravnih lica – vlasnika sertifikata.

Tip kvalifikovanih elektronskih sertifikata	Ključ	Važenje
Root sertifikat pružaoca usluga od poverenja HALCOM BG CA	Privatni ključ	20 godina
	Javni ključ	20 godina
Intermediate sertifikat pružaoca usluga od poverenja HALCOM BG CA	Privatni ključ	10 godina
	Javni ključ	10 godina
Napredni sertifikati	Privatni ključ	3 godine
	Javni ključ	3 godine

(2) Pružalac usluga od poverenja HALCOM BG CA može u iznimnim slučajevima za pojedinačne sertifikate odrediti i kraći rok važenja sertifikata (tj. javnog ključa u sertifikatu). Kraći rok važenja sertifikata se određuje u slučajevima izdavanja sertifikata nerezidentima u odnosu na trajanje njihovog identifikacionog dokumenta, ukoliko je trajanje identifikacionog dokumenta kraće od 3 (tri) godine.

6.4. AKTIVACIONI PODACI

6.4.1 GENERISANJE I INSTALACIJA AKTIVACIONIH PODATAKA

PIN kodovi služe za korišćenje naprednih sertifikata a za otključavanje PUK kod, koji se generišu u HALCOM BG CA. Vlasnik sertifikata mora promeniti PIN kod pri prvoj upotrebi.

6.4.2 ZAŠTITA AKTIVACIONIH PODATAKA

PIN/PUK kodovi za smart karticu/USB ključ korisnika bezbedno se generišu u okviru pružaoca usluga od poverenja HALCOM BG CA. HALCOM BG CA isporučuje vlasniku sertifikata PIN/PUK kod lično u okviru registracionog tela, odnosno putem kurirske službe. HALCOM BG CA preporučuje da se oba koda čuvaju na sigurnom mestu, na kojem pristup ima samo vlasnik.

6.4.3 DRUGI ASPEKTI U VEZI AKTIVACIONIH PODATAKA

Ovo poglavlje nije primenljivo u okviru ovog CP.

6.5 BEZBEDNOSNE KONTROLE RAČUNARA

6.5.1 SPECIFIČNI ZAHTEVI ZA BEZBEDNOST RAČUNARA

Detaljna odredbe su u skladu sa važećim propisima, standardima i preporukama koja su uključena u Opšta pravila rada i interna pravila rada HALCOM BG CA.

6.5.2 NIVO BEZBEDNOSTI

Detaljna odredbe su u skladu sa važećim propisima, standardima i preporukama koja su uključena u Opšta pravila rada i interna pravila rada HALCOM BG CA.

6.6 ŽIVOTNI CIKLUS TEHNIČKIH BEZBEDNOSNIH KONTROLA

6.6.1 KONTROLE SISTEMSKOG RAZVOJA

HALCOM BG CA upotrebljava softver i hardver koji je sertifikovan u skladu da FIPS PUB 140-2 nivo 3 i/ili Common Criteria EAL4+.

6.6.2 KONTROLE UPRAVLJANJA BEZBEDNOŠĆU

Detaljne odredbe su u skladu sa važećim propisima, standardima i preporukama koja su uključena u Opšta pravila rada i interna pravila rada HALCOM BG CA.

6.6.3 ŽIVOTNI CIKLUS BEZBEDNOSNIH KONTROLA

Detaljni tehnički uslovi su navedeni u internim pravilima pružaoca usluga od poverenja HALCOM BG CA.

6.7 MREŽNE BEZBEDNOSNE KONTROLE

Detaljne odredbe su u skladu sa važećim propisima, standardima i preporukama koja su uključena u Opšta pravila rada i interna pravila rada HALCOM BG CA.

6.8 VREMENSKI PEČAT

Ovo poglavlje nije primenljivo u okviru ovog CP.

7. PROFIL KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA, CRL i OCSP

Ovo poglavlje specificira formate kvalifikovanih elektronskih sertifikata i registra opozvanih kvalifikovanih elektronskih sertifikata (CRL) koje izdaje HALCOM BG CA pružalac usluga od poverenja.

7.1 PROFIL KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA

(1) U skladu sa CPS i politikama HALCOM BG CA izdaje sledeće napredne sertifikate.

(2) Sertifikati sadrže informacije koje su prema propisima označeni kao kvalifikovani sertifikati.

(3) Sertifikati HALCOM BG CA prate standard X.509.

7.1.1 BROJ VERZIJE

HALCOM BG CA pružalac usluga od poverenja izdaje elektronske sertifikate u formatu X.509 tako da su svi sertifikati verzije 3.

7.1.2 EKSTENZIJE U SERTIFIKATU

(1) Profil **ROOT sertifikata** Halcom BG Root CA

Nazivi polja	**Vrednost odnosno značenje**
Osnovna polja u sertifikatima	
Varijanta engl. *Version*	V3
Identifikaciona oznaka kvalifikovanih elektronskih sertifikata engl. *Serial Number*	6e 95 f3 d2 71 f5 e5 6b
Algoritam za potpis, engl. *Signature algorithm*	Sha256RSA (OID 1.2.840.113549.1.1.11)
Izdavalac engl. *Issuer*	CN = Halcom BG Root CA 2.5.4.97 = VATRS-102193722 2.5.4.97 = MB:RS-17419722 O = Halcom a.d. Beograd C = RS
Valjanost, engl. *Validity*	Valid from: <16.10.2018 10:00:00 GMT> Valid to: <16.10.2038 10:00:00 GMT>
Vlasnik, engl. Subject	CN = Halcom BG Root CA 2.5.4.97 = VATRS-102193722 2.5.4.97 = MB:RS-17419722 O = Halcom a.d. Beograd C = RS
Algoritam za javni ključ, engl. *Subject Public Key Algorithm*	rsaEncryption (OID 1.2.840.113549.1.1.1)

Javni ključ, engl. *Public Key (... bits)*	30 82 01 0a 02 82 01 01 00 e6 cf d3 da 3b c5 9d e3 ac 77 31 73 2a e7 f5 89 7f 5c 36 ed 58 8b 63 19 61 17 5c 3e 29 e5 af 58 c4 6e 08 41 2f 37 dd 3a e3 ab c5 3e 45 c8 6a f4 19 3a d8 54 a6 01 23 83 0b e5 97 65 ae 60 09 e4 a9 d2 1a 6b 3e 18 3a 92 e5 6f 09 5d bd 14 e4 7b 64 46 15 b7 d2 27 09 38 4b 5b 3d 46 2f 7a cd c0 a2 57 1d 05 93 6a 54 9b 43 0e c0 cf 07 f7 e2 98 82 b6 32 c6 a0 27 67 dc a7 b9 ae 18 ff ff a5 b2 aa 25 64 ce 15 18 e8 14 18 89 7b b9 b6 8c 4f 78 0e 7c c2 a2 94 b0 e6 78 9a 7c be d0 c0 0e aa f0 f5 90 74 ea e1 ee 25 12 34 cf ec be 48 45 01 58 36 9c 03 24 b4 90 3d a1 3b 29 86 87 a3 6d fd 2d f9 87 cd af e7 3d 87 53 1e 4c e0 d0 b0 62 c4 6e 3b 9b 35 f5 e0 cb d0 04 92 35 34 c6 3f 9e 31 9d b6 de 4d c3 fc bb b3 20 fe 6a d7 8a e2 a5 68 76 eb 81 4c be be 29 4c 88 64 a1 8a 47 f8 61 d1 83 02 03 01 00 01
Vlasnikov javni ključ koji pripada odgovarajućem paru, ključeva, šifriran alg. RSA, engl. *RSA Public Key*	dužina ključa je 2048 bitova
Ekstenzije u okviru X.509v3 standarda	
korišćenje ključa, OID 2.5.29.15, *engl. Key Usage*	Certificate Signing, Off-line CRL Signing, CRL Signing
Identifikator ključa vlasnika, OID 2.5.*29.14,* *engl. Subject Key Identifier*	identifikator ključa vlasnika 49 2c 22 39 ad 8d a4 e0
Osnovna ograničenja, OID 2.5.29.19, engl. *Basic Constraints*	Subject Type=CA Path Length Constraint=None
Dodatna identifikacija (nije deo kvalifikovanih elektronskih sertifikata)	
Prepoznavan otisak kvalifikovanih elektronskih sertifikata -SHA1 engl. *Certificate Fingerprint – SHA1*	89 8f cb b2 fe 5b 82 d2 ec ad 5b a5 ac 28 f5 6f ef 20 8f e6

(2) Profil **intermediate sertifikata**:

- Halcom PL e-signature

Nazivi polja	**Vrednost odnosno značenje**

Osnovna polja u sertifikatima	
Varijanta engl. *Version*	V3
Identifikaciona oznaka kvalifikovanog elektronskog sertifikata engl. *Serial Number*	3b 26 33 b1 68 bd 81 68
Algoritam za potpis, engl. *Signature algorithm*	Sha256RSA (1.2.840.113549.1.1.11)
Izdavalac engl. *Issuer*	CN = Halcom BG Root CA 2.5.4.97 = VATRS-102193722 2.5.4.97 = MB:RS-17419722 O = Halcom a.d. Beograd C = RS
Valjanost, engl. *Validity*	Valid from: <16.10.2018 11:00:00 GMT> Valid to: <16.10.2028 11:00:00GMT>
Vlasnik, engl. *Subject*	CN = Halcom BG CA PL e-signature 2.5.4.97 = VATRS-102193722 2.5.4.97 = MB:RS-17419722 O = Halcom a.d. Beograd C = RS
Algoritam za javni ključ, engl. *Subject Public Key Algorithm*	rsaEncryption (OID 1.2.840.113549.1.1.1)

ISO 9001
ISO 27001
BUREAU VERITAS
Certification
Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 330 6500, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 6619, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

Javni ključ, engl. *Public Key (... bits)*	30 82 01 0a 02 82 01 01 00 a6 a9 4d ea 92 25 60 81 3e 73 f0 d6 56 a4 ea 6b f6 fb fe 43 45 f0 6f 38 4c 64 ca 77 f0 92 38 af f3 8b 5c 60 3c 16 29 dd fe 14 85 3b a4 ce 0a 7d 6c 72 90 dd 1d 62 be 3e a0 43 84 11 95 1e c3 88 89 0b ff d6 ea 5d cc f1 74 7e 32 17 08 af a0 be b2 77 5f d9 91 30 2c c9 0d 45 48 58 52 67 48 94 ad f2 df 67 68 9e 89 16 54 2b 2b 03 2f 3c 3f dd e1 ec 0b 60 38 0c 8d 2c 78 86 a7 d3 36 54 e1 dc cf 7c 3c fb 01 3e 53 25 19 00 08 0b 6b 52 1d 92 fc b6 15 b1 94 0c ac cb 45 60 c1 fb 25 58 7a 69 4f f7 22 7c 81 de 05 d4 42 d7 6d 84 32 61 b1 ce 3e 08 33 41 5f c4 9c ac db 08 ef 08 7d a1 8a 19 1a 56 eb 26 6a f7 dd 26 24 f8 8c d5 49 0f df 31 e8 05 3d ae 79 be da fa 6a 07 27 25 3a b2 69 56 bf 9b 36 f2 89 1a d7 b6 7f 50 81 6a e6 97 dc 9e bc ab b0 d6 6a 5d f0 68 a7 cb c0 fe 0c a6 25 f7 02 03 01 00 01
Vlasnikov javni ključ koji pripada odgovarajućem paru, ključeva, šifriran alg. RSA, engl. *RSA Public Key*	dužina ključa je 2048 bitova
Ekstenzije u okviru X.509v3 standarda	
Objava registra opozvanih kvalifikovanih elektronskih sertifikata, OID 2.5.29.31, engl. *CRL Distribution Points*	URL=ldap://ldap.halcom.rs/cn=Halcom%20BG%20Root%20CA,o=Halcom%20a.d.%20Beograd,c=RS?certificaterevocationlist;binary) URL=http://domina.halcom.rs/crls/Halcom_BG_Root_CA.crl
korišćenje ključa, OID 2.5.29.15, *engl. Key Usage*	Certificate Signing, Off-line CRL Signing, CRL Signing
Identifikator ključa pružaoca usluga od poverenja, OID 2.5.29.35, engl. Authority *Key Identifier*	KeyID=49 2c 22 39 ad 8d a4 e0
Identifikator ključa vlasnika, OID 2.5.*29.14,* *engl. Subject Key Identifier*	47 60 61 7d 9d 0b 7c 36

Politika, u nadležnosti koje je sertifikat izdat, sa URL adresom CPS-a , OID 2.5.29.32, engl. certificatePolicies	Certificate Policy: Policy Identifier=All issuance policies [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.halcom.rs/UserFiles/File/CPS_HalcomCA.pdf
Osnovna ograničenja, OID 2.5.29.19, engl. *Basic Constraints*	Subject Type=CA Path Length Constraint=None
Dodatna identifikacija (nije deo kvalifikovanog elektronskog sertifikata)	
Prepoznavan otisak kvalifikovanog elektronskog sertifikata -SHA1 engl. *Certificate Fingerprint – SHA1*	8c ab b3 5e 3a 8a 27 3e d6 53 86 cc 82 47 87 68 bf 51 f6 ed

(3) Profil sertifikata krajnjih korisnika

- Halcom BG CA PL e-signature

Nazivi polja	**Vrednost odnosno značenje**
Osnovna polja u sertifikatima	
Varijanta engl. *Version*	V3
Identifikaciona oznaka kvalifikovanog elektronskog sertifikata engl. *Serial Number*	Jedinstven interni broj kvalifikovanih elektronskih sertifikata
Algoritam za potpis, engl. *Signature algorithm*	Sha256RSA (1.2.840.113549.1.1.11)
Izdavalac engl. *Issuer*	CN = Halcom BG CA PL e-signature 2.5.4.97 = VATRS-102193722 2.5.4.97 = MB:RS-17419722 O = Halcom a.d. Beograd C = RS

Valjanost, engl. *Validity*	Valid from: <početak validnosti prema GMT> Valid to: <kraj validnosti prema GMT>
Vlasnik, engl. *Subject*	Jedinstveno ime, pogledati poglavlje 3.1.1.
Algoritam za javni ključ, engl. *Subject Public Key Algorithm*	rsaEncryption (OID 1.2.840.113549.1.1.1)
Javni ključ, engl. *Public Key (... bits)*	modulus, eksponent,...
Vlasnikov javni ključ koji pripada odgovarajućem paru, ključeva, šifriran alg. RSA, engl. *RSA Public Key*	dužina ključa je min 2048 bitova, pogledaj poglavlje 6.1.5.
Ekstenzije u okviru X.509v3 standarda	
Objava registra opozvanih kvalifikovanih elektronskih sertifikata, OID 2.5.29.31, engl. *CRL Distribution Points*	URL=ldap://ldap.halcom.rs/cn=Halcom%20BG%20CA%20PL%20e-signature,o=Halcom%20a.d.%20Beograd,c=RS?certificaterevocationlist;binary) URL=http://domina.halcom.rs/crls/Halcom_BG_CA_PL_e-signature.crl
Politika, u nadležnosti koje je sertifikat izdat, sa URL adresom CPS-a , OID 2.5.29.32, engl. certificatePolicies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.5939.10.1.5 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.halcom.rs/UserFiles/File/CPS_HalcomCA.pdf [2]Certificate Policy: Policy Identifier=0.4.0.194112.1.2
korišćenje ključa, OID 2.5.29.15, *engl. Key Usage*	Napredni sertifikati: Digital Signature, Non Repudiation, Key Encipherment

Identifikator ključa pružaoca usluga od poverenja, OID 2.5.29.35, engl. Authority *Key Identifier*	KeyID=47 60 61 7d 9d 0b 7c 36

Ekstenzija *namena korišćenja ključa* (engl. *Key Usage*) označena je kao kritična (engl. *critical*).

7.1.2.1. ZAHTEVI SA ELEKTRONSKOM ADRESOM

(1) HALCOM BG CA zadržava pravo odbijanja zahteva za sertifikat ako utvrdi da je elektronska adresa:

- neodgovarajuća ili uvredljiva,
- pogrešna za treće strane,
- suprotna važećim propisima i standardima.

(2) Ne postoje druga ograničenja u elektronskoj adresi.

7.1.3 OBJEKTNI IDENTIFIKATORI ALGORITMA

(1) Kvalifikovani elektronski sertifikati koje izdaje pružalac usluga od poverenja HALCOM BG CA potpisani su primenom kriptografskog algoritma, određenim u polju *signature algorithm*: vrednost "sha256RSA, identifiakatorska oznaka: OID 1.2.840.113549.1.1.11".

(2) Celokupan skup algoritama, formata podataka i protokola dostupan je kod ovlašćenih lica HALCOM BG CA.

7.1.4 FORME IMENA

Pogledati poglavlje 3.1.1.

7.1.5 OGRANIČENJA IMENA

Ograničenja vezana za imena (polje u sertifikatu engl. *nameConstraints*) nisu specificirane.

7.1.6 OBJEKTNI IDENTIFIKATOR CP

Pogledati poglavlje 7.1.2.

7.1.7 OGRANIČENJA UPOTREBE

Ograničenja upotrebe (polje u sertifikatu engl. *usage policy constraints extension*) nisu specificirane.

7.1.8 SINTAKSA I SEMANTIKA „Policy Qualifier"-SA

U sertifikatima, koje izdaje pružalac usluga od poverenja HALCOM BG CA, upisuje se specifičan podatak policyQualifiers, koji je u skladu sa standardima IETF RFC i ETSI.

7.1.9 VAŽNOST SUŠTINSKIH DOPUNSKIH POLITIKA

Nije podržano u okviru ovog dokumenta CP

7.2. PROFIL REGISTRA OPOZVANIH SERTIFIKATA(CRL)

(1) Registar opozvanih kvalifikovanih elektronskih sertifikata (CRL) izdaje pružalac usluga od poverenja HALCOM BG CA:

- Registar opozvanih intermediate/podređenih sertifikata

  CN= Halcom BG Root CA

  O = Halcom a.d. Beograd

  C = RS

- Registar opozvanih sertifikata za e-potpis pravnih lica

  CN= Halcom BG CA PL e-signature

  O=Halcom a.d. Beograd

  C=RS

(2) Registar opozvanih intermediate/podređenih sertifikata se objavljuje najmanje jednom godišnje, ostali registri opozvanih sertifikata se osvežavaju po svakom opozivu ili najmanje jednom dnevno, ukoliko nije bilo novih opoziva (24h po zadnjem osvežavanju).

(3) Registar opozvanih kvalifikovanih elektronskih sertifikata sadrži jednoznačni interni serijski broj opozvanog kvalifikovanih elektronskih sertifikata, kao i vreme i datum opoziva.

7.2.1 BROJE VERZIJE

(1) Registar opozvanih sertifikata odgovara preporuci ITU-T X.509 (2005) i ISO/IEC 9594-8:2014.

(2) Registar opozvanih kvalifikovanih elektronskih sertifikata je dostupan je putem:

- LDAP protokola i
- HTTP protokola.

7.2.2 SADRŽAJ CRL I CRL ENTRY EKSTENZIJE

(1) Registar opozvanih kvalifikovanih elektronskih sertifikata uz ostale podatke, u skladu sa preporukom *X.509* sadrži (osnovna polja i ekstenzije detaljnije su prikazani u donjoj tabeli):

- identifikacione oznake opozvanih sertifikata i
- vreme i datum opoziva.

(2) Korenski (Root) registar opozvanih sertifikata (CRL intermediate/podređenih sertifikata):

Naziv polja	**Vrednost odnosno značenje**
Osnovna polja u CRL	
Verzija, engl. *Version*	V2
Algoritam za digitalni potpis CRL, engl. *Signature Algorithm*	Sha256RSA

Potpis pružaoca usluga od poverenja, engl. Signature	potpis HALCOM BG CA
Jedinstveno ime pružaoca usluga od poverenja engl. *Issuer*	CN = Halcom BG Root CA 2.5.4.97 = VATRS-102193722 2.5.4.97 = MB:RS-17419722 O = Halcom a.d. Beograd C = RS
Vreme izdavanja CRL, engl. *thisUpdate*	Effective date: *<vreme izdavanja prema GMT>*
Vreme izdavanja sledeće CRL, engl. *nextUpdate*	Next Update: *<vreme izdavanja sledeće CRL prema GMT>*
Identifikacione oznake (serijski brojevi) opozvanih kvalifikovanih elektronskih sertifikata i vreme opoziva, engl. *revokedCertificate*	Serial Number: *<identifikaciona oznaka (serijski broj) opozvanog kvalifikovanog elektronskog kvalifikovanih elektronskih sertifikata>* Revocation Date: *<vreme opoziva prema GMT>*
Ekstenzije X.509v2 CRL	
redni broj CRL engl. *CRL number*	Redni broj izdatog registra opozvanih kvalifikovanih elektronskih sertifikata
identifikator ključa pružaoca usluga od poverenja, engl. *Authority Key Identifier (OID 2.5.29.35)*	KeyID=49 2c 22 39 ad 8d a4 e0
angl. issuerAltName (OID 2.5.28.18)	Ne upotrebljava se
angl. deltaCRLindicator (OID 2.5.29.27)	Ne upotrebljava se
angl. issuingDistribuitionPoint (OID 2.5.29.28)	Ne upotrebljava se

(3) Intermediate/podređenih registar opozvanih sertifikata (CRL sertifikata krajnjih korisnika)

- Halcom BG CA PL e-signature

Naziv polja	**Vrednost odnosno značenje**
Osnovna polja u CRL	
Verzija, engl. *Version*	V2
Algoritam za digitalni potpis CRL, engl. *Signature Algorithm*	Sha256RSA
Potpis pružaoca usluga od poverenja, engl. Signature	potpis HALCOM BG CA
Jedinstveno ime pružaoca usluga od poverenja engl. *Issuer*	CN = Halcom BG CA PL e-signature 2.5.4.97 = VATRS-102193722 2.5.4.97 = MB:RS-17419722 O = Halcom a.d. Beograd C = RS

Vreme izdavanja CRL, engl. *thisUpdate*	Effective date: *<vreme izdavanja prema GMT>*
Vreme izdavanja sledeće CRL, engl. *nextUpdate*	Next Update: *<vreme izdavanja sledeće CRL prema GMT>*
Identifikacione oznake (serijski brojevi) opozvanih kvalifikovanih elektronskih sertifikata i vreme opoziva, engl. *revokedCertificate*	Serial Number: *<identifikaciona oznaka (serijski broj) opozvanog kvalifikovanog elektronskog kvalifikovanih elektronskih sertifikata>* Revocation Date: *<vreme opoziva prema GMT>*
Ekstenzije X.509v2 CRL	
redni broj CRL engl. *CRL number*	Redni broj izdatog registra opozvanih kvalifikovanih elektronskih sertifikata
identifikator ključa pružaoca usluga od poverenja, engl. *Authority Key Identifier (OID 2.5.29.35)*	KeyID=47 60 61 7d 9d 0b 7c 36
angl. issuerAltName (OID 2.5.28.18)	Ne upotrebljava se
angl. deltaCRLindicator (OID 2.5.29.27)	Ne upotrebljava se
angl. issuingDistribuitionPoint (OID 2.5.29.28)	Ne upotrebljava se

7.2.3 OBJAVA REGISTRA OPOZVANIH SERTIFIKATA

HALCOM BG CA objavljuje registar opozvanih sertifikata u javnom spisku na serveru ldap://ldap.halcom.rs putem LDAP protokola i http://domina.halcom.rs/crls putem HTTP protokola.

7.3 OCSP PROFIL(PROFIL U TOKU PROVERE PROVERE STATUSA SERTIFIKATA)

(1) Stalna provera statusa digitalnih sertifikata dostupna je na http://ocsp.halcom.rs.

(2) Profil OCSP poruke (zahtev/odgovor) za proveru statusa u realnom vremenu je u skladu sa preporukom IETF RFC.

7.3.1 BROJ VERZIJE

Pružalac usluga od poverenja HALCOM BG CA koristi OCSP poruke verzije 1 u skladu sa preporukom IETF RFC.

7.3.2 OCSP EKSTENZIJE

OCSP poruke (zahtevi/odgovori) za stalnu proveru statusa sertifikata podržavaju ekstenziju Nonce, koja nije označena kao kritična.

8. PROVERA USKLAĐENOSTI I DRUGA OCENJIVANJA

(1) U okviru pružaoca usluga od poverenja HALCOM BG CA postoji jedinica za unutrašnju kontrolu i usklađenost koju čine stručnjaci sa odgovarajućim tehnološkim i pravnim znanjima, a koji ne vrše zadatke vezane za upravljanje kvalifikovanim elektronskim sertifikatima.

(2) Poverenik za unutrašnju kontrolu nadzire rad HALCOM BG CA. U slučaju otkrivenih nedostataka definiše odgovarajuće mere za uklanjanje tih nedostataka, koje je pružalac

usluga od poverenja HALCOM BG CA dužno da sprovede, i nadzire sprovođenje definisanih mera.

(3) Sistem evidentičar vrši nadzor rada pružaoca usluga od poverenja najmanje jedanput u godini.

8.1 FREKVENCIJA I USLOVI OCENJIVANJA

(1) Sistem evidentičar vrši nadzor najmanje jednom godišnje.

(2) Poverenik za eksternu kontrolu za ISO 9001 i ISO 27001 vrši proveru jednom godišnje. Poverenik za eksternu kontrolu za rad u skladu sa ETSI i drugim standardima vrši kontrolu jednom u dve godine.

8.2 IDENTITET/KVALIFIKACIJE PROCENJIVAČA

(1) Sistem evidentičar čine stručnjaci sa odgovarajućim tehnološkim i pravnim znanjima.

(2) Poverenik za eksternu kontrolu ima odgovarajuća tehnološka i pravna znanja.

8.3 ODNOS OCENJIVAČA PREMA OCENJIVANOM ENTITETU – NEZAVISNOST KONTROLE

(1) Sistem evidentičar ne vrši poslove koji se odnose na rad sa sertifikatima.

(2) Poverenik za eksternu kontrolu ne vrši poslove koji se odnose na rad sa sertifikatima.

8.4 PODRUČJA NADZORA

Područja nadzora određena su u internim pravilima rada pružaoca usluga od poverenja HALCOM BG CA.

8.5 AKTIVNOSTI PREDUZETE KAO REZULTAT UTVRĐENIH NEDOSTATAKA

U slučaju utvrđenih nedostataka ili grešaka u radu pružaoca usluga od poverenja, poverenik za unutrašnju kontrolu definiše mere za uklanjanje tih nedostataka, koje je HALCOM BG CA dužno da sprovede, i nadzire izvođenje definisanih mera.Detalji oko sprovođenja navedenih mera definišu se u internim pravilima rada pružaoca usluga od poverenja HALCOM BG CA.

8.6 OBJAVA REZULTATA NADZORA

Rezultati sprovođenja nadzora čuvaju se u okviru pružaoca usluga od poverenja HALCOM BG CA.

9. DRUGI POSLOVNI I PRAVNI ASPEKTI

9.1. CENE

HALCOM BG CA važeči cenovnik korišćenja sertifikata, svojih usluga, potrebne opreme i infrastrukture i objavljuje na svojoj web stranici.

9.1.1 CENA IZDAVANJA ILI OBNOVE KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA

Cena izdavanja i obnavljanja kvalifikovanih elektronskih sertifikata definisana je važećim cenovnikom u registracionim centrima.

9.1.2 CENA PRISTUPA SERTIFIKATIMA

Ovo poglavlje nije primenljivo u okviru ovih CP.

9.1.3 CENA PRISTUPA INFORMACIJAMA O STATUSU KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA I REGISTRU OPOZVANIH SERTIFIKATA

Pristup registru opozvanih sertifikata (CRL) je besplatan osim ako se stranke ne dogovore drugačije.

9.1.4 CENE ZA DRUGE SERVISE

Cene drugih usluga, opreme i infrastrukture određene su važećim cenovnikom.

9.1.5 POLITIKA POVRAĆAJA NOVCA

Ovo poglavlje nije primenljivo u okviru ovog CP.

9.2 FINANSIJSKA ODGOVORNOST

9.2.1 POKRIVENOST OSIGURANJEM

(1) HALCOM BG CA obezbeđuje osiguranje za pokrivanje svih odgovornosti opisanih u ovom CP dokumentu. Detaljne informacije o osiguranju objavljene su na zvaničnoj web strani pružaoca usluga od poverenja.

(2) HALCOM BG CA ne prihvata nikakvu drugu odgovornost koja izlazi iz pokrivanja definisanog ovim CP dokumentom.

9.2.2 DRUGA DIBRA

Ovo poglavlje nije primenljivo u okviru ovog CP.

9.2.3 OSIGURANJE ILI GARANCIJSKA POKRIVENOST ZA KRAJNJE KORISNIKE

Ovo poglavlje nije primenljivo u okviru ovog CP.

9.3 POVERLJIVOST POSLOVNIH INFORMACIJA

9.3.1 OPSEG POVERLJIVIH INFORMACIJA

(1) Pružalac usluga od poverenja HALCOM BG CA postupa poverljivo sa sledećim podacima:

- sa svim zahtevima za dobijanje kvalifikovanog elektronskog sertifikata ili drugih usluga,
- sve moguće poverljive podatke vezane za finansijske obaveze,
- sve moguće poverljive podatke koji predstavljaju predmet međusobnih ugovora sa trećim licima i
- sve ostale podatke koji su navedeni u internim pravilima rada pružaoca usluga od poverenja HALCOM BG CA.

(2) U toku obrade svih mogućih poverljivih podataka o vlasnicima sertifikata i trećim licima, koji su nužno potrebni za usluge upravljanja kvalifikovanim elektronskim sertifikatima, HALCOM BG CA postupa u skladu sa važećim zakonodavstvom.

9.3.2 INFORMACIJE KOJE NISU U OPSEGU POVERLJIVIH INFORMACIJA

Pružalac usluga od poverenja HALCOM BG CA javno objavljuje samo one poslovne podatke koji nisu poverljive prirode, a u skladu sa važećim zakonodavstvom.

9.3.3 ODGOVORNOST ZA ZAŠTITU INFORMACIJA

(1) Pružalac usluga od poverenja HALCOM BG CA ne preuzima nikakve odgovornosti za sadržaj podataka koje vlasnik kvalifikovanog elektronskog sertifikata elektronski šifruje ili potpisuje. Takođe, pružalac usluga od poverenja ne preuzima nikakve odgovornosti za pitanja da li su vlasnik ili treće lice poštovali sve važeće propise, sve odredbe politike pružanja usluga i drugih pravila pružaoca usluga od poverenja HALCOM BG CA, odnosno vodili računa o svim objavljenim uputstvima.

(2) Pružalac usluga od poverenja HALCOM BG CA ne preuzima nikakve odgovornosti za posledice do kojih dolazi ukoliko vlasnik kvalifikovanog elektronskog sertifikata nije postupao u skladu sa sigurnosnim zahtevima iz poglavlja 4.5.1 ovog CP dokumenta.

9.4 PRIVATNOST LIČNIH PODATAKA

9.4.1 PLAN PRIVATNOSTI

(1) HALCOM BG CA pridržava se pravila zaštite privatnosti ličnih podataka i pravila poverljivosti kako je propisano u CPS dokumentu, kao i u odgovarajućim zakonskim dokumentima.

(2) Sa svim ličnim i poverljivim podacima o vlasnicima kvalifikovanih elektronskih sertifikata koji su nužno potrebni za usluge upravljanja kvalifikovanim elektronskim sertifikatima, pružalac usluga od poverenja HALCOM BG CA postupa u skladu sa važećim zakonodavstvom.

9.4.2 INFORMACIJE KOJE SE TRETIRAJU KAO PRIVATNE

(1) Pružalac usluga od poverenja HALCOM BG CA tretira privatnim sve informacije koje se odnose na korisnike kvalifikovanih elektronskih sertifikata.

(2) Poverljivi podaci koji se čuvaju su svi lični podaci koje HALCOM BG CA prikupi u okviru zahteva za svoje usluge ili u odgovarajućim registrima za dokazivanje identiteta vlasnika. Podaci u sertifikatima i registru opozvanih sertifikata su zbog prirode upotrebe sertifikata, važećih pravila i standarda dostupni trećima licima koja se oslanjaju na sertifikate ili proveravaju njihovu validnost.

9.4.3 INFORMACIJE KOJE SE NE SMATRAJU PRIVATNIM

Drugih mogućih ličnih podataka koji se javno objavljuju od strane pružaoca usluga od poverenja, osim ovih navedenih u sertifikatu i registru opozvanih sertifikata, nema.

9.4.4 ODGOVORNOST ZA ZAŠTITU PRIVATNIH INFORMACIJA

(1) Pružalac usluga od poverenja HALCOM BG CA je odgovoran za zaštitu privatnosti korisnikovih informacija.

(2) Pružalac usluga od poverenja HALCOM BG CA postupa u skladu sa Zakonom o zaštiti podataka o ličnosti i drugim važećim zakonodavstvom vezanim za čuvanje i zaštitu ličnih podataka.

HALCOM BG CA 9.4.5 OBAVEŠTENJE I SAGLASNOST ZA KORIŠĆENJE PRIVATNIH INFORMACIJA

Vlasnik ovlašćuje HALCOM BG CA za korišćenje ličnih podataka koji se nalaze na zahtevu za dobijanje kvalifikovanih elektronskih sertifikata, u skladu sa zakonom o zaštiti ličnih podataka.

9.4.6 OTKRIVANJE INFORMACIJA SHODNO PRAVNIM I ADMINISTRATIVNIM PROCESIMA

(1) Pružalac usluga od poverenja HALCOM BG CA ne prosleđuje lične podatke o vlasnicima kvalifikovanih elektronskih sertifikata trećim licima koja nisu navedena u kvalifikovanim elektronskim sertifikatima, osim ako se određeni podaci posebno zahtevaju za izvođenje specifičnih usluga odnosno aplikacija vezanih za sertifikate, a vlasnik kvalifikovanog elektronskog sertifikata je za te svrhe ovlastio HALCOM BG CA (pogledati prethodno poglavlje), ili na zahtev nadležnog suda ili administrativnog organa.

(2) Lični podaci se prosleđuju i bez pismenog odobrenja vlasnika kvalifikovanog elektronskog sertifikata ukoliko je tako definisanom zakonodavstvom, odnosno važećim propisima.

9.4.7 DRUGE OKOLNOSTI ZA OTKRIVANJE INFORMACIJA

Ovo poglavlje nije primenljivo u okviru ovog CP.

9.5 PRAVA INTELEKTUALNOG VLASNIŠTVA

Odredbe vezane na autorska, srodna i druga prava intelektualnog vlasništva:

- u vezi privatnog ključa - pripadaju sva prava vlasniku kvalifikovanog elektronskog sertifikata,
- u vezi javnih ključeva – sva prava nad svim podacima u sertifikatu, registru opozvanih kvalifikovanih elektronskih sertifikata, kao i na ovom CP dokumentu pripadaju pružaocu usluga od poverenja HALCOM BG CA.

9.6. PREDSTAVLJANJA I GARANCIJE

9.6.1 HALCOM BG CA PREDSTAVLJANJA I GARANCIJE

(1) Pružalac usluga od poverenja HALCOM BG CA je obavezan da:

- posluje u skladu sa svojim internim pravilima i drugim važećim propisima i zakonima,
- postupa u skladu sa međunarodnim preporukama,
- objavi sve obavezne dokumente koji određuju njegovo funkcionisanje (politike rada, zahteve, cenovnik, uputstva za sigurno korišćenje kvalifikovanih elektronskih sertifikata itd.),
- na svojoj web stranici ažurno objavljuje sve informacije u vezi sa promenama aktivnosti pružaoca usluga od poverenja, koje na bilo koji način mogu uticati na vlasnike sertifikata i treće strane,
- dogovori rad registracionih tela u skladu sa odredbama HALCOM BG CA i drugim važećim propisima,
- pridržava se odredbi koje se odnose na pouzdano rukovanje ličnim i poverljivim informacijama o pružaocima usluga od poverenja, vlasnicima sertifikata i trećim osobama,
- opozove sertifikata i objavi opozvani sertifikat u registru opozvanih sertifikata kada utvrdi da su navedeni razlozi za ovu politiku ili druge primenjive propise,
- izda kvalifikovane elektronske sertifikate u skladu sa ovom politikama, drugim propisima i preporukama.

(2) Pružalac usluga od poverenja HALCOM BG CA je dužan da:

- osigura tačnost podataka izdatih sertifikata,
- osigura ispravnost objavljivanja registra opozvanih sertifikata,
- osigura jedinstvenost imena,
- obezbedi odgovarajuću fizičku bezbednost prostorija i pristup samim prostorijama HALCOM BG CA,
- obezbedi neometano funkcionisanje i maksimalnu dostupnost svoje usluge,
- brine za najveću moguću dostupnost usluge,
- vodi računa o neometanom radu svih ostalih pratećih službi,
- pokuša da reši probleme koji nastanu na najbolji mogući način u najkraćem roku,
- pobrine se za optimizaciju hardvera i softvera,
- informiše korisnike o važnim pitanjima i
- ispuni sve druge uslove u skladu sa ovom politikom.

(3) HALCOM BG CA obezbeđuje maksimalnu dostupnost svojih usluga, svaki dan u godini, ali se ne uzimaju u obzir sledeći slučajevi:

- planirane i unapred najavljene tehničke ili uslužne intervencije na infrastrukturi,
- neplanirane tehničke ili uslužne intervencije na infrastrukturi kao rezultat nepredviđenih okolnosti ili slomova,
- nepristupačnost kao rezultat više sile ili vanrednih događaja.

(4) Održavanje ili nadogradnju infrastrukture pružalac usluga od poverenja HALCOM BG CA najavljuje najmanje tri (3) dana pre početka radova.

(5) HALCOM BG CA je odgovoran za sve informacije u ovom dokumentu i implementaciji svih odredbi ove politike.

(6) Ostale obaveze i odgovornosti HALCOM BG CA mogu se definisati sporazumom sa trećim licem.

9.6.2 OBAVEZE I ODGOVORNOSTI REGISTRACIONIH TELA

(1) Registraciona tela su obavezna da:

- provere identitet vlasnika ili budućih vlasnika,
- prime zahteve za usluge HALCOM BG CA,
- provere zahtev,
- izdaju potrebnu dokumentaciju pravnim licima, vlasnicima ili budućim vlasnicima,
- dostave zahteve i druge podatke na siguran način u HALCOM BG CA.

(2) Registraciona tela su odgovorna za primenu svih odredbi, politika i drugih zahteva iz CP-a, koje su dogovorene sa HALCOM BG CA.

9.6.3 OBAVEZE I ODGOVORNOSTI VLASNIKA SERTIFIKATA

(1) Pravna lica su odgovorna za:

- štetu nastalu u slučaju zloupotrebe sertifikata od prijave opoziva do opoziva,
- bilo koju štetu koja je direktno ili indirektno prouzrokovana tako što je omogućena zloupotreba sertifikata vlasnika od strane neovlašćenih lica,
- bilo koju štetu nastalu zbog nepoštovanja CP-a, politika, drugih obaveštenja HALCOM BG CA i važećim propisima.

(2) Obaveze vlasnika sertifikata u pogledu upotrebe sertifikata navedene su u poglavlju 4.5.1.

9.6.4 OBAVEZE I ODGOVORNOSTI TREĆIH STRANA

(1) Nakon prve upotrebe sertifikata, treća strana koja se oslanja na sertifikat mora pažljivo pročitati politiku i od tada redovno pratiti sva obaveštenja od HALCOM BG CA.

(2) Treća strana mora redovno proveravati da sertifikat nije u registru opozvanih sertifikata.

(3) Ako sertifikat sadrži informacije o trećoj strani, obavezan je da zatraži opoziv sertifikata ako sazna, da je privatni ključ ugrožen na način koji utiče na pouzdanost korišćenja ili postoji rizik od zloupotrebe ili ako su se podaci promenili.

(4) Treća strana se može osloniti na takav sertifikat do opoziva sertifikata.

(5) Treća strana može u svako doba zatražiti bilo koju informaciju o važnosti izdatog sertifikata, odredbe politike ili obaveštenja HALCOM BG CA.

9.6.5 OBAVEZE I ODGOVORNOSTI DRUGIH UČESNIKA

Ovo poglavlje nije primenljivo u okviru ovih CP.

9.7. OGRANIČENJA I ODGOVORNOSTI

Pružalac usluga od poverenja HALCOM BG CA nije odgovorno za štetu koja proizlazi iz:

- korišćenje kvalifikovanih elektronskih sertifikata za namene i na način koji nije izričito predviđen u politici sertifikacije i ovom CP dokumentu,
- nepravilnog ili pogrešnog obezbeđenja lozinki ili privatnih ključeva vlasnika kvalifikovanog elektronskog sertifikata, otkrivanje poverljivih podataka ili ključeva trećim licima i neodgovornog postupanja vlasnika kvalifikovanog elektronskog sertifikata,
- zloupotrebe odnosno upada u informacioni sistem vlasnika kvalifikovanog elektronskog sertifikata i na taj način dolaska do podataka o kvalifikovanim elektronskim sertifikatima od strane neovlašćenih lica,
- nepostupanja ili lošeg postupanja sa podacima u okviru informacione infrastrukture vlasnika kvalifikovanog elektronskog sertifikata ili trećih lica,
- neproveravanja podataka i validnosti (statusa povučenosti) kvalifikovanih elektronskih sertifikata u registru opozvanih kvalifikovanih elektronskih sertifikata,
- neproveravanja vremena validnosti kvalifikovanih elektronskih sertifikata,
- postupanja vlasnika kvalifikovanog elektronskog sertifikata ili trećeg lica suprotno informacijama i obaveštenjima koje objavljuje HALCOM BG CA, politikom sertifikacije, ovim CP dokumentom i drugim propisima,

- omogućenog korišćenja odnosno zloupotrebe vlasnikovog kvalifikovanog elektronskog sertifikata od strane neovlašćenih lica,
- izdatog kvalifikovanog elektronskog sertifikata sa pogrešnim i neverodostojnim podacima, ili drugim radnjama vlasnika kvalifikovanog elektronskog sertifikata ili pružaoca usluga od poverenja,
- korišćenja kvalifikovanih elektronskih sertifikata koji nisu validni, uz promenu podataka iz kvalifikovanih elektronskih sertifikata, elektronskih adresa ili promena imena vlasnika,
- ispada infrastrukture koja nije u domenu upravljanja HALCOM BG CA,
- samih podataka koji se šifruju ili potpisuju korišćenjem kvalifikovanih elektronskih sertifikata,
- upotrebe i pouzdanosti rada mašinske i programske opreme vlasnika kvalifikovanog elektronskog sertifikata.

9.8. OGRANIČENJE U POTREBI

Ovo poglavlje nije primenljivo u okviru ovih CP.

9.9. ODŠTETE

Za štetu je odgovorna stranka koja je istu prouzrokovala zbog nepoštovanja odredba iz ove politike pružanja usluga, CPS dokumenta i važećeg zakonodavstva.

9.10. PERIOD VAŽNOSTI I KRAJ VALIDNOSTI OVE POLITIKE

(1) Pružalac usluga od poverenja HALCOM BG CA zadržava pravo da izmeni politiku pružanja usluga i da nadogradi infrastrukturu bez prethodnog obaveštavanja vlasnika kvalifikovanog elektronskog sertifikata.

(2) Ova politika stupa na snagu na dan kada je odobrena i objavljena od strane pružaoca usluga od poverenja HALCOM BG CA.

9.10.1 VAŽNOST

(1) Nova verzija, odnosno promene, politike pružaoca usluga od poverenja HALCOM BG CA se prethodno, osam (8) dana pre zvaničnog datuma validnosti, objavi na web stranici pružaoca usluga od poverenja HALCOM BG CA sa novim identifikacionim brojem (CP_{OID}) i označenim datumom početka validnosti.

9.10.2 KRAJ VALIDNOSTI POLITIKE

(1) Prilikom objavljivanja nove politike, za sve sertifikate izdate po osnovu te politike, ostaju validne one odredbe koje smisaono ne mogu da se nadomeste odgovarajućim odredbama nove politike (na primer postupak koji određuje način na koji je bio izdat taj sertifikat, i sl.).

(2) Pružalac usluga od poverenja HALCOM BG CA može za pojedinačne odredbe validne politike da objavi amandmane kao što je to navedeno u poglavlju 9.12.

9.10.3 EFEKAT ZAVRŠETKA I PONOVNOG RADA

(1) Prilikom objavljivanja nove politike, svi kvalifikovani elektronski sertifikati izdati nakon tog datuma se procesiraju prema novoj politici.

(2) Nova politika ne utiče na validnost sertifikata koji su bili izdati prema prethodnim politikama. Takvi kvalifikovani elektronski sertifikati ostaju važeći do isteka validnosti

pri čemu se, gde god je to moguće procesiraju i/ili tretiraju prema novoj politici sertifikacije.

9.11. POJEDINAČNA OBAVEŠTAVANJA I KOMUNIKACIJA SA UČESNICIMA

(1) Kontaktni podaci pružaoca usluga od poverenja objavljeni su na web stranicama istog i navedeni u poglavlju 1.3.1.

(2) Kontaktni podaci vlasnika kvalifikovanog elektronskog sertifikata dostavljeni su u zahtevima vezanim za sertifikate.

(3) Kontaktni podaci trećih lica dostavljeni su u mogućem međusobnom dogovoru između trećeg lica i pružaoca usluga od poverenja HALCOM BG CA.

9.12. ISPRAVKE, MODIFIKACIJE I DODACI

9.12.1 PROCEDURE ZA ISPRAVKU, MODIFIKACIJU ILI DODATAK

(1) Promene ili dopune ove politike pružalac usluga od poverenja može da objavi u obliku promena ili dopuna ovoj politici ako se ne radi o suštinskim promenama operativnog rada pružaoca usluga od poverenja HALCOM AD BG.

(2) Dopune se usvajaju i prihvataju istim postupkom kao i sama politika.

(3) Način za označavanje dopuna definiše pružalac usluga od poverenja HALCOM BG CA.

9.12.2 MEHANIZAM I PERIOD OBAVEŠTAVANJA

(1) Pružalac usluga od poverenja HALCOM BG CA definiše početak i kraj validnosti promena i dopuna.

(2) Promene i dopune se objave osam (8) dana pre početka validnosti na web stranicama HALCOM BG CA.

9.12.3 PROMENA IDENTIFIKACIONOG BROJA POLITIKE

Ako prihvaćene promene i dopune utiču na korišćenje sertifikata, pružalac usluga od poverenja HALCOM BG CA određuje novi identifikacioni broj (CPOID) za novu politiku, odnosno promene i dopune.

9.13. ODREDBE REŠAVANJA SPOROVA

(1) Sve pritužbe vlasnika sertifikata rešavaju poverenici za unutrašnju kontrolu i zakonsku regulativu.

(2) Moguće sporove između vlasnika kvalifikovanog elektronskog sertifikata ili trećeg lica i pružaoca usluga od poverenja HALCOM BG CA rešava nadležni sud.

9.14. VAŽEĆE ZAKONODAVSTVO

Ovaj CP dokument je izrađen u potpunosti u skladu sa odgovarajućom zakonskom regulativom države Srbije, i to pre svega sa Zakonom o elektronskom dokumentu, elektronskoj identifikaciji i drugim uslugama od poverenja u elektronskom poslovanju i odgovarajućim podzakonskim aktima.

9.15. USKLAĐENOST SA VEŽEĆIM ZAKONODAVSTVOM

(1) Nadzor nad usklađenošću operativnog rada pružaoca usluga od poverenja HALCOM BG CA sa važećim zakonodavstvom i propisima sprovodi nadležna služba ili akreditovani organ.

(2) Akreditovani organ za ocenjivanje usaglašenosti za HALCOM BG CA sprovode reviziju usaglašenosti najmanje na svaka 24 meseca. Svrha revizije je da potvrdi da li je pružalac usluge od poverenja ispunjava zakonske uslove.

(3) Interne provere usaglašenosti rada sprovode ovlašćena lica u okviru HALCOM BG CA.

9.16. OPŠTE ODREDBE

(1) Sa ostalim subjektima pružalac usluga od poverenja može da sklopi međusobne dogovore ako tako definiše važeće zakonodavstvo, odnosno drugi propisi.

(2) Ako bilo koja odredba ove politike bude ili postane nevažna, to neće uticati na druge odredbe. Nevažna odredba zameniće se važećom.

9.17. DRUGE ODREDBE

Ovo poglavlje nije primenljivo u okviru ovih CP.

Direktor Halcom a.d. Beograd

Aleksandar Spremić

ISO 9001
ISO 27001
BUREAU VERITAS
Certification
Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 330 6500, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 6619, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR