NAPOMENA: DOKUMENT SE ODNOSI NA SVE KVALIFIKOVANE ELEKTRONSKE SERTIFIKATE IZDATE NAKON 01.08.2014. GODINE

Za kvalifikovane sertifikate izdate do 31.07.2014. godine važi dokument dostupan na:
http://halcom.rs/ebb-bg/UserFiles/File/CP_Pravna_Lica_OLD.pdf

Sertifikaciono telo Halcom A.D. Beograd (HALCOM BG CA)

Opšta pravila

za izdavanje kvalifikovanih elektronskih sertifikata za pravna lica

CPName: HALCOM BG CA PL

CPOID: 1.3.6.1.4.1.5939.10.1.2

Dokument važi od: 01.08.2014.

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

Sadržaj

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

1. UVOD

Ovaj dokument predstavlja opšta pravila (CP – Certificate Policy) sertifikacionog tela HALCOM BG CA za fizička lica koja se identifikuju kao pripadnici pravnog lica za potrebe sistema elektronskog bankarstva u Srbiji.

Dokument se odnosi na izdavanje kvalifikovanih elektronskih sertifikata, definiše cilj, delovanje i metodologiju upravljanja kvalifikovanim elektronskim sertifikatima za pravna lica, kao i sigurnosne zahteve, koje moraju ispunjavati sertifikaciono telo HALCOM BG CA, vlasnici sertifikata i treća lica, koja se pozivaju na te sertifikate, i odgovornost svih nabrojanih osoba.

HALCOM BG CA je sertifikaciono telo koje izdaje i upravlja kvalifikovanim elektronskim sertifikatima za verifikaciju elektronskog potpisa. HALCOM BG CA sertifikaciono telo namenjeno je izdavanju kvalifikovanih elektronskih sertifikata za pravna i fizička lica i obavljanju tehnoloških usluga u vezi sa elektronskim potpisima.

Sve odredbe ove CP u odnosu na delovanje HALCOM BG CA propisno su prenesene i podrobnije utvrđene u odredbama internih pravila rada sertifikacionog tela koje čine dokumenti poverljive prirode, koji definišu infrastrukturu, odredbe u vezi sa zaposlenim u HALCOM BG CA (nadležnosti, zadaci, ovlašćenja i zahtevani uslovi pojedinih zaposlenih), fizičku zaštita (pristup prostorijama, upravljanje hardverskom i programskom opremom), programsku zaštita (zaštitni softver, zaštitne kopije, …), kao i interni nadzor (kontrola fizičkih pristupa, ovlašćenja, …).

Oblik i sadržaj ovog CP dokumenta usklađen je sa međunarodnom preporukom RFC 3647 (»Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework«) i evropskim standardom ETSI TS 101 456 (»Policy requirements for certification authorities issuing qualified certificates).

1.1. PREGLED

Ova politika sertifikacije uređuje nameru, delovanje i metodologiju upravljanja kvalifikovanim elektronskim sertifikatima, te zahteve bezbednosti koje mora da ispunjava sertifikaciono telo HALCOM BG CA, vlasnici sertifikata, treća lica i operateri koji se uzdaju u te sertifikate, te odgovornost svih pomenutih lica.

HALCOM BG CA je sertifikaciono telo koje izdaje i upravlja kvalifikovanim elektronskim sertifikatima za verifikaciju kvalifikovanog elektronskog potpisa. HALCOM BG CA deluje i kao glavno sertifikaciono telo (root CA) koje zajedno sa svojim podređenim sertifikacionom telima predstavlja hijerarhijsku mrežu sertifikacionih tela koja je namenjena izdavanju kvalifikovanih elektronskih sertifikata i vršenju tehnoloških usluga vezanih za kvalifikovane elektronske potpise.

HALCOM BG CA izdaje dva kvalifikovana elektronska sertifikata (dva para asimetričnih ključeva) sa obaveznim korišćenjem bezbednosnog nosioca (smart kartice) za pravna lica za potrebe bezbednog elektronskog bankarstva u Srbiji putem servisnog centra Halcom a.d. Beograd. Pogledati glavu 1.3.3.

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

HALCOM BG CA sertifikaciono telo, izdaje kvalifikovane elektronske sertifikate i vrši ostale delatnosti sertifikacionih tela u skladu sa: važećom pravnom regulativom Republike Srbije, nacionalnim propisima sa područja elektronskog poslovanja i elektronskog potpisa, dokumentima ETSI ESI TS 101 862 „Qualified Certificate Profile", RFC 3739 „Internet X.509 Public Key Infrastructure: Qualified Certificates Profile", RFC 5280 „Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" i ETSI TS 102 280 „X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons" i sa obaveznim sadržajem definisanim u članu 17. Zakona o elektronskom potpisu.

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. objavljuje na svojoj web stranici.

1.2. IDENTIFIKACIONI PODACI POLITIKE SERTIFIKACIJE

Identifikaciona oznaka ove politike sertifikacije HALCOM BG CA je:

CPName: HALCOM BG CA PL

CPOID: 1.3.6.1.4.1.5939.10.1.1

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.

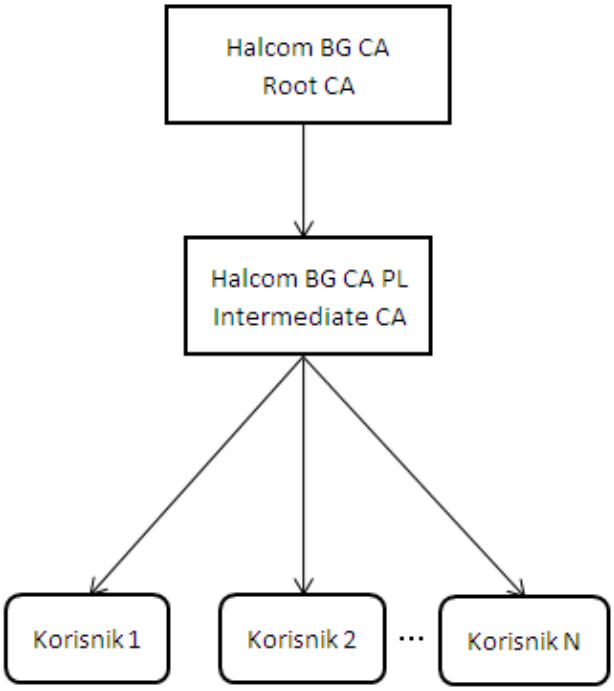
1.3. SUBJEKTI

1.3.1 SERTIFIKACIONO TELO HALCOM BG CA

HALCOM BG CA je sertifikaciono telo koje izdaje i upravlja kvalifikovanim elektronskim sertifikatima za verifikaciju kvalifikovanog elektronskog potpisa. HALCOM BG CA predstavlja takođe Root sertifikaciono telo koje zajedno sa svojim podređenim sertifikacionim telima čini hijerarhijsku mrežu sertifikacionih tela (Slika 1) koja izdaje kvalifikovane elektronske sertifikate fizičkim licima koji se identifikuju kao pripadnici pravnih lica, kao i vršenju drugih tehnoloških usluga vezanih za kvalifikovane elektronske potpise.

Sertifikaciono telo HALCOM BG CA izdaje kvalifikovane elektronske sertifikate fizičkim licima koji se identifikuju kao pripadnici pravnih lica u Srbiji za potrebe bezbednog elektronskog bankarstva putem servisnog centra Halcom a.d. Beograd.

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR



Slika 1: Hijerarhijska mreža

1.3.2 REGISTRACIONA TELA HALCOM BG CA

Registraciono telo (RA ili prijavna služba) vrše sledeće aktivnosti za potrebe sertifikacionog tela:

1. proveravanje identiteta budućih vlasnika kvalifikovanih elektronskih sertifikata, kao i proveravanje ostalih podataka važnih za upravljanje kvalifikovanim elektronskim sertifikatima,
2. primanje zahteva za dobijanje sertifikata,
3. primanje zahteva za opozivanje/povlačenje sertifikata,
4. izdavanje nužne dokumentacije vlasnicima, odnosno budućim vlasnicima, kvalifikovanih elektronskih sertifikata
5. prosleđivanje zahteva i ostalih podataka sigurnim putem do HALCOM BG CA sertifikacionog tela.

Sertifikaciono telo HALCOM BG CA može za izvršavanje zadataka registracionog tela (RA), uz svoje sopstveno RA, takođe ovlastiti i druge organizacije u poslovnom i javnom sektoru. Svaku takvu organizaciju sertifikaciono telo HALCOM BG CA ugovorom obaveže za ispunjavanje strogih bezbednosnih uslova u skladu sa važećim evropskim, i lokalnim propisima te međunarodnim, evropskim, i lokalnim standardima i preporukama, kao i internim pravilima HALCOM BG CA.

Sertifikaciono telo HALCOM BG CA ima široku uspostavljenu geografsku mrežu RA (registracionih tela), što budućim vlasnicima omogućuje jednostavnu prijavu u blizini sedišta datog pravnog lica.

1.3.3 VLASNICI KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA

Vlasnici kvalifikovanih elektronskih sertifikata koriste svoje podatke (par asimetričnih ključeva), dodeljene od strane sertifikacionog tela, za bezbedno elektronsko potpisivanje i kvalifikovane elektronske sertifikate za verifikaciju tog elektronskog potpisa.

Sertifikati korisnika koje izdaje Halcom BG CA:

- Digital Signature ,Non-Repudiation
- Digital Signature, Key Encipherment

1.3.4 TREĆA LICA

Treća lica su lica koja se uzdaju u izdate sertifikate sertifikacionog tela HALCOM BG CA, i mogu da budu pravna ili fizička lica.

Treća lica moraju da vrše aktivnosti u skladu i prema uputstvima sertifikacionog tela HALCOM BG CA i moraju uvek da provere da li je sertifikat važeći ili ne, rok trajanja sertifikata, itd. Detaljnije obaveze i odgovornosti trećih lica navedene su u poglavljima 4.5.2. i 9.6.4.

Treća lica nisu nužno i vlasnici sertifikata sertifikacionog tela HALCOM BG CA ili kvalifikovanih elektronskih sertifikata drugih sertifikacionih tela.

1.3.5 OSTALA LICA

Za korišćenje kvalifikovanih elektronskih sertifikata prema ovoj CP su, pored vlasnika sertifikata, RA, HALCOM BG CA, drugih sertifikacionih tela i trećih lica, bitna i druga lica koja omogućuju elektronsko potpisivanje ili neke druge usluge u kojima se koriste kvalifikovani elektronski sertifikati HALCOM BG CA.

1.4. NAMENE KORIŠĆENJA KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA

HALCOM BG CA sertifikaciono telo upravlja (izdaje i overava, opoziva, objavljuje) kvalifikovanim elektronskim sertifikatima za verifikaciju kvalifikovanog elektronskog potpisa koji su namenjeni fizičkim licima koji se identifikuju kao pripadnici pravnih lica.

1.4.1 PRAVILNO KORIŠĆENJE SERTIFIKATA I KLJUČEVA

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

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

- identifikaciju vlasnika sertifikata,
- dokazivanje identiteta vlasnika sertifikata,
- potpisivanje dokumenata u elektronskom obliku i njihovu verifikaciju,

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

- šifrovanje dokumenata u elektronskom obliku primenom simetričnih kriptografskih algoritama,
- kontrolu pristupa

Elektronski potpis može da se koristi u aplikacijama kao što su na primer:

- elektronsko odnosno mobilno bankarstvo,
- aplikacije e-uprave ili m-uprave,
- potpisivanje elektronskih formulara.
- bezbedno poslovanje sa organima i organizacijama javnog sektora te ostalim pravnim ili fizičkim licima,
- ostale aplikacije odnosno usluge u kojima se zahteva korišćenje kvalifikovanog elektronskog sertifikata.

Sertifikaciono telo HALCOM BG CA upravlja (izdaje i overava, opoziva, obnavlja, čuva i objavljuje) kvalifikovanim elektronskim sertifikatima pravnih lica za verifikaciju kvalifikovanog elektronskog potpisa, koje su izdate ovlašćenim, odnosno zaposlenim osobama pravnih lica, registrovanim za obavljanje delatnosti.

1.4.2 NEDOPUŠTENO KORIŠĆENJE

Zabranjeno je korišćenje kvalifikovanih elektronskih sertifikata, izdatih u skladu sa ovom CP, u suprotnosti sa odredbama same politike sertifikacije, ili važećih propisa, ili izvan opsega dozvoljenog korišćenja, određenog u prethodnom poglavlju.

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

1.5. UPRAVLJANJE POLITIKOM SERTIFIKACIJE

1.5.1 ODGOVORNOST ZA UPRAVLJANJE POLITIKOM SERTIFIKACIJE

Sa ovim CP dokumentom, kao i ostalim opštim i internim pravilima rada, upravlja sertifikaciono telo HALCOM BG CA.

Adresa sertifikacionog tela:

Halcom A.D. Beograd

HALCOM BG CA

Beogradska 39

11000 Beograd

Srbija

Tel.: (+381) 11 33 48 998

Fax: (+381) 11 33 48 994

http://www. halcom.rs/

1.5.2 OVLAŠĆENA LICA ZA KONTAKT

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

Adresa EBB:

Ivan Lacković

Halcom A.D. Beograd

HALCOM BG CA

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 LICE ODGOVORNO ZA USKLAĐENOST POSLOVANJA SERTIFIKACIONOG TELA HALCOM BG CA SA OVOM POLITIKOM SERTIFIKACIJE

Za usklađenosti poslovanja sertifikacionog tela HALCOM BG CA sa ovim CP dokumentom je, u skladu sa svojim nadležnostima, odgovorna ovlašćena lica za kontakt definisana u poglavlju 1.5.2.

1.5.4 POSTUPAK ZA USVAJANJE NOVE POLITIKE SERTIFIKACIJE

Svaki predlog nove izmenjene politike sertifikacije se razmatra sa tehnološkog i pravnog aspekta u cilju garantovanja zakonitosti, bezbednosti i kvaliteta. Nakon toga, nova politika sertifikacije se potvrđuje od strane direktora Halcom A.D. Beograd.

1.6. SKRAĆENICE I IZRAZI

1.6.1 SKRAĆENICE

CA	Sertifikaciono telo (*engl.: Certification Authority* ili *Certification Agency).*

CCPS	*Certificate and Card Production Service* – usluga izrade kvalifikovanih elektronskih sertifikata i kartica i uključuje: 1. Izdavanje CA ključa za svako podređeno sertifikaciono telo 2. Konfiguracija CA parametara u CCPS sistemu za svako podređeno sertifikaciono telo 3. Pred personalizacija smart kartica, u skladu sa nizom standardizovanih produkta 4. Izrada SA ključeva dužine 1024 bitova 5. Čuvanje integriteta pred personalizovanih smart kartica 6. Personalizacija smart kartica za konačnog korisnika/vlasnika sa povezivanjem podataka vlasnika i njegovog javnog ključa, dakle izdavanje kvalifikovanih elektronskih sertifikata X.509v3 i njihovo punjenje u smart kartice
CPName	Ime politike sertifikacije (*engl.: Certification Policy Name*), jednoznačno povezan sa međunarodno jedinstvenim brojem politike sertifikacije CPOID (*engl.: Certification Policy Object Identifier*).
CPOID	Međunarodni broj koji jednoznačno definiše politiku sertifikacije (*engl.: Certification Policy Object IDentifier*).
CRL	*Certificate Revocation List* – registar opozvanih kvalifikovanih elektronskih sertifikata
DN	Jednoznačno karakteristično ime (*engl.: Distinguished Name).*
LDAP	*Lightweight Directory Access Protocol* je protokol koji omogućava pristup sertifikatima i registru opozvanih sertifikata CRL koje izdaje sertifikaciono telo a specificiran prema IETF (*Internet Engineering Task Force*) preporuci RFC 1777.
S/MIME	*Secure Multipurpose Internet Mail Extensions*
SSL	*Secure Sockets Layer*
TLS	*Transport Layer Security*
PKI	*Public Key Infrastructure* je infrastruktura javnih ključeva
WPKI	*Wireless Public Key Infrastructure* je infrastruktura javnih ključeva koja deluje preko bežičnih veza (npr. mobilni telefoni i uređaji).
AR Admin	*Aplikacija za administraciju sertifikata izdatih u Halcom BG CA.*
AR ID	*Identifikacioni broj korisnika u AR Registru.*

1.6.2 IZRAZI

Identifikacija	Identifikacija je utvrđivanje identitete lica koje se izvodi lično, uz pomoć važećeg ličnog dokumenta ili u elektronskom obliku, uz pomoć važećeg kvalifikovanog elektronskog sertifikata.
Sertifikaciono telo	Pravno lice koje izdaje kvalifikovane elektronske sertifikate ili vrši ostale usluge vezane za verifikaciju ili elektronske potpise (*engl.: Certification Authority - CA*).

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

Registraciono telo	Služba ili lice koje prima zahteve za kvalifikovane elektronske sertifikate i preuzima odgovornost za identifikaciju i proveru identiteta budućih vlasnika sertifikata u ime sertifikacionog tela (*engl.: Registration Authority – RA)*.
Karakteristično ime	Jednoznačno ime u kvalifikovanom elektronskom sertifikatu (DN – Distinguished Name) koje nedvosmisleno i jednoznačno definiše datog korisnika u strukturi spiska sertifikata sertifikacionog tela.
Bezbednosni nosilac	Smart kartica, SIM (engl.: *Subscriber Identity Module*) kartica ili USB smart kartica sa ugrađenom posebnom memorijom za bezbedno čuvanje privatnih ključeva, kao i matematički procesor za realizaciju kriptografskih operacija sa tim ključevima. Namenjen je bezbednom generisanju, korišćenju i čuvanju asimetričnih kriptografskih ključeva.

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

2. OBJAVLJIVANJE INFORMACIJA I REGISTAR OPOZVANIH KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA

2.1. REPOZITORIJUM DOKUMENATA

Sertifikaciono telo HALCOM BG CA javno objavljuje sve informacije koje se odnose na rad sertifikacionog tela, obaveštenja korisnicima i trećim licima, kao i ostale važne dokumente, na web stranicama Halcom A.D. Beograd na adresi http://www.halcom.rs

Dokumenti koji su javno dostupni na web sajtu su:

- opšta pravila za izdavanje kvalifikovanih sertifikata (CP),
- opsta pravila rada (CPS),
- prijavni formulari za usluge sertifikacionog tela,
- uputstva za bezbedno korišćenje kvalifikovanih elektronskih sertifikata,
- informacije o važećem zakonodavstvu vezano za delovanje sertifikacionog tela
- ostale informacije vezane na delovanje HALCOM BG CA.

Međutim javno nisu dostupni dokumenti koji predstavljaju interna pravila sertifikacionog tela HALCOM BG CA.

2.2. REGISTAR OPOZVANIH KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA

Opozvani kvalifikovani elektronski sertifikati se objavljuju u registru opozvanih kvalifikovanih elektronskih sertifikata (CRL) periodično, na svaka dvadesetčetiri (24) sata (detaljnije o tome u poglavlju 4.9.8.), dok se ostale javno dostupne informacije odnosno dokumenti, objavljuju prema potrebi.

2.3. UČESTANOST OBJAVLJIVANJA

Nova modifikovana politika se objavljuje odmah nakon prihvatanja i odobravanja iste od strane menadžmenta sertifikacionog tela.

Lista opozvanih sertifikata se obnovi jedanput dnevno 24 sata nakon poslednje obnove CRL Sa zakašnjenjem od nekoliko minuta tako obnovljena CRL se prenese i na web stranice HALCOM BG CA.

Javno dostupne informacije, odnosno dokumenti, (osim gore navedenih) objavljuju se prema potrebi.

2.4. UPRAVLJANJE PRISTUPOM REPOZITORIJUMU DOKUMENATA

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

Registar opozvanih kvalifikovanih elektronskih sertifikata je javno dostupan na serveru ldap.halcom.rs, TCP port 389 u skladu sa LDAP protokolom.

Odgovarajućim tehničkim uslovima (mašinska i programska oprema) HALCOM BG CA garantuje kontrole koje sprečavaju neovlašćeno dodavanje, menjanje ili brisanje podataka u javnom registru opozvanih kvalifikovanih elektronskih sertifikata. Detalji o načinu sprečavanja neovlašćenog dodavanja, menjanja ili brisanja podataka opisani su u internim pravilima sertifikacionog tela Halcom BG CA.

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

3. IDENTITET VLASNIKA SERTIFIKATA

3.1. DODELA IMENA

Karakteristična imena koje sadrži kvalifikovani elektronski sertifikat nedvosmisleno i jednoznačno definišu vlasnika sertifikata.

3.1.1 KARAKTERISTIČNA IMENA

U skladu sa RFC 5280 svaki kvalifikovani elektronski sertifikat sadrži podatke o vlasniku i izdavaocu kvalifikovanog elektronskog sertifikata u obliku karakterističnog imena. Karakteristično ime je formirano u skladu sa RFC 5280 i standardom X501.

Izdavalac sertifikata je u izdatom sertifikatu naveden u polju Izdavač, engl. *Issuer*.

Osnovni podaci o vlasniku koje sadrži karakteristično ime vlasnika kvalifikovanog elektronskog sertifikata nalaze se u izdatom sertifikatu navedeni u polju Nosilac engl. *Subject*.

Jedinstveni serijski broj korisnika u okviru sertifikacionog tela koji se takođe sadrži u karakterističnom imenu određuje izdavalac HALCOM BG CA. (više u poglavlju 3.1.5.)

Vrsta sertifikata	Naziv polja	Karakteristično ime
Kvalifikovani elektronski sertifikat sertifikacionog tela HALCOM BG CA	Izdavalac engl. *Issuer*	C= RS O= Halcom a.d. Beograd CN= HALCOM BG CA PL
Kvalifikovani elektronski sertifikat za korisnike	Korisnik, engl. *Subject*	C= RS G= <ime> SN= <prezime> CN=<ime, prezime, AR ID,- JMBG> O = <ime organizacije>

3.1.2 ZAHTEVI KOD KREIRANJA KARAKTERISTIČNOG IMENA

U skladu sa karakterističnim imenom, AR ID-em i jedinstvenim matičnim brojem vlasnik kvalifikovanog elektronskog sertifikata je nedvosmisleno i jednoznačno definisan.

Karakteristično ime zajedno sa AR ID-em i jedinstvenim matičnim brojem jedinstveno je u okviru sertifikacionog tela, tj. formirano je na način da je iz istog moguće jednoznačno identifikovati pojedinca .

3.1.3 UPOTREBA ANONIMNIH IMENA ILI PSEUDONIMA

Upotreba anonimnih imena ili pseudonima nije dozvoljena.

ISO 9001 BUREAU VERITAS Certification
Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

3.1.4 PRAVILA ZA INTERPRETACIJU KARAKTERISTIČNOG IMENA

Podaci o vlasniku kvalifikovanog elektronskog sertifikata u karakterističnom imenu sadrže slova srpske azbuke, dok se preostali znakovi transformišu prema donjim pravilima:

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

Odgovarajućom kombinacijom slova sertifikaciono telo obezbeđuje korišćenje ostalih nepredvidivih znakova.

3.1.5 JEDNOZNAČNOST KARAKTERISTIČNIH IMENA

Karakteristično ime zajedno sa AR ID-em i jedinstvenim matičnim brojem jedinstveno je u okviru sertifikacionog tela, tj. formirano je na način da je iz istog moguće jednoznačno identifikovati pojedinca.

3.1.6 ZAŠTITA IMENA ODNOSNO ROBNIH MARKI

Vlasnici sertifikata ne smeju da zahtevaju imena koja pripadaju nekome drugome čime bi se kršila autorska ili druga prava trećih lica.

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

3.2. PROVERAVANJE IDENTITETA VLASNIKA / KORISNIKA KOD PRVOG IZDAVANJA KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA

Budući vlasnik kvalifikovanog elektronskog sertifikata mora da zahteva kvalifikovani elektronski sertifikat u svoje lično ime i ime korisnika u okviru pravnog lica, kao ovlašćeno lice odgovarajućeg pravnog lica. Prijavna služba proverava identitet budućeg vlasnika kvalifikovanog elektronskog sertifikata. Budući vlasnik se mora lično identifikovati u prijavnoj službi sertifikacionog tela radi neophodne identifikacije lica.

3.2.1 PROVERAVANJE IDENTITETA ORGANIZACIJE

Identitet organizacije se proverava na osnovu pravnih dokumenata o uspostavljanju date organizacije, kao i ovlašćenjem da dato fizičko lice ima ovlašćenje da dobije kvalifikovani elektronski sertifikat u ime date organizacije.

3.2.2 PROVERAVANJE IDENTITETA VLASNIKA SERTIFIKATA

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

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

Dakle, u cilju identifikacije i autentikacije korisnika koji aplicira za dobijanje sertifikata, kao ovlašćeno lice datog pravnog lica, od strane HALCOM BG CA sertifikacionog tela, CA može primeniti korake koji uključuju ali nisu ograničeni na:

- Provera dokumenata kao što su identifikaciona kartica i pasoš, u skladu sa važećim zakonom za pojedinca – fizičko lice za sebe lično, odnosno fizičko lice koje aplicira za sertifikat kao ovlašćeno lice pravnog lica
- Utvrđivanje identiteta datog pojedinca koja se bazira na dostavljenoj dokumentaciji.
- Zahtev je da se pojedinac fizički pojavi u RA u odgovarajućoj fazi pre nego što se sertifikat izda.

3.2.3 PROVERAVANJE OVLAŠĆENJA ZAPOSLENIH ZA STICANJE SERTIFIKATA U IME ORGANIZACIJE

Ovlašćeno lice organizacije sa 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 u prijavnoj službi sertifikacionog tela. Pravno lice se kao poslodavac vlasnika sertifikata obavezuje, da će ispunjavati sve odredbe ovog CP dokumenta i važeće propise.

3.2.4 MEĐUSOBNO PRIZNAVANJE

Sertifikaciono telo HALCOM BG CA priznaje, a nije dužno ugovorno sarađivati ili garantovati za ostala sertifikaciona tela čak iako drugo sertifikaciono telo ima status akreditovanog sertifikacionog tela za izdavanje kvalifikovanih elektronskih sertifikata.

Sertifikaciono telo HALCOM BG CA obezbeđuje da će ispoštovati međusobnu saradnju sa drugim sertifikacionim telima isključivo nakon potpisivanja pismenog ugovora sa drugim sertifikacionim telima koji moraju da ispune nivo sigurnosnih zahteva koje su uporedive ili više od onih koje propisuje sertifikaciono telo HALCOM BG CA.

Ovlašćena lica sertifikacionog tela HALCOM BG CA proveravaju opšta i interna pravila drugog sertifikacionog tela, kao i njegovo ispunjavanje sigurnosnih zahteva.

Troškove potrebne infrastrukture koju zahteva sertifikaciono telo HALCOM BG CA za međusobno priznavanje pokriva drugo sertifikaciono telo.

3.3. PROVERAVANJE VLASNIKA ZA PONOVNO IZDAVANJE KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA

3.3.1 PROVERAVANJE VLASNIKA SERTIFIKATA KOD OBNOVE KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

Identitet vlasnika kod ponovnog izdavanja kvalifikovanog elektronskog sertifikata se proverava:

- Ličnim prisustvom vlasnika kvalifikovanog elektronskog sertifikata u registracionom telu, sertifikacionog tela HALCOM BG CA

3.3.2 PROVERAVANJE VLASNIKA SERTIFIKATA ZA PONOVO IZDAVANJE KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA NAKON OPOZIVA

Proveravanje vlasnika sertifikata u ovom slučaju se vrši u skladu sa odredbama iz poglavlja 3.2.3.

3.4. PROVERAVANJE IDENTITETA KOD ZAHTEVA ZA OPOZIV SERTIFIKATA

U cilju sprovođenja procedura identifikacije i autentikacije zahteva za povlačenjem sertifikata za odgovarajuće tipove subjekata (CA, RA, korisnici ili drugi učesnici), zahtevi se upućuju odgovarajućem RA ili putem komunikacije do samog CA. RA sprovodi takve zahteve do HALCOM BG CA sertifikacionog tela u cilju realizacije procedure povlačenja sertifikata.

Primeri bezbednog dostavljanja zahteva za povlačenjem su overeni zahtevi od strane samih korisnika koji žele da im se povuče sertifikat (ukoliko je takva mogućnost dozvoljena u okviru CPS) ili overeni zahtevi od strane RA ili CA ovlašćenih službenika.

Dakle, zahtev za opoziv svog kvalifikovanog elektronskog sertifikata vlasnik preda:

- Lično registracionom telu gde ovlašćena lica registracionog tela provere identitet podnosioca zahteva,
- U slučaju da vlasnik kvalifikovanog elektronskog sertifikata putem telefona, elektronske pošte ili FAX-a zahteva opoziv sertifikata, sertifikaciono telo HALCOM BG CA prvo definiše suspenziju sertifikata. Tek na osnovu prijema overenog pismenog zahteva za opoziv sertifikata, koji vlasnik lično dostavi registracionom telu faktički se sprovodi sam opoziv sertifikata.

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

4. UPRAVLJANJE KVALIFIKOVANIM ELEKTRONSKIM SERTIFIKATIMA

4.1. 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 ovlašćenja lica odgovarajućih pravnih lica.

4.1.2 POSTUPAK BUDUĆEG VLASNIKA SERTIFIKATA ZA STICANJE KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA I PRIDRUŽENE ODGOVORNOSTI

Kvalifikovani elektronski sertifikat se izdaje na osnovu pravilno ispunjene i potpisane narudžbenice za izdavanje kvalifikovanog elektronskog sertifikata (u daljem tekstu narudžbenica) od strane zakonitog zastupnika pravnog lica i budućeg vlasnika sertifikata.

Narudžbenica se preda registracionom telu (RA) HALCOM BG CA lično od strane budućeg vlasnika kvalifikovanog elektronskog sertifikata.

Narudžbenice za izdavanje kvalifikovanog elektronskog sertifikata dostupne su kako kod registracionih tela (RA) HALCOM BG CA tako i na web stranici HALCOM BG CA.

Budući vlasnik kvalifikovanog elektronskog sertifikata lično preda narudžbenicu u pismenom obliku.

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 sertifikacionog tela HALCOM BG CA.

HALCOM BG CA zadržava pravo da negativno reši zahtev korisnika za izdavanje kvalifikovanog elektronskog sertifikata ako je u suprotnosti važećim propisima Republike Srbije ili Evropske Unije.

4.2. POSTUPAK KOD PRIJEMA ZAHTEVA ZA DOBIJANJE KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA

4.2.1 PROVERAVANJE IDENTITETA BUDUĆEG VLASNIKA SERTIFIKATA

Ovlašćeno lice registracionog tela proveri identitet budućeg vlasnika. Budući vlasnik mora da dokaže svoj identitet važećim ličnim dokumentom sa fotografijom i ličnim prisustvom u registracionom telu. Pod ličnim identifikacionim dokumentom smatraju se važeća lična karta i pasoš.

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

Ovlašćena lica registracionog ili sertifikacionog tela su dužna da provere identitet budućeg vlasnika sertifikata, odnosno sve one podatke koji su navedeni u narudžbenici a dostupni su u službenim evidencijama odnosno u drugim službeno važećim dokumentima.

Ovlašćena lica registracionog tela proverene ispunjene narudžbenice, kao i dopunsku originalnu dokumentaciju koja se zahteva, prosleđuju sertifikacionom telu HALCOM BG CA.

4.2.2 ODOBRENJE/ODBIJANJE ZAHTEVA

Ovlašćena lica sertifikacionog tela HALCOM BG CA odobravaju, odnosno u slučaju nepravilnih ili nedostajućih podataka ili neispunjavanja obaveza, odbijaju zahtev za dobijanje kvalifikovanog elektronskog sertifikata ako je u suprotnosti važećim propisima Republike Srbije ili Evropske Unije. O tome su zakoniti zastupnik pravnog lica ili budući korisnici obavešteni lično ili elektronskom poštom.

4.2.3 VREME ZA IZDAVANJE KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA

HALCOM BG CA se po osnovu odobrenog zahteva za izdavanje kvalifikovanog elektronskog sertifikata obavezuje da najkasnije u roku od pet (5) dana izda kvalifikovani elektronski sertifikat na smart kartici ili USB ključu i lozinku za upotrebu sertifikata (PIN/PUK kod) i pošalje ih odvojeno prijavnoj službi koja dalje distribuira sertifikate do budućih vlasnika.

4.3. IZDAVANJE KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA

4.3.1 POSTUPAK SERTIFIKACIONOG TELA HALCOM BG CA

Proizvodni postupak za generisanje kvalifikovanih elektronskih sertifikata za dva para asimetričnih ključeva sastoji se iz jasno odvojenih koraka (ili funkcija), sa odvojenim podsistemima:

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

Kvalifikovani elektronski sertifikat na bezbednom mediju i odgovarajuća lična lozinka (PIN/PUK kod) se do registracionog tela dostavlja putem dva odvojena kanala u dve odvojene pošiljke, dok se vlasniku isporučuje lično na šalterima prijemne službe, u dve odvojene pošiljke, na dva različita šaltera.

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

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

4.3.2 OBAVEŠTENJE VLASNIKU O IZDAVANJU SERTIFIKATA

Po prijemu medija sa kvalifikovanim elektronskim sertifikatom registraciono telo obavesti budućeg vlasnika sertifikata o izdavanju i mogućnosti preuzimanja kvalifikovanog elektronskog sertifikata.

4.4. PREUZIMANJE KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA

4.4.1 POSTUPAK PREUZIMANJA KVALIFIKOVANOG ELEKTRONSKOG 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 prijemne službe HALCOM BG CA, pogledati poglavlje 4.3.1.

4.4.2 OBJAVLJIVANJE KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA

Kvalifikovani elektronski sertifikati se u skladu sa Zakonom i podzakonskim aktima javno ne objavljuju.

4.4.3 OBAVEŠTENJE OD STRANE SERTIFIKACIONOG TELA O IZDAVANJU SERTIFIKATA DRUGIM PREDUZEĆIMA ODNOSNO ORGANIZACIJAMA

Sertifikaciono telo ne obaveštava druga preduzeća, odnosno organizacija, o izdavanju sertifikata.

4.5. OBAVEZE I ODGOVORNOSTI KORISNIKA VEZANE NA KORIŠĆENJE KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA

4.5.1 OBAVEZE VLASNIKA KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA

Vlasnik, odnosno budući vlasnik, kvalifikovanog elektronskog sertifikata je dužan:

- Upoznati se sa ovom politikom sertifikacije pre izdavanja kvalifikovanog elektronskog sertifikata,
- Postupati u skladu sa ovom politikom sertifikacije i ostalim važećim propisima,
- Nakon preuzimanja kvalifikovanog elektronskog sertifikata proveriti odštampane podatke na smart kartici i koverti PIN/PUK koda i o eventualnim greškama odmah obavestiti prijemnu službu ili HALCOM BG CA
- Pratiti sva obaveštenja HALCOM BG CA i postupati u skladu sa njima,
- u skladu sa obaveštenjima primereno osavremenjivati potrebnu mašinsku i programsku opremu za bezbedan rad sa kvalifikovanim elektronskim sertifikatima,
- odmah obavestiti sertifikaciono telo HALCOM BG CA o svim promenama koje su povezane sa kvalifikovanim elektronskim sertifikatom,
- zahtevati opoziv kvalifikovanog elektronskog sertifikata u slučaju da je privatni ključ bio ugrožen na način koji utiče na sigurnost upotrebe ili ako postoji opasnost od zloupotrebe,

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

- korišćenje kvalifikovanog elektronskog sertifikata samo za namene definisane u sertifikatu (pogledati poglavlje 7.1), i na način koji je određen ovom politikom sertifikacije HALCOM BG CA.

Vlasnik, odnosno budući vlasnik, kvalifikovanog elektronskog sertifikata je u odnosu na bezbednost privatnog ključa dužan takođe da:

- PIN/PUK kod brižljivo čuva od neovlašćenih lica,
- čuva privatni ključ i kvalifikovani elektronski sertifikat na način i na sredstvima za bezbedno čuvanje privatnih ključeva u skladu sa obaveštenjima i preporukama HALCOM BG CA,
- privatni ključ i sve ostale poverljive podatke štiti prikladnom lozinkom u skladu sa preporukama HALCOM BG CA ili na drugi način tako da su dostupni samo vlasniku,
- brižljivo čuva PIN/PUK kod za zaštitu privatnog ključa,
- nakon isteka valjanosti odnosno nakon opoziva kvalifikovanog elektronskog sertifikata postupa u skladu sa obaveštenjima sertifikacionog tela HALCOM BG CA

4.5.2 OBAVEZE TREĆIH LICA

Treće lice koje se pouzdaje u kvalifikovani elektronski sertifikat izdat od strane sertifikacionog tela HALCOM BG CA mora:

- Postupati i koristiti kvalifikovane elektronske sertifikate u skladu i namenom definisanom ovom politikom sertifikacije i ostalim važećim propisima,
- Brižno proučiti sve mogućnosti rizikovanja i odgovornosti kod korišćenja kvalifikovanih elektronskih sertifikata i odrediti politiku načina upotrebe,
- Obavestiti HALCOM BG CA ako sazna da su privatni ključevi vlasnika kvalifikovanog elektronskog sertifikata u koga se uzdaju bili ugroženi na način koji utiče na sigurnost korišćenja, ili ako postoji opasnost zloupotrebe, ili ako su se promenili podaci navedeni u kvalifikovanom elektronskom sertifikatu,
- Uzdati se u kvalifikovani elektronski sertifikat samo za namere određene u sertifikatu (pogledati poglavlje 6.1.7.) na način koji određuje politika sertifikacije,
- Za vreme korišćenja kvalifikovanog elektronskog sertifikata proveriti da li se sertifikat nalazi u registru opozvanih sertifikata,
- Za vreme korišćenja kvalifikovanog elektronskog sertifikata proveriti potpis kvalifikovanog elektronskog sertifikata od strane sertifikacionog tela HALCOM BG CA koji je objavljen u ovoj politici sertifikacije, a takođe i na web stranicama HALCOM BG CA odnosno drugih izdavalaca kvalifikovani elektronskih sertifikata.
- Uvažavanje drugih odredaba ukoliko je sa sertifikacionim telom HALCOM BG CA sklopila dogovor o korišćenju kvalifikovanih elektronskih sertifikata.

Treće lice mora za verifikaciju potpisa odnosno druge kriptografske operacije upotrebljavati programsku i mašinsku opremu kojom je moguće na verodostojan način proveriti sve gore navedene zahteve za bezbedno korišćenje kvalifikovanih elektronskih sertifikata.

4.6. OBNOVA KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

Obnova kvalifikovanog elektronskog sertifikata moguća je samo na osnovu zahteva vlasnika.

Postupak podnošenja zahteva za obnovu kvalifikovanog elektronskog sertifikata isti je kao i kod prvobitnog izdavanja.

4.6.1 OKOLNOSTI KOJE ZAHTEVAJU OBNOVU KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA

Pre isteka validnosti kvalifikovanog elektronskog sertifikata, dostavljanjem zahteva za obnovu kvalifikovanog elektronskog sertifikata, vlasnici sertifikata obezbeđuju kontinuitet korišćenja kvalifikovanog elektronskog sertifikata.

Zahtev za obnovu je moguće uložiti i nakon isteka validnosti kvalifikovanog elektronskog sertifikata.

4.6.2 LICA KOJA MOGU DA TRAŽE OBNOVU KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA

Samo vlasnik kvalifikovanog elektronskog sertifikata može da traži obnovu sertifikata.

4.6.3 POSTUPAK OBRADE ZAHTEVA ZA OBNOVU KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA

Postupak obrade zahteva za obnovu kvalifikovanog elektronskog sertifikata je isti kao postupak za prvobitno izdavanje sertifikata.

Postupak garantuje da je lice koje uloži zahtev za obnovu kvalifikovanog elektronskog sertifikata doista vlasnik sertifikata.

4.6.4 OBAVEŠTENJE VLASNIKU O OBNOVLJENOM KVALIFIKOVANOM ELEKTRONSKOM SERTIFIKATU

Pogledati poglavlje 4.4.2.

4.6.5 POSTUPAK PREUZIMANJA OBNOVLJENOG KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA

Pogledati poglavlje 4.4.1.

4.6.6 OBAVEŠTENJE SERTIFIKACIONOG TELA O IZDAVANJU KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA DRUGIM SUBJEKTIMA

Sertifikaciono telo o izdavanju pojedinačnih kvalifikovanih elektronskih sertifikata vlasnicima ne obaveštava preduzeća i druge organizacije.

4.7. OBNAVLJANJE KLJUČEVA

4.7.1 RAZLOZI ZA OBNAVLJANJE KLJUČEVA

Nije primenljivo u ovoj CP.

4.7.2 KO MOŽE DA ZAHTEVA OBNAVLJANJE KLJUČEVA

Nije primenljivo u ovoj CP.

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

4.7.3 POSTUPAK ZA IZDAVANJE ZAHTEVA ZA OBNAVLJANJE KLJUČEVA

Nije primenljivo u ovoj CP.

4.7.4 OBAVEŠTENJE VLASNIKU KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA O NOVO IZDATOM PARU KLJUČEVA

Nije primenljivo u ovoj CP.

4.7.5 POSTUPAK PREUZIMANJA

Nije primenljivo u ovoj CP.

4.7.6 OBJAVA KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA IZDAVAOCA SERTIFIKATA SA NOVIM PAROM KLJUČEVA

Nije primenljivo u ovoj CP.

4.7.7 OBAVEŠTENJE OD STRANE SERTIFIKACIONOG TELA O IZDAVANJU SERTIFIKATA DRUGIM SUBJEKTIMA

Sertifikaciono telo o izdavanju pojedinačnog kvalifikovanog elektronskog sertifikata vlasnicima sertifikata ne obaveštava preduzeća i druge organizacije.

4.8. PROMENA KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA

U slučaju promene podataka koji utiču na validnost karakterističnog imena odnosno drugih podataka u kvalifikovanom elektronskom sertifikatu, sertifikat je potrebno neizostavno opozvati.

Za dobijanje novog kvalifikovanog elektronskog sertifikata potrebno je ponoviti postupak za sticanje novog sertifikata kao što je navedeno u pod-poglavlju 4.1.

4.8.1 OKOLNOSTI ZA PROMENU KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA

Nije primenljivo u ovoj CP.

4.8.2 KO MOŽE DA ZAHTEVA PROMENU

Nije primenljivo u ovoj CP.

4.8.3 POSTUPAK KOD ZAHTEVA ZA PROMENU

Nije primenljivo u ovoj CP.

4.8.4 OBAVEST O IZDAVANJU NOVOG KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA

Nije primenljivo u ovoj CP.

4.8.5 PREUZIMANJE PROMENJENOG KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA

Nije primenljivo u ovoj CP.

4.8.6 OBJAVLJIVANJE PROMENJENOG KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA

Nije primenljivo u ovoj CP.

4.8.7 OBAVEŠTENJE DRUGIH SUBJEKATA O PROMENI

Nije primenljivo u ovoj CP.

4.9. OPOZIV I SUSPENZIJA KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA

Opoziv svog kvalifikovanog elektronskog sertifikata vlasnik može da zahteva bilo kada, ali svakako mora da ga zahteva u slučaju:

1. promene karakterističnog imena (DN),
2. kada se ustanovi ili sumnja da je došlo bilo do pronevere ili zloupotrebe privatnog ključa za elektronsko potpisivanje,
3. zamene kvalifikovanog elektronskog sertifikata drugim sertifikatom (npr. kod gubitka bezbednosnog nosioca).

Sertifikaciono telo 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 nadležnog državnog organa.

Opoziv kvalifikovanog elektronskog sertifikata je moguć 24 sata dnevno. Precizna uputstva za opoziv kvalifikovanog elektronskog sertifikata objavljena su na web stranicama sertifikaciono telo HALCOM BG CA.

Sertifikaciono telo HALCOM BG CA će na osnovu pravilnog zahteva za opoziv sertifikata, isti opozvati u roku od četiri (4) sata. Opozvani kvalifikovani elektronski sertifikat će biti označen u registru opozvanih sertifikata (CRL) prilikom izdavanja prve sledeće CRL liste koja se izdaje periodično, na svaka dvadesetčetiri sata. U slučaju da vlasnik kvalifikovanog elektronskog sertifikata isporuči sertifikacionom telu HALCOM BG CA nepravilan zahtev za opoziv istog, biće mu poslato upozorenje o nepravilnom zahtevu za opoziv sertifikata i biće upoznat sa U slučaju da vlasnik kvalifikovanog elektronskog sertifikata isporuči sertifikacionom telu HALCOM BG CA nepravilan zahtev za opoziv istog, 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 OPOZIVA

Opoziv svog kvalifikovanog elektronskog sertifikata vlasnik mora da zahteva u slučaju:

- Ako je privatni ključ vlasnika sertifikata ugrožen na način koji utiče na pouzdanost i bezbednost primene,
- Ako postoji opasnost zloupotrebe privatnog ključa ili sertifikata vlasnika,
- Ako su se promenili odnosno se utvrdi da su pogrešni ključni podaci navedeni u sertifikatu.

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

Sertifikaciono telo HALCOM BG CA opoziva sertifikat odmah i bez zahteva vlasnika sertifikata, ukoliko postoji informacija:

- da je podatak u kvalifikovanom elektronskom sertifikatu pogrešan ili da je sertifikat izdat na osnovu pogrešnih podataka,
- da je došlo do greške kod provere identiteta korisnika u registracionom telu,
- da su se promenile druge okolnosti koje utiču na validnost sertifikata,
- da vlasnik sertifikata ne ispunjava svoje obaveze preuzete potpisivanjem odgovarajućeg ugovora sa sertifikacionim telom,
- da nisu podmireni eventualni troškovi za upravljanje kvalifikovani elektronskim sertifikatima,
- da je infrastruktura sertifikacionog tela ugrožena na način koji utiče na pouzdanost procesa izdavanja sertifikata,
- da je privatni ključ vlasnika sertifikata ugrožen na način koji utiče na pouzdanost primene istog,
- da će sertifikaciono telo HALCOM BG CA prekinuti sa izdavanjem kvalifikovanih elektronskih sertifikata ili da je sertifikacionom telu zabranjeno upravljanje sertifikatima a da njegovo poslovanje nije preuzelo drugo sertifikaciono telo,
- da je opoziv naložio nadležni sud ili drugi administrativni organ.

4.9.2 KO ZAHTEVA OPOZIV

Opoziv kvalifikovanog elektronskog sertifikata može da zahteva:

- Ovlašćeno lice sertifikacionog tela HALCOM BG CA,
- Zakoniti zastupnik pravnog lica,
- Vlasnik sertifikata,
- Nadležni sud ili
- Nadležni državni organ.

4.9.3 POSTUPAK OPOZIVA

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,

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 sertifikacionom telu HALCOM BG CA elektronski potpisanu poruku sa zahtevom za opoziv. Na osnovu te poruke sertifikaciono telo privremeno suspenduje sertifikat, a po prijemu odgovarajućeg svojeručno potpisanog zahteva za opoziv kvalifikovanog elektronskog sertifikata sertifikaciono telo opoziva sertifikat.

O datumu i vremenu opoziva, podnosiocu zahteva za opoziv, kao i o uzrocima opoziva, vlasnik sertifikata mora da bude obavešten.

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

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

4.9.4 VREME IZDAVANJA ZAHTEVA ZA OPOZIV

Neophodno je da se zahtev za opoziv sertifikata podnese odmah ukoliko se radi o mogućnosti zloupotrebe ili nepouzdanosti sertifikata, kao i u sličnim nužnim slučajevima.

U ostalim slučajevima opoziv se može zahtevati prvog radnog dana, i to u radno vreme registracionog tela (pogledati sledeće poglavlje).

4.9.5 VREME OD PRIMLJENOG ZAHTEVA ZA OPOZIV DO IZVRŠENJA OPOZIVA

Sertifikaciono telo HALCOM BG CA je u obavezi da nakon prijema validnog zahteva za opoziv sertifikata:

- U roku od četiri (4) sata opozove kvalifikovani elektronski sertifikat

Nakon opoziva, opozvani kvalifikovani elektronski sertifikat se upisuje u registar opozvanih kvalifikovanih elektronskih sertifikata (CRL) i objavljuje izdavanjem nove CRL koja se izdaje periodično, na svaka dvadesetčetiri (24) sata.

4.9.6 ZAHTEVI ZA PROVERAVANJE REGISTRA OPOZVANIH SERTIFIKATA ZA TREĆA LICA

Pre korišćenja kvalifikovanih elektronskih sertifikata izdatih od sertifikacionog tela HALCOM BG CA, treća lica koja se pouzdaju u dati sertifikat moraju da provere najnoviji objavljeni registar opozvanih kvalifikovanih elektronskih sertifikata (CRL). Iz razloga verodostojnosti i celovitosti potrebno je uvek da se proveri i verodostojnost i integritet tog registra koji je elektronsko potpisan sa strane HALCOM BG CA sertifikacionog tela.

4.9.7 UČESTANOST OBJAVLJIVANJA REGISTRA OPOZVANIH SERTIFIKATA

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

- Jedanput dnevno 24 sata nakon poslednje obnove CRL.

4.9.8 VREME OBJAVLJIVANJA REGISTRA OPOZVANIH SERTIFIKATA

Objavljivanje novog registra opozvanih sertifikata izvrši se:

- U registru opozvanih sertifikata na serveru ldap.halcom.rs svakih 24 sata ,
- A na web stranici http://domina.halcom.rs/crls sa zakašnjenjem od najviše deset (10) minuta.

4.9.9 ON-LINE PROVERA STATUSA SERTIFIKATA

Protokol za on-line proveru statusa sertifikata - OCSP (engl. *Online Certificate Status* Protocol) nije podržan.

4.9.10 ZAHTEVI ZA ONLINE PROVERU STATUSA SERTIFIKATA

Treća lica moraju u slučaju korišćenja datog kvalifikovanog elektronskog sertifikata uvek da provere, da li je sertifikat u koji se pouzdaju opozvan. Po standardu RFC 5280 sistem koji upotrebljava kvalifikovane elektronske sertifikate mora pre upotrebe sertifikata proveriti dali je sertifikat još validan i da nije opozvan (da se serijski broj sertifikata ne nalazi u registru opozvanih sertifikata – CRL-ju).

4.9.11 DRUGI NAČINI ZA PRISTUP STATUSU SERTIFIKATA

Nisu podržani.

4.9.12 POSEBNI ZAHTEVI KOD ZLOUPOTREBE PRIVATNOG KLJUČA

Nisu određeni.

4.9.13 RAZLOZI ZA SUSPENZIJU SERTIFIKATA

Razlozi za suspenziju sertifikata su:

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

- U slučaju da vlasnik sertifikata, druga ili treća lica, državni ili drugi odgovarajući organi odnosno samo sertifikaciono telo, izraze sumnju da se u vezi sa sertifikatom postupa suprotno ovoj politici sertifikacije, odnosno važećim propisima, taj se kvalifikovani elektronski sertifikat privremeno suspenduje do konačne odluke.

4.9.14 KO ZAHTEVA SUSPENZIJU

Pogledati poglavlje 4.9.13.

4.9.15 POSTUPAK SUSPENZIJE

Pogledati poglavlje 4.9.13.

4.9.16 VREME SUSPENZIJE

Pogledati poglavlje 4.9.13.

4.10. PROVERAVANJE STATUSA SERTIFIKATA

4.10.1 PRISTUP PROVERAVANJU

Registar opozvanih sertifikata je javno objavljen na serveru ldap.halcom.rs putem LDAP protokola i na http://domina.halcom.rs/crls putem HTTP protokola, detalji o objavljivanju i načinu pristupa nalaze se u poglavljima 7.2 i 7.3.

4.10.2 RASPOLOŽIVOST

Proveravanje statusa sertifikata je raspoloživo 24 sata na dan, svih dana u godini.

4.10.3 DRUGE INFORMACIJE ZA PROVERAVANJE STATUSA

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

Nisu propisane.

4.11. PREKID ODNOSA VLASNIKA I SERTIFIKACIONOG TELA

Odnos vlasnika i sertifikacionog tela prekida se ako:

- Vlasnikov sertifikat istekne a on ga ne obnovi
- je sertifikat opozvan a vlasnik ne podnese zahtev za novi.

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

5. UPRAVLJANJE I SIGURNOSNI NADZOR INFRASTRUKTURE

HALCOM BG CA sertifikaciono telo planira i izvodi sve bezbednosne mere u skladu sa standardima ISO/IEC 27001, 27002 i 27005, sa tehničkim zahtevima ETSI TS 101 456 - *Policy requirements for certification authorities issuing qualified certificates*.

Oprema sertifikacionog tela 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.

Sertifikaciono telo 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 sertifikata, u cilju obezbeđenja kontinuiteta poslovanja u slučajevima kada se iz nekih razloga unište podaci na osnovnoj lokaciji.

Detaljan opis infrastrukture sertifikacionog tela HALCOM BG CA, operativni rad, postupci upravljanja infrastrukturom, kao i nadzor vezan za politiku bezbednosti operativnog rada, definisani su u internim pravilima rada sertifikacionog tela.

5.1. FIZIČKO OBEZBEĐENJE

Oprema sertifikacionog tela je obezbeđena sistemima fizičkog i elektronskog obezbeđenja na više nivoa.

Obezbeđenje infrastrukture sertifikacionog tela realizuje se u skladu sa preporukama struke za najviši nivo obezbeđenja.

Celokupan opis infrastrukture sertifikacionog tela, primenjene procedure i obezbeđenje infrastrukture definisani su internim pravilima sertifikacionog tela.

5.1.1 LOKACIJA I ZGRADA SERTIFIKACIONOG TELA

Oprema sertifikacionog tela HALCOM BG CA je postavljena u posebnim, bezbednim i odvojenim prostorijama.

Osigurana je sistemom fizičkog i elektronskog obezbeđenja na više nivoa.

Detaljne odredbe nalaze se u internim pravilima sertifikacionog tela HALCOM BG CA.

5.1.2 FIZIČKI PRISTUP INFRASTRUKTURI SERTIFIKACIONOG TELA

Pristup infrastrukturi sertifikacionog tela omogućen je samo ovlašćenim licima sertifikacionog tela u skladu sa njihovim zadacima i ovlašćenjima, pogledati poglavlje 5.2.1.

Svi pristupi obezbeđeni su u skladu sa zakonodavstvom i preporukama.

Detaljne odredbe nalaze se u internim pravilima sertifikacionog tela HALCOM BG CA.

5.1.3 NAPAJANJE I VENTILACIJA

U okviru infrastrukture sertifikacionog tela obezbeđeno je kontinualno napajanje i odgovarajući klimatski sistemi.

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

Svi detalji se nalaze u internim pravilima rada sertifikacionog tela HALCOM BG CA.

5.1.4 ZAŠTITA OD POPLAVA

Infrastruktura sertifikacionog tela HALCOM BG CA nije izložena opasnosti od poplava osim u slučaju više sile.

Svi detalji se nalaze u internim pravilima rada sertifikacionog tela HALCOM BG CA.

5.1.5 ZAŠTITA OD POŽARA

Prostorije sertifikacionog tela su osigurane od mogućih izbijanja požara.

Svi detalji se nalaze u internim pravilima rada sertifikacionog tela HALCOM BG CA.

5.1.6 ČUVANJE NOSIOCA PODATAKA

Nosioci podataka, na papiru ili u elektronskom obliku, bezbedno se čuvaju u zaštićenim objektima.

Bezbedne kopije programske opreme i šifrovanih baza sertifikacionog tela HALCOM BG CA redovno se obnavljaju i čuvaju u dve odvojene i fizički obezbeđene prostorije na različitim lokacijama.

5.1.7 UKLANJANJE OTPADAKA

Sertifikaciono telo HALCOM BG CA obezbeđuje sigurno uklanjanje i uništavanje dokumenata u fizičkom/papirnom i elektronskom obliku.

Detaljne odredbe o uništavanju podataka definišu se u internim pravilima rada sertifikacionog tela HALCOM BG CA

Uklanjanje otpadaka izvodi specijalna komisija u skladu sa internim pravilima sertifikacionog tela HALCOM BG CA.

Svi detalji se nalaze u internim pravilima rada sertifikacionog tela HALCOM BG CA.

5.1.8 ČUVANJE PODATAKA NA UDALJENOJ LOKACIJI

Pogledati poglavlje 5.1.6.

5.2. ORGANIZACIONA STRUKTURA SERTIFIKACIONOG TELA

5.2.1 ORGANIZACIONE GRUPE

Operativni, organizacioni i stručni rad sertifikacionog tela HALCOM BG CA sprovodi rukovodilac interne organizacione jedinice koja je odgovorna za upravljanje kvalifikovanim elektronskim sertifikatima.

Ovlašćenim licima sertifikacionog tela HALCOM BG CA smatraju se:

- zaposleni u sertifikacionom telu HALCOM BG CA i

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

- zaposleni u registracionim telima.

Zaposleni u sertifikacionom telu HALCOM BG CA su raspoređeni u tri organizacione jedinice koje pokrivaju područja sledećeg sadržaja:

- upravljanje informacionim sistemom,
- upravljanje kvalifikovanim elektronskim sertifikatima,
- obezbeđenje i kontrola,

Organizaciona jedinica	Uloga	Osnovni zadaci	Broj osoba
Obezbeđenje i kontrola	Glavni administrator bezbednosti	Administriranje i implementacija procedura za rad sertifikacionog tela HALCOM BG CA	2
Upravljanje kvalifikovanim elektronskim sertifikatima	Sistem administrator		
	Prvi inženjeri bezbednosti	1. Upravljanje postupcima za izdavanje sertifikata 2. Štampanje PIN/PUK kodova 3. Pristup protokolu kvalifikovanog elektronskog potpisivanja (generisanja) sertifikata	2
	Drugi inženjer bezbednosti	1. Priprema kvalifikovanih elektronskih sertifikata 2. Personalizacija smart kartica 3. Opoziv kvalifikovanih elektronskih sertifikata	2
	Administratori sertifikata	distribucija sertifikata	1
	Administratori PIN/PUK kodova	distribucija PIN/PUK kodova	1
Upravljanje informacionim sistemom	Sistem operator	Upravljanje telekomunikacijama i odgovornost za rad bezbednih sistema sertifikacionog tela	2
Evidencija	Sistem evidentičar	Odgovornost za održavanje arhiva i log fajlova	2

5.2.2 BROJ OSOBA ZA POJEDINAČNE ZADATKE

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 administrator bezbednosti

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

Broj osoba: 2

Zadaci:

Odgovornost za administriranje i implementaciju bezbednosnih funkcija i procedura

Upravljanje aktivnostima na dodatnom unapređenju poslova generisanja, opoziva i suspenzije kvalifikovanih elektronskih sertifikata

Organizaciona jedinica: Upravljanje kvalifikovanim elektronskim sertifikatima

Uloga: prvi inženjer bezbednosti

Broj osoba: 2

Zadaci:

Upravljanje postupcima za izdavanje sertifikata

Štampanje PIN/PUK kodova

Pristup protokolu kvalifikovanog elektronskog potpisivanja (generisanja) CA sertifikata

Organizaciona jedinica: Upravljanje kvalifikovanim elektronskim sertifikatima

Uloga: drugi inženjer bezbednosti

Broj osoba: 2

Zadaci:

Pred-personalizacija smart kartica (generisanje ključeva i PIN/PUK koda)

Priprema kvalifikovanih elektronskih sertifikata (obrada potpisanih zahteva za sertifikate)

Personalizacija smart kartica (izrada kvalifikovanih elektronskih sertifikata, programiranje smart kartica upis generisanog sertifikata na smart karticu), štampanje podataka vlasnika na smart karticu - vizuelna personalizacija)

Opoziv kvalifikovanih elektronskih sertifikata

Organizaciona jedinica: Upravljanje kvalifikovanim elektronskim sertifikatima

Uloga: administrator sertifikata

Broj osoba: 1

Zadaci:

Bezbedna distribucija sertifikata vlasnicima

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

Organizaciona jedinica: Upravljanje kvalifikovanim elektronskim sertifikatima

Uloga: administrator PIN kodova

Broj osoba: 1

Zadaci:

Distribucija PIN/PUK kodova

Organizaciona jedinica: Upravljanje informacionom sistemom

Uloga: sistem operator

Broj osoba: 2

Zadaci:

Priprema početne konfiguracije sistema, uključujući bezbedno startovanje i obustavu operativnog rada sistema

Početno podešavanje parametara novih podređenih sertifikacionih tela u infrastrukturi HALCOM BG CA

Postavljanje početne konfiguracije računarske mreže

Priprema medijuma za krizni ponovni start sistema u slučaju katastrofalnog gubitka sistema, tj. incidenta sa katastrofalnim posledicama

Priprema sistemskih kopija, nadgradnja i obnova programske opreme, bezbedno čuvanje i distribucija kopija i nadgradnji na odvojenu lokaciju

Administrativne funkcije koje su vezane na održavanje baze podataka sertifikacionog tela i koje pomažu kod istraživanja eventualnog odstupanja od pravila

Promene imena servera i/ili mrežnih IP adrese

Sprovođenje arhiviranja zahtevanih sistemskih zapisa

Organizaciona jedinica: Evidencija

Uloga: sistem evidentičar

Broj osoba: 2

Zadaci:

Održavanje arhiva i log fajlova bezbednih sistema sertifikacionog tela

Naveden je minimalan broj zaposlenih za pojedinačne uloge.

5.2.3 DOKAZIVANJE IDENTITETA / AUTORIZACIJA ZA IZVRŠAVANJE POJEDINAČNIH ZADATAKA

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 internom pravilima sertifikacionog tela HALCOM BG CA.

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

5.2.4 NEKOMPATIBILNOST ZADATAKA

U internim pravilima rada sertifikacionog tela HALCOM BG CA, svakoj od prethodno navedenih uloga je vrlo 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. NADZOR

U okviru sertifikacionog tela HALCOM BG CA postoji i organizaciona jedinica za nadzor i usklađenost koju čine stručnjaci odgovarajućih tehnoloških i pravnih znanja koji ne vrše zadatke vezane za upravljanje kvalifikovanim elektronskim sertifikatima.

Navedena organizaciona jedinica nadzire rad sertifikacionog tela HALCOM BG CA. Ta organizaciona jedinica u slučaju otkrivenih nedostataka definiše odgovarajuće mere za uklanjanje tih nedostataka koje je sertifikaciono telo HALCOM BG CA dužno da sprovede i nadzire izvršavanje određenih mera.

5.3.1 POTREBNE KVALIFIKACIJE I ISKUSTVA ZAPOSLENIH

Sertifikaciono telo HALCOM BG CA zapošljava pouzdane i stručno osposobljene zaposlene koji provereno nisu kažnjavani za bilo kakvo kriminalno delo. Svi zaposleni se redovno usavršavaju i stiču dodatna znanja vezana za svoje stručno područje.

5.3.2 POGODNOST KVALIFIKACIJA ZAPOSLENIH

Zaposleni u sertifikacionom telu HALCOM BG CA imaju odgovarajuće kvalifikacije i iskustva u skladu sa zakonskim odredbama.

5.3.3 DODATNO USAVRŠAVANJE ZAPOSLENIH

Osobama koje izvršavaju zadatke gore navedenih organizacionih jedinica, kao i zadatke u domenu registracionog tela, omogućeno je svo neophodno usavršavanje.

5.3.4 ZAHTEVI ZA REDOVNA USAVRŠAVANJA

Zaposleni se usavršavaju u skladu sa potrebama odnosno novostima vezanim za operativni rad infrastrukture sertifikacionog tela HALCOM BG CA.

5.3.5 IZMENA ZADATAKA

Nije propisano.

5.3.6 SANKCIJE

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

5.3.7 ZAHTEVI ZA SPOLJNE SARADNIKE

Za moguće spoljne saradnike važe isti zahtevi kao i za ovlašćena lica sertifikacionog tela HALCOM BG CA.

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

5.3.8 PRISTUP ZAPOSLENIH DO DOKUMENTACIJE

Ovlašćenim licima sertifikacionog tela je na raspolaganju sva potrebna dokumentacija u skladu sa njihovim odgovornostima, zaduženjima i zadacima.

5.4. BEZBEDNOSNI PREGLEDI SISTEMA

5.4.1 VRSTE DNEVNIKA

Sertifikaciono telo HALCOM BG CA redovno proverava i evidentira sve što značajno utiče na:

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

Detaljni podaci o tome su dati u internim pravilima rada sertifikacionog tela HALCOM BG CA.

5.4.2 UČESTANOST PREGLEDA DNEVNIKA

Sertifikaciono telo HALCOM BG CA sprovodi sigurnosne preglede svoje infrastrukture, odnosno dnevnika, jednom dnevno.

5.4.3 VREME ČUVANJA DNEVNIKA

Dnevnici se čuvaju trajno u arhivi sertifikacionog tela.

5.4.4 ZAŠTITA DNEVNIKA

Dnevnici su osigurani u skladu sa sigurnosnim mehanizmima koji garantuju najviši nivo sigurnosti.

Detalji su dati u internim pravilima rada sertifikacionog tela HALCOM BG CA.

5.4.5 SIGURNOSNE KOPIJE DNEVNIKA

Sigurnosne kopije dnevnika se izrađuju na dnevnoj bazi.

Detalji su dati u internim pravilima rada sertifikacionog tela HALCOM BG CA.

5.4.6 SAKUPLJANJE PODATAKA ZA DNEVNIKE

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

Detalji su dati u internim pravilima rada sertifikacionog tela HALCOM BG CA.

5.4.7 OBAVEŠTAVANJE LICA KOJA SU PROUZROKOVALA ODGOVARAJUĆI BEZBEDNOSNI DOGAĐAJ

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

Lica koja su prouzrokovala odgovarajući događaje se ne obaveštavaju o sakupljanju podataka za dnevnike.

5.4.8 OCENA RANJIVOSTI SISTEMA

Analiza dnevnika i nadzor nad sprovođenjem svih postupaka redovno se sprovode od strane ovlašćenih lica sertifikacionog tela ili automatski odgovarajućim sigurnosnim mehanizmima na svoj računarsko-komunikacionoj opremi koja je u nadležnosti sertifikacionog tela.

Ocena ranjivosti se sprovodi na osnovu analize dnevnika.

Detalji su dati u internim pravilima rada sertifikacionog tela HALCOM BG CA.

5.5. DUGOTRAJNO ČUVANJE PODATAKA

5.5.1 VRSTE DUGOROČNO ČUVANIH PODATAKA

Sertifikaciono telo 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 dobijanjem sertifikata,
- kvalifikovane elektronske sertifikate i registre opozvanih sertifikata,
- politike sertifikacije i druge dokumente sertifikacionog tela (opšta i interna pravila rada),
- objave i obaveštenja sertifikacionog tela HALCOM BG CA i
- druge dokumente u skladu sa valjanim propisima.

5.5.2 ROK ČUVANJA

Podaci se čuvaju u skladu sa zakonskim odredbama.

5.5.3 ZAŠTITA DUGOTRAJNO ČUVANIH PODATAKA

Podaci se čuvaju u skladu sa zakonskim odredbama.

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

5.5.4 BEZBEDNE KOPIJE DUGOTRAJNO ČUVANIH PODATAKA

Kopija dugotrajno čuvanih podataka, bezbedno je sačuvana.

Detaljne odredbe dugotrajnog čuvanja kopija podataka se definišu u internim pravilima rada sertifikacionog tela HALCOM BG CA a u skladu sa važećim propisima, standardima i preporukama.

5.5.5 ZAHTEVI ZA VREMENSKI PEČAT

Nisu propisani.

5.5.6 NAČIN SAKUPLJANJA PODATAKA

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

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

5.5.7 POSTUPAK PRISTUPA DUGOTRAJNO ČUVANIM PODACIMA I NJIHOVA VERIFIKACIJA

Pristup dugotrajno čuvanim podacima omogućen je samo ovlašćenim licima.

Detaljne odredbe u vezi pristupa dugotrajno čuvanim podacima se definišu u internim pravilima rada sertifikacionog tela HALCOM BG CA a u skladu sa važećim propisima, standardima i preporukama.

5.6. PROMENA JAVNOG KLJUČA SERTIFIKACIONOG TELA HALCOM BG CA

U slučaju novo izdatog sopstvenog kvalifikovanog elektronskog sertifikata sertifikacionog tela HALCOM BG CA isti se odmah objavljuje na web stranicama sertifikacionog tela HALCOM BG CA.

5.7. PLAN ZA OPORAVAK POSLOVANJA

5.7.1 POSTUPAK U SLUČAJU UPADA I ZLOUPOTREBE

Detaljne odredbe se definišu u internim pravilima rada sertifikacionog tela HALCOM BG CA a u skladu sa važećim propisima, standardima i preporukama.

5.7.2 POSTUPAK U SLUČAJU KVARA PROGRAMSKE OPREME, PODATAKA

Detaljne odredbe se definišu u internim pravilima rada sertifikacionog tela HALCOM BG CA a u skladu sa važećim propisima, standardima i preporukama.

5.7.3 POSTUPAK U SLUČAJU UGROŽENOG PRIVATNOG KLJUČA SERTIFIKACIONOG TELA HALCOM BG CA

Detaljne odredbe se definišu u internim pravilima rada sertifikacionog tela HALCOM BG CA a u skladu sa važećim propisima, standardima i preporukama.

5.7.4 PLAN ZA OPORAVAK POSLOVANJA

Detaljne odredbe se definišu u internim pravilima rada sertifikacionog tela HALCOM BG CA a u skladu sa važećim propisima, standardima i preporukama.

ISO 9001 BUREAU VERITAS Certification
Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

5.8. PRESTANAK OPERATIVNOG RADA HALCOM BG CA

Detaljne odredbe se definišu u internim pravilima rada sertifikacionog tela HALCOM BG CA a u skladu sa važećim propisima, standardima i preporukama.

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

6. TEHNIČKI BEZBEDNOSNI ZAHTEVI

6.1. GENERISANJE I ZAŠTITA KLJUČEVA

6.1.1 GENERISANJE KLJUČEVA

Asimetrični par ključeva sertifikacionog tela HALCOM BG CA za elektronsko potpisivanje sertifikata i verifikaciju potpisa se generiše tokom uspostave sertifikacionog tela HALCOM BG CA (CA ceremonija).

Za korisnike, vlasnike sertifikata, sertifikaciono telo HALCOM BG CA generiše dva asimetrična para ključeva i dva sertifikata:

- privatni ključ za potpisivanje (za potrebe kvalifikovanog elektronskog potpisivanja),
- privatni ključ za dešifriranje (za potrebe dešifriranja),
- javni ključ za verifikaciju potpisa (za verifikaciju kvalifikovanog elektronskog potpisa) i
- javni ključ za šifriranje (za potrebe šifriranje).

Oba para ključeva za vlasnika sertifikata se generišu na smart kartici u okviru sertifikacionog tela HALCOM BG CA gde se vrši i kompletna personalizacija smart kartice i štampanje PIN/PUK koda.

Halcom BG CA sertifikati su u osnovi namenjeni elektronskom potpisivanju jednostranih ili međusobnih komunikacija vlasnika sertifikata te korišćenju u različitim aplikacijama. Pored toga sertifikati se mogu upotrebiti i za različite namene koje se pojave na tržištu, između ostalog i za šifrovanje.

Halcom BG CA zbog bezbednosnih razloga upotrebljava „on-board" sistem za generisanje ključeva. To podrazumeva da se asimetrični parovi ključeva (privatni i javni) za vlasnike sertifikata generišu u smart kartici i samo se čuvaju u smart kartici i ne mogu se pročitati sa nje. Zbog svega gore navedenog otkrivanje kopije ključeva za dešifrovanje (engl. Key pair recovery) u Halcom BG CA sertifikacionom telu nije podržano.

Sertifikaciono telo dostavlja korisniku (vlasniku sertifikata) kompletno isprogramiranu smart karticu (sa dva para ključeva i dva sertifikata) kao i odštampan PIN/PUK kod.

6.1.2 DOSTAVA PRIVATNOG KLJUČA VLASNICIMA

Sertifikaciono telo dostavlja korisniku (vlasniku sertifikata) kompletno isprogramiranu smart karticu (sa dva para ključeva (privatni i javni ključ) i dva sertifikata) kao i odštampan PIN/PUK kod.

6.1.3 DOSTAVA JAVNOG KLJUČA KORISNIKA SERTIFIKACIONOM TELU

Nije primenljivo. Asimetrični parovi ključeva (privatni i javni ključ) za korisnike – vlasnike sertifikata sa generišu u okviru sertifikacionog tela.

6.1.4 DOSTAVA JAVNOG KLJUČA SERTIFIKACIONOG TELA KORISNICIMA I TREĆIM LICIMA

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

Kvalifikovani elektronski sertifikat sa javnim ključem sertifikacionog tela HALCOM BG CA je vlasnicima sertifikata, odnosno trećim licima, dostupan:

- putem web stranice sertifikacionog tela http://www.halcom.rs/UserFiles/File/HalcomBGCAPLIntermediate.crt

6.1.5 DUŽINA ASIMETRIČNIH KLJUČEVA

Sertifikat	Dužina ključa prema RSA [bit]
Sertifikat sertifikacionog tela HALCOM BG CA (root i intermediate)	2048
Sertifikati za korisnike	1024

6.1.6 GENERISANJE I KVALITET PARAMETARA ASIMETRIČNIH PAROVA KLJUČEVA

Kvalitet parametara asimetričnog para ključa sertifikacionog tela HALCOM BG CA garantovana je od strane proizvođača programske opreme, HSM (Hardware Security Module), koja koristi kvalitetne i sertifikovane hardverske generatore slučajnih brojeva (engl. *random number generator*).

6.1.7 UPOTREBA KLJUČEVA I SERTIFIKATA

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

Elektronsko potpisivanje sertifikata i registra opozvanih sertifikata se vrši privatnim ključem sertifikacionog tela HALCOM BG CA, dok se za verifikaciju pomenutih potpisa koristi javni ključ iz kvalifikovanog elektronskog sertifikata sertifikacionog tela. U tom smislu, *keyUsage* ekstenzija u sertifikatu sertifikacionog tela sadrži odgovarajuće vrednosti.

Profili kvalifikovanih elektronskih sertifikata koje izdaje sertifikaciono telo HALCOM BG CA su navedeni u poglavlju 7.1.

6.2. ZAŠTITA PRIVATNIH KLJUČEVA

6.2.1 STANDARDI ZA KRIPTOGRAFSKI MODUL

Privatni ključ sertifikacionog tela HALCOM BG CA zaštićen je kriptografskim modulom koji je sertifikovan u skladu sa standardima FIPS 140-2 nivo 3 i Common Criteria EAL4+.

6.2.2 NADZOR PRISTUPA PRIVATNOM KLJUČU OD STRANE OVLAŠĆENIH LICA SERTIFIKACIONOG TELA

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

Odredbe vezane za aktivaciju privatnog ključa sertifikacionog tela HALCOM BG CA definisane su u internim pravilima rada sertifikacionog tela HALCOM BG CA.

6.2.3 OTKRIVANJE KOPIJE PRIVATNOG KLJUČA

Nije primenljivo.

6.2.4 BEZBEDNA KOPIJA PRIVATNOG KLJUČA

Odredbe vezane za bezbedno kopiranje privatnog ključa sertifikacionog tela HALCOM BG CA definisane su u internim pravilima rada sertifikacionog tela HALCOM BG CA.

6.2.5 ARHIVIRANJE PRIVATNOG KLJUČA

Privatni ključ mogu kopirati i čuvati samo ovlašćena lica sertifikacionog tela. Sigurnosne kopije privatnog ključa se čuvaju na istom nivou bezbednosti kao i ključevi u upotrebi.

Detaljnije odredbe vezane za arhiviranje privatnog ključa sertifikacionog tela HALCOM BG CA definisane su u internim pravilima rada sertifikacionog tela HALCOM BG CA.

6.2.6 PRENOS PRIVATNOG KLJUČA IZ/U KRIPTOGRAFSKI MODUL

Asimetrični par ključeva (privatni i javni) sertifikacionog tela se generiše u HSM uređaju. Detaljnije odredbe vezane za prenos privatnog ključa sertifikacionog tela HALCOM BG CA definisane su u internim pravilima rada sertifikacionog tela HALCOM BG CA.

Asimetrični parovi ključeva (privatni i javni) za vlasnike sertifikata se generišu u smart kartici i ne mogu se pročitati sa kartice.

6.2.7 ČUVANJE PRIVATNOG KLJUČA U KRIPTOGRAFSKOM MODULU

Asimetrični par ključeva (privatni i javni) sertifikacionog tela se generiše i čuva u HSM uređaju.

Asimetrični parovi ključeva (privatni i javni) za vlasnike sertifikata se generišu u smart kartici i samo se čuvaju u smart kartici i ne mogu se pročitati sa nje.

6.2.8 POSTUPAK ZA AKTIVIRANJE PRIVATNOG KLJUČA

Postupak aktivacije privatnog ključa sertifikacionog tela i procedura distribuirane odgovornosti u vezi tog postupka su definisane u internim pravilima rada sertifikacionog tela.

6.2.9 POSTUPAK ZA DEAKTIVIRANJE PRIVATNOG KLJUČA

Postupak za deaktivaciju/uništavanje privatnog ključa sertifikacionog tela HALCOM BG CA vrši se bezbednim načinom u skladu sa odredbama internih pravila rada sertifikacionog tela HALCOM BG CA. Privatni ključ se uništava na takav način da ga nije moguće ponovo koristiti.

6.2.10 POSTUPAK ZA UNIŠTENJE PRIVATNOG KLJUČA

Postupak za uništenje privatnog ključa sertifikacionog tela se bazira na odgovarajućim funkcijama koje su podržane u HSM uređaju koji zadovoljava standarde navedene u poglavlju 6.2.1.

6.2.11 KARAKTERISTIKE KRIPTOGRAFSKOG MODULA

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

HSM uređaj koji se koristi od strane sertifikacionog tela HALCOM BG CA zadovoljava standarde navedene u poglavlju 6.2.1.

6.3. OSTALI ASPEKTI UPRAVLJANJA KLJUČEVIMA

6.3.1 ARHIVIRANJE JAVNOG KLJUČA

Sertifikaciono telo HALCOM BG CA arhivira svoj javni ključ, kao i javne ključeve vlasnika sertifikata, kao što je navedeno u poglavlju 5.5.

6.3.2 VREME VAŽENJA JAVNIH I PRIVATNIH KLJUČEVA

U dole navedenoj tabeli su data vremena važenja privatnih i javnih ključeva sertifikacionog tela HALCOM BG CA i ovlašćenih korisnika pravnih lica – vlasnika sertifikata.

Tip sertifikata	Ključ	Važenje
Root sertifikat sertifikacionog tela Halcom BG CA	Privatni ključ	20 godina
	Javni ključ	20 godina
Intermediate sertifikat sertifikacionog tela Halcom BG CA PL	Privatni ključ	10 godina
	Javni ključ	10 godina
Sertifikati za korisnike	Privatni ključ	3 godine
	Javni ključ	3 godine

Sertifikaciono telo HALCOM BG CA može u iznimnim slučajevima za pojedinačne sertifikate odrediti i kraći rok važenja sertifikata (tj. javnog ključa u sertifikatu).

6.4. LOZINKE ZA PRISTUP PRIVATNIM KLJUČEVIMA

6.4.1 GENERISANJE LOZINKE

Za potrebe pristupa privatnim ključevima vlasnika sertifikata koriste se PIN/PUK kodovi za pristup karticama koji se generišu u sertifikacionom telu HALCOM BG CA.

PIN/PUK kod za smart karticu generiše se i štampa na specijalnim PIN/PUK kovertama u okviru sertifikacionog tela HALCOM BG CA.

Vlasnik može da promeni PIN kod nakon preuzimanja.

6.4.2 ZAŠTITA LOZINKE

PIN/PUK kodovi za smart karticu korisnika se bezbedno generišu u okviru sertifikacionog tela HALCOM BG CA.

Sertifikaciono telo HALCOM BG CA isporučuje vlasniku sertifikata PIN/PUK kod lično u okviru registracionog tela.

Sertifikaciono telo HALCOM BG CA preporučuje vlasniku da promeni PIN kod nakon preuzimanja ili ga čuva na sigurnom mestu koje je dostupno samo njemu.

6.4.3 DRUGI ASPEKTI KORIŠĆENJA LOZINKE

Nisu propisani.

6.5. SIGURNOSNI ZAHTEVI ZA RAČUNARSKU OPREMU SERTIFIKACIONOG TELA

6.5.1 SPECIFIČNI TEHNIČKI SIGURNOSNI ZAHTEVI

Detalji su dati u internim pravilima rada sertifikacionog tela HALCOM BG CA.

6.5.2 NIVOI SIGURNOSNE ZAŠTITE

Detalji su dati u internim pravilima rada sertifikacionog tela HALCOM BG CA.

6.6. TEHNIČKI NADZOR ŽIVOTNOG CIKLUSA SERTIFIKACIONOG TELA

6.6.1 NADZOR RAZVOJA SISTEMA

Sertifikaciono telo HALCOM BG CA upotrebljava programsku opremu proizvođača Nexus (Švedska) i kriptografski modul, koji je sertifikovan u skladu sa FIPS 140-2 nivo 3 i Common Criteria EAL4+.

6.6.2 UPRAVLJANJE SIGURNOŠĆU

Detalji su dati u internim pravilima rada sertifikacionog tela HALCOM BG CA.

6.6.3 NADZOR ŽIVOTNOG CIKLUSA SERTIFIKACIONOG TELA

Detalji su dati u internim pravilima rada sertifikacionog tela HALCOM BG CA.

6.7. SIGURNOSNA KONTROLA RAČUNARSKE MREŽE

Detalji su dati u internim pravilima rada sertifikacionog tela HALCOM BG CA.

6.8. VREMENSKI PEČAT

Nije propisano.

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

7. PROFIL SERTIFIKATA I REGISTRA OPOZVANIH SERTIFIKATA

7.1. PROFIL SERTIFIKATA

Na osnovu ove politike sertifikacije, sertifikaciono telo HALCOM BG CA izdaje sertifikate za pravna lica (pogledati poglavlje 6.1.1).

Kvalifikovani elektronski sertifikati koje izdaje sertifikaciono telo HALCOM BG CA zadovoljavaju standard *X.509 v3.*

7.1.1 VERZIJE SERTIFIKATA

Svi kvalifikovani elektronski sertifikati koje izdaje sertifikaciono telo HALCOM BG CA zadovoljavaju standard *X.509*, i to verziju 3.

7.1.2 PROFIL SERTIFIKATA SA KORIŠĆENIM EKSTENZIJAMA

Profil root sertifikata – Halcom BG CA

Nazivi polja	**Vrednost odnosno značenje**
Osnovna polja u sertifikatima	
Varijanta engl. *Version*	V3
Identifikaciona oznaka sertifikata engl. *Serial Number*	Jedinstven interni broj sertifikata
Algoritam za potpis, engl. *Signature algorithm*	sha1RSA (OID1.2.840.113549.1.15)
Izdavač engl. *Issuer*	C=RS, O=Halcom a.d. Beograd, CN=Halcom BG CA
Valjanost, engl. *Validity*	Valid from: <početak valjanosti prema GMT> Valid to: <kraj valjanosti prema GMT>
Vlasnik, engl. Subject	CN = Halcom BG CA 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)*	modulus, eksponent,...
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 47 d1 d3 ab c5 a4 28 04
Osnovna ograničenja, OID 2.5.29.19, engl. *Basic Constraints*	Subject Type=CA Path Length Constraint=None
Dodatna identifikacija (nije deo elektronskih sertifikata)	
Prepoznavan otisak sertifikata -SHA1 engl. *Certificate Fingerprint – SHA1*	Prepoznavan otisak sertifilkata prema SHA1

Profil intermediate sertifikata – Halcom BG CA PL

Nazivi polja	**Vrednost odnosno značenje**
Osnovna polja u sertifikatima	
Varijanta engl. *Version*	V3
Identifikaciona oznaka sertifikata engl. *Serial Number*	Jedinstven interni broj sertifikata
Algoritam za potpis, engl. *Signature algorithm*	sha1RSA (OID1.2.840.113549.1.15)
Izdavač engl. *Issuer*	C=RS, O=Halcom a.d. Beograd, CN=Halcom BG CA
Valjanost, engl. *Validity*	Valid from: <početak valjanosti prema GMT> Valid to: <kraj valjanosti prema GMT>
Vlasnik, engl. *Subject*	C=RS, O=Halcom a.d. Beograd, CN=Halcom BG CA PL
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 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 izdavača, OID 2.5.29.35, engl. Auth*ority Key Identifier*	KeyID=47 d1 d3 ab c5 a4 28 04
Identifikator ključa vlasnika, OID 2.5.*29.14,* *engl. Subject Key Identifier*	identifikator ključa vlasnika 47 dd ba a4 63 34 d3 24
Osnovna ograničenja, OID 2.5.29.19, engl. *Basic Constraints*	Subject Type=CA Path Length Constraint=None
Dodatna identifikacija (nije deo elektronskih sertifikata)	
Prepoznavan otisak sertifikata -SHA1 engl. *Certificate Fingerprint – SHA1*	Prepoznavan otisak sertifilkata prema SHA1

Podaci u sertifikatima za pravna lica su navedeni su sledećoj tabeli.

Nazivi polja	**Vrednost odnosno značenje**
Osnovna polja u sertifikatima	
Varijanta engl. *Version*	V3
Identifikaciona oznaka sertifikata engl. *Serial Number*	Jedinstven interni broj sertifikata
Algoritam za potpis, engl. *Signature algorithm*	sha1RSA (OID1.2.840.113549.1.15)
Izdavač engl. *Issuer*	C=RS, O=Halcom a.d. Beograd, CN=Halcom BG CA PL
Valjanost, engl. *Validity*	Valid from: <početak valjanosti prema GMT> Valid to: <kraj valjanosti prema GMT>

Vlasnik, engl. *Subject*	karakteristično ime vlasnika, 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 1024 bitova, pogledaj alineju 6.1.5.
Ekstenzije u okviru X.509v3 standarda	
Objava registra opozvanih sertifikata, OID 2.5.29.31, engl. *CRL Distribution Points*	URL=ldap://ldap.halcom.rs/cn=Halcom%20BG%20CA%20PL,o=Halcom%20a.d.%20Beograd,c=RS?certificaterevocationlist;binary
korišćenje ključa, OID 2.5.29.15, *engl. Key Usage*	Digital Signature, Non-Repudiation, Key Encipherment
Identifikator ključa sertifikacionog tela OID 2.5.29.35, engl. Auth*ority Key Identifier*	KeyID=47 dd ba a4 63 34 d3 24
Identifikator ključa vlasnika, OID 2.5.*29.14,* *engl. Subject Key Identifier*	identifikator ključa vlasnika
Politika, u nadležnosti koje je sertifikat izdat, OID 2.5.29.32, engl. certificatePolicies	Certificate Policy: Policy Identifier=1.3.6.1.4.1.5939.10.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.halcom.rs/UserFiles/File/CPS.pdf
Oznaka kvalifikovanog kvalifikovanih elektronskih sertifikata na SSCD engl. QC SSCD Statement	30 14 30 08 06 06 04 00 0.0..... 8e 46 01 01 30 08 06 06 .F..0... 04 00 8e 46 01 04 ...F.

Objava ključa izdavača OID 1.3.6.1.5.5.7.48.2 engl. Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.halcom.rs/UserFiles/File/HalcomBGCAPLIntermediate.crt
Osnovna ograničenja, OID 2.5.29.19, engl. *Basic Constraints*	Subject Type=End Entity Path Length Constraint=None
Dodatna identifikacija (nije deo kvalifikovanog elektronskog sertifikata)	
Prepoznatljiv otisak sertifikata-SHA1 engl. *Certificate Fingerprint – SHA1*	Prepoznatljiv otisak sertifikata prema SHA1

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

7.1.3 IDENTIFIKACIONE OZNAKE KRIPTOGRAFSKIH ALGORITAMA

Kvalifikovani elektronski sertifikati koje izdaje sertifikaciono telo HALCOM BG CA potpisani su primenom kriptografskog algoritma, određenim u polju *signature algorithm*: vrednost sha1RSA, identifikator objekta: OID 1.2.840.113549.1.1.5.

7.1.4 OBLIK KARAKTERISTIČNIH IMENA KORISNIKA

Pogledati poglavlje 3.1.1.

7.1.5 OGRANIČENJA VEZANA ZA IMENA

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

7.1.6 OZNAKA POLITIKE SERTIFIKACIJE

Pogledati poglavlje 7.1.2.

7.1.7 OGRANIČENJA KORIŠĆENJA

Ograničenja korišćenja (polje u sertifikatu engl. *usage policy constraints extension*) nisu propisana.

7.1.8 SINTAKSA I ZNAČENJE OZNAKA POLITIKE SERTIFIKATA

Pogledati poglavlje 7.1.2.

7.1.9 ZNAČENJE BITNIH DODATAKA POLITIKE

Nije podržano.

7.2. PROFIL REGISTRA OPOZVANIH SERTIFIKATA

Registar opozvanih sertifikata (CRL) izdaje sertifikaciono telo HALCOM BG CA sa karakterističnim imenom:

CN= HALCOM BG CA PL

O = Halcom a.d. Beograd

C = RS

Registar opozvanih sertifikata se obnavlja jedanput dnevno 24 sata nakon poslednje obnove CRL.

Registar opozvanih sertifikata sadrži jednoznačni interni serijski broj opozvanog sertifikata, kao i vreme i datum opoziva.

7.2.1 VERZIJA

Registar opozvanih sertifikata odgovara preporuci ITU-T X.509 (1997) uključujući i verziju 2 i ISO/IEC 9594-8:1997.

Registar opozvanih sertifikata je dostupan u javnom spisku sertifikata (pogledaj poglavlje 2.3) putem:

- LDAP protokola i
- HTTP protokola.

7.2.2 SADRŽAJ CRL I PRIDRUŽENE EKSTENZIJE

Registar opozvanih sertifikata uz ostale podatke, u skladu sa preporukom *X.509v2* sadrži (osnovna polja i ekstenzije detaljnije su prikazani u donjoj tabeli):

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

Naziv polja	**Vrednost odnosno značenje**
Osnovna polja u CRL	
Verzija, engl. *Version*	V2
Algoritam za kvalifikovani elektronski potpis CRL, engl. *Signature Algorithm*	sha1RSA
Potpis sertifikacionog tela, engl. Signature	potpis HALCOM BG CA PL

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

Karakteristično ime sertifikacionog tela engl. *Issuer*	C=RS, O=Halcom a.d. Beograd, CN=Halcom BG CA PL
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 sertifikata i vreme opoziva, engl. *revokedCertificate*	Serial Number: *<identifikaciona oznaka (serijski broj) opozvanog kvalifikovanog elektronskog sertifikata>* Revocation Date: *<vreme opoziva prema GMT>*
Ekstenzije X.509v2 CRL	
redni broj CRL engl. *CRL number*	Redni broj izdatog registra opozvanih sertifikata
identifikator ključa sertifikacionog tela, engl. *Authority Key Identifier (OID 2.5.29.35)*	KeyID= 47 dd ba a4 63 34 d3 24

Opozvani kvalifikovani elektronski sertifikati kojima je istekla validnost, ostaju izlistani u CRL, tj. ne brišu se iz CRL nakon isteka važnosti.

7.2.3 OBJAVLJIVANJE REGISTRA OPOZVANIH SERTIFIKATA

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

7.3. PROFIL OCSP

Protokol za on-line proveru statusa sertifikata - OCSP (engl. *Online Certificate Status Protocol*) nije podržan.

7.3.1 VERZIJA OCSP PROTOKOLA

Protokol OCSP nije podržan.

7.3.2 PROFIL OCSP PROTOKOLA

Protokol OCSP nije podržan.

8. NADZOR

U okviru sertifikacionog tela HALCOM BG CA postoji organizaciona jedinica za nadzor i usklađenost koju čine stručnjaci sa odgovarajućim tehnološkim i pravnim znanjima, a koji ne vrše zadatke vezane za upravljanje sertifikatima.

Pomenuta organizaciona jedinica nadzire rad sertifikacionog tela HALCOM BG CA. Organizaciona jedinica u slučaju otkrivenih nedostataka definiše odgovarajuće mere za uklanjanje tih nedostataka, koje je sertifikaciono telo HALCOM BG CA dužno da sprovede, i nadzire sprovođenje definisanih mera.

8.1. UČESTANOST NADZORA

Organizaciona jedinica za nadzor i usklađenost vrši nadzor rada sertifikacionog tela najmanje jedanput u godini.

8.2. VRSTA NADZORA I OSPOSOBLJENOST ZAPOSLENIH

Organizacionu jedinicu za nadzor i usklađenost čine stručnjaci sa odgovarajućim tehnološkim i pravnim znanjima.

8.3. NEZAVISNOST NADZORA

Organizacionu jedinicu za nadzor i usklađenost čine članovi koji ne vrše zadatke vezane za upravljanje kvalifikovanim elektronskim sertifikatima.

8.4. PODRUČJA NADZORA

Područja nadzora određena su u internim pravilima rada sertifikacionog tela HALCOM BG CA.

8.5. MERE KOJE PRIMENJUJE SERTIFIKACIONO TELO

U slučaju utvrđenja nedostataka ili grešaka u radu sertifikacionog tela, organizaciona jedinica definiše mere za uklanjanje tih nedostataka, koje je sertifikaciono telo HALCOM BG CA dužno da sprovede, i nadzire izvođenje definisanih mera.

Detalji oko sprovođenja navedenih mera se definišu u internim pravilima rada sertifikacionog tela HALCOM BG CA.

8.6. OBJAVLJIVANJE REZULTATA NADZORA

Rezultati sprovođenja nadzora se čuvaju u okviru sertifikacionog tela HALCOM BG CA.

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

9. FINANSIJSKE I OSTALE PRAVNE STVARI

9.1. CENOVNIK

Sertifikaciono telo HALCOM BG CA definiše cenovnik korišćenja sertifikata, svojih usluga, potrebne opreme i infrastrukture.

9.1.1 CENA IZDAVANJA I OBNAVLJANJA SERTIFIKATA

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

9.1.2 CENA PRISTUPA STATUSU SERTIFIKATA I REGISTRU OPOZVANIH SERTIFIKATA

Registar opozvanih sertifikata je besplatno dostupan svim korisnicima, bilo da su oni vlasnici sertifikata izdatih od strane sertifikacionog tela HALCOM BG CA ili treća lica.

9.1.3 CENE DRUGIH USLUGA SERTIFIKACIONOG TELA

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

9.1.4 POVRATAK TROŠKOVA

Nije primenljivo.

9.2. FINANSIJSKA ODGOVORNOST

9.2.1 OSIGURANJE

Sertifikaciono telo HALCOM BG CA poseduje odgovarajuće osiguranje za bilo koju štetu koju mogu da pretrpe treća lica a za koju je odgovorno sertifikaciono telo. Detaljne informacije objavljene su na web stranicama.

9.2.2 OSTALA POKRIĆA

Nije primenljivo.

9.2.3 OSIGURANJE VLASNIKA

Nije propisano.

9.3. ČUVANJE POSLOVNIH PODATAKA

9.3.1 POVERLJIVI PODACI KOJI SE ČUVAJU

Sertifikaciono telo HALCOM BG CA postupa poverljivo sa sledećim podacima:

- Sa svim zahtevima za dobijanje sertifikata ili drugih usluge
- 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 sertifikacionog tela HALCOM BG CA.

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

U toku obrade svih mogućih poverljivih podataka o vlasnicima sertifikata i trećim licima, koji su nužno potrebni za usluge upravljanja sertifikata, sertifikaciono telo HALCOM BG CA postupa u skladu sa važećim zakonodavstvom.

9.3.2 PODACI KOJI SE JAVNO OBJAVLJUJU

Sertifikaciono telo HALCOM BG CA javno objavljuje samo one poslovne podatke koji nisu poverljive prirode a u skladu sa važećim zakonodavstvom.

9.3.3 ODGOVORNOST U VEZI ČUVANJA PODATAKA

Sertifikaciono telo HALCOM BG CA ne preuzima nikakve odgovornosti za sadržaj podataka koje vlasnik sertifikata elektronski šifruje ili potpisuje. Takođe, sertifikaciono telo ne preuzima nikakve odgovornosti za pitanja da li je vlasnik ili treće lice poštovao sve važeće propise, sve odredbe politike sertifikacije i drugih pravila sertifikacionog tela HALCOM BG CA, odnosno vodio računa o svim objavljenim uputstvima.

Sertifikaciono telo HALCOM BG CA ne preuzima nikakve odgovornosti za posledice do kojih dolazi ukoliko vlasnik sertifikata nije postupao u skladu sa sigurnosnim zahtevima iz tačke 5.1 ove politike sertifikacije.

9.4. ČUVANJE LIČNIH PODATAKA

9.4.1 PLAN ČUVANJA I ZAŠTITE LIČNIH PODATAKA

Sa svim ličnim i poverljivim podacima o vlasnicima sertifikata koji su nužno potrebni za usluge upravljanja sertifikatima, sertifikaciono telo HALCOM BG CA postupa u skladu sa važećim zakonodavstvom.

9.4.2 LIČNI PODACI KOJI SE ČUVAJU/ŠTITE I NE OBJAVLJUJU

Lični podaci koji se čuvaju su svi lični podaci koje sertifikaciono telo HALCOM BG CA prikupi sa zahtevima za svoje usluge ili u odgovarajućim registrima za dokazivanje identiteta vlasnika.

9.4.3 LIČNI PODACI KOJI SE OBJAVLJUJU

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

9.4.4 ODGOVORNOST VEZANA ZA ČUVANJE/ZAŠTITU LIČNIH PODATAKA

Sertifikaciono telo HALCOM BG CA postupa u skladu sa Zakonom o zaštiti podataka o ličnosti i drugim važećim zakonodavstvom vezanim za čuvanje i zaštitu ličnih podataka.

9.4.5 OVLAŠĆENJE VEZANO ZA KORIŠĆENJE LIČNIH PODATAKA

Vlasnik ovlašćuje sertifikaciono telo HALCOM BG CA za korišćenje ličnih podataka na zahtevu za dobijanje sertifikata ili kasnije u pismenom obliku.

9.4.6 PROSLEĐIVANJE LIČNIH PODATAKA VLASNIKA SERTIFIKATA

Sertifikaciono telo HALCOM BG CA ne prosleđuje lične podatke o vlasnicima sertifikata trećim licima koja nisu navedena u sertifikatima, osim ako se određeni podaci posebno zahtevaju za izvođenje specifičnih usluga odnosno aplikacija vezanih za sertifikate a

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

vlasnik sertifikata je za te svrhe ovlastio sertifikaciono telo HALCOM BG CA (pogledati prethodno poglavlje), ili na zahtev nadležnog suda ili administrativnog organa.

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

9.4.7 DRUGE ODREDBE VEZANE ZA ČUVANJE LIČNIH PODATAKA

Nisu propisane.

9.5. ODREDBE VEZANE NA PRAVA INTELEKTUALNOG VLASNIŠTVA

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

- U vezi privatnog ključa - pripadaju sva prava vlasniku sertifikata,
- U vezi javnih ključeva – sva prava nad svim podacima u sertifikatu, javnom registru opozvanih sertifikata, kao i na ovoj politici sertifikacije pripadaju sertifikacionom telu HALCOM BG CA.

9.6. OBAVEZE I ODGOVORNOSTI

9.6.1 OBAVEZE I ODGOVORNOSTI SERTIFIKACIONOG TELA HALCOM BG CA

Sertifikaciono telo HALCOM BG CA dužno je:

- Vršiti usluge u skladu sa svojim internim pravilima i ostalim važećim propisima i zakonodavstvom,
- Vršiti usluge u skladu sa međunarodnim preporukama,
- Objavljivati sve važne dokumente koji definišu njegov operativni rad (politike sertifikacije, zahteve, cenovnik, uputstva za bezbedno korišćenje kvalifikovanih elektronskih sertifikata, i sl.),
- Objavljivati na svojim web stranicama sve informacije o onim promenama vezanim za delatnosti sertifikacionog tela koje na bilo koji način utiču na vlasnike sertifikata i treća lica,
- Omogućiti rad registracionih tela u skladu sa odredbama politike sertifikacije HALCOM BG CA i ostalim važećim propisima,
- Poštovati odredbe vezane za bezbedno postupanje sa ličnim, poslovnim i poverljivim podacima sertifikacionog tela, vlasnika sertifikata ili trećih lica,
- Opozvati kvalifikovani elektronski sertifikat i objaviti opozvani sertifikat u registru opozvanih sertifikata u slučaju uslova i razloga definisanih ovom politikom sertifikacije ili drugim važećim propisima,
- Izdavati kvalifikovane elektronske sertifikate u skladu sa ovom politikom sertifikacije i ostalim propisima i preporukama.

Sertifikaciono telo HALCOM BG CA dužno je:

- Osigurati tačnost podataka u izdatim sertifikatima,
- Osigurati pravilnost objavljivanja registra opozvanih sertifikata,
- Osigurati jednoznačnost karakterističnih imena,

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

- Osigurati odgovarajuću fizičku bezbednost prostorija i pristupa samim prostorijama sertifikacionog tela,
- Kao dobar privrednik brinuti se za neometano delovanje i što veću raspoloživost usluga,
- Kao dobar privrednik brinuti se za što veću dostupnost usluga,
- Kao dobar privrednik brinuti se za neometano delovanje svih ostalih pratećih usluga,
- Pokušati otkloniti eventualne nastale probleme što kvalitetnije i u najkraćem mogućem vremenu,
- Brinuti se za optimizaciju mašinske i programske opreme i
- Obaveštavati korisnike o važnim stvarima i ispunjavati sve druge zahteve u skladu sa ovom politikom sertifikacije.

Sertifikaciono telo HALCOM BG CA obezbeđuje što veći pristup svojim uslugama i to 24 sata na dan/7 dana u nedelji/365 dana u godini, izuzimajući:

- planirane i unapred predviđene tehničke ili servisne intervencije na infrastrukturi,
- neplanirane tehničke ili servisne intervencije na infrastrukturi kao posledica nepredviđenih/iznenadnih kvarova,
- tehničke ili servisne intervencije zbog kvarova infrastrukture van opsega odgovornosti sertifikacionog tela HALCOM BG CA i
- nedostupnost kao posledica više sile ili vanrednih događaja.

Radove održavanja ili nadgradnje infrastrukture sertifikaciono telo HALCOM BG CA mora najaviti korisnicima i trećim licima barem tri (3) dana pre početka radova.

Sertifikaciono telo HALCOM BG CA je odgovorno za sve navode u ovom dokumentu i za sprovođenje svih odredaba iz ove politike sertifikacije.

Ostale obaveze odnosno odgovornosti sertifikacionog tela HALCOM BG CA definisane su mogućim međusobnim dogovorom sa korisnicima ili trećim licima.

9.6.2 OBAVEZE I ODGOVORNOSTI REGISTRACIONOG TELA

Registraciono telo je dužno:

- proveravati identitet vlasnika sertifikata, odnosno budućih vlasnika sertifikata,
- primati zahteve za sertifikacione usluge HALCOM BG CA,
- proveravati zahteve za dobijanjem sertifikata,
- izdavati potrebnu dokumentaciju vlasnicima odnosno budućim vlasnicima sertifikata,
- prosleđivati zahteve i ostale podatke do sertifikacionog tela HALCOM BG CA.

Registraciono telo je odgovorno za sprovođenje svih odredaba iz ove politike sertifikacije i drugih zahteva koje dogovori sa sertifikacionim telo HALCOM BG CA.

9.6.3 OBAVEZE I ODGOVORNOSTI VLASNIKA SERTIFIKATA

Vlasnik sertifikata je odgovoran za:

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

- Nastalu štetu u slučaju zloupotrebe sertifikata od prijave opoziva do samog opoziva,
- Svaku štetu koja je, bilo indirektno ili direktno, prouzrokovana zbog omogućenog korišćenja, odnosno zloupotrebe, vlasnikovog privatnog ključa od strane neovlašćenih lica,
- Svaku drugu štetu koja nastane iz nepoštovanja odredbi ove politike sertifikacije i drugih dokumenata sertifikacionog tela HALCOM BG CA, kao i važećih propisa.

Obaveze vlasnika sertifikata su, vezano za korišćenje sertifikata, definisane u poglavlju 4.5.1.

9.6.4 OBAVEZE I ODGOVORNOSTI TREĆIH LICA

Sa početkom korišćenja sertifikata izdatih od strane sertifikacionog tela HALCOM BG CA, a u skladu sa ovom politikom sertifikacije, treće lice koje se uzda u dati kvalifikovani elektronski sertifikat mora pažljivo da prouči ovu politiku sertifikacije i od tog trenutka da redovno prati sva obaveštenja sertifikacionog tela HALCOM BG CA.

Treće lice mora uvek, ukoliko želi da koristi dati sertifikat za neku kriptografsku operaciju, pouzdano da proveri da li je sertifikat povučen, tj. da li se nalazi u registru opozvanih sertifikata.

Treće lice može da se pouzda u sertifikat do eventualnog opoziva sertifikata.

9.6.5 OBAVEZE I ODGOVORNOSTI DRUGIH LICA

Nije primenljivo.

9.7. OGRANIČENJE ODGOVORNOSTI

Sertifikaciono telo HALCOM BG CA nije odgovorno za štetu koja proizlazi iz:

- Korišćenja sertifikata za namene i na način koji nije izričito predviđen u ovoj politici sertifikacije,
- nepravilnog ili pogrešnog obezbeđenja lozinka ili privatnih ključeva vlasnika sertifikata, otkrivanje poverljivih podataka ili ključeva trećim licima i neodgovornog postupanja vlasnika sertifikata,
- zloupotrebe odnosno upada u informacioni sistem vlasnika sertifikata i na taj način dolaska do podataka o sertifikatima od strane neovlašćenih lica,
- nepostupanja ili lošeg postupanja sa podacima u okviru informacione infrastrukture vlasnika sertifikata ili trećih lica,
- ne proveravanja podataka i validnosti (statusa povučenosti) sertifikata u registru opozvanih sertifikata,
- ne proveravanje vremena validnosti sertifikata,
- postupanja vlasnika sertifikata ili trećeg lica u suprotnosti sa informacijama i obaveštenjima koje objavljuje sertifikaciono telo HALCOM BG CA, ovom politikom sertifikacije i drugim propisima,
- omogućenog korišćenja odnosno zloupotrebe vlasnikovog sertifikata od strane neovlašćenih lica,
- izdatog sertifikata sa pogrešnim podacima, ili drugim radnjama vlasnika sertifikata ukoliko vlasnik sertifikata nije po prijemu prijavio grešku, u skladu sa tačkom 4.5.1.,

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

- korišćenja sertifikata koji nisu validni, uz promenu podataka iz sertifikata, elektronskih adresa ili promena imena vlasnika,
- ispada infrastrukture koja nije u domenu upravljanja sertifikacionog tela HALCOM BG CA,
- podataka koji se šifruju ili potpisuju korišćenjem kvalifikovanih elektronskih sertifikata,
- upotrebe i pouzdanosti rada mašinske i programske opreme vlasnika sertifikata.

9.8. GARANCIJA VEZANA NA KORIŠĆENJE SERTIFIKATA

Sertifikaciono telo HALCOM BG CA garantuje za vrednost pojedinačnog pravnog posla vezanog za kvalifikovani elektronski sertifikat pravnog lica u visini polise osiguranja koje je u skladu sa zakonom.

9.9. PODMIRENJE ŠTETE

Za štetu je odgovorna stranka koja je istu prouzrokovala zbog nepoštovanja odredaba iz ove politike sertifikacije i važećeg zakonodavstva.

9.10. VALIDNOST POLITIKE SERTIFIKACIJE

Sertifikaciono telo HALCOM BG CA zadržava pravo da izmeni politiku sertifikacije i da nadogradi infrastrukturu bez prethodnog obaveštavanja vlasnika sertifikata. Važeći sertifikati tako ostaju važeći do isteka njihove validnosti i za njih još uvek važi ona politika sertifikacije koja je važila u vreme njihovog izdavanja. Za sve sertifikate izdate nakon početka validnosti nove politike sertifikacije, važi nova politika.

Ova politika sertifikacije stupa na snagu onoga dana kada je odobrena i objavljena od strane sertifikacionog tela HALCOM BG CA.

9.10.1 PERIOD VALIDNOSTI

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

Kraj validnosti politike sertifikacije nije određen niti je povezan sa periodom validnosti sertifikata izdatih na osnovu ove politike sertifikacije.

9.10.2 KRAJ VALIDNOSTI POLITIKE SERTIFIKACIJE

Prilikom objavljivanja nove politike sertifikacije, za sve sertifikate izdate po osnovu te politike sertifikacije, 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.).

Sertifikaciono telo može za pojedinačne odredbe validne politike sertifikacije da objavi amandmane kao što je to navedeno u poglavlju 9.12.

9.10.3 UČINAK ISTEKA VALIDNOSTI POLITIKE SERTIFIKACIJE

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

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

Nova politika sertifikacije ne utiče na validnost sertifikata koji su bili izdati prema prethodnim politikama. Takvi kvalifikovani elektronski sertifikata ostaju važeći do isteka validnosti pri čemu se, gde god je to moguće procesiraju i/ili tretiraju prema novoj politici sertifikacije.

9.11. KOMUNIKACIJA SUBJEKATA

Kontaktni podaci sertifikacionog tela objavljeni su na web stranicama istog i navedeni u poglavlju 1.3.1.

Kontaktni podaci vlasnika sertifikata dostavljeni su u zahtevima vezanim za sertifikate.

Kontaktni podaci trećih lica dostavljeni su u mogućem međusobnom dogovoru između trećeg lica i sertifikacionog tela HALCOM BG CA.

9.12. PROMENE I DOPUNE

9.12.1 POSTUPAK ZA PRIHVATANJE PROMENA I DOPUNA

Promene ili dopune ove politike sertifikacije sertifikaciono telo može da objavi u obliku promena ili dopuna ovoj politici ako se ne radi o suštinskim promenama operativnog rada sertifikacionog tela.

Amandmani se usvajaju i prihvataju istim postupkom kao i sama politika.

Ako promene i dopune suštinski utiču na operativni rad sertifikacionog tela, o tome se obaveštava nadležno ministarstvo istim postupkom kao što to važi i za samu politiku.

Način za označavanje amandmana definiše sertifikaciono telo HALCOM BG CA.

9.12.2 VALIDNOST I OBJAVA PROMENA I DOPUNA

Sertifikaciono telo HALCOM BG CA definiše početak i kraj validnosti promena i dopuna.

Promene i dopune se objave sedam (7) dana pre početka validnosti na web stranicama sertifikacionog tela HALCOM BG CA.

9.12.3 PROMENA IDENTIFIKACIONOG BROJA POLITIKE SERTIFIKACIJE

Ako prihvaćene promene i dopune utiču na korišćenje sertifikata, sertifikaciono telo HALCOM BG CA određuje novi identifikacioni broj (CP_{OID}) za novu politiku, odnosno promene i dopune.

9.13. POSTUPAK U SLUČAJU SPOROVA

Sve pritužbe vlasnika sertifikata rešava organizaciona jedinica za nadzor i usklađenost (poglavlje 5.3).

Moguće sporove između vlasnika sertifikata ili trećeg lica i sertifikacionog tela HALCOM BG CA rešava nadležni sud.

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR

9.14. VAŽEĆE ZAKONODAVSTVO

Za odlučivanje o ovoj politici sertifikacije upotrebljava se pravo Republike Srbije.

9.15. USKLAĐENOST SA VAŽEĆIM ZAKONODAVSTVOM

Nadzor nad usklađenošću operativnog rada sertifikacionog tela HALCOM BG CA sa važećim zakonodavstvom i propisima sprovodi nadležna inspekcijska služba.

Interne provere usklađenosti operativnog rada sprovode ovlašćena lica u okviru sertifikacionog tela HALCOM BG CA.

9.16. OPŠTE ODREDBE

Sa ostalim subjektima sertifikaciono telo može da sklopi međusobne dogovore ako tako definiše važeće zakonodavstvo, odnosno drugi propisi.

9.17. DRUGE ODREDBE

Nisu propisane.

Halcom a.d. Beograd, Beogradska 39, 11000 Beograd, Tel: +381 11 3348 995, Fax: +381 11 3348 994, www.halcom.rs info@halcom.rs
PIB: 102193722, MB: 17419722, ŠD: 67130, Reg. Br. APR: BD2771/2005, Kapital: 182.828,60 EUR