

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

Politika sertifikacije za pravna lica

CPName: HALCOM BG CA

CPOID: 1.3.6.1.4.1.5939.1.3.1

Dokument važi od: 25.12.2009.

Sadržaj

1. UVOD	9
1.1. Pregled	9
1.2. Identifikacioni podaci politike sertifikacije	10
1.3. Subjekti	10
1.3.1 Sertifikaciono telo HALCOM BG CA	10
1.3.2 Registraciona tela HALCOM BG CA	10
1.3.3 Vlasnici digitalnih sertifikata	11
1.3.4 Treća lica	11
1.3.5 Ostala lica	11
1.4. Namene korišćenja digitalnih sertifikata	11
1.4.1 Pravilno korišćenje sertifikata i ključeva	12
1.4.2 Nedopušteno korišćenje	12
1.5. Upravljanje politikom sertifikacije	12
1.5.1 Odgovornost za upravljanje politikom sertifikacije	13
1.5.2 Ovlašćena lica za kontakt	13
1.5.3 Lice odgovorno za usklađenost poslovanja sertifikacionog tela HALCOM BG CA sa ovom politikom sertifikacije	13
1.5.4 Postupak za usvajanje nove politike sertifikacije	13
1.6. Skraćenice i izrazi	14
1.6.1 Skraćenice	14
1.6.2 Izrazi	14
2. OBJAVLJIVANJE INFORMACIJA I JAVNI IMENIK DIGITALNIH SERTIFIKATA	16
2.1. Repozitorijum dokumenata	16
2.2. Javni imenik digitalnih sertifikata	16
2.3. Učestanost objavljivanja	16
2.4. Upravljanje pristupom repozitorijumu dokumenata	17
3. IDENTITET VLASNIKA SERTIFIKATA	18
3.1. Dodela imena	18
3.1.1 Karakteristična imena	18
3.1.2 Zahtevi kod kreiranja karakterističnog imena	18
3.1.3 Upotreba anonimnih imena ili pseudonima	19
3.1.4 Pravila za interpretaciju karakterističnog imena	19
3.1.5 Jednoznačnost karakterističnih imena	19
3.1.6 Zaštita imena odnosno robnih marki	19
3.2. Proveravanje identiteta vlasnika / korisnika kod prvog izdavanja	

digitalnog sertifikata	20
3.2.1 Proveravanje identiteta organizacije	20
3.2.2 Proveravanje identiteta vlasnika sertifikata	20
3.2.3 Neprovereni podaci u digitalnim sertifikatima	20
3.2.4 Proveravanje ovlašćenja zaposlenih za sticanje sertifikata u ime organizacije	20
3.2.5 Međusobno priznavanje	20
3.3. Proveravanje vlasnika za ponovno izdavanje digitalnog sertifikata	20
3.3.1 Proveravanje vlasnika sertifikata kod produžavanja roka važnosti digitalnih sertifikata (obnavljanje)	21
3.3.2 Proveravanje vlasnika sertifikata za ponovo izdavanje digitalnog sertifikata nakon opoziva	21
3.4. Proveravanje identiteta kod zahteva za opoziv sertifikata	21
4. UPRAVLJANJE DIGITALNIM SERTIFIKATIMA	22
4.1. Dobijanje digitalnog sertifikata	22
4.1.1 Ko može da dobije digitalni sertifikat	22
4.1.2 Postupak budućeg vlasnika sertifikata za sticanje digitalnog sertifikata i pridružene odgovornosti	22
4.2. Postupak kod prijema zahteva za dobijanje digitalnog sertifikata	22
4.2.1 Proveravanje identiteta budućeg vlasnika sertifikata	22
4.2.2 Odobrenje/odbijanje zahteva	23
4.2.3 Vreme za izdavanje digitalnog sertifikata	23
4.3. Izdavanje digitalnog sertifikata	23
4.3.1 Postupak sertifikacionog tela HALCOM BG CA	23
4.3.2 Obaveštenje vlasniku o izdavanju sertifikata	23
4.4. Preuzimanje digitalnog sertifikata	24
4.4.1 Postupak preuzimanja digitalnog sertifikata	24
4.4.2 Objavljivanje digitalnog sertifikata	24
4.4.3 Obaveštenje od strane sertifikacionog tela o izdavanju sertifikata drugim preduzećima odnosno organizacijama	24
4.5. Obaveze i odgovornosti korisnika vezane na korišćenje digitalnih sertifikata	24
4.5.1 Obaveze vlasnika digitalnog sertifikata	24
4.5.2 Obaveze trećih lica	25
4.6. Ponovno izdavanje digitalnog sertifikata	25
4.6.1 Okolnosti koje zahtevaju ponovno izdavanje digitalnog sertifikata	25
4.6.2 Lica koja mogu da traže ponovno izdavanje digitalnog sertifikata	26
4.6.3 Postupak obrade zahteva za ponovno izdavanje digitalnog sertifikata	26
4.6.4 Obaveštenje vlasniku o novo izdatom digitalnom sertifikatu	26
4.6.5 Postupak preuzimanja novo izdatog digitalnog sertifikata	26
4.6.6 Objavljivanje novo izdatog digitalnog sertifikata	26
4.6.7 Obaveštenje sertifikacionog tela o izdavanju digitalnog sertifikata drugim subjektima	26
4.7. Obnavljanje ključeva	26
4.7.1 Razlozi za obnavljanje ključeva	26
4.7.2 Ko može da zahteva obnavljanje ključeva	26

4.7.3	Postupak za izdavanje zahteva za obnavljanje ključeva	26
4.7.4	Obaveštenje vlasniku digitalnog sertifikata o novo izdatom sertifikatu	27
4.7.5	Postupak preuzimanja	27
4.7.6	Objava digitalnog sertifikata izdavaoca sertifikata sa novim parom ključeva	27
4.7.7	Obaveštenje od strane sertifikacionog tela o izdavanju sertifikata drugim subjektima	27
4.8.	Promena digitalnog sertifikata	27
4.8.1	Okolnosti za promenu digitalnog sertifikata	27
4.8.2	Ko može da zahteva promenu	27
4.8.3	Postupak kod zahteva za promenu	27
4.8.4	Obavest o izdavanju novog digitalnog sertifikata	27
4.8.5	Preuzimanje promenjenog digitalnog sertifikata	27
4.8.6	Objavljivanje promenjenog digitalnog sertifikata	27
4.8.7	Obaveštenje drugih subjekata o promeni	28
4.9.	Opoziv i suspenzija digitalnog sertifikata	28
4.9.1	Razlozi opoziva	28
4.9.2	Ko zahteva opoziv	29
4.9.3	Postupak opoziva	29
4.9.4	Vreme izdavanja zahteva za opoziv	29
4.9.5	Vreme od primljenog zahteva za opoziv do izvršenja opoziva	30
4.9.6	Zahtevi za proveravanje registra opozvanih sertifikata za treća lica	30
4.9.7	Učestanost objavljivanja registra opozvanih sertifikata	30
4.9.8	Vreme objavljivanja registra opozvanih sertifikata	30
4.9.9	Sinhrona provera statusa sertifikata	30
4.9.10	Zahtevi za sinhronu proveru statusa sertifikata	30
4.9.11	Drugi načini za pristup statusu sertifikata	31
4.9.12	Posebni zahtevi kod zloupotrebe privatnog ključa	31
4.9.13	Razlozi za suspenziju sertifikata	31
4.9.14	Ko zahteva suspenziju	31
4.9.15	Postupak suspenzije	31
4.9.16	Vreme suspenzije	31
4.10.	Proveravanje statusa sertifikata	31
4.10.1	Pristup proveravanju	31
4.10.2	Raspoloživost	31
4.10.3	Druge informacije za proveravanje statusa	32
4.11.	Prekid odnosa vlasnika i sertifikacionog tela	32
4.12.	Otkrivanje kopije ključeva za dešifrovanje	32
4.12.1	Razlozi za otkrivanje kopije ključeva za dešifrovanje	32
4.12.2	Ko zahteva otkrivanje kopije ključeva za dešifrovanje	32
4.12.3	Postupak kod zahteva za otkrivanje kopije ključeva za dešifrovanje	32
5.	UPRAVLJANJE I SIGURNOSNI NADZOR INFRASTRUKTURE	33
5.1.	Fizičko obezbeđenje	33
5.1.1	Lokacija i zgrada sertifikacionog tela	33
5.1.2	Fizički pristup infrastrukturi sertifikacionog tela	33
5.1.3	Napajanje i ventilacija	33
5.1.4	Zaštita od poplava	34
5.1.5	Zaštita od požara	34
5.1.6	Čuvanje nosioca podataka	34

5.1.7 Uklanjanje otpadaka	34
5.1.8 Čuvanje podataka na udaljenoj lokaciji	34
5.2. Organizaciona struktura sertifikacionog tela	34
5.2.1 Organizacione grupe	34
5.2.2 Broj osoba za pojedinačne zadatke	35
5.2.3 Dokazivanje identiteta / autorizacija za izvršavanje pojedinačnih zadataka	37
5.2.4 Nekompatibilnost zadataka	37
5.3. Nadzor	38
5.3.1 Potrebne kvalifikacije i iskustva zaposlenih	38
5.3.2 Pogodnost kvalifikacija zaposlenih	38
5.3.3 Dodatno usavršavanje zaposlenih	38
5.3.4 Zahtevi za redovna usavršavanja	38
5.3.5 Izmena zadataka	38
5.3.6 Sankcije	38
5.3.7 Zahtevi za spoljne saradnike	38
5.3.8 Pristup zaposlenih do dokumentacije	39
5.4. Bezbednosni pregledi sistema	39
5.4.1 Vrste dnevnika	39
5.4.2 Učestanost pregleda dnevnika	39
5.4.3 Vreme čuvanja dnevnika	39
5.4.4 Zaštita dnevnika	39
5.4.5 Sigurnosne kopije dnevnika	39
5.4.6 Sakupljanje podataka za dnevnik	39
5.4.7 Obaveštavanje lica koja su prouzrokovala odgovarajući bezbednosni događaj	40
5.4.8 Ocena ranjivosti sistema	40
5.5. Dugotrajno čuvanje podataka	40
5.5.1 Vrste dugoročno čuvanih podataka	40
5.5.2 Rok čuvanja	40
5.5.3 Zaštita dugotrajno čuvanih podataka	40
5.5.4 Bezbedne kopije dugotrajno čuvanih podataka	41
5.5.5 Zahtevi za vremenski pečat	41
5.5.6 Način sakupljanja podataka	41
5.5.7 Postupak pristupa dugotrajno čuvanim podacima i njihova verifikacija	41
5.6. Promena javnog ključa sertifikacionog tela HALCOM BG CA	41
5.7. Plan za oporavak poslovanja	41
5.7.1 Postupak u slučaju upada i zloupotrebe	41
5.7.2 Postupak u slučaju kvara programske opreme, podataka	41
5.7.3 Postupak u slučaju ugroženog privatnog ključa overavača HALCOM BG CA	42
5.7.4 Plan za oporavak poslovanja	42
5.8. Prestanak operativnog rada HALCOM BG CA	42
6. TEHNIČKI BEZBEDNOSNI ZAHTEVI	43
6.1. Generisanje i zaštita ključeva	43
6.1.1 Generisanje ključeva	43
6.1.2 Dostava privatnog ključa vlasnicima	43
6.1.3 Dostava javnog ključa korisnika sertifikacionom telu	43
6.1.4 Dostava javnog ključa sertifikacionog tela korisnicima i trećim licima	43

6.1.5 Dužina asimetričnih ključeva	44
6.1.6 Generisanje i kvalitet parametara asimetričnih parova ključeva	44
6.1.7 Upotreba ključeva i sertifikata	44
6.2. Zaštita privatnih ključeva	44
6.2.1 Standardi za kriptografski modul	44
6.2.2 Nadzor pristupa privatnom ključu od strane ovlašćenih lica sertifikacionog tela	44
6.2.3 Otkrivanje kopije privatnog ključa	44
6.2.4 Bezbedna kopija privatnog ključa	44
6.2.5 Arhiviranje privatnog ključa	45
6.2.6 Prenos privatnog ključa iz/u kriptografski modul	45
6.2.7 Čuvanje privatnog ključa u kriptografskom modulu	45
6.2.8 Postupak za aktiviranje privatnog ključa	45
6.2.9 Postupak za deaktiviranje privatnog ključa	45
6.2.10 Postupak za uništenje privatnog ključa	45
6.2.11 Karakteristike kriptografskog modula	45
6.3. Ostali aspekti upravljanja ključevima	45
6.3.1 Arhiviranje javnog ključa	46
6.3.2 Vreme važenja javnih i privatnih ključeva	46
6.4. Lozinke za pristup privatnim ključevima	46
6.4.1 Generisanje lozinke	46
6.4.2 Zaštita lozinke	46
6.4.3 Drugi aspekti korišćenja lozinke	47
6.5. Sigurnosni zahtevi za računarsku opremu sertifikacionog tela	47
6.5.1 Specifični tehnički sigurnosni zahtevi	47
6.5.2 Nivoi sigurnosne zaštite	47
6.6. Tehnički nadzor životnog ciklusa sertifikacionog tela	47
6.6.1 Nadzor razvoja sistema	47
6.6.2 Upravljanje sigurnošću	47
6.6.3 Nadzor životnog ciklusa sertifikacionog tela	47
6.7. Sigurnosna kontrola računarske mreže	47
6.8. Vremenski pečat	47
7. PROFIL SERTIFIKATA I REGISTRA OPOZVANIH SERTIFIKATA	48
7.1. Profil sertifikata	48
7.1.1 Verzije sertifikata	48
7.1.2 Profil sertifikata sa korišćenim ekstenzijama	48
7.1.3 Identifikacione oznake kriptografskih algoritama	49
7.1.4 Oblik karakterističnih imena korisnika	49
7.1.5 Ograničenja vezana za imena	50
7.1.6 Oznaka politike sertifikacije	50
7.1.7 Ograničenja korišćenja	50
7.1.8 Sintaksa i značenje oznaka politike sertifikata	50
7.1.9 Značenje bitnih dodataka politike	50
7.2. Profil registra opozvanih sertifikata	50

7.2.1 Verzija	50
7.2.2 Sadržaj CRL i pridružene ekstenzije	51
7.2.3 Objavljivanje registra opozvanih sertifikata	52
7.3. Profil OCSP	52
7.3.1 Verzija OCSP protokola	52
7.3.2 Profil OCSP protokola	52
8. NADZOR	53
8.1. Učestanost nadzora	53
8.2. Vrsta nadzora i ospodobljenost zaposlenih	53
8.3. Nezavisnost nadzora	53
8.4. Područja nadzora	53
8.5. Mere koje primenjuje sertifikaciono telo	53
8.6. Objavljivanje rezultata nadzora	53
9. FINANSIJSKE I OSTALE PRAVNE STVARI	54
9.1. Cenovnik	54
9.1.1 Cena izdavanja i obnavljanja sertifikata	54
9.1.2 Cena pristupa digitalnim sertifikatima	54
9.1.3 Cena pristupa statusu sertifikata i registru opozvanih sertifikata	54
9.1.4 Cene drugih usluga sertifikacionog tela	54
9.1.5 Povratak troškova	54
9.2. Finansijska odgovornost	54
9.2.1 Osiguranje	54
9.2.2 Ostala pokrića	54
9.2.3 Osiguranje vlasnika	54
9.3. Čuvanje poslovnih podataka	54
9.3.1 Poverljivi podaci koji se čuvaju	54
9.3.2 Podaci koji se javno objavljuju	55
9.3.3 Odgovornost u vezi čuvanja podataka	55
9.4. Čuvanje ličnih podataka	55
9.4.1 Plan čuvanja i zaštite ličnih podataka	55
9.4.2 Lični podaci koji se čuvaju/štite i ne objavljuju	55
9.4.3 Lični podaci koji se objavljuju	55
9.4.4 Odgovornost vezana za čuvanje/zaštitu ličnih podataka	55
9.4.5 Ovlašćenje vezano za korišćenje ličnih podataka	56
9.4.6 Prosleđivanje ličnih podataka vlasnika sertifikata	56
9.4.7 Druge odredbe vezane za čuvanje ličnih podataka	56
9.5. Odredbe vezane na prava intelektualnog vlasništva	56
9.6. Obaveze i odgovornosti	56
9.6.1 Obaveze i odgovornosti sertifikacionog tela HALCOM BG CA	56

9.6.2 Obaveze i odgovornosti registracionog tela	57
9.6.3 Obaveze i odgovornosti vlasnika sertifikata	58
9.6.4 Obaveze i odgovornosti trećih lica	58
9.6.5 Obaveze i odgovornosti drugih lica	59
9.7. Ograničenje odgovornosti	59
9.8. Ograničenje vezano na korišćenje sertifikata	59
9.9. Podmirenje štete	59
9.10. Validnost politike sertifikacije	60
9.10.1 Period validnosti	60
9.10.2 Kraj validnosti politike sertifikacije	60
9.10.3 Učinak isteka validnosti politike sertifikacije	60
9.11. Komunikacija subjekata	60
9.12. Promene i dopune	61
9.12.1 Postupak za prihvatanje promena i dopuna	61
9.12.2 Validost i objava promena i dopuna	61
9.12.3 Promena identifikacionog broja politike sertifikacije	61
9.13. Postupak u slučaju sporova	61
9.14. Važeće zakonodavstvo	61
9.15. Usklađenost sa važećim zakonodavstvom	61
9.16. Opšte odredbe	62
9.17. Druge odredbe	62

1. UVOD

Ovaj dokument predstavlja politiku sertifikacije (CP – Certificate Policy) sertifikacionog tela HALCOM BG CA za pravna lica za potrebe sistema elektronsko bankarstva u Srbiji.

Dokument se odnosi na izdavanje digitalnih sertifikata, definiše cilj, delovanje i metodologiju upravljanja digitalnim 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 digitalnim sertifikatima za verifikaciju elektronskog potpisa. HALCOM BG CA sertifikaciono telo namenjeno je izdavanju digitalnih sertifikata za pravna i fizička lica i obavljanju tehnoloških usluga u vezi sa elektronskim potpisima. Delovanje uređuju drugi dokumenti druga pravila i to nije u ovoj CP, niti je u bilo kakvoj vezi sa njom.

Sve odredbe ove CP u odnosu na delovanje HALCOM BG CA propisno su prenesene i detaljnije 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), fizička zaštita (pristup prostorijama, upravljanje hardverskom i programskom opremom), programska zaštita (zaštitni softver, zaštitne kopije, ...) 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, koja predstavlja nedeljivu celinu javnog dela internih pravila sertifikacionog tela HALCOM BG CA a vezano za izdavanje digitalnih sertifikata, uređuju nameru, delovanje i metodologiju upravljanja digitalnim 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 digitalnim sertifikatima za verifikaciju elektronskog potpisa. HALCOM BG CA deluje i kao glavno sertifikaciono telo (root CA) koje zajedno sa svojim podređenim sertifikacionim telima predstavlja hijerarhijsku mrežu sertifikacionih tela koja je namenjena izdavanju digitalnih sertifikata i vršenju tehnoloških usluga vezanih za bezbedne elektronske potpise.

HALCOM BG CA izdaje dva digitalna 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.

HALCOM BG CA sertifikaciono telo, izdaje digitalne 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 3280 „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 prijavnih službi i operatera (RA – Registration Authority) koji omogućuju podnošenje zahteva za dobijanje digitalnih 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

CPOID: 1.3.6.1.4.1.5939.1.3.1

U svakom digitalnom 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 digitalnim sertifikatima za verifikaciju elektronskog potpisa. HALCOM BG CA predstavlja takođe Root sertifikaciono telo koje zajedno sa svojim podređenim sertifikacionim telima čini hijerarhijsku mrežu sertifikacionih tela koja izdaje digitalne sertifikate pravnim i fizičkim licima, kao i vršenju drugih tehnoloških usluga vezanih za bezbedne elektronske potpise.

Sertifikaciono telo HALCOM BG CA izdaje digitalne sertifikate pravnim licima u Srbiji za potrebe bezbednog elektronskog bankarstva putem servisnog centra EBB.

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 digitalnih sertifikata, kao i proveravanje ostalih podataka važnih za upravljanje digitalnim sertifikatima,
2. primanje zahteva za dobijanje sertifikata,

3. primanje zahteva za opozivanje/povlačenje sertifikata,
4. izdavanje nužne dokumentacije vlasnicima, odnosno budućim vlasnicima, digitalnih sertifikata
5. prosleđivanje zahteva i ostalih podataka sigurnim putem do HALCOM BG CA sertifikacionog tela.

Sertifikaciono telo HALCOM BG CA može za izvršavanje zadataka prijavnice službe (RA), uz svoje sopstveno RA, takođe opunomoćiti 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 te internim pravilima HALCOM BG CA.

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

1.3.3 VLASNICI DIGITALNIH SERTIFIKATA

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

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, nameru upotrebe sertifikata, 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 digitalnih sertifikata drugih sertifikacionih tela.

1.3.5 OSTALA LICA

Za korišćenje digitalnih 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 digitalni sertifikati HALCOM BG CA.

1.4. NAMENE KORIŠĆENJA DIGITALNIH SERTIFIKATA

HALCOM BG CA sertifikaciono telo upravlja (izdaje i overava, opoziva, produžava, objavljuje) digitalnim sertifikatima za verifikaciju elektronskog potpisa koji su namenjeni pravnim licima.

1.4.1 PRAVILNO KORIŠĆENJE SERTIFIKATA I KLJUČEVA

Digitalni 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.

Digitalni sertifikati se između ostalog mogu koristiti za:

- identifikaciju vlasnika sertifikata,
- dokazivanje identiteta vlasnika sertifikata,
- potpisivanje dokumenata u elektronskom obliku i njegovu verifikaciju,
- šifrovanje dokumenata u elektronskom obliku primenom asimetričnih kriptografskih algoritama.

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 ili mobilnih formulara,
- bezbedno poslovanje sa organima i organizacijama javnog sektora te ostalim pravnim ili fizičkim licima,
- ostale aplikacije odnosno usluge u kojima se zahteva korišćenje digitalnog sertifikata,
- kontrola pristupa.

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

1.4.2 NEDOPUŠTENI KORIŠĆENJE

Zabranjeno je korišćenje digitalnih 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.

Digitalni 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 30 32 432

Fax: (+381) 11 33 48 998

<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:

Halcom A.D. Beograd

HALCOM BG CA

Beogradska 39

11000 Beograd

Srbija

Tel.: (+381) 11 30 32 432

Fax: (+381) 11 33 48 998

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 (<i>engl.: Certification Authority ili Certification Agency</i>).
CCPS	<i>Certificate and Card Production Service</i> – usluga izrade digitalnih 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 proizvoda 4. Izrada visoko kvalitetnih RSA 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 digitalnih sertifikata x509 v3 i njihovo punjenje u smart kartice
CPName	Ime politike sertifikacije (<i>engl.: Certification Policy Name</i>), jednoznačno povezan sa međunarodno jedinstvenim brojem politike sertifikacije CPOID (<i>engl.: Certification Policy Object Identifier</i>).
CPOID	Međunarodni broj koji jednoznačno definiše politiku sertifikacije (<i>engl.: Certification Policy Object Identifier</i>).
CRL	<i>Certificate Revocation List</i> – lista opozvanih digitalnih sertifikata
DN	Jednoznačno karakteristično ime (<i>engl.: Distinguished Name</i>).
LDAP	<i>Leightweight Directory Access Protocol</i> je protokol koji omogućava pristup sertifikatima i CRL koje izdaje sertifikaciono telo a specificiran prema IETF (<i>Internet Engineering Task Force</i>) preporuci RFC 1777.
S/MIME	<i>Secure Multipurpose Internet Mail Extensions</i>
SSL	<i>Secure Sockets Layer</i>
TLS	<i>Transport Layer Security</i>
PKI	<i>Public Key Infrastructure</i> je infrastruktura javnih ključeva
WPKI	<i>Wireless Public Key Infrastructure</i> je infrastruktura javnih ključeva koja deluje preko bežičnih veza (npr. GSM telefona).

1.6.2 IZRAZI

Imenik digitalnih sertifikata	Imenik digitalnih sertifikata prema preporuci X.500 predstavlja mesto gde se čuvaju izdati digitalni sertifikati u formatu X.509 v3 i do kojih je moguć pristup putem LDAP protokola.
Identifikacija	Identifikacija je utvrđivanje identitete lica koje se izvodi lično, uz pomoć važećeg ličnog dokumenta ili u elektronskom obliku, uz pomoć važećeg digitalnog sertifikata.
Sertifikaciono telo	Pravno lice koje izdaje digitalne sertifikate ili vrši ostale usluge vezane za verifikaciju ili elektronske potpise (<i>engl.: Certification Authority - CA</i>).
Registraciono telo	Služba ili lice koje prima zahteve za digitalne sertifikate i preuzima odgovornost za identifikaciju i proveru identiteta budućih vlasnika sertifikata u ime sertifikacionog tela (<i>engl.: Registration Authority - RA</i>).
Karakteristično ime	Jednoznačno ime u digitalnom sertifikatu (DN – Distinguished Name) koje nedvosmisleno i jednoznačno definiše datog korisnika u strukturi imenika sertifikacionog tela.
Bezbednosni nosilac	Smart kartica, SIM (<i>engl.: Subscriber Identity Module</i>) kartica ili USB smart kartica sa ugrađenom posebnom memorijom za bezbedno čuvanje privatnih ključeva, kao i o matematički procesor za realizaciju kriptografskih operacija sa tim ključevima. Namenjen je bezbednom generisanju, korišćenju i čuvanju asimetričnih kriptografskih ključeva.

2. OBJAVLJIVANJE INFORMACIJA I JAVNI IMENIK DIGITALNIH 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:

- politike sertifikacije,
- prijavni formulari za usluge sertifikacionog tela,
- uputstva za bezbedno korišćenje digitalnih 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. JAVNI IMENIK DIGITALNIH SERTIFIKATA

Nove modifikovane politike sertifikacije se objavljuju u skladu sa navodima u poglavlju 9.10.

Digitalni sertifikati se objavljuju u javnom imeniku odmah nakon njihovog izdavanja.

Opozvani digitalni sertifikati se objavljuju u registru opozvanih digitalnih sertifikata (CRL) odmah (detaljnije o tome u poglavlju 4.9.8.), dok se ostale javno dostupne informacijem 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.

HALCOM BG CA je odgovorno da se digitalni sertifikati objavljuju u javnom imeniku odmah nakon njihovog izdavanja.

Lista opozvanih sertifikata se obnovi svakih 24 sata ili odmah nakon opoziva digitalnog sertifikata u javnom imeniku opozvanih digitalnih sertifikata. 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

Javni imenik je javno dostupan na serveru ldap.halcom.si, 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 imeniku digitalnih sertifikata.

3. IDENTITET VLASNIKA SERTIFIKATA

3.1. DODELA IMENA

Karakteristična imena koje sadrži digitalni sertifikat nedvosmisleno i jednoznačno definišu vlasnika sertifikata osim ako se, ovim aktom ili sadržajem digitalnog sertifikata, drugačije zahteva.

3.1.1 KARAKTERISTIČNA IMENA

U skladu sa RFC 5280 svaki digitalni sertifikat sadrži podatke o vlasniku i izdavaocu digitalnog 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 digitalnog 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
Digitalni sertifikat sertifikacionog tela HALCOM BG CA	Izdavalac engl. <i>Issuer</i> i	C= SI O= Halcom 2.5.4.54 = EBBBG2 CN= EBB Beograd CA 2
Digital signature	Korisnik, engl. <i>Subject</i>	C= YU O = <ime organizacije> CN=<ime i prezime> SN= <prezime> G= <ime>
Nonrepudiation digitalni sertifikat	Korisnik, engl. <i>Subject</i>	C= YU O = <ime organizacije> CN=<ime i prezime> SN= <prezime> G= <ime>

3.1.2 ZAHTEVI KOD KREIRANJA KARAKTERISTIČNOG IMENA

U skladu sa karakterističnim imenom vlasnik digitalnog sertifikata je nedvosmisleno i jednoznačno definisan.

Karakteristično ime mora da bude jedinstveno u okviru sertifikacionog tela, tj. da je formirano na način da je iz istog moguće jednoznačno identifikovati pojedinca odnosno organizaciju.

3.1.3 UPOTREBA ANONIMNIH IMENA ILI PSEUDONIMA

Upotreba anonimnih imena ili pseudonima nije dozvoljena.

3.1.4 PRAVILA ZA INTERPRETACIJU KARAKTERISTIČNOG IMENA

Podaci o vlasniku sertifikata u karakterističnom imenu sadrže slova engleske abecede, dok se preostali znakovi transformišu prema dole navedenoj tabeli:

Znak	Transformacija
Č	C
Ć	C
Đ	DJ
Š	S
Ž	Z
Ü	Ue
Ö	Oe
Ø	Oe
ß	Ss
Ñ	N
Ř	Rz

Odgovarajućom kombinacijom slova sertifikaciono telo obezbeđuje korišćenje ostalih nepredvidivih znakova.

3.1.5 JEDNOZNAČNOST KARAKTERISTIČNIH IMENA

Karakteristična imena jednoznačna su za svaki izdati digitalni sertifikat i nedvosmisleno i jednoznačno identifikuju vlasnika u strukturi javnog imenika.

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 digitalnog sertifikata.

3.2. PROVERAVANJE IDENTITETA VLASNIKA / KORISNIKA KOD PRVOG IZDAVANJA DIGITALNOG SERTIFIKATA

Budući vlasnik digitalnog sertifikata može da zahteva digitalni sertifikat u svoje lično ime i ime korisnika u okviru pravnog lica, kao ovlašćeno lice odgovarajućeg pravnog lica. Pijavna služba proverava identitet budućeg vlasnika digitalnog sertifikata.

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 digitalni sertifikat u ime date organizacije.

3.2.2 PROVERAVANJE IDENTITETA VLASNIKA SERTIFIKATA

Identitet korisnika proverava ovlašćeno lice organizacije, a operater proverava identitet ovlašćenog lica pravnog lica.

3.2.3 NEPROVERENI PODACI U DIGITALNIM SERTIFIKATIMA

Ovo poglavlje nije primenljivo u ovom CP dokumentu.

3.2.4 PROVERAVANJE OVLAŠĆENJA ZAPOSLENIH ZA STICANJE SERTIFIKATA U IME ORGANIZACIJE

Ovlašćeno lice organizacije sa potpisom na dokumentima za izdavanje digitalnog sertifikata garantuje da je neosporno proverio identitet budućih vlasnika sertifikata. Pravno lice se kao poslodavac vlasnika sertifikata obavezuje, da će zaposleni ispunjavati sve odredbe ovog CP dokumenta i važeće propise.

3.2.5 MEĐUSOBNO PRIZNAVANJE

Sertifikaciono telo HALCOM BG CA nije dužno ugovorno saradivati ili garantovati za ostala sertifikaciona teka čak iako drugo sertifikaciono telo ima status akreditovanog sertifikacionog tela za izdavanje kvalifikovanih digitalnih sertifikata.

Sertifikaciono telo HALCOM BG CA obezbeđuje da će ispoštovati međusobno priznavanje sertifikacionih tela 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 PONOVO IZDAVANJE DIGITALNOG SERTIFIKATA

3.3.1 PROVERAVANJE VLASNIKA CERTIFIKATA KOD PRODUŽAVANJA ROKA VAŽNOSTI DIGITALNIH CERTIFIKATA (OBNAVLJANJE)

Identitet vlasnika kod ponovnog izdavanja digitalnog sertifikata se proverava:

- kod prijavne službe, u registracionom telu, sertifikacionog tela HALCOM BG CA
- na osnovu već izdatog važećeg digitalnog sertifikata koga je izdalo sertifikaciono telo HALCOM BG CA. Tom prilikom će sertifikaciono telo HALCOM BG CA da proveriti lične podatke o vlasniku sertifikata u odgovarajućim registrima.

3.3.2 PROVERAVANJE VLASNIKA CERTIFIKATA ZA PONOVO IZDAVANJE DIGITALNOG CERTIFIKATA 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 CERTIFIKATA

Zahtev za opoziv digitalnog sertifikata vlasnik preda:

- Lično prijavnoj službi (registracionom telu) gde ovlašćena lica sertifikacionog tela provere identitet podnosioca molbe,
- Elektronski - zahtev za opozivom sertifikata mora biti digitalno potpisan na taj način da se njegov digitalni potpis može verifikovati pomoću digitalnog sertifikata koji se takođe verifikuje u cilju dodatnog utvrđivanja identiteta podnosioca zahteva.
- U slučaju da vlasnik digitalnog sertifikata putem telefona, elektronske pošte ili FAX-a zahteva opoziv digitalnog sertifikata, sertifikaciono telo HALCOM BG CA prvo definiše suspenziju digitalnog sertifikata. Tek na osnovu pismenog zahteva za opoziv digitalnog sertifikata, faktički se sprovodi sam opoziv digitalnog sertifikata.

Detaljan postupak za opoziv je dat u poglavlju 4.9.3.

4. UPRAVLJANJE DIGITALNIM SERTIFIKATIMA

4.1. DOBIJANJE DIGITALNOG SERTIFIKATA

4.1.1 KO MOŽE DA DOBIJE DIGITALNI SERTIFIKAT

Budući vlasnici digitalnih sertifikata koji se izdaju u skladu sa ovim CP dokumentom su fizička lica koj predstavljaju ovlašćenja lica odgovarajućih pravnih lica.

4.1.2 POSTUPAK BUDUĆEG VLASNIKA SERTIFIKATA ZA STICANJE DIGITALNOG SERTIFIKATA I PRIDRUŽENE ODGOVORNOSTI

Digitalni sertifikat se izdaje na osnovu pravilno ispunjene i potpisane narudžbenice za izdavanje digitalnog sertifikata (u daljem tekstu narudžbenica) od strane zakonitog zastupnika i budućeg vlasnika.

Narudžbenica se preda prijavnoj službi (registracionom telu) HALCOM BG CA.

Narudžbenice za izdavanje digitalnog sertifikata dostupne su kako kod prijavnih službi (registracionih tela) HALCOM BG CA tako i na web stranici HALCOM BG CA.

Zakoniti zastupnik pravnog lica preda narudžbenu/molbu u pismenom obliku.

Pre izdavanja narudžbenice, HALCOM BG CA je u obavezi da upozna dato pravno lice, kao i njegovog zakonitog zastupnika 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 molbu korisnika za izdavanje digitalnog sertifikata bez objašnjenja.

4.2. POSTUPAK KOD PRIJEMA ZAHTEVA ZA DOBIJANJE DIGITALNOG SERTIFIKATA

4.2.1 PROVERAVANJE IDENTITETA BUDUĆEG VLASNIKA SERTIFIKATA

Ovlašćeno lice registracionog tela proverava identitet budućeg vlasnika sertifikata prilikom lične predaje zahteva za dobijanjem sertifikata. Zakoniti zastupnik pravnog lica svojim potpisom garantuje da je neosporno proverio identitet budućih vlasnika digitalnih sertifikata za koje prilaže kopije važećeg identifikacionog dokumenta, a svoj identitet mora da dokaže važećim ličnim dokumentom sa fotografijom. Po potrebi su moguće i dodatne provere identiteta.

Ovlašćena lica registracionog ili sertifikacionog tela su dužna da provere identitet budućeg vlasnika sertifikata, odnosno sve one podatke koji su navedeni u zahtevu a

dostupni su u službenim evidencijama odnosno u drugim službeno važećim dokumentima.

Ovlašćena lica registracionog tela proverene ispunjene molbe/narudžbenice, kao i dopunsku originalnu dokumentaciju koja se zahteva, bezbednim putem prosleđuju ka 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 digitalnog sertifikata o čemu je zakoniti zastupnik pravnog lica i budući korisnici odmah obavješteni lično ili elektronskom poštom.

4.2.3 VREME ZA IZDAVANJE DIGITALNOG SERTIFIKATA

HALCOM BG CA po osnovu odobrenog zahteva za izdavanje digitalnog sertifikata obavezuje da najkasnije u roku od pet (5) dana izda digitalni sertifikat i pošalje lozinku za preuzimanje digitalnog sertifikata prijemnoj službi koja dalje distribuira sertifikate do budućih vlasnika.

4.3. IZDAVANJE DIGITALNOG SERTIFIKATA

4.3.1 POSTUPAK SERTIFIKACIONOG TELA HALCOM BG CA

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

1. pred personalizacija bezbednosnog nosioca (generisanje ključeva na kartici),
2. obrada molbi za izdavanje digitalnog sertifikata,
3. priprema digitalnog sertifikata
4. personalizacija bezbednosnog nosioca (izdavanje i zapis sertifikata, štampanje podataka vlasnika),
5. štampanje lične lozinke (PIN koda),
6. isporučivanje digitalnog sertifikata i lične lozinke (PIN koda), kao i dostavljanje obavještenja vlasniku.

Digitalni sertifikat na bezbednom mediju i odgovarajuća lična lozinka (PIN kod) se vlasniku isporučuje lično na šalterima prijemne službe, u dve odvojene pošiljke, na dva različita šaltera.

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

4.3.2 OBAVEŠTENJE VLASNIKU O IZDAVANJU SERTIFIKATA

Pogledati prethodno poglavlje.

4.4. PREUZIMANJE DIGITALNOG SERTIFIKATA

4.4.1 POSTUPAK PREUZIMANJA DIGITALNOG SERTIFIKATA

Preuzimanje digitalnih sertifikata se vrši tako što budući vlasnik primi digitalni sertifikat na bezbednom mediju i odgovarajuću ličnu lozinku (PIN kod) lično na šalterima prijemne službe HALCOM BG CA, pogledati poglavlje 4.3.1.

4.4.2 OBJAVLJIVANJE DIGITALNOG SERTIFIKATA

Postupak je opisan u 2. poglavlju.

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 digitalnog sertifikata.

4.5. OBAVEZE I ODGOVORNOSTI KORISNIKA VEZANE NA KORIŠĆENJE DIGITALNIH SERTIFIKATA

4.5.1 OBAVEZE VLASNIKA DIGITALNOG SERTIFIKATA

Vlasnik, odnosno budući vlasnik, digitalnog sertifikata je dužan:

- Upoznati se i postupati u skladu sa ovom politikom sertifikacije pre izdavanja digitalnog sertifikata,
- Postupati u skladu sa ovom politikom sertifikacije i ostalim važećim propisima,
- Nakon preuzimanja digitalnog sertifikata proveriti podatke u sertifikatu i o eventualnim greškama ili problemima odmah obavestiti prijemnu službu ili HALCOM BG CA
- Pratiti sva obaveštenja HALCOM BG CA i postupati u skladu sa istima,
- u skladu sa obaveštenjima primereno osavremenjivati potrebnu mašinsku i programsku opremu za bezbedan rad sa digitalnim setifikatima,
- odmah obavestiti sertifikaciono telo HALCOM BG CA o svim promenama koje su povezane sa digitalnim sertifikatom,
- zahtevati opoziv digitalnog sertifikata u slučaju da je privatni ključ bio ugrožen na način koji utiče na sigurnost upotrebe ili ako postoji opasnost od zloupotrebe,
- korišćenje digitalnog 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, digitalnog sertifikata je u odnosu na bezbednost privatnog ključa dužan takođe da:

- podatke za preuzimanje digitalnog sertifikata brižljivo čuva od neovlašćenih lica,
- čuva privatni ključ i digitalni sertifikat na način i na sredstvima za bezbedno čuvanje privatnih ključeva u skladu sa obaveštanjima 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 lozinku za zaštitu privatnog ključa,
- nakon isteka valjanosti odnosno nakon opoziva digitalnog sertifikata postupa u skladu sa obaveštenjima sertifikacionog tela HALCOM BG CA

4.5.2 OBAVEZE TREĆIH LICA

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

- Postupati i koristiti digitalne sertifikate u skladu i namenom definisanom ovom politikom sertifikacije i ostalim važećim propisima,
- Brižno proučiti sve mogućnosti rizikovanja i odgovornosti kod korišćenja digitalnih sertifikata i odrediti politiku načina upotrebe,
- Obavestiti HALCOM BG CA ako sazna da su privatni ključevi vlasnika digitalnog 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 digitalnom sertifikatu,
- Brinuti za arhiv dokumenata,
- Uzdati se u digitalno sertifikat samo za namere određene u sertifikatu (pogledati poglavlje 6.1.7.) na način koji određuje politika sertifikacije,
- Za vreme korišćenja digitalnog sertifikata proveriti da li se sertifikat nalazi u registru opozvanih sertifikata,
- Za vreme korišćenja digitalnog sertifikata proveriti da li je digitalni potpis sertifikata kreiran u vreme važenja i sa odgovarajućom namenom digitalnog sertifikata,
- Za vreme korišćenja digitalnog sertifikata proveriti potpis digitalnog 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 digitalnih sertifikata.
- Uvažavanje drugih odredaba ukoliko je sa sertifikacionim telom HALCOM BG CA sklopila dogovor o korišćenju digitalnih 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 digitalnih sertifikata.

4.6. PONOVO IZDAVANJE DIGITALNOG SERTIFIKATA

Produžavanje validnosti digitalnog sertifikata je moguće samo dostavljanjem posebne molbe/narudžbenice od strane vlasnika.

Nakon isteka validnosti digitalnog sertifikata, vlasnik mora ponovno da dostavi zahtev za reizdavanje digitalnog sertifikata.

4.6.1 OKOLNOSTI KOJE ZAHTEVAJU PONOVO IZDAVANJE DIGITALNOG

SERTIFIKATA

Pre isteka validnosti digitalnog sertifikata, dostavljanjem elektronskog zahteva za ponovnim izdavanjem digitalnog sertifikata, vlasnici sertifikata obezbeđuju kontinuitet korišćenja digitalnog sertifikata.

Zahtev za novo izdavanje je moguće uložiti i nakon isteka validnosti digitalno sertifikata.

4.6.2 LICA KOJA MOGU DA TRAŽE PONOVO IZDAVANJE DIGITALNOG SERTIFIKATA

Samo vlasnik digitalnog sertifikata može da traži ponovno izdavanje sertifikata.

4.6.3 POSTUPAK OBRADJE ZAHTEVA ZA PONOVO IZDAVANJE DIGITALNOG SERTIFIKATA

Postupak garantuje da je pravno, odnosno fizičko, lice koje uloži zahtev za ponovno izdavanje digitalnog sertifikata bez promene javnog ključa doista vlasnik sertifikata.

4.6.4 OBAVEŠTENJE VLASNIKU O NOVO IZDATOM DIGITALNOM SERTIFIKATU

Pogledati poglavlje 4.3.2.

4.6.5 POSTUPAK PREUZIMANJA NOVO IZDATOG DIGITALNOG SERTIFIKATA

Pogledati poglavlje 4.4.1.

4.6.6 OBJAVLJIVANJE NOVO IZDATOG DIGITALNOG SERTIFIKATA

Postupak je opisan u 2. poglavlju.

4.6.7 OBAVEŠTENJE SERTIFIKACIONJOG TELA O IZDAVANJU DIGITALNOG SERTIFIKATA DRUGIM SUBJEKTIMA

Sertifikaciono telo o izdavanju pojedinačnih digitalnih 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.

4.7.3 POSTUPAK ZA IZDAVANJE ZAHTEVA ZA OBNAVLJANJE KLJUČEVA

Nije primenljivo u ovoj CP.

4.7.4 OBAVEŠTENJE VLASNIKU DIGITALNOG CERTIFIKATA O NOVO IZDATOM CERTIFIKATU

Nije primenljivo u ovoj CP.

4.7.5 POSTUPAK PREUZIMANJA

Nije primenljivo u ovoj CP.

4.7.6 OBJAVA DIGITALNOG CERTIFIKATA IZDAVAOCA CERTIFIKATA SA NOVIM PAROM KLJUČEVA

Nije primenljivo u ovoj CP.

4.7.7 OBAVEŠTENJE OD STRANE CERTIFIKACIONOG TELA O IZDAVANJU CERTIFIKATA DRUGIM SUBJEKTIMA

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

4.8. PROMENA DIGITALNOG CERTIFIKATA

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

Za dobijanje novog digitalnog sertifikata potrebno je ponoviti postupak za sticanje novog sertifikata kao što je navedeno u potpogl. 4.1.

4.8.1 OKOLNOSTI ZA PROMENU DIGITALNOG CERTIFIKATA

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 DIGITALNOG CERTIFIKATA

Nije primenljivo u ovoj CP.

4.8.5 PREUZIMANJE PROMENJENOG DIGITALNOG CERTIFIKATA

Nije primenljivo u ovoj CP.

4.8.6 OBJAVLJIVANJE PROMENJENOG DIGITALNOG CERTIFIKATA

Nije primenljivo u ovoj CP.

4.8.7 OBAVEŠTENJE DRUGIH SUBJEKATA O PROMENI

Nije primenljivo u ovoj CP.

4.9. OPOZIV I SUSPENZIJA DIGITALNOG SERTIFIKATA

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

1. promene karakterističnog imena (DN),
2. kada vlasnik sertifikata promeni ključne podatke, vezane za digitalni sertifikat (ime ili prezime, elektronsku adresu, zaposlenje i slično)
3. kada se ustanovi ili sumnja da je došlo bilo do pronevere ili zloupotrebe privatnog ključa za digitalno potpisivanje,
4. zamenjivanja digitalnog sertifikata drugim sertifikatom (npr. kod gubitka bezbednosnog nosioca, gubitka lozinke/PIN za pristup podacima na kartici i slično).

Sertifikaciono telo HALCOM BG CA može da opozove digitalni sertifikat bez zahteva vlasnika u slučajevima navedenim u prvom paragrafu ili na osnovu zahteva nadležnog suda, prekršajnih organa ili drugih administrativnog organa.

Opoziv digitalnog sertifikata je moguć 24 sata dnevno. Precizna uputstva za opoziv digitalnog 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 najkasnije u roku od dvadestčetiri (24) sata. U slučaju da dođe do nepredvidivih okolnosti, sertifikaciono telo HALCOM BG CA će izuzetno da opozove digitalni sertifikat najkasnije u roku od 48 (četrdesetosam) sati nakon prijema pravilnog zahteva za opoziv istog. U tom će roku opozvani digitalni sertifikat da bude označen u javnom imeniku kao opozvan i biće dodat u registar opozvanih sertifikata (CRL). U slučaju da vlasnik diggitalnog 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 digitalnog 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.

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

- da je podatak u digitalnom sertifikatu pogrešan ili da je sertifikat izdat na osnovu pogrešnih podataka,
- da je došlo do greške kod provere identiteta podataka 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 digitalnim sertifikatima,
- da je infrastruktura digitalnog sertifikata 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 digitalnih 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 digitalnog 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 radi o mogućnosti zloupotrebe ili nepouzdanosti digitalnog sertifikata, a inače u vreme koje prema važećem zakonodavstvu važi za radno vreme državnih organa,

Ako se opoziv zahteva:

- Lično - potrebno je ispuniti odgovarajući zahtev za opoziv digitalnog sertifikata i predati ga registracionom telu;
- Elektronski - vlasnik sertifikata mora da dostavi sertifikacionom telu HALCOM BG CA elektronsku poruku sa zahtevom za opoziv.

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

Sudovi i administrativni organi koji takođe mogu da zahtevaju opoziv digitalnih 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:

- Najkasnije u roku od dvadestečetiri (24) sata opozove sertifikat ukoliko se radi o opozivu iz razloga opasnosti zloupotrebe ili nepouzdanosti sertifikata, ili sumnje da je proneveren privatni ključ vlasnika sertifikata,
- A inače prvog radnog dana nakon prijema zahteva za opoziv

Nakon opoziva, opozvani digitalni sertifikat se odmah upisuje u registar opozvanih sertifikata (CRL).

4.9.6 ZAHTEVI ZA PROVERAVANJE REGISTRA OPOZVANIH SERTIFIKATA ZA TREĆA LICA

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

- Nakon svakog opoziva sertifikata,
- Jedanput dnevno ako nema novih zapisa odnosno promena u registru opozvanih sertifikata, i to 24 sata nakon poslednje obnove CRL.

4.9.8 VREME OBJAVLJIVANJA REGISTRA OPOZVANIH SERTIFIKATA

Objavljivanje novog registra opozvanih sertifikata izvrši se:

- U javnom imeniku na serveru ldap.halcom.si odmah,
- A na web stranici <http://domina.halcom.si/crls> sa zakašnjenjem od najviše deset (10) minuta.

4.9.9 SINHRONA PROVERA STATUSA SERTIFIKATA

Protokol za sinhronu proveru statusa sertifikata - OCSF (engl. *Online Certificate Status Protocol*) nije podržan.

4.9.10 ZAHTEVI ZA SINHRONU PROVERU STATUSA SERTIFIKATA

Treća lica moraju u slučaju korišćenja datog digitalnog sertifikata uvek da provere, da li je sertifikat u koji se pouzdaju opozvan.

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

U slučaju da vlasnik sertifikata telefonski, elektronski ili FAX-om dostavlja 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 digitalni 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.si putem LDAP protokola i na <http://domina.halcom.si/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

Nisu propisane.

4.11. PREKID ODNOSA VLASNIKA I SERTIFIKACIONOG TELA

Odnos vlasnika i overavača prekida se ako:

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

4.12. OTKRIVANJE KOPIJE KLJUČEVA ZA DEŠIFROVANJE

4.12.1 RAZLOZI ZA OTKRIVANJE KOPIJE KLJUČEVA ZA DEŠIFROVANJE

Nije podržano.

4.12.2 KO ZAHTEVA OTKRIVANJE KOPIJE KLJUČEVA ZA DEŠIFROVANJE

Nije podržano.

4.12.3 POSTUPAK KOD ZAHTEVA ZA OTKRIVANJE KOPIJE KLJUČEVA ZA DEŠIFROVANJE

Nije podržano.

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, FIPS 140-1 level 3 i 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 protivprovalnog 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.

Sertifikacionog 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 internom 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.

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.

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 digitalnim sertifikatima.

Ovlašćenim licima sertifikacionog tela HALCOM BG CA smatraju se:

- zaposleni u sertifikacionom telu HALCOM BG CA i
- 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 digitalnim 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 digitalnim sertifikatima	Sistem administrator		
	Prvi inženjeri bezbednosti	1. Upravljanje postupcima za izdavanje sertifikata 2. Štampanje PIN kodova 3. Pristup protokolu digitalnog potpisivanja (generisanja) sertifikata	2
	Drugi inženjer bezbednosti	1. Priprema digitalnih sertifikata 2. Personalizacija smart kartica 3. Opoziv digitalnih sertifikata	2
	Administratori sertifikata	distribucija sertifikata	1
	Administratori PIN kodova	distribucija PIN kodova	1
Upravljanje informacionim sistemom	Sistem operator	Upravljanje telekomunikacijama i odgovornost za rad bezbednih sistema sertifikacionog tela	2
	Sistem evidentičar	Odgovornost za pregledanje i 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

Broj osoba: 2

Zadaci:

1. Odgovornost za administriranje i implementaciju bezbednosnih funkcija i procedura
2. Upravljanje aktivnostima na dodatnom unapređenju poslova generisanja, opoziva i suspenzije kvalifikovanih elektronskih sertifikata

Organizaciona jedinica: Upravljanje digitalnim sertifikatima

Uloga: prvi inženjer bezbednosti

Broj osoba: 2

Zadaci:

1. Upravljanje postupcima za izdavanje sertifikata
2. Pomoć podređenim sertifikacionim telima
3. Ovlašćenja podređenih sertifikacionih tela
4. Štampanje PIN kodova
5. Pristup protokolu digitalnog potpisivanja (generisanja) sertifikata

Organizaciona jedinica: Upravljanje digitalnim sertifikatima

Uloga: drugi inženjer bezbednosti

Broj osoba: 2

Zadaci:

1. Priprema digitalnih sertifikata (obrada potpisanih zahteva za sertifikate)
2. Personalizacija smart kartica (izrada digitalnih sertifikata, programiranje smart kartica (generisanje ključeva i upis izgenerisanog sertifikata na smart karticu), štampanje podataka vlasnika na smart karticu - vizuelna personalizacija)
3. Opoziv digitalnih sertifikata

Organizaciona jedinica: Upravljanje digitalnim sertifikatima

Uloga: administrator sertifikata

Broj osoba: 1

Zadaci:

1. Bezbedna distribucija sertifikata vlasnicima

Organizaciona jedinica: Upravljanje digitalnim sertifikatima

Uloga: administrator PIN kodova

Broj osoba: 1

Zadaci:

1. Distribucija PIN kodova

Organizaciona jedinica: Upravljanje informacionom sistemom

Uloga: sistem operator

Broj osoba: 2

Zadaci:

1. Priprema početne konfiguracije sistema, uključujući bezbedno startovanje i obustavu operativnog rada sistema
2. Početno podešavanje parametara novih podređenih sertifikacionih tela u infrastrukturi HALCOM BG CA
3. Postavljanje početne konfiguracije računarske mreže
4. Priprema medijuma za krizni ponovni start sistema u slučaju katastrofalnog gubitka sistema, tj. incidenta sa katastrofalnim posledicama
5. Priprema sistemskih kopija, nadgradnja i obnova programske opreme, bezbedno čuvanje i distribucija kopija i nadgradnji na odvojenu lokaciju
6. Administrativne funkcije koje su vezane na održavanje baze podataka sertifikacionog tela i koje pomažu kod istraživanja eventualnog odstupanja od pravila
7. Promene imena servera i/ili mrežnih IP adrese
8. Sprovođenje arhiviranja zahtevanih sistemskih zapisa

Organizaciona jedinica: Upravljanje informacionom sistemom

Uloga: sistem evidentičar

Broj osoba: 2

Zadaci:

1. Pregledanje i 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.

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 digitalnim 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.

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.

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

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/registratoruski materijal:

- dnevnike,
- zapisnike,
- sva dokazna sredstva o izvršenoj proveri identiteta vlasnika sertifikata,
- sve zahteve za dobijanjem sertifikata,
- digitalne 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 trajno.

5.5.3 ZAŠTITA DUGOTRAJNO ČUVANIH PODATAKA

Podaci koji se čuvaju dugotrajno se bezbedno čuvaju.

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 digitalnog 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 OVERAVAČA 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.

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.

6. TEHNIČKI BEZBEDNOSNI ZAHTEVI

6.1. GENERISANJE I ZAŠTITA KLJUČEVA

6.1.1 GENERISANJE KLJUČEVA

Asimetrični par ključeva sertifikacionog tela HALCOM BG CA za digitalno 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:

- Digital signature – za potrebe digitalnog potpisivanja i verifikacije digitalnog potpisa vlasnika
- Nonrepudiation sertifikat – za eventualne naknadne primene (u ovom trenutku se ne koristi)

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 koda.

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

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

- u javnom imeniku ldap.halcom.si putem LDAP protokola (pogledati poglavlje 2.3),
- putem web stranice sertifikacionog tela

6.1.5 DUŽINA ASIMETRIČNIH KLJUČEVA

Sertifikat	Dužina ključa prema RSA [bit]	
Sertifikat sertifikacionog tela HALCOM BG CA	1024	
Sertifikati za korisnike	Digital signature	1024
	Nonrepudiation	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.509 v3 standardom i definisana je u odgovarajućoj ekstenziji sertifikata: *korišćenje ključa* (engl. *keyUsage*) i *prošireno korišćenje ključa* (engl. *extended keyUsage*).

Digitalno 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 digitalnog sertifikata sertifikacionog tela. U tom smislu, *keyUsage* ekstenzija u sertifikatu sertifikacionog tela sadrži odgovarajuće vrednosti.

Profili digitalnih 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 FIPS 140-2 nivo 3 i Common Criteria EAL4+.

6.2.2 NADZOR PRISTUPA PRIVATNOM KLJUČU OD STRANE OVLAŠĆENIH LICA SERTIFIKACIONOG TELA

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

Nije primenljivo.

6.2.5 ARHIVIRANJE PRIVATNOG KLJUČA

Nije primenljivo.

6.2.6 PRENOS PRIVATNOG KLJUČA IZ/U KRIPTOGRAFSKI MODUL

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

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

6.2.7 ČUVANJE PRIVATNOG KLJUČA U KRIPTOGRAFSKOM MODULU

Asimetrični par ključeva (privatni i javni) sertifikacionog tela se generiše u HSM uređaju i samo se čuvaju u okviru HSM uređaja.

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 iščitati 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

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 EBB BEOGRAD CA2	Privatni ključ	15 godina
	Javni ključ	15 godina
Digital signature sertifikat	Privatni ključ	3 godine
	Javni ključ	3 godine
Nonrepudiation sertifikat	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 kodovi za pristup karticama koji se generišu u sertifikacionom telu HALCOM BG CA.

PIN kod za smart karticu, kao i administrativni PIN kod za deblokadu kartica (PUK kod) generišu se i štampaju na specijalnim PIN kovertama u okviru sertifikacionog tela HALCOM BG CA.

Vlasnik može da promeni PIN kod nakon preuzimanja.

6.4.2 ZAŠTITA LOZINKE

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

Sertifikaciono telo HALCOM BG CA isporučuje vlasniku sertifikata oba koda/lozinke preporučenom poštom, a u iznimnim ih slučajevima isporuči lično u okviru registracionog tela.

Sertifikaciono telo HALCOM BG CA preporučuje da se oba koda čuvaju na sigurnom mestu koje je dostupno samo vlasniku.

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 SERTIFIKACIONOG TELA CIKLUSA

6.6.1 NADZOR RAZVOJA SISTEMA

Sertifikaciono telo HALCOM BG CA upotrebljava programsku opremu proizvođača Nexus (Švedska) koja je sertifikovana u skladu sa FIPS 140-2 nivo 2 ili 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.

7. PROFIL SERTIFIKATA I REGISTRA OPOZVANIH SERTIFIKATA

7.1. PROFIL SERTIFIKATA

Na osnovu ove politike sertifikacije, sertifikaciono telo HALCOM BG CA izdaje dve vrste sertifikata za pravna lica:

- Digital signature sertifikate za digitalno potpisivanje i šifrovanje
- Nonrepudiation sertifikate za neke buduće primene

Digitalni sertifikati koje izdaje sertifikaciono telo HALCOM BG CA zadovoljavaju standard X.509 v3.

7.1.1 VERZIJE SERTIFIKATA

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

7.1.2 PROFIL SERTIFIKATA SA KORIŠĆENIM EKSTENZIJAMA

Podaci u sertifikatima su navedeni su sledećooj tabeli.

Nazivi polja	Vrednost odnosno značenje
Osnovna polja u sertifikatima	
Verzija engl. <i>Version</i>	V3
Identifikaciona oznaka sertifikata (serijski broj) engl. <i>Serial Number</i>	<i>Jedinstven interni broj sertifikata u okviru sertifikacionog tela EBB BEOGRAD CA2</i>
Algoritam za digitalni potpis, engl. <i>Signature algorithm</i>	sha1RSA (OID1.2.840.113549.1.1.5)
Izdavalac engl. <i>Issuer</i>	CN=EBB Beograd CA 2 O=Halcom 2.5.4.54 = EBBBG2 C=SI
Validnost, engl. <i>Validity</i>	Valid from: < <i>početak validnosti prema GMT</i> > Valid to: < <i>kraj vaidnosti prema GMT</i> >
Vlasnik, engl. <i>Subject</i>	<i>karakteristično ime vlasnika, u zavisnosti od vrste sertifikata, pogledati poglavlje 3.1.1.</i>

Algoritam za upotrebu javnog ključa, engl. <i>Subject Public Key Algorithm</i>	rsaEncryption (OID 1.2.840.113549.1.1.1)
Javni ključ, engl. <i>Public Key (... bits)</i>	<i>modulus, eksponent, ...</i>
Ekstenzije u okviru X.509v3 standarda	
Objava registra opozvanih sertifikata, OID 2.5.29.31, engl. <i>CRL Distribution Points</i>	URL=ldap://ldap.halcom.si/cn=EBB%20Beograd%20OCA%202,o=Halcom,c=SI?certificaterevocationlist;
korišćenje ključa, OID 2.5.29.15, engl. <i>Key Usage</i>	Digital Signature (standardni sertifikat), Key Encipherment (standardni sertifikat), Non-Repudiation (nonrepudiation sertifikat)
Identifikator javnog ključa sertifikacionog tela, OID 2.5.29.35, engl. <i>Authority Key Identifier</i>	KeyID= 45 42 42 5f 42 47
Identifikator ključa vlasnika, OID 2.5.29.14, engl. <i>Subject Key Identifier</i>	<i>identifikator ključa vlasnika</i>
Politika sertifikacije po kojoj je sertifikat izdat, OID 2.5.29.32, engl. <i>certificatePolicies</i>	Certificate Policy: Policy Identifier= 1.3.6.1.4.1.5939.1.3.1
Osnovna ograničenja, OID 2.5.29.19, engl. <i>Basic Constraints</i>	Subject Type=End Entity

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

Vlasnik sertifikata u jednom trenutku može imati samo jedan validan sertifikat odgovarajuće vrste.

7.1.3 IDENTIFIKACIONE OZNAKE KRIPTOGRAFSKIH ALGORITAMA

Digitalni 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 poglavleje 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= EBB Beograd CA 2

O = Halcom

2.5.4.54 = EBBBG2

C = SI

Registar opozvanih sertifikata se obnavlja nakon svakog opoziva, odnosno najmanje jedanput dnevno ako nema novih opoziva, odnosno promena u registru opozvanih sertifikata (ili svakih 24 sata).

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 imeniku 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. <i>Version</i>	V2
Algoritam za digitalni potpis CRL, engl. <i>Signature Algorithm</i>	sha1RSA
Potpis sertifikacionog tela, engl. <i>Signature</i>	<i>potpis EBB BEOGRAD CA2</i>
Karakteristično ime sertifikacionog tela engl. <i>Issuer</i>	CN=EBB Beograd CA 2 O=Halcom 2.5.4.54 = EBBBG2 C=SI
Vreme izdavanja CRL, engl. <i>thisUpdate</i>	Effective date: < <i>vreme izdavanja prema GMT</i> >
Vreme izdavanja sledeće CRL, engl. <i>nextUpdate</i>	Next Update: < <i>vreme izdavanja sledeće CRL prema GMT</i> >
Identifikacione oznake (serijski brojevi) opozvanih sertifikata i vreme opoziva, engl. <i>revokedCertificate</i>	Serial Number: < <i>identifikaciona oznaka (serijski broj) opozvanog digitalnog sertifikata</i> > Revocation Date: < <i>vreme opoziva prema GMT</i> >
Ekstenzije X.509v2 CRL	
redni broj CRL engl. <i>CRL number</i>	Redni broj izdatog registra opozvanih sertifikata
identifikator ključa sertifikacionog tela, engl. <i>Authority Key Identifier (OID 2.5.29.35)</i>	KeyID= 45 42 42 5f 42 47

Opozvani digitalni 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 imeniku na serveru ldap.halcom.si putem LDAP protokola i <http://domina.halcom.si/crls> putem HTTP protokola.

7.3. PROFIL OCSP

Protokol za online 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 OSPODOBLJENOST 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 digitalnim 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.

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 DIGITALNIM SERTIFIKATIMA

Pristup javnom imeniku sertifikata je besplatan osim ako se stranke ne dogovore drugačije.

9.1.3 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.

9.1.4 CENE DRUGIH USLUGA SERTIFIKACIONOG TELA

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

9.1.5 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.

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.

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 u 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 šifrjuje 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 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 imeniku sertifikata i 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

Overavač HALCOM BG CA dužan 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 digitalnih 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 digitalni sertifikat i objaviti opozvani sertifikat u registru opozvanih sertifikata u slučaju uslova i razloga definisanih ovom politikom sertifikacije ili drugim važećim propisima,
- Izdavati digitalne sertifikate u skladu sa ovom politikom sertifikacije i ostalim propisima i preporukama.

Sertifikaciono telo HALCOM BG CA dužno je:

- Osigurati tačnost podataka u izdanim sertifikatima,
- Osigurati pravilnost objavljivanja registra opozvanih sertifikata,
- Osigurati jednoznačnost karakterističnih imena,
- 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 sedmici/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 na bezbedan način 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:

- 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 sertifikata od strane neovlašćenih lica,
- Svaku drugu štetu koja nastane iz nepoštovanja odredaba 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 digitalni 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 korisit dati sertifikat za neku kriptografsku operaciju, pouzdano da proveri da li je sertifikat povučen, tj. da li se nalazi u registru opozvanih sertifikata.

Odgovarajuće ovlašćeno lice datog pravnog lica, koje nije lice koje je vlasnik sertifikata ovlašćeno od strane istog pravnog lica, dužno je da zahteva opoziv datog sertifikata ako sazna da je privatni ključ koji je pridružen datom sertifikatu ugrožen na način koji utiče na bezbednost korišćenja, ili ako postoji opasnost zloupotrebe, ili ako su se promenili podaci navedeni u sertifikatu.

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

Treće lice može bilo kada da zahteva sve informacije vezane za validnost bilo kog izdatog sertifikata, odredbe ove politike sertifikacije, kao i za bilo koja obaveštenja izdata od strane sertifikacionog tela HALCOM BG CA.

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:

- Korišćenje sertifikata za namene i na način koji nije izričito predviđen u ovoj politici sertifikacije,
- nepravilnog ili pogrešnog obezbeđenja lozinki 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 i neverodostojnim podacima, ili drugim radnjama vlasnika sertifikata ili sertifikacionog tela,
- 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 digitalnij sertifikata,
- postupanja vlasnika sertifikata u slučaju korišćenja sertifikata u slučajevima u kojima vlasnik ili treće lice poštuje sve odredbe ove politike sertifikacije, informacije ili obaveštenja objavljena od strane sertifikacionog tela HALCOM BG CA ili drugih važećih propisa,
- upotrebe i pouzdanosti rada mašinske i programske opreme vlasnika sertifikata.

9.8. OGRANIČENJE VEZANO NA KORIŠĆENJE SERTIFIKATA

Sertifikaciono telo HALCOM BG CA garantuje za vrednost pojedinačnog pravnog posla vezanog za digitalni sertifikat pravnog lica u vrednosti do visine 1 (jedan) milion eura.

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 smislaono 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

Prilikom objavljivanja nove politike sertifikacije, svi digitalni 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 digitalni 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

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

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

Kontaktne 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 VALIDOST 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 može da odredi 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.

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 inspeksijska 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.