

**Pružalac usluga od poverenja  
Halcom a.d  
Beograd (HALCOM BG CA)  
Politika pružanja usluga**

**Za izdavanje kvalifikovanih sertifikata za  
elektronski potpis fizičkih lica**

**CPName: HALCOM BG CA FL e-signature**

**CPOID:1.3.6.1.4.1.5939.11.2.4**

**Dokument važi od: 12.07.2019.**

Pregled prethodnih izdanja:

<b>Izdanje</b>	<b>Broj dokumenata i priloga</b>	<b>Opis izmene</b>	<b>Autor</b>	<b>Datum poslednje izmene</b>
<b>1</b>	79-6-4/10	Početno izdanje	Ana Stojaković	01.10.2010.
<b>2</b>	79-9-5/15	Dopuna vezana za kvalifikovane sertifikate za fizička lica	Ana Stojaković	18.12.2015.
<b>3</b>	79-10-8/17	Novi podređeni/intermediate sertifikati	Ana Teodosić	16.08.2017.
<b>4</b>	79-12-3/18	Nova CA struktura i usklađivanje sa novim zakonom	Ana Graovac	19.10.2018.
<b>5</b>	79-12-34/19	Izmena profila korisničkih sertifikata – dodavanje AR ID BROJA u CN	Ana Graovac	05.07.2019

## SADRŽAJ

<b>1. UVOD .....</b>	<b>10</b>
<b>1.1. PREGLED.....</b>	<b>10</b>
<b>1.2. NAZIV DOKUMENATA I IDENTIFIKACIJA .....</b>	<b>10</b>
<b>1.3. SUBJEKTI .....</b>	<b>11</b>
1.3.1 Pružalac usluga od poverenja HALCOM BG CA.....	11
1.3.2 Registraciona tela HALCOM BG CA.....	11
1.3.3 Naručioci i vlasnici sertifikata.....	11
1.3.4 Treće strane .....	11
<b>1.4. UPOTREBA KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA.....</b>	<b>12</b>
1.4.1 Prihvatljivo korišćenje kvalifikovanih elektronskih sertifikata.....	12
1.4.2 Nedoželjena upotreba .....	12
<b>1.5. UPRAVLJANJE DOKUMENTIMA.....</b>	<b>12</b>
1.5.1 Organizacija administriranja dokumenata.....	12
1.5.2 Ovlašćene kontakt osobe .....	13
1.5.3 Lice odgovorno za usklađenost CP dokumenta .....	13
1.5.4 Procedura odobravanja CP dokumenta.....	13
<b>1.6. SKRAĆENICE I IZRAZI .....</b>	<b>13</b>
1.6.1 Skraćenice .....	13
1.6.2 Izrazi.....	14
<b>2. ODGOVORNOSTI ZA PUBLIKACIJE I REPOZITORIJUME.....</b>	<b>15</b>
<b>2.1. LISTA DOKUMENATA .....</b>	<b>15</b>
<b>2.2. REGISTAR SERTIFIKATA.....</b>	<b>15</b>
<b>2.3. UČESTANOST OBJAVLJIVANJA.....</b>	<b>15</b>
<b>2.4. UPRAVLJANJE PRISTUPOM DO LISTE DOKUMENATA .....</b>	<b>16</b>
<b>3. IDENTIFIKACIJA I PROVERA KORISNIKA .....</b>	<b>16</b>
<b>3.1. DODELA IMENA.....</b>	<b>16</b>
3.1.1 Tipovi imena.....	16
3.1.2 Zahtevi kod kreiranja jedinstvenog imena .....	17
3.1.3 Anonimni korisnici i korišćenje pseudonima .....	17
3.1.4 Pravila za interpretaciju različitih formi imena.....	17
3.1.5 Jedinstvenost imena .....	17
3.1.6 Zaštićena imena ili robne marke .....	17
<b>3.2. PROVERAVA IDENTITETA VLASNIKA SERTIFIKATA PRI PRVOM IZDAVANJU SERTIFIKATA .....</b>	<b>17</b>
3.2.1 Metod za posedovanje privatnog ključa.....	18
3.2.2 Proveravanje identiteta organizacije .....	18
3.2.3 Proverava identiteta vlasnika sertifikata .....	18
3.2.4 Neprovereni podaci u sertifikatima .....	18
3.2.5 Provera identiteta zaposlenih za dobijanje sertifikata .....	18

3.2.6 Međusobno priznavanje .....	18
<b>3.3. IDENTIFIKACIJA I PROVERA ZAHTEVA ZA OBNAVLJANJE KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA .....</b>	<b>19</b>
3.3.1 Identifikacija vlasnika sertifikata prilikom obnavljanja sertifikata.....	19
3.3.2 Identifikacija i provera za obnavljanje sertifikata nakon opoziva .....	19
<b>3.4. IDENTIFIKACIJA I PROVERA ZAHTEVA ZA OPOZIV KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA .....</b>	<b>19</b>
<b>4. UPRAVLJANJE SERTIFIKATIMA .....</b>	<b>19</b>
<b>4.1. ZAHTEV ZA DOBIJANJE KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA .....</b>	<b>19</b>
4.1.1 Ko može da zahteva kvalifikovani elektronski sertifikat .....	19
4.1.2 Proces dostavljanja zahteva za izdavanje kvalifikovanog elektronskog sertifikata (enrolment) i odgovornosti .....	19
<b>4.2. PROCESIRANJE ZAHTEVA ZA DOBIJANJE KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA .....</b>	<b>20</b>
4.2.1 Proveravanje identiteta korisnika .....	20
4.2.2 Potvrđivanje ili odbijanje zahteva za dobijanje kvalifikovanog sertifikata korisnika .....	20
4.2.3 Potrebno vreme procesiranja zahteva korisnika .....	20
<b>4.3. IZDAVANJE KVALIFIKOVANIH ELEKTRONSKOG SERTIFIKATA .....</b>	<b>21</b>
4.3.1 Postupak izdavanja kvalifikovanih elektronskih sertifikata HALCOM BG CA .....	21
4.3.2 Obaveštenje vlasnika o izdavanju sertifikata.....	21
<b>4.4. PREUZIMANJE KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA .....</b>	<b>21</b>
4.4.1 Postupak preuzimanja kvalifikovanog elektronskog sertifikata .....	21
4.4.2 Objavljivanje kvalifikovanog elektronskog sertifikata .....	21
4.4.3 Obaveštenje trećih strana o izdatom sertifikatu .....	21
<b>4.5. OBAVEZE I ODGOVORNOSTI KORISNIKA.....</b>	<b>21</b>
<b>SERTIFIKATA.....</b>	<b>21</b>
4.5.1 Obaveze vlasnika sertifikata .....	21
4.5.2 Obaveze i odgovornosti trećih strana .....	22
<b>4.6. OBNAVLJANJE KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA .....</b>	<b>22</b>
4.6.1 Uslovi za obnavljanje kvalifikovanih elektronskih sertifikata.....	23
4.6.2 Ko može zahtevati obnavljanje kvalifikovanog elektronskog sertifikata .....	23
4.6.3 Procesiranje zahteva za obnavljanjem kvalifikovanih elektronskih sertifikata .....	23
4.6.4 Obaveštenje korisnika da mu je izdat obnovljeni kvalifikovani elektronski sertifikat .....	23
4.6.5 Sprovođenje procesa preuzimanja obnovljenog kvalifikovanog elektronskog sertifikata .....	23
4.6.6 Objavljivanje obnovljenog kvalifikovanog elektronskog sertifikata.....	23
4.6.7 Obaveštenje trećih strana od strane HALCOM BG CA o obnovi datog kvalifikovanog elektronskog sertifikata.....	23
<b>4.7. REGENERACIJA PARA KLJUČEVA I KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA .....</b>	<b>24</b>
4.7.1 Uslovi za regeneraciju para ključeva kvalifikovanog elektronskog sertifikata .....	24
4.7.2 Ko može da zahteva regeneraciju ključeva .....	24
4.7.3 Procesiranje zahteva za regeneraciju ključeva .....	24
4.7.4 Obaveštenje korisnika da mu je izdat novi kvalifikovani elektronski sertifikat.....	24

4.7.5 Postupak preuzimanja .....	24
4.7.6 Objavljivanje novog kvalifikovanog elektronskog sertifikata od strane CA.....	24
4.7.7 Obaveštavanje drugih entiteta od strane CA o izdavanju novog kvalifikovanog elektronskog sertifikata.....	24
<b>4.8. PROMENA KVALIFIKOVANOG ELEKTRONSKOG .....</b>	<b>24</b>
<b>SERTIFIKATA.....</b>	<b>24</b>
4.8.1 Uslovi za promenu kvalifikovanog elektronskog sertifikata.....	24
4.8.2 Ko može da zahteva promenu kvalifikovanog elektronskog sertifikata.....	24
4.8.3 Procesiranje zahteva za promenu kvalifikovanog elektronskog sertifikata .....	25
4.8.4 Obaveštavanje korisnika da mu je izdat novi kvalifikovani elektronski sertifikat .....	25
4.8.5 Sprovođenje procesa prihvatanja novog promenjenog kvalifikovanog elektronskog sertifikata.....	25
4.8.6 Objavljivanje novog promenjenog kvalifikovanog elektronskog sertifikata od strane CA	25
4.8.7 Obaveštenje drugih entiteta od strane CA o izdavanju novog promenjenog kvalifikovanog elektronskog sertifikata.....	25
<b>4.9. OPOZIV I SUSPENZIJA KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA .....</b>	<b>25</b>
4.9.1 Razlozi za opoziv kvalifikovanih elektronskih sertifikata.....	26
4.9.2 Ko može zahtevati opoziv kvalifikovanih elektronskih sertifikata .....	26
4.9.3 Procedura podnošenja zahteva za opoziv kvalifikovanih elektronskih sertifikata .....	26
4.9.4 Vreme za izdavanja zahteva za opozivom kvalifikovanih elektronskih sertifikata .....	27
4.9.5 Vreme za koje CA mora da procesira zahtev za opoziv kvalifikovanih elektronskih sertifikata .....	27
4.9.6 Zahtevi za treće strane u vezi provere statusa kvalifikovanih elektronskih sertifikata ....	27
4.9.7 Frekvencija izdavanja registra opozvanih sertifikata (CRL) .....	27
4.9.8 Vreme objave registra opozvanih sertifikata (CRL) .....	27
4.9.9 Raspoloživost procedure „on line“ provere statusa kvalifikovanih elektronskih sertifikata .....	28
4.9.10 Zahtevi „on line“ provere statusa kvalifikovanih elektronskih sertifikata .....	28
4.9.11 Raspoloživost drugih formi objavljivanja statusa kvalifikovanih elektronskih sertifikata	28
4.9.12 Specijalni zahtevi u odnosu na kompromitaciju privatnog ključa .....	28
4.9.13 Uslovi za suspenziju kvalifikovanih elektronskih sertifikata .....	28
4.9.14 Ko može zahtevati suspenziju kvalifikovanih elektronskih sertifikata .....	28
4.9.15 Procedura zahteva za suspenzijom kvalifikovanih elektronskih sertifikata .....	28
4.9.16 Ograničenje perioda suspenzije kvalifikovanih elektronskih sertifikata.....	28
<b>4.10. SERVISI PROVERE STATUSA KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA</b>	<b>29</b>
4.10.1 Pristup za provere .....	29
4.10.2 Raspoloživost servisa .....	29
4.10.3 Druge informacije za proveravanje statusa .....	29
<b>4.11. PRESTANAK KORIŠĆENJA KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA .</b>	<b>29</b>
<b>4.12. OTKRIVANJE KOPIJE KLJUČEVA ZA DEŠIFROVANJE .....</b>	<b>29</b>
4.12.1 Razlozi za otkrivanje kopije ključeva za dešifrovanje.....	29
4.12.2 Ko može zahtevati kopiju ključeva za dešifrovanje .....	29

4.12.3 Postupak kod zahteva kopijom ključeva za dešifrovanje .....	29
--	----

## **5. UPRAVNE, OPERATIVNE I FIZIČKE BEZBEDNOSNE KONTROLE ..... 29**

### **5.1. FIZIČKE BEZBEDNOSNE KONTROLE ..... 30**

5.1.1 Lokacija i zgrada pružaoca usluga od poverenja .....	30
5.1.2 Fizički pristup .....	30
5.1.3 Električno napajanje i klimatizacija .....	30
5.1.4 Zaštita od poplava .....	31
5.1.5 Prevencija i zaštita od požara .....	31
5.1.6 Medijumi za čuvanje podataka .....	31
5.1.7 Odlaganje otpada .....	31
5.1.8 Čuvanje podataka na udaljenoj lokaciji .....	31

### **5.2. ORGANIZACIONA PRUŽAOCA USLUGA OD POVERENJA ..... 31**

5.2.1 Organizacione grupe .....	31
5.2.2 Broj osoba za pojedinačne zadatke .....	33
5.2.3 Identifikacija i provera za svaku ulogu .....	35
5.2.4 Uloge koje zahtevaju razdvajanje dužnosti .....	36

### **5.3. KADROVSKE BEZBEDNOSNE KONTROLE ..... 36**

5.3.1 Kvalifikacija i iskustvo .....	36
5.3.2 Provera zaposlenih .....	36
5.3.3 Dodatne obuke zaposlenih .....	36
5.3.4 Učestalost i zahtevi ponovne obuke .....	36
5.3.5 Frekvencija i sekvenca rotacije poslova .....	36
5.3.6 Kaznene mere u odnosu na zaposlene za neautorizovane aktivnosti .....	36
5.3.7 Zahtevi za nezavisna lica pod ugovorom .....	36
5.3.8 Dokumentacija koja se dostavlja zaposlenima .....	37

### **5.4. PROVERE BEZBEDNOSNI SISTEMA ..... 37**

5.4.1 Vrste evidencija .....	37
5.4.2 Frekvencija proveravanja evidencija .....	37
5.4.3 Period čuvanja audit logova .....	37
5.4.4 Zaštita audit logova .....	37
5.4.5 Procedure backup-a audit logova .....	37
5.4.6 Sistem sakupljanje audit logova .....	37
5.4.7 Obaveštavanje subjekta koji je prouzrokovao događaj .....	37
5.4.8 Procena ranjivosti sistema .....	38

### **5.5. ARHIVIRANJE ZAPISA ..... 38**

5.5.1 Tipovi arhiviranih zapisa .....	38
5.5.2 Period čuvanja arhive .....	38
5.5.3 Zaštita arhive .....	38
5.5.4 Procedura backup-a arhive .....	38
5.5.5 Zahtevi za vremenskim pečatom zapisa .....	38
5.5.6 Sistem sakupljanja zapisa .....	39

5.5.7 Procedure za dobijanje i verifikaciju informacija iz arhive .....	39
<b>5.6. IZMENA KLJUČEVA PRUŽAOCA USLUGA OD POVERENJA.....</b>	<b>39</b>
<b>5.7. KOMPROMITACIJA I OPORAVAK U SLUČAJU KATASTROFE .....</b>	<b>39</b>
5.7.1 Procedure za postupanje u incidentnim i kompromitujućim situacijama.....	39
5.7.2 Računarski resursi, softver ili podaci koji su oštećeni .....	39
5.7.3 Procedure koje se sprovode kod kompromitacije privatnog ključa korisnika .....	39
5.7.4 Plan poslovanja nakon katastrofe .....	39
<b>5.8 ZAVRŠETAK RADA CA ILI RA.....</b>	<b>39</b>
<b>6. TEHNIČKE BEZBEDNOSNE KONTROLE .....</b>	<b>40</b>
<b>6.1. GENERISANJE I INSTALACIJA ASIMETRIČNOG PARA KLJUČEVA .....</b>	<b>40</b>
6.1.1 Proces generisanja asimetričnog para ključeva HALCOM BG CA pružaoca usluga od poverenja.....	40
6.1.2 Dostava privatnog ključa vlasnicima .....	40
6.1.3 Dostava javnog ključa korisnika pružaocu usluga od poverenja .....	41
6.1.4 Dostava javnog ključa pružaoca usluga od poverenja korisnicima i trećim licima .....	41
6.1.5 Dužine ključeva .....	41
6.1.6 Generisanje kriptografskih parametara i provera kvaliteta.....	41
6.1.7 Moguće „Key Usage“ opcije - svrha ključeva i sertifikata .....	41
<b>6.2. ZAŠTITA PRIVATNOG KLJUČA I TEHNIČKE KONTROLE KRIPTOGRAFSKOG MODULA .....</b>	<b>42</b>
6.2.1 Standardi i kontrole kriptografskog hardverskog modula .....	42
6.2.2 Kontrola privatnog ključa od strane ovlašćenih osoba .....	42
6.2.3 Otkrivanje kopije privatnog ključa .....	42
6.2.4 Backup ključeva HALCOM BG CA pružaoca usluga od poverenja.....	42
6.2.5 Arhiviranje privatnog ključa.....	42
6.2.6 Transfer privatnog ključa na hardverski kriptografski modul .....	42
6.2.7 Čuvanje privatnog ključa na hardverskom kriptografskom modulu .....	42
6.2.8 Metoda aktivacije privatnog ključa.....	43
6.2.9 Metoda deaktiviranja privatnog ključa.....	43
6.2.10 Metoda uništavanja privatnog ključa .....	43
6.2.11 Karakteristike kriptografskih hardverskih modula .....	43
<b>6.3. NEKI DRUGI ASPEKTI UPRAVLJANJA PAROM KLJUČEVA.....</b>	<b>43</b>
6.3.1 Arhiviranje javnog ključa.....	43
6.3.2 Periodi validnosti kvalifikovanog elektronskog sertifikata i privatnog ključa.....	43
<b>6.4. AKTIVACIONI PODACI.....</b>	<b>44</b>
6.4.1 Generisanje i instalacija aktivacionih podataka.....	44
6.4.2 Zaštita aktivacionih podataka .....	44
6.4.3 Drugi aspekti u vezi aktivacionih podataka .....	44
<b>6.5. BEZBEDNOSNE KONTROLE RAČUNARA .....</b>	<b>44</b>
6.5.1 Specifični zahtevi za bezbednost računara .....	44
6.5.2 Nivo bezbednosti.....	44
<b>6.6. ŽIVOTNI CIKLUS TEHNIČKIH BEZBEDNOSNIH KONTROLA .....</b>	<b>44</b>

6.6.1	Kontrole sistemskog razvoja.....	44
6.6.2	Kontrole upravljanja bezbednošću.....	44
6.6.3	Životni ciklus bezbednosnih kontrola.....	45
<b>6.7.</b>	<b>MREŽNE BEZBEDNOSNE KONTROLE.....</b>	<b>45</b>
<b>6.8.</b>	<b>VREMENSKI PEČAT.....</b>	<b>45</b>
<b>7.</b>	<b>PROFIL KVALIFIKOVANOG SERTIFIKATA CRL I OCSP.....</b>	<b>45</b>
<b>7.1.</b>	<b>PROFILI KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA.....</b>	<b>45</b>
7.1.1	Broj verzije.....	45
7.1.2	Ekstenzije u sertifikatu.....	45
7.1.3	Identifikacione oznake kriptografskih algoritama.....	50
7.1.4	Forme imena.....	51
7.1.5	Ograničenja imena.....	51
7.1.6	Objektni identifikator.....	51
7.1.7	Ograničenja upotrebe.....	51
7.1.8	Sintaksa i semantika „Policy Qualifier“-sa.....	51
7.1.9	Značenje bitnih dodataka politike.....	51
<b>7.2.</b>	<b>PROFIL REGISTRA OPOZVANIH SERTIFIKATA (CRL).....</b>	<b>51</b>
7.2.1	Broj verzije.....	51
7.2.2	CRL i CRL entry ekstenzije.....	52
7.2.3	Objava registra opozvanih sertifikata.....	53
<b>7.3.</b>	<b>OCSP PROFIL (PROFIL U TOKU PROVERE STATUSA SERTIFIKATA).....</b>	<b>53</b>
7.3.1	Broj verzije.....	54
7.3.2	OCSP ekstenzije.....	54
<b>8.</b>	<b>PROVERA USKLAĐENOSTI I DRUGA OCENJIVANJA.....</b>	<b>54</b>
<b>8.1.</b>	<b>FREKVENCIJA ILI USLOVI OCENJIVANJA.....</b>	<b>54</b>
<b>8.2.</b>	<b>IDENTITET/KVALIFIKACIJE PROCENJIVAČA.....</b>	<b>54</b>
<b>8.3.</b>	<b>ODNOS OCENJIVAČA PREMA OCENJIVANOM ENTITETU - NEZAVISNOST NADZORA.....</b>	<b>54</b>
<b>8.4.</b>	<b>PODRUČJA NADZORA.....</b>	<b>54</b>
<b>8.5.</b>	<b>AKTIVNOSTI PREDUZETE KAO REZULTAT UTVRĐENIH NEDOSTATAKA.....</b>	<b>55</b>
<b>8.6.</b>	<b>OBJAVLJIVANJE REZULTATA NADZORA.....</b>	<b>55</b>
<b>9.</b>	<b>DRUGI POSLOVNI I PRAVNI ASPEKTI.....</b>	<b>55</b>
<b>9.1.</b>	<b>CENE.....</b>	<b>55</b>
9.1.1	Cene izdavanja ili obnove kvalifikovanih elektronskih sertifikata.....	55
9.1.2	Cena pristupa sertifikatima.....	55
9.1.3	Cena pristupa informacijama o statusu kvalifikovanih elektronskih sertifikata i registru opozvanih sertifikata.....	55
9.1.4	Cene za druge servise.....	55
9.1.5	Povratak troškova.....	55
<b>9.2.</b>	<b>FINANSIJSKA ODGOVORNOST.....</b>	<b>55</b>
9.2.1	Pokrivenost osiguranjem.....	55
9.2.2	Druga dobra.....	56



9.2.3 Osiguranje ili garancijska pokrivenost za krajnje korisnike .....	56
<b>9.3 POVERLJIVOST POSLOVNIH INFORMACIJA .....</b>	<b>56</b>
9.3.1 Opseg poverljivih informacija.....	56
9.3.2 Informacije koje nisu u opsegu poverljivih informacija .....	56
9.3.3 Odgovornost za zaštitu poverljivih informacija .....	56
<b>9.4. PRIVATNOST LIČNIH PODATAKA.....</b>	<b>56</b>
9.4.1 Plan privatnosti.....	56
9.4.2 Informacije koje se tretiraju kao privatne.....	57
9.4.3 Informacije koje se ne smatraju privatnim .....	57
9.4.4 Odgovornost za zaštitu privatnih informacija .....	57
9.4.5 Obaveštenje i saglasnost za korišćenje privatnih informacija .....	57
9.4.6 Otkrivanje informacija shodno pravnim i administrativnim procesima .....	57
9.4.7 Druge okolnosti za otkrivanje informacija.....	57
<b>9.5. PRAVA INTELEKTUALNOG VLASNIŠTVA .....</b>	<b>57</b>
<b>9.6. PREDSTAVLJANJA I GARANCIJE .....</b>	<b>58</b>
9.6.1 HALCOM BG CA predavljanja i garancije .....	58
9.6.2 Obaveze i odgovornosti registracionih tela.....	59
9.6.3 Obaveze i odgovornosti vlasnika sertifikata .....	59
9.6.4 Obaveze i odgovornosti trećih lica .....	59
9.6.5 Obaveze i odgovornosti drugih lica .....	59
<b>9.7. OGRANIČENJE ODGOVORNOSTI .....</b>	<b>59</b>
<b>9.8. OGRANIČENJE U UPOTREBI .....</b>	<b>60</b>
<b>9.9. ODŠTETE.....</b>	<b>60</b>
<b>9.10. PERIOD VAŽENJA I KRAJ VALIDNOSTI OVE POLITIKE.....</b>	<b>60</b>
9.10.1 Važnost.....	61
9.10.2 Kraj validnosti.....	61
9.10.3 Efekat završetka i ponovnog rada.....	61
<b>9.11. POJEDINAČNA OBAVEŠTENJA I KOMUNIKACIJA SA UČESNICIMA .....</b>	<b>61</b>
<b>9.12. ISPRAVKE, MODIFIKACIJE I DOPUNE.....</b>	<b>61</b>
9.12.1 Procedure za ispravku, modifikaciju ili dopune .....	61
9.12.2 Mehanizam i period obaveštavanja .....	62
9.12.3 Promena identifikacionog broja politike pružanja usluga od poverenja.....	62
<b>9.13. ODREDBE REŠAVANJA SPOROVA .....</b>	<b>62</b>
<b>9.14. VAŽEĆE ZAKONODAVSTVO .....</b>	<b>62</b>
<b>9.15. USKLAĐENOST SA VAŽEĆIM ZAKONODAVSTVOM.....</b>	<b>62</b>
<b>9.16. OPŠTE ODREDBE.....</b>	<b>62</b>
<b>9.17. DRUGE ODREDBE .....</b>	<b>62</b>

## 1. UVOD

- (1) Pružalac usluga od poverenja HALCOM BG CA za implementaciju svojih usluga u oblasti elektronskog potpisivanja koristi najsigurnije tehnologije, uključujući korišćenje bezbednih prenosioca podataka.
- (2) Ova politika je javni deo internih pravila HALCOM BG CA za kvalifikovane elektronske sertifikate za fizička lica.
- (3) Sadržaj ove politike je u skladu sa važećim zakonom i podzakonskim aktima Republike Srbije, uredbom eIDAS, ETSI tehničkim zahtevima, standardom IETF RFC i drugim srodnim standardima.

### 1.1. PREGLED

- (1) Ova politika pružanja usluga uređuje nameru, delovanje i metodologiju upravljanja kvalifikovanim elektronskim sertifikatima, te zahteve bezbednosti koje mora da ispunjava pružalac usluga od poverenja HALCOM BG CA, vlasnici sertifikata, treća lica koji se uzdaju u te sertifikate, te odgovornost svih pomenutih lica.
- (2) HALCOM BG CA je pružalac usluga od poverenja koje izdaje i upravlja kvalifikovanim elektronskim sertifikatima za verifikaciju elektronskog potpisa. HALCOM BG CA deluje u okviru Halcom a.d. Beograd.
- (3) HALCOM BG CA izdaje kvalifikovan elektronski sertifikat (par asimetričnih ključeva) sa obaveznim korišćenjem bezbednosnog nosioca (smart kartice/USB ključa) za fizička lica za potrebe bezbednog elektronskog plaćanja u Srbiji putem servisnog centra Halcom a.d. Beograd, elektronskog potpisivanja jednostranih ili međusobnih komunikacija vlasnika sertifikata te korišćenja u različitim aplikacijama i za različite namene koje se pojavljuju na tržištu.
- (4) Sve odredbe ove politike vezane za delovanje HALCOM BG CA su propisno i detaljno opisane u dokumentu Opšta pravila rada (CPS) i detaljnije utvrđene u odredbama internih pravila rada pružaoca usluga od poverenja koja predstavljaju dokumente poverljive prirode i koji definišu infrastrukturu, odredbe u vezi sa zaposlenim u HALCOM BG CA (nadležnosti, zadaci, ovlašćenja i zahtevani uslovi pojedinih zaposlenih), fizičku zaštitu (pristup prostorijama, upravljanje hardverskom i programskom opremom), programsku zaštitu (zaštitni softver, zaštitne kopije, ...) i interni nadzor (kontrola fizičkih pristupa, ovlašćenja, ...).
- (5) HALCOM BG CA izdaje kvalifikovane elektronske sertifikate i druge usluge od poverenja u skladu sa važećim zakonom i podzakonskim aktima Republike Srbije, uredbom eIDAS, ETSI tehničkim zahtevima, standardom IETF RFC, standardom ISO/IEC i drugim srodnim standardima.
- (6) Listu registracionih tela i operatera (RA – Registration Authority) koji omogućuju podnošenje zahteva za dobijanje kvalifikovanih elektronskih sertifikata za fizička lica od HALCOM BG CA, Halcom a.d. Beograd objavljuje na svojoj web stranici.

### 1.2. NAZIV DOKUMENATA I IDENTIFIKACIJA

- (1) Identifikaciona oznaka ove politike pružanja usluga od poverenja HALCOM BG CA FL e-signature je:

Kvalifikovani elektronski sertifikati za potpisivanje:

- CPOID:1.3.6.1.4.1.5939.11.2.4

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

### **1.3. SUBJEKTI**

#### **1.3.1 Pružalac usluga od poverenja HALCOM BG CA**

HALCOM BG CA je pružalac usluga od poverenja koji izdaje i upravlja kvalifikovanim elektronskim sertifikatima za verifikaciju elektronskog potpisa za fizička lica. Pružalac usluga od poverenja HALCOM BG CA posluje u okviru Halcom a.d. Beograd.

#### **1.3.2 Registraciona tela HALCOM BG CA**

- (1) Registraciono telo (RA ili prijavna služba) vrši sledeće aktivnosti za potrebe pružaoca usluga od poverenja:
1. proveravanje identiteta vlasnika kvalifikovanih elektronskih sertifikata, kao i proveravanje ostalih podataka važnih za upravljanje kvalifikovanim elektronskim sertifikatima,
  2. prijem zahteva za dobijanje sertifikata,
  3. prijem zahteva za opozivanje/povlačenje sertifikata,
  4. izdavanje potrebne dokumentacije vlasnicima, odnosno budućim vlasnicima, kvalifikovanih elektronskih sertifikata,
  5. prosleđivanje zahteva i ostalih podataka sigurnim putem do HALCOM BG CA.
- (2) Pružalac usluga od poverenja HALCOM BG CA može za izvršavanje zadataka registracionog tela (RA), uz svoje sopstveno RA, takođe ovlastiti i druge organizacije u poslovnom i javnom sektoru. Svaku takvu organizaciju HALCOM BG CA ugovorom obaveže za ispunjavanje strogih bezbednosnih uslova u skladu sa važećim evropskim, i nacionalnim propisima te međunarodnim, evropskim i nacionalnim standardima i preporukama, kao i internim pravilima HALCOM BG CA.
- (3) Pružalac usluga od poverenja HALCOM BG CA ima široku uspostavljenu geografsku mrežu RA (registracionih tela), što budućim vlasnicima omogućuje jednostavnu prijavu u blizini sedišta datog fizičkog lica.

#### **1.3.3 Naručioци i vlasnici sertifikata**

- (1) Vlasnici kvalifikovanih elektronskih sertifikata koriste svoje podatke (par asimetričnih ključeva), dodeljene od strane pružaoca usluga od poverenja, za elektronsko potpisivanje i kvalifikovane elektronske sertifikate za verifikaciju tog elektronskog potpisa.
- (2) Vlasnik sertifikata je fizičko lice.

#### **1.3.4 Treće strane**

- (1) Treće strane su entiteti, kao na primer fizička lica (pojedinci) i/ili pravna lica (kompanije), koja prihvataju sertifikate i verifikuju elektronski potpis određenih elektronskih dokumenata koji su potpisani od strane korisnika HALCOM BG CA, kao i koja vrše validaciju kvalifikovanih elektronskih sertifikata izdatih od strane HALCOM BG CA.
- (2) Treće strane moraju se ponašati u skladu sa uputstvima pružaoca usluga od poverenja HALCOM BG CA i moraju redovno proveravati validnost sertifikata, svrhu korišćenja sertifikata, kao i period važenja. Detaljnije obaveze i odgovornosti trećih strana su navedene u poglavlju 4.5.2. i 9.6.4.

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

## **1.4. UPOTREBA KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA**

HALCOM BG CA upravlja (izdaje i overava, opoziva, objavljuje) kvalifikovanim elektronskim sertifikatima za za elektronsko potpisivanje. Sertifikati su namenjeni fizičkim licima.

### **1.4.1 Prihvatljivo korišćenje kvalifikovanih elektronskih sertifikata**

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

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

1. identifikaciju vlasnika sertifikata,
  2. dokazivanje identiteta vlasnika sertifikata,
  3. potpisivanje dokumenata u elektronskom obliku i njihovu verifikaciju,
  4. šifrovanje dokumenata u elektronskom obliku primenom simetričnih kriptografskih algoritama.
- (2) Elektronski potpis može da se koristi u aplikacijama kao što su na primer:
1. elektronsko odnosno mobilno bankarstvo,
  2. aplikacije e-uprave ili m-uprave,
  3. potpisivanje elektronskih formulara,
  4. bezbedno poslovanje sa organima i organizacijama javnog sektora te ostalim pravnim ili fizičkim licima,
  5. ostale aplikacije odnosno usluge u kojima se zahteva korišćenje kvalifikovanog elektronskog sertifikata,
  6. kontrola pristupa.

### **1.4.2 Nedozvoljena upotreba**

- (1) Zabranjeno je korišćenje kvalifikovanih elektronskih sertifikata, izdatih u skladu sa ovom CP, u suprotnosti sa odredbama same politike pružanja usluge, opštih pravila rada (CPS) ili važećih propisa, ili izvan opsega dozvoljenog korišćenja, određenog u prethodnom poglavlju.
- (2) Kvalifikovani elektronski sertifikati izdati od strane HALCOM BG CA nisu namenjeni daljoj prodaji.

## **1.5. UPRAVLJANJE DOKUMENTIMA**

### **1.5.1 Organizacija administriranja dokumenata**

- (1) Sa ovim CP dokumentom, kao i ostalim opštim i internim pravilima rada, upravlja pružalac usluga od poverenja HALCOM BG CA, koji posluje u sklopu Halcom a.d. Beograd.
- (2) Adresa pružaoca usluga od poverenja:

**Halcom a.d. Beograd**  
**HALCOM BG CA**  
Beogradska 39  
11000 Beograd  
Srbija

### 1.5.2 Ovlašćene kontakt osobe

- (1) 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.
- (2) Adresa:

**Aleksandar Spremić**  
**Halcom a.d. Beograd**  
**HALCOM BG CA**  
Beogradska 39  
11000 Beograd  
Srbija  
Tel.: (+381) 11 33 06 500  
Fax: (+381) 11 33 48 994  
Mail: [ca@halcom.rs](mailto:ca@halcom.rs)  
<http://www.halcom.rs>

### 1.5.3 Lice odgovorno za usklađenost CP dokumenta

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

### 1.5.4 Procedura odobravanja CP dokumenta

- (1) Svaki predlog nove izmenjene politike pružanja usluga se razmatra sa tehnološkog i pravnog aspekta u cilju garantovanja zakonitosti, bezbednosti i kvaliteta. Nakon toga, nova politika pružanja usluge se potvrđuje od strane direktora Halcom a.d. Beograd.
- (2) Pružalac usluga od poverenja može izdati izmene i dopune ove politike u skladu sa postupkom opisanim u poglavlju 9.12.

## 1.6. SKRAĆENICE I IZRAZI

### 1.6.1 Skraćenice

<b>CA</b>	Pružalac usluga od poverenja, koji izdaje sertifikate ( <i>engl.: Certification Authority ili Certification Agency</i> ).
<b>CPName</b>	Ime politike rada pružaoca usluga od poverenja ( <i>engl.: Certification Policy Name</i> ), jednoznačno povezan sa međunarodno jedinstvenim brojem politike pružanja usluge CPOID ( <i>engl.: Certification Policy Object Identifier</i> ).
<b>CPOID</b>	Međunarodni broj koji jednoznačno definiše politiku ( <i>engl.: Certification Policy Object Identifier</i> ).
<b>CRL</b>	<i>Certificate Revocation List</i> – registar opozvanih kvalifikovanih elektronskih sertifikata
<b>DN</b>	Jedinstveno ime ( <i>engl.: Distinguished Name</i> ).
<b>CP</b>	Politika pružaoca usluge od poverenja ( <i>engl. Certificate Policy</i> ). Politika koja uređuje svrhu, rad i metodologiju upravljanja uslugama, odgovornosti i sigurnosnih zahteva, koje mora ispuniti pružalac usluga od poverenja, vlasnici sertifikata (korisnici usluga) i treća lica, koja se oslanjaju na ove sertifikate/usluge

<b>CPS</b>	CPS (engl. Certification Practice Statement) predstavlja opšte uslove za pružanje usluge i opšta pravila pružaoca usluga od poverenja.
<b>LDAP</b>	<i>Lightweight Directory Access Protocol</i> je protokol koji omogućava pristup sertifikatima i registru opozvanih sertifikata CRL koje izdaje pružalac usluga od poverenja a specificiran prema IETF ( <i>Internet Engineering Task Force</i> ) preporuci IETF RFC 3494.
<b>S/MIME</b>	<i>Secure Multipurpose Internet Mail Extensions</i>
<b>AR ID BROJ</b>	Identifikacioni broj korisnika u AR Registru pružaoca usluga od poverenja
<b>SSL</b>	<i>Secure Sockets Layer</i>
<b>TLS</b>	<i>Transport Layer Security</i>
<b>PKI</b>	<i>Public Key Infrastructure</i> je infrastruktura javnih ključeva
<b>HSM</b>	eng. Hardware Security Module je bezbedni kriptografski uređaj za skladištenje i upravljanje ključevima pružaoca usluge od poverenja.
<b>QSCD</b>	<i>Qualified Signature Creation Device</i> je bezbedni kriptografski uređaj za kreiranje kvalifikovanih elektronskih potpisa (npr. HSM, smart kartica, USB ključ itd.)

### 1.6.2 Izrazi

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

## **2. ODGOVORNOSTI ZA PUBLIKACIJE I REPOZITORIJUME**

### **2.1. LISTA DOKUMENATA**

- (1) Pružalac usluga od poverenja HALCOM BG CA javno objavljuje sve informacije koje se odnose na rad pružaoca usluga od poverenja, obaveštenja korisnicima i trećim licima, kao i ostale važne dokumente, na web stranicama Halcom a.d. Beograd na adresi <http://www.halcom.rs>.
- (2) Dokumenti koji su javno dostupni na web stranicama su:
  - cenovnik,
  - politika korišćenja usluga od poverenja (CP),
  - opšta pravila rada pružaoca usluga od poverenja (CPS),
  - obrasce za naručivanje i druge ugovore o uslugama pružaoca usluga od poverenja
  - uputstva za bezbedno korišćenje kvalifikovanih elektronskih sertifikata,
  - informacije o važećem zakonodavstvu vezano za rad pružaoca usluga od poverenja, ostale informacije vezane u vezi sa radom HALCOM BG CA.
- (3) Međutim, javno nisu dostupni dokumenti koji predstavljaju interna pravila pružaoca usluga od poverenja HALCOM BG CA.

### **2.2. REGISTAR SERTIFIKATA**

- (1) Nove politike objavljuju se u skladu sa navodima u poglavlju 9.10.
- (2) Svi sertifikati pružaoca usluga od poverenja su zasnovani na standardu X.509 i objavljeni su u centralnom direktorijumu na serveru [ldap.halcom.rs](http://ldap.halcom.rs), kojim rukovodi HALCOM BG CA. Javno dostupan je samo deo direktorijuma u kome su opozvani sertifikati.
- (3) Opozvani sertifikati se odmah objavljuju u registru opozvanih sertifikata (detaljnije u delu 4.9.8.), dok se druge javno dostupne informacije i dokumenti objavljuju po potrebi.
- (4) Pristup direktorijumu izdatih sertifikata je omogućen samo ovlašćenim osobama, koji proveravaju veći broj izdatih sertifikata.

### **2.3. UČESTANOST OBJAVLJIVANJA**

- (1) Nove politike se objavljuju najkasnije narednog dana nakon prihvatanja.
- (2) HALCOM BG CA obezbeđuje da se sertifikati objavljuju u centralnom direktorijumu odmah (najviše 5 sekundi) nakon njihovog izdavanja.
- (3) Registar opozvanih sertifikata se osvežava odmah (najviše 5 sekundi) nakon opoziva sertifikata u javnom registru. Nakon nekoliko minuta, osvežava se i web stranica sa listom opozvanih sertifikata.
- (4) Javno dostupne informacije i dokumenti (osim gore navedenog) objavljuju se po potrebi.

## 2.4. UPRAVLJANJE PRISTUPOM DO LISTE DOKUMENATA

- (1) Registar izdatih kvalifikovanih elektronskih sertifikata je dostupan na serveru ldap.halcom.rs, TCP port 389 u skladu sa LDAP protokolom. Javno dostupan je samo deo registra, registar opozvanih sertifikata.
- (2) Odgovarajućim tehničkim uslovima (mašinska i programska oprema) HALCOM BG CA garantuje kontrole, koje sprečavaju neovlašćeno dodavanje, menjanje ili brisanje podataka u registru opozvanih kvalifikovanih elektronskih sertifikata.

## 3. IDENTIFIKACIJA I PROVERA KORISNIKA

### 3.1. DODELA IMENA

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

#### 3.1.1 Tipovi imena

- (1) U skladu sa IETF RFC 5280 svaki kvalifikovani elektronski sertifikat sadrži podatke o vlasniku i izdavaocu kvalifikovanog elektronskog sertifikata u obliku karakterističnog imena. Karakteristično ime je formirano u skladu sa IETF RFC 5280 i standardom X501.
- (2) Pružalac usluga od poverenja je u izdatom sertifikatu naveden u polju Izdavalac, engl. Issuer. Osnovni podaci o vlasniku koje sadrži karakteristično ime vlasnika kvalifikovanog elektronskog sertifikata nalaze se u izdatom sertifikatu navedeni u polju Nosilac engl. Subject.
- (3) Jedinstveni serijski broj korisnika u okviru pružaoca usluga od poverenja koji se takođe sadrži u karakterističnom imenu određuje izdavalac HALCOM BG CA. (više u poglavlju 3.1.5.)

Vrsta sertifikata	Naziv polja	Karakteristično ime
Kvalifikovani elektronski sertifikat pružaoca usluga od poverenja HALCOM BG CA	Izdavalac engl. Issuer	CN = Halcom BG Root CA 2.5.4.97 = VATRS-102193722 2.5.4.97 = MB:RS-17419722 O = Halcom a.d. Beograd C = RS
Intermediate/podređeni sertifikati za fizičko lice	Izdavalac engl. Issuer	CN = Halcom BG Root CA 2.5.4.97 = VATRS-102193722 2.5.4.97 = MB:RS-17419722 O = Halcom a.d. Beograd C = RS
	Korisnik eng. Subject	CN = Halcom BG CA FL e-signature 2.5.4.97 = VATRS-102193722 2.5.4.97 = MB:RS-17419722 O = Halcom a.d. Beograd C = RS
Kvalifikovani elektronski sertifikat za fizička lica	Izdavalac engl. Issuer	CN = Halcom BG CA FL e-signature 2.5.4.97 = VATRS-102193722 2.5.4.97 = MB:RS-17419722 O = Halcom a.d. Beograd C = RS



	Korisnik eng. Subject	E= <elektronska pošta> SERIALNUMBER = PNORS-<JMBG> ili SERIALNUMBER = PASGB-<broj pasoša> ili SERIALNUMBER = IDCRS-<broj lične karte> i SERIALNUMBER = CA:RS-<AR ID BROJ> G = <ime> SN = <prezime> CN = <ime i prezime AR ID BROJ> C = RS
--	--------------------------	--

### 3.1.2 Zahtevi kod kreiranja jedinstvenog imena

Oznaka fizičkog lica, koja je u skladu sa opisanim poglavlju 3.1.1, uključen u jedinstveno ime, mora ispunjavati sledeće uslove:

- mora biti jednoznačno povezan sa nosiocem,
- maksimalna dužina može biti četrdeset dva (42) karaktera.

### 3.1.3 Anonimni korisnici i korišćenje pseudonima

HALCOM BG CA ne izdaje anonimne sertifikate korisnicima.

### 3.1.4 Pravila za interpretaciju različitih formi imena

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

Znak	Transformacija
Ū	Ue
Ö	Oe
Ø	Oe
ß	Ss
Ñ	N
Ř	Rz

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

### 3.1.5 Jedinstvenost imena

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

### 3.1.6 Zaštićena imena ili robne marke

- (1) Vlasnici kvalifikovanih elektronskih sertifikata ne smeju da zahtevaju imena koja pripadaju nekome drugome čime bi se kršila prava trećih lica.
- (2) Eventualne sporove rešavaju isključivo oštećena strana i vlasnik kvalifikovanog elektronskog sertifikata.

## 3.2. PROVERAVA IDENTITETA VLASNIKA SERTIFIKATA PRI PRVOM IZDAVANJU SERTIFIKATA

Budući vlasnik kvalifikovanog elektronskog sertifikata mora da zahteva kvalifikovani elektronski sertifikat u svoje lično ime.

### 3.2.1 Metod za posjedovanje privatnog ključa

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

### 3.2.2 Proveravanje identiteta organizacije

Nije primenljivo u ovoj CP.

### 3.2.3 Proverava identiteta vlasnika sertifikata

- (1) Proveravanje identiteta vlasnika kvalifikovanog sertifikata izvršava operater registracionog tela HALCOM BG CA, odnosno ovlašćeni kurir kurirske službe sa kojom pružalac usluge od poverenja ima potpisan ugovor o bezbednoj distribuciji sertifikata, tako što proveri lične podatke o vlasniku na osnovu ličnog identifikacionog dokumenta, a po potrebi i u odgovarajućim registrima.
- (2) Dakle, u cilju identifikacije i autentifikacije korisnika koji aplicira za dobijanje kvalifikovanog sertifikata za fizičko lice od strane HALCOM BG CA, CA može primeniti korake koji uključuju ali nisu ograničeni na:
  - provera dokumenata kao što su lična karta i pasoš, u skladu sa važećim zakonom za pojedinca – fizičko lice za sebe lično,
  - utvrđivanje identiteta datog pojedinca koja se bazira na dostavljenoj dokumentaciji,
  - zahtev je da se pojedinac fizički pojavi u registracionom telu (RA), odnosno da se lično identifikuje pred ovlašćenim kurirom.

### 3.2.4 Neprovereni podaci u sertifikatima

HALCOM BG CA ne proverava tačnosti i rada e-mail adrese vlasnika kvalifikovanog elektronskog sertifikata za fizička lica.

### 3.2.5 Provera identiteta zaposlenih za dobijanje sertifikata

Nije primenljivo u ovoj CP.

### 3.2.6 Međusobno priznavanje

- (1) Pružalac usluga od poverenja HALCOM BG CA nije dužan ugovorno saradivati ili garantovati za ostale pružaoce usluga od poverenja čak iako drugi pružalac usluga od poverenja ima status kvalifikovanog pružaoce usluga od poverenja za izdavanje kvalifikovanih elektronskih sertifikata.
- (2) HALCOM BG CA obezbeđuje da će ispoštovati međusobnu saradnju sa drugim pružaoce usluga od poverenja isključivo nakon potpisivanja pismenog ugovora sa drugim pružaoce usluga od poverenja koji moraju da ispune nivo sigurnosnih zahteva koje su uporedive ili više od onih koje propisuje HALCOM BG CA.
- (3) Ovlašćena lica HALCOM BG CA proveravaju opšta i interna pravila drugog pružaoce usluga od poverenja, kao i njegovo ispunjavanje sigurnosnih zahteva, ukoliko nema spoljne i nezavisne ocene usklađenosti drugog pružaoce usluge od poverenja
- (4) Troškove potrebne infrastrukture koju zahteva HALCOM BG CA za međusobno priznavanje pokriva drugi pružalac usluga od poverenja, osim ukoliko nije ugovorom dogovoreno drugačije.

### **3.3. IDENTIFIKACIJA I PROVERA ZAHTEVA ZA OBNAVLJANJE KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA**

#### **3.3.1 Identifikacija vlasnika sertifikata prilikom obnavljanja sertifikata**

Provera identiteta vlasnika sertifikata prilikom obnove sertifikata vrši:

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

#### **3.3.2 Identifikacija i provera za obnavljanje sertifikata nakon opoziva**

Provera identiteta vlasnika je u skladu sa odredbama u poglavlju 3.2.3

### **3.4. IDENTIFIKACIJA I PROVERA ZAHTEVA ZA OPOZIV KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA**

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

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

(2) Detaljan postupak opoziva: Poglavlje 4.9.3.

## **4. UPRAVLJANJE SERTIFIKATIMA**

### **4.1. ZAHTEV ZA DOBIJANJE KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA**

#### **4.1.1 Ko može da zahteva kvalifikovani elektronski sertifikat**

Budući vlasnici kvalifikovanih elektronskih sertifikata izdanih prema ovoj politici uvek su fizička lica.

#### **4.1.2 Proces dostavljanja zahteva za izdavanje kvalifikovanog elektronskog sertifikata (enrolment) i odgovornosti**

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

- (2) Narudžbenica se predaje registracionom telu (RA) HALCOM BG CA. Narudžbenica i cenovnik usluga se nalazi na web stranici HALCOM BG CA.
- (3) Narudžbenice za izdavanje kvalifikovanog elektronskog sertifikata dostupne su kako kod registracionih tela (RA) HALCOM BG CA tako i na web stranici HALCOM BG CA.
- (4) Pre izdavanja narudžbenice, HALCOM BG CA je u obavezi da upozna budućeg vlasnika sa ovim CP dokumentom, kao i sa ostalim informacijama o elektronskom potpisivanju i operativnom radu pružaoca usluga od poverenja HALCOM BG CA.
- (5) HALCOM BG CA zadržava pravo da negativno reši molbu korisnika za izdavanje kvalifikovanog elektronskog sertifikata ako je u suprotnosti sa važećim propisima Republike Srbije ili Evropske Unije.

## **4.2. PROCESIRANJE ZAHTEVA ZA DOBIJANJE KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA**

### **4.2.1 Proveravanje identiteta korisnika**

- (1) Ovlašćeno lice registracionog tela HALCOM BG CA proverava identitet budućeg vlasnika. Budući vlasnik mora da dokaže svoj identitet važećim ličnim dokumentom sa fotografijom, ličnim prisustvom prilikom preuzimanja sertifikata u registracionom telu, odnosno ovlašćenom kuriru kurirske službe pružaoca usluge od poverenja. Pod ličnim identifikacionim dokumentom smatraju se važeća lična karta i pasoš.
- (2) Ovlašćena lica registracionog tela i kurirska služba dužni su da provere identitet vlasnika sertifikata, odnosno sve one podatke koji su navedeni u narudžbenici a dostupni su u službenim evidencijama odnosno u drugim službeno važećim dokumentima.
- (3) Ovlašćena lica registracionog tela proveravaju ispunjene molbe/narudžbenice, kao i dopunsku originalnu dokumentaciju koja se zahteva, prosleđuju je pružaocu usluga od poverenja HALCOM BG CA.

### **4.2.2 Potvrđivanje ili odbijanje zahteva za dobijanje kvalifikovanog sertifikata korisnika**

- (1) Nakon toga, HALCOM BG CA ili RA potvrđuju ili odbijaju zahtev za izdavanje kvalifikovanih elektronskih sertifikata. Takvo potvrđivanje ili odbijanje neophodno je da bude obrazloženo lično ili e-mailom podnosiocu ili bilo kojoj drugoj strani ako je u suprotnosti sa poslovnim i etičkim standardima za koje se zalaže HALCOM BG CA.
- (2) Nakon potvrđivanja zahteva za izdavanje kvalifikovanih elektronskih sertifikata, RA šalje zahtev za izdavanje kvalifikovanih elektronskih sertifikata do HALCOM BG CA pružaoca usluga od poverenja.

### **4.2.3 Potrebno vreme procesiranje zahteva korisnika**

HALCOM BG CA se po osnovu odobrene narudžbenice za izdavanje kvalifikovanog elektronskog sertifikata i izmirenih finansijskih obaveza obavezuje da najkasnije u roku od pet (5) dana izda kvalifikovani elektronski sertifikat na smart kartici/USB ključu i lozinku za upotrebu sertifikata (PIN/PUK kod) i pošalje ih odvojeno registracionom telu koje dalje distribuira sertifikate fizičkom licu kome se sertifikat izdaje.

## **4.3. IZDAVANJE KVALIFIKOVANIH ELEKTRONSKOG SERTIFIKATA**

### **4.3.1 Postupak izdavanja kvalifikovanih elektronskih sertifikata HALCOM BG CA**

- (1) Proizvodni postupak za izdavanje kvalifikovanih elektronskih sertifikata sastoji se iz jasno odvojenih koraka (ili funkcija), sa odvojenim podsistemima:
  - predpersonalizacija bezbednosnog nosioca (generisanje ključeva i PIN/PUK koda),
  - obrada zahteva za izdavanje kvalifikovanog elektronskog sertifikata,
  - priprema kvalifikovanih elektronskih sertifikata
  - personalizacija smart kartice/USB ključa (izdavanje i upis sertifikata, štampanje podataka vlasnika na smart kartici/USB ključu),
  - štampanje lične lozinke (PIN/PUK koda),
  - isporuka kvalifikovanog elektronskog sertifikata na smart kartici/USB ključu i lične lozinke (PIN/PUK koda).
- (2) Svi opisani postupci zasnovani su tako da ih ne može izvesti samostalno jedna osoba.
- (3) Kvalifikovani elektronski sertifikat na bezbednom mediju i odgovarajuća lična lozinka (PIN/PUK kod) se do registracionog tela ili samog fizičkog lica dostavlja u dva različita dana u dve odvojene pošiljke ili istog dana odvojenim kurirskim službama ili se vlasniku isporučuje lično na šalterima RA..

### **4.3.2 Obaveštenje vlasnika o izdavanju sertifikata**

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

## **4.4. PREUZIMANJE KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA**

### **4.4.1 Postupak preuzimanja kvalifikovanog elektronskog sertifikata**

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

### **4.4.2 Objavljivanje kvalifikovanog elektronskog sertifikata**

Postupak je opisan u poglavlju 2.

### **4.4.3 Obaveštenje trećih strana o izdatom sertifikatu**

Pružalac usluga od poverenja ne obaveštava druga preduzeća, odnosno organizacije, o izdavanju kvalifikovanog elektronskog sertifikata.

## **4.5. OBAVEZE I ODGOVORNOSTI KORISNIKA**

### **SERTIFIKATA**

#### **4.5.1 Obaveze vlasnika sertifikata**

- (1) Vlasnik ili budući vlasnik sertifikata dužan je:
  - da se upozna i postupa u skladu sa politikom, pre izdavanja sertifikata,

- da se pridržava politike i drugih važećih propisa,
- nakon prijema sertifikata ili aktiviranja sertifikata proveri podatke na sertifikatu, i da za bilo kakve greške ili probleme obavesti HALCOM BG CA ili zatraži opoziv sertifikata,
- prati i poštuje sva obaveštenja HALCOM BG CA,
- prema obaveštenjima, ažurira potreban hardver ili softver za siguran rad sa sertifikatima,
- da odmah obavesti HALCOM BG CA o svim promenama vezano za sertifikat,
- da zatraži opoziv sertifikata ako privatni ključ ugrožen na način koji pogađa pouzdanost upotrebe ili ako postoji rizik od zloupotrebe,
- koristi sertifikat za svrhu koja je naznačena u sertifikatu (videti poglavlje 7.1) i način koji je u skladu sa politikom HALCOM BG CA.

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

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

#### **4.5.2 Obaveze i odgovornosti trećih strana**

(1) Treća strana koja prihvata sertifikate mora:

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

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

### **4.6. OBNAVLJANJE KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA**

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

- (2) Po isteku važnosti naprednog sertifikata nosilac ima pravo da ponovo podnese zahtev za sertifikat.
- (3) Postupak podnošenja zahteva za ponovno izdavanje kvalifikovanog elektronskog sertifikata isti je kao i kod prvobitnog izdavanja.

#### **4.6.1 Uslovi za obnavljanje kvalifikovanih elektronskih sertifikata**

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

#### **4.6.2 Ko može zahtevati obnavljanje kvalifikovanog elektronskog sertifikata**

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

#### **4.6.3 Procesiranje zahteva za obnavljanjem kvalifikovanih elektronskih sertifikata**

- (1) Ponovno izdavanje kvalifikovanog elektronskog sertifikata zahteva korisnik dostavljanjem propisane dokumentacije za obnovu kvalifikovanog elektronskog sertifikata prijemnoj službi HALCOM BG CA.
- (2) Postupak garantuje da je fizičko lice koje uloži zahtev za obnovu kvalifikovanog elektronskog sertifikata doista vlasnik kvalifikovanog elektronskog sertifikata.
- (3) Pružalac usluga od poverenja obnavlja kvalifikovani elektronski sertifikat, tj. procesira dostavljeni zahtev i dostavlja obnovljeni kvalifikovani elektronski sertifikat korisniku.
- (4) Provera korisnika u cilju obnove kvalifikovanog elektronskog sertifikata vrši se na isti način kao i provera pri izdavanju kvalifikovanog elektronskog sertifikata prvi put.

#### **4.6.4 Obaveštenje korisnika da mu je izdat obnovljeni kvalifikovani elektronski sertifikat**

Pogledati poglavlje 4.3.2.

#### **4.6.5 Sprovođenje procesa preuzimanja obnovljenog kvalifikovanog elektronskog sertifikata**

Pogledati poglavlje 4.4.1.

#### **4.6.6 Objavljivanje obnovljenog kvalifikovanog elektronskog sertifikata**

Postupak je opisan u 2. poglavlju.

#### **4.6.7 Obaveštenje trećih strana od strane HALCOM BG CA o obnovi datog kvalifikovanog elektronskog sertifikata**

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

## **4.7. REGENERACIJA PARA KLJUČEVA I KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA**

### **4.7.1 Uslovi za regeneraciju para ključeva kvalifikovanog elektronskog sertifikata**

Nije primenljivo u ovoj CP.

### **4.7.2 Ko može da zahteva regeneraciju ključeva**

Nije primenljivo u ovoj CP.

### **4.7.3 Procesiranje zahteva za regeneraciju ključeva**

Nije primenljivo u ovoj CP.

### **4.7.4 Obaveštenje korisnika da mu je izdat novi kvalifikovani elektronski sertifikat**

Nije primenljivo u ovoj CP.

### **4.7.5 Postupak preuzimanja**

Nije primenljivo u ovoj CP.

### **4.7.6 Objavljivanje novog kvalifikovanog elektronskog sertifikata od strane CA**

Nije primenljivo u ovoj CP.

### **4.7.7 Obaveštavanje drugih entiteta od strane CA o izdavanju novog kvalifikovanog elektronskog sertifikata**

HALCOM BG CA o izdavanju pojedinačnog kvalifikovanog elektronskog sertifikata ne obaveštava preduzeća i druge organizacije.

## **4.8. PROMENA KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA**

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

(2) Za dobijanje novog kvalifikovanog elektronskog sertifikata potrebno je ponoviti postupak za izdavanje novog sertifikata kao što je navedeno u poglavlju 4.1.

### **4.8.1 Uslovi za promenu kvalifikovanog elektronskog sertifikata**

Nije primenljivo u ovoj CP.

### **4.8.2 Ko može da zahteva promenu kvalifikovanog elektronskog sertifikata**

Nije primenljivo u ovoj CP.



#### **4.8.3 Procesiranje zahteva za promenu kvalifikovanog elektronskog sertifikata**

Nije primenljivo u ovoj CP.

#### **4.8.4 Obaveštavanje korisnika da mu je izdat novi kvalifikovani elektronski sertifikat**

Nije primenljivo u ovoj CP.

#### **4.8.5 Sprovođenje procesa prihvatanja novog promenjenog kvalifikovanog elektronskog sertifikata**

Nije primenljivo u ovoj CP.

#### **4.8.6 Objavljivanje novog promenjenog kvalifikovanog elektronskog sertifikata od strane CA**

Nije primenljivo u ovoj CP.

#### **4.8.7 Obaveštenje drugih entiteta od strane CA o izdavanju novog promenjenog kvalifikovanog elektronskog sertifikata**

Nije primenljivo u ovoj CP.

### **4.9. OPOZIV I SUSPENZIJA KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA**

- (1) Opoziv svog kvalifikovanog elektronskog sertifikata vlasnik može da zahteva bilo kada, ali svakako mora da ga zahteva u slučaju:
  1. promene karakterističnog imena (DN),
  2. kada vlasnik sertifikata promeni ključne, lične podatke, povezane sa sertifikatom (ime ili prezime),
  3. kada se ustanovi ili sumnja da je došlo bilo do pronevere ili zloupotrebe privatnog ključa za elektronsko potpisivanje,
  4. gubitka poslovne sposobnosti, prestanka ili zabrane rada.
- (2) Pružalac usluga od poverenja HALCOM BG CA može da opozove kvalifikovani elektronski sertifikat bez zahteva vlasnika u slučajevima navedenim u prvom paragrafu ili na osnovu zahteva nadležnog suda ili drugog državnog nadležnog organa.
- (3) Opoziv kvalifikovanog elektronskog sertifikata je moguć 24 sata dnevno. Precizna uputstva za opoziv kvalifikovanog elektronskog sertifikata objavljena su na web stranicama pružaoca usluga od poverenja HALCOM BG CA.
- (4) HALCOM BG CA će na osnovu pravilnog zahteva za opoziv sertifikata, isti opozvati u roku od četiri (4) sata. U slučaju nastanka nepredviđenih okolnosti HALCOM BG CA može opozvati sertifikat u roku od osam (8) sati. Opozvani kvalifikovani elektronski sertifikat će biti označen u registru opozvanih sertifikata (CRL) prilikom izdavanja prve sledeće CRL liste. Ukoliko nije bilo opoziva sertifikata CRL lista će biti izdata najmanje na svaka dvadeset četiri sata (24). U slučaju da vlasnik kvalifikovanog elektronskog sertifikata isporuči HALCOM BG CA nepravilan zahtev za opoziv, biće mu poslato

upozorenje o nepravilnom zahtevu za opoziv sertifikata i biće upoznat sa uputstvima za dostavljanje pravilnog zahteva za opoziv.

#### 4.9.1 Razlozi za opoziv kvalifikovanih elektronskih sertifikata

- (1) Opoziv svog kvalifikovanog elektronskog sertifikata vlasnik mora da zahteva u slučaju:
  - ako je privatni ključ vlasnika sertifikata ugrožen na način koji utiče na pouzdanost i bezbednost primene,
  - ako postoji rizik zloupotrebe privatnog ključa ili sertifikata vlasnika,
  - ako su se promenili odnosno se utvrdi da su pogrešni ključni podaci navedeni u sertifikatu.
- (2) Pružalac usluga od poverenja HALCOM BG CA će opozvati sertifikat bez zahteva vlasnika odmah, ako dođe do saznanja da:
  - podaci u sertifikatu nisu ispravni ili je sertifikat izdat na osnovu netačnih podataka,
  - je došlo do greške u verifikaciji podataka u RA,
  - da su se promenile okolnosti koje utiču na ispravnost sertifikata,
  - je došlo do neispunjavanja obaveza vlasnika sertifikata,
  - nisu izmirene finansijske obaveze u vezi sa sertifikatom,
  - da je ugrožena infrastruktura pružaoca usluga od poverenja na način koji utiče na pouzdanost upotrebe,
  - je privatni ključ vlasnika sertifikata ugrožen na način koji utiče na pouzdanost upotrebe,
  - HALCOM BG CA prestane da izdaje sertifikate ili da mu se zabrani rad sa sertifikatima a drugi pružalac usluga od poverenja ne preuzme njegove aktivnosti,
  - da je opoziv naređen od strane nadležnog suda, prekršajnog ili drugog državnog organa.
- (3) Vlasnik sertifikata može zahtevati ponovno kreiranje PIN koda za kvalifikovane elektronske sertifikate, u slučaju da su podaci zaboravljeni. Pod krivičnom odgovornošću garantuje da nema mogućnosti da privatni ključ bude ugrožen na način koji utiče na pouzdanost upotrebe i da ne postoji rizik od zloupotrebe privatnog ključa ili sertifikata.

#### 4.9.2 Ko može zahtevati opoziv kvalifikovanih elektronskih sertifikata

Opoziv kvalifikovanog elektronskog sertifikata može da zahteva:

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

#### 4.9.3 Procedura podnošenja zahteva za opoziv kvalifikovanih elektronskih sertifikata

- (1) Opoziv može da zahteva vlasnik sertifikata:
  - lično u radno vreme registracionog tela,
  - elektronski, 24 sata na dan, svih dana u godini.
- (2) Ako se opoziv zahteva:
  - lično - potrebno je ispuniti odgovarajući zahtev za opoziv kvalifikovanog elektronskog sertifikata i predati ga registracionom telu,
  - elektronski - vlasnik sertifikata mora da dostavi pružaocu usluga od poverenja HALCOM BG CA elektronski potpisan zahtev za opoziv,

- telefonom ili elektronskom poštom zahteva opoziv sertifikata - na osnovu te poruke pružalac usluge od poverenja privremeno suspenduje sertifikat, a po prijemu odgovarajućeg svojeručno potpisanog zahteva za opoziv kvalifikovanog elektronskog sertifikata pružalac usluge od poverenja opoziva sertifikat.
- (3) O datumu i vremenu opoziva, podnosiocu zahteva za opoziv, kao i o uzrocima opoziva, vlasnik sertifikata mora da bude obavešten.
- (4) Sudovi i administrativni organi koji takođe mogu da zahtevaju opoziv kvalifikovanih elektronskih sertifikata, taj proces izvršavaju u skladu sa propisanim procedurama.
- (5) Odredbe koje se odnose na opoziv primenjuju se i na procedure u vezi sa ponovnim generisanjem PIN kodova za napredne sertifikate.

#### **4.9.4 Vreme za izdavanja zahteva za opozivom kvalifikovanih elektronskih sertifikata**

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

#### **4.9.5 Vreme za koje CA mora da procesira zahtev za opoziv kvalifikovanih elektronskih sertifikata**

- (1) Pružalac usluga od poverenja HALCOM BG CA je u obavezi da nakon prijema validnog zahteva za opoziv sertifikata:
- u roku od četiri (4) sata opozove kvalifikovani elektronski sertifikat, u slučaju sumnje na zloupotrebu,
  - inače, prvog radnog dana nakon prijema zahteva za opoziv.
- (2) Po opozivu, sertifikat se upisuje u listu opozvanih sertifikata odmah (najviše 5 sekundi).

#### **4.9.6 Zahtevi za treće strane u vezi provere statusa kvalifikovanih elektronskih sertifikata**

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

#### **4.9.7 Frekvencija izdavanja registra opozvanih sertifikata (CRL)**

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

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

#### **4.9.8 Vreme objave registra opozvanih sertifikata (CRL)**

(1) Objavljivanje novog registra opozvanih sertifikata vrši se:

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

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

#### **4.9.9 Raspoloživost procedure „on line“ provere statusa kvalifikovanih elektronskih sertifikata**

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

#### **4.9.10 Zahtevi „on line“ provere statusa kvalifikovanih elektronskih sertifikata**

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

#### **4.9.11 Raspoloživost drugih formi objavljivanja statusa kvalifikovanih elektronskih sertifikata**

Ovo poglavlje nije primenljivo u okviru ove CP.

#### **4.9.12 Specijalni zahtevi u odnosu na kompromitaciju privatnog ključa**

Ovo poglavlje nije primenljivo u okviru ove CP.

#### **4.9.13 Uslovi za suspenziju kvalifikovanih elektronskih sertifikata**

- (1) U slučaju da vlasnik sertifikata telefonski, elektronski ili FAX-om dostavi zahtev za opoziv sertifikata, isti se do prijema originala zahteva u pisanom obliku privremeno suspenduje.
- (2) U slučaju da vlasnik sertifikata, druga ili treća lica, državni ili drugi odgovarajući organi odnosno sam pružalac usluge od poverenja, izraze sumnju da se u vezi sa sertifikatom postupa suprotno ovoj politici pružanja usluge, odnosno važećim propisima, taj se kvalifikovani elektronski sertifikat privremeno suspenduje do konačne odluke.

#### **4.9.14 Ko može zahtevati suspenziju kvalifikovanih elektronskih sertifikata**

Pogledati poglavlje 4.9.13.

#### **4.9.15 Procedura zahteva za suspenzijom kvalifikovanih elektronskih sertifikata**

Pogledati poglavlje 4.9.13.

#### **4.9.16 Ograničenje perioda suspenzije kvalifikovanih elektronskih sertifikata**

Pogledati poglavlje 4.9.13.

## **4.10. SERVISI PROVERE STATUSA KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA**

### **4.10.1 Pristup za provere**

- (1) Registar opozvanih kvalifikovanih elektronskih sertifikata je javno objavljen na serveru <ldap://ldap.halcom.rs/> putem LDAP protokola i na <http://domina.halcom.rs/crls> putem HTTP protokola.
- (2) On-line provera statusa sertifikata je dostupna na linku <http://ocsp.halcom.rs>.
- (3) Detalji o objavljivanju i načinu pristupa nalaze se u poglavljima 7.2 i 7.3.

### **4.10.2 Raspoloživost servisa**

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

### **4.10.3 Druge informacije za proveravanje statusa**

Ovo poglavlje nije primenljivo u okviru ove CP.

## **4.11. PRESTANAK KORIŠĆENJA KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA**

Odnos vlasnika i pružaoca usluga od poverenja se prekida ako:

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

## **4.12. OTKRIVANJE KOPIJE KLJUČEVA ZA DEŠIFROVANJE**

### **4.12.1 Razlozi za otkrivanje kopije ključeva za dešifrovanje**

Ovo poglavlje nije primenljivo u okviru ove CP.

### **4.12.2 Ko može zahtevati kopiju ključeva za dešifrovanje**

Ovo poglavlje nije primenljivo u okviru ove CP.

### **4.12.3 Postupak kod zahteva kopijom ključeva za dešifrovanje**

Ovo poglavlje nije primenljivo u okviru ove CP.

## **5. UPRAVNE, OPERATIVNE I FIZIČKE BEZBEDNOSNE KONTROLE**

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

- (2) Oprema pružaoca usluga od poverenja HALCOM BG CA je postavljena u posebnim, odvojenim prostorijama i osigurana sistemom fizičkog i protiv-provalnog tehničkog obezbeđenja na više nivoa. Oprema je osigurana od neovlašćenog pristupa. Oprema je takođe obezbeđena i zaštićena protivpožarnim sistemom, sistemom protiv izliva vode, sistemom ventilacije i sistemom kontinuiranog napajanja u više nivoa.
- (3) Pružalac usluga od poverenja HALCOM BG CA čuva rezervne i distributivne medijume tako da se u najvećoj meri sprečava gubitak, upad ili neovlašćena upotreba ili promena sačuvanih informacija. Kako za obnovu podataka tako i za arhiviranje važnih informacija obezbeđene su rezervne kopije koje su sačuvane na drugom mestu od onoga gde se drži programska oprema za upravljanje sertifikata, u cilju obezbeđenja kontinuiteta poslovanja u slučajevima kada se iz nekih razloga unište podaci na osnovnoj lokaciji.
- (4) Detaljan opis infrastrukture HALCOM BG CA, operativni rad, postupci upravljanja infrastrukturom, kao i nadzor vezan za politiku bezbednosti operativnog rada, definisani su u internim pravilima rada pružaoca usluga od poverenja.

## **5.1. FIZIČKE BEZBEDNOSNE KONTROLE**

- (1) Oprema pružaoca usluga od poverenja je obezbeđena sistemima fizičkog i elektronskog obezbeđenja na više nivoa.
- (2) Obezbeđenje infrastrukture pružaoca usluga od poverenja realizuje se u skladu sa preporukama struke za najviši nivo obezbeđenja.
- (3) Celokupan opis infrastrukture pružaoca usluga od poverenja, primenjene procedure i obezbeđenje infrastrukture definisani su internim pravilima pružaoca usluga od poverenja.

### **5.1.1 Lokacija i zgrada pružaoca usluga od poverenja**

- (1) Oprema pružaoca usluga od poverenja HALCOM BG CA je postavljena u posebnim, bezbednim i odvojenim prostorijama.
- (2) Oprema je osigurana je sistemom fizičkog i elektronskog obezbeđenja na više nivoa.
- (3) Detaljne odredbe nalaze se u internim pravilima pružaoca usluga od poverenja HALCOM BG CA.

### **5.1.2 Fizički pristup**

- (1) Pristup infrastrukturi pružaoca usluga od poverenja omogućen je samo ovlašćenim licima pružaoca usluga od poverenja u skladu sa njihovim zadacima i ovlašćenjima, pogledati poglavlje 5.2.1.
- (2) Svi pristupi obezbeđeni su u skladu sa zakonodavstvom i preporukama.
- (3) Detaljne odredbe nalaze se u internim pravilima pružaoca usluga od poverenja HALCOM BG CA.

### **5.1.3 Električno napajanje i klimatizacija**

- (1) U okviru infrastrukture pružaoca usluga od poverenja obezbeđeno je kontinuiranog napajanje i odgovarajući klimatski sistemi.
- (2) Svi detalji se nalaze u internim pravilima rada pružaoca usluga od poverenja HALCOM BG CA.

#### **5.1.4 Zaštita od poplava**

- (1) Infrastruktura pružaoca usluga od poverenja HALCOM BG CA nije izložena opasnosti od poplava osim u slučaju više sile.
- (2) Svi detalji se nalaze u internim pravilima rada pružaoca usluga od poverenja HALCOM BG CA.

#### **5.1.5 Prevencija i zaštita od požara**

- (1) Prostorije pružaoca usluga od poverenja su osigurane od mogućih izbijanja požara.
- (2) Svi detalji se nalaze u internim pravilima rada pružaoca usluga od poverenja HALCOM BG CA.

#### **5.1.6 Medijumi za čuvanje podataka**

- (1) Nosioci podataka, na papiru ili u elektronskom obliku, bezbedno se čuvaju u zaštićenim prostorijama/objektima.
- (2) Bezbedne kopije programske opreme i šifrovanih baza pružaoca usluga od poverenja HALCOM BG CA redovno se obnavljaju i čuvaju u dve odvojene i fizički obezbeđene prostorije na različitim lokacijama.

#### **5.1.7 Odlaganje otpada**

- (1) HALCOM BG CA obezbeđuje sigurno uklanjanje i uništavanje dokumenata u fizičkom/papirnom i elektronskom obliku.
- (2) Uklanjanje otpadaka izvodi specijalna komisija u skladu sa internim pravilima pružaoca usluga od poverenja HALCOM BG CA.
- (3) Svi detalji o odlaganju smeća se nalaze u internim pravilima rada pružaoca usluga od poverenja HALCOM BG CA.

#### **5.1.8 Čuvanje podataka na udaljenoj lokaciji**

Pogledati poglavlje 5.1.6.

## **5.2. ORGANIZACIONA PRUŽAOCA USLUGA OD POVERENJA**

### **5.2.1 Organizacione grupe**

- (1) Operativni, organizaciono i profesionalno funkcionisanje pružaoca usluga od poverenja HALCOM BG CA rukovodi Sistem administrator, koji je odgovoran za upravljanje procedurama HALCOM BG CA.
- (2) Ovlašćenim licima pružaoca usluga od poverenja HALCOM BG CA smatraju se:
  - zaposleni u pružaocu usluga od poverenja HALCOM BG CA i
  - zaposleni u registracionim telima.
- (3) Zaposleni u HALCOM BG CA su raspoređeni u četiri organizacione jedinice koje pokrivaju područja sledećeg sadržaja:
  - upravljanje informacionim sistemom,
  - upravljanje kvalifikovanim elektronskim sertifikatima,
  - bezbednost i kontrola,
  - regulativna jedinica.

Organizaciona jedinica	Uloga	Opis osnovnih zadataka	Broj osoba
Upravljanje informacionim sistemom	Glavni sistem administrator	<ul style="list-style-type: none"> <li>• Priprema početne konfiguracije sistema,</li> <li>• Inicijalno podešavanje parametara novih podređenih pružalaca usluga od poverenja,</li> <li>• Podešavanje početne konfiguracije mreže</li> <li>• Priprema medija za ponovno pokretanje sistema u slučaju katastrofe</li> <li>• Bezbedno skladištenje i distribucija kopija i nadogradnja na odvojenoj lokaciji</li> </ul>	2
	Sistem administrator	<ul style="list-style-type: none"> <li>• Upravljanje procedurama izdavanja sertifikata</li> <li>• Pomoć podređenim pružaocima usluga od poverenja</li> <li>• Ovlašćenje potčinjenih pružalaca usluga poverenja</li> <li>• Pristup protokolu potpisivanje sertifikata</li> <li>• Bezbedno skladištenje i distribucija kopija i nadogradnja na odvojenoj lokaciji</li> </ul>	2
Upravljanje kvalifikovanim elektronskim sertifikatima	Sistem operater	<ul style="list-style-type: none"> <li>• Priprema sistemskih kopija, nadogradnja i obnova softvera, bezbedno skladištenje i distribuiranje kopija i nadogradnje</li> <li>• Administrativne funkcije vezane za održavanje</li> <li>• Izvođenje arhiviranja zahtevanih sistemskih zapisa</li> <li>• Dnevni pregled sistema</li> <li>• Štampanje PIN kodova</li> </ul>	2
	Operater za autorizaciju	<ul style="list-style-type: none"> <li>• Potvrđivanje izdavanja sertifikata i aktiviranje lozinki</li> </ul>	2
	Administrator za elektronske sertifikate	<ul style="list-style-type: none"> <li>• Predpersonalizacija pametnih kartica</li> <li>• Priprema sertifikata (obrada potpisanih zahteva za sertifikate)</li> <li>• Personalizacija (kreiranje sertifikata, upisivanje na sigurnom nosiocu, štampanje podataka vlasnika na sigurnom mediju)</li> <li>• Distribucija sertifikata</li> </ul>	2
	Administrator za PIN kodove	<ul style="list-style-type: none"> <li>• Distribucija PIN kodova</li> </ul>	2



	Službenik za prijave	<ul style="list-style-type: none"> <li>• Identifikacija vlasnika ili budućeg vlasnika sertifikata</li> <li>• Prihvatanje dokumenata za izdavanje i opoziv sertifikata</li> </ul>	2
	Službenik za opoziv	<ul style="list-style-type: none"> <li>• Priprema zahteva za opoziv</li> <li>• Opoziv sertifikata</li> </ul>	2
Bezbednost i kontrola	Glavni administrator bezbednosti	<ul style="list-style-type: none"> <li>• Određivanje sigurnosnih pravila i praćenje njihovog poštovanja</li> <li>• Pregled dokumentacije sistema i kontrolnih evidencija za praćenje rada</li> <li>• Lična saradnja i pomoć u godišnjem popisu dokumentacije podređenih pružalaca usluga od poverenja</li> </ul>	2
	Sistem evidentičar	<ul style="list-style-type: none"> <li>• Kontrola bezbednosnih pravila i njihovog poštovanja</li> <li>• Kontrola systemske dokumentacije i kontrolnih evidencija za praćenje rada</li> </ul>	2
Pravno administrativno	Poverenik za privatnost	<ul style="list-style-type: none"> <li>• Samostalno i nezavisno usmeravanje, zaštita privatnosti i zaštita ličnih podataka</li> <li>• Stručna pomoć menadžmentu i zaposlenima u operativnoj primeni mera za poštovanje privatnosti</li> </ul>	1
	Poverenik za regulativu i usklađenost	<ul style="list-style-type: none"> <li>• Obezbeđivanje usklađenosti sa važećim evropskim i domaćim propisima, međunarodnim standardima i preporukama</li> <li>• Stručna pomoć menadžmentu i zaposlenima u operativnoj primeni mera za i regulatornu usklađenost.</li> </ul>	1

### 5.2.2 Broj osoba za pojedinačne zadatke

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

**Organizaciona jedinica:** Upravljanje informacionim sistemom

**Uloga:** Glavni sistem administrator

**Broj osoba:** 2

**Zadaci:**

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

**Organizaciona jedinica:** Upravljanje informacionim sistemom

**Uloga:** Sistem administrator

**Broj osoba:** 2

**Zadaci:**

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

**Organizaciona jedinica:** Upravljanje kvalifikovanim elektronskim sertifikatima

**Uloga:** Sistem operater

**Broj osoba:** 2

**Zadaci:**

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

**Organizaciona jedinica:** Upravljanje kvalifikovanim elektronskim sertifikatima

**Uloga:** Operater za autorizaciju

**Broj osoba:** 2

**Zadaci:**

- potvrđivanje izdavanja sertifikata i aktiviranje lozinki.

**Organizaciona jedinica:** Upravljanje kvalifikovanim elektronskim sertifikatima

**Uloga:** Administrator za sertifikate

**Broj osoba:** 2

**Zadaci:**

- Predpersonalizacija pametnih kartica,
- Priprema sertifikata (obrada potpisanih zahteva za sertifikate),
- Personalizacija (kreiranje sertifikata, upisivanje na sigurnom nosiocu, štampanje podataka vlasnika na sigurnom mediju),
- Distribucija sertifikata.

**Organizaciona jedinica:** Upravljanje kvalifikovanim elektronskim sertifikatima

**Uloga:** Administrator za PIN/PUK kodove

**Broj osoba:** 2

**Zadaci:**

- distribucija PIN kodova.

**Organizaciona jedinica:** Upravljanje kvalifikovanim elektronskim sertifikatima

**Uloga:** Službenik za prijavu

**Broj osoba:** 2

**Zadaci:**

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

**Organizaciona jedinica:** Upravljanje kvalifikovanim elektronskim sertifikatima

**Uloga:** Službenik za opoziv

**Broj osoba:** 2

**Zadaci:**

- priprema zahteva za opoziv,
- opoziv sertifikata.

**Organizaciona jedinica:** Bezbednost i kontrola

**Uloga:** Glavni administrator bezbednosti

**Broj osoba:** 2

**Zadaci:**

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

**Organizaciona jedinica:** Bezbednost i kontrola

**Uloga:** Sistem evidentičar

**Broj osoba:** 2

**Zadaci:**

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

**Organizaciona jedinica:** Pravno administrativna

**Uloga:** Poverenik za privatnost

**Broj osoba:** 1

**Zadaci:**

- Samostalno i nezavisno usmeravanje, zaštita privatnosti i zaštita ličnih podataka
- Stručna pomoć menadžmentu i zaposlenima u operativnoj primeni mera za poštovanje privatnosti

**Organizaciona jedinica:** Pravno administrativna

**Uloga:** Poverenik za regulativu i usklađenost

**Broj osoba:** 1

**Zadaci:**

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

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

### 5.2.3 Identifikacija i provera za svaku ulogu

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

#### **5.2.4 Uloge koje zahtevaju razdvajanje dužnosti**

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

### **5.3. KADROVSKE BEZBEDNOSNE KONTROLE**

- (1) Operativni, organizacioni i profesionalni rad pružaoca usluga od poverenja HALCOM BG CA kontroliše sistem evidentičar koji ne radi posao upravljanja sertifikatima.
- (2) Sistem evidentičar nadgleda rad HALCOM BG CA. Sistem evidentičar u slučaju otkrivanja manjkavosti, određuje odgovarajuće mere za eliminisanje tih manjkavosti, koje je HALCOM BG CA dužan izvesti, dok sistem evidentičar nadgleda izvođenje određenih mera.

#### **5.3.1 Kvalifikacija i iskustvo**

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

#### **5.3.2 Provera zaposlenih**

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

#### **5.3.3 Dodatne obuke zaposlenih**

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

#### **5.3.4 Učestalost i zahtevi ponovne obuke**

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

#### **5.3.5 Frekvencija i sekvenca rotacije poslova**

Ovo poglavlje nije primenljivo u okviru ove CP.

#### **5.3.6 Kaznene mere u odnosu na zaposlene za neautorizovane aktivnosti**

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

#### **5.3.7 Zahtevi za nezavisna lica pod ugovorom**

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

### **5.3.8 Dokumentacija koja se dostavlja zaposlenima**

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

## **5.4. PROVERE BEZBEDNOSNI SISTEMA**

### **5.4.1 Vrste evidencija**

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

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

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

### **5.4.2 Frekvencija proveravanja evidencija**

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

### **5.4.3 Period čuvanja audit logova**

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

### **5.4.4 Zaštita audit logova**

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

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

### **5.4.5 Procedure backup-a audit logova**

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

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

### **5.4.6 Sistem sakupljanje audit logova**

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

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

### **5.4.7 Obaveštavanje subjekta koji je prouzrokovao događaj**

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

### 5.4.8 Procena ranjivosti sistema

- (1) Analiza dnevnika i nadzor nad sprovođenjem svih postupaka redovno se sprovode od strane ovlašćenih lica pružaoca usluga od poverenja ili automatski odgovarajućim sigurnosnim mehanizmima na svoj računarsko-komunikacionoj opremi koja je u nadležnosti pružaoca usluga od poverenja.
- (2) Ocena ranjivosti se sprovodi na osnovu analize dnevnika.
- (3) Detalji procene ranjivosti sistema dati su u internim pravilima rada pružaoca usluga od poverenja HALCOM BG CA.
- (4) Analiza konfiguracija sistema i njihova usaglašenost sa internim politikama redovno se sprovodi, najmanje četiri puta godišnje.

## 5.5. ARHIVIRANJE ZAPISA

### 5.5.1 Tipovi arhiviranih zapisa

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

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

### 5.5.2 Period čuvanja arhive

- (1) Podaci se čuvaju u skladu sa zakonskim odredbama.
- (2) Dugoročno uskladišteni podaci koji se odnose na ključeve i sertifikate čuvaju se najmanje deset (10) godina nakon isteka sertifikata na koje se odnosi informacija, ako posebnim zakonom nije određen duži rok.
- (3) Ostali dugoročno uskladišteni podaci se čuvaju najmanje deset (10) godina nakon njihovog nastanka, pod uslovom da poseban zakon ne predviđa duži rok.

### 5.5.3 Zaštita arhive

- (1) Podaci koji se čuvaju dugotrajno čuvaju se bezbedno.
- (2) Detaljne odredbe dugotrajnog čuvanja se definišu u internim pravilima rada pružaoca usluga od poverenja HALCOM BG CA a u skladu sa važećim propisima, standardima i preporukama.

### 5.5.4 Procedura backup-a arhive

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

### 5.5.5 Zahtevi za vremenskim pečatom zapisa

Ovo poglavlje nije primenljivo u okviru ove CP.

### **5.5.6 Sistem sakupljanja zapisa**

- (1) Podaci se sakupljaju na način koji je u skladu sa vrstom dokumenta.
- (2) Detaljne odredbe načina sakupljanja podataka se definišu u internim pravilima rada pružaoca usluga od poverenja HALCOM BG CA a u skladu sa važećim propisima, standardima i preporukama.

### **5.5.7 Procedure za dobijanje i verifikaciju informacija iz arhive**

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

## **5.6. IZMENA KLJUČEVA PRUŽAOCA USLUGA OD POVERENJA**

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

## **5.7. KOMPROMITACIJA I OPORAVAK U SLUČAJU KATASTROFE**

### **5.7.1 Procedure za postupanje u incidentnim i kompromitujućim situacijama**

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

### **5.7.2 Računarski resursi, softver ili podaci koji su oštećeni**

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

### **5.7.3 Procedure koje se sprovode kod kompromitacije privatnog ključa korisnika**

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

### **5.7.4 Plan poslovanja nakon katastrofe**

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

## **5.8 ZAVRŠETAK RADA CA ILI RA**

- (1) Pre nego što prekine svoje aktivnosti pružanja usluga od poverenja, HALCOM BG CA:
  - obezbeđuje svojim korisnicima koji imaju validne sertifikate obaveštenje o nameri da prestane sa pružanjem usluga od poverenja, tj. da prestane da izvršava aktivnosti u svojstvu CA,

- opozove sve sertifikate koji su još uvek validni (tj. one koji nisu opozvani i nije im istekao rok važnosti), nakon obaveštenja, a bez zahteva za saglasnošću korisnika,
- blagovremeno obaveštava o povlačenju kvalifikovanih elektronskih sertifikata sve korisnike na koje se to odnosi (vlasnike sertifikata, treća lica koja se pouzdaju u sertifikate i odgovarajuće državne organe). korisnike sa kojima ima posebne ugovore obaveštava individualno a sve ostale putem internet stranice,
- čini razumne mere u cilju zaštite zapisa koje čuva u skladu sa ovim cp dokumentom.
- ukoliko je to moguće, obezbeđuje odgovarajuće mere obezbeđenja sukcesije u smislu ponovnog izdavanja kvalifikovanih elektronskih sertifikata od strane drugog ca tela koje je sukcesor – nastavljač izdavanja kvalifikovanih elektronskih sertifikata datog ca – i koje poštuje ekvivalentne CP i CPS dokumente,
- odredi odgovarajuće telo da preuzme vođenje crl listi,
- odredi odgovarajuće telo da preuzme vođenje dokumentaciju ( zahteve, dnevnike, opozive),
- opoziva ovlašćenja Registracionih tela,
- uništava svoje privatne ključeve.

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

## 6. TEHNIČKE BEZBEDNOSNE KONTROLE

### 6.1. GENERISANJE I INSTALACIJA ASIMETRIČNOG PARA KLJUČEVA

#### 6.1.1 Proces generisanja asimetričnog para ključeva HALCOM BG CA pružaoca usluga od poverenja

- (1) Asimetrični par ključeva pružaoca usluga od poverenja HALCOM BG CA za elektronsko potpisivanje sertifikata i verifikaciju potpisa generiše se prema najvišim sigurnosnim standardima u sigurnom okruženju pružaoca usluga od poverenja HALCOM BG CA.
- (2) Za korisnike, vlasnike sertifikata, pružalac usluga od poverenja HALCOM BG CA generiše sledeće asimetrične ključeve i sertifikate:

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

#### 6.1.2 Dostava privatnog ključa vlasnicima

Pružalac usluga od poverenja dostavlja korisniku (vlasniku sertifikata) kompletno isprogramiranu smart karticu/USB ključ (sa parom ključeva (privatni i javni ključ) i sertifikatom) kao i odštampan PIN/PUK kod.



### 6.1.3 Dostava javnog ključa korisnika pružaocu usluga od poverenja

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

### 6.1.4 Dostava javnog ključa pružaoca usluga od poverenja korisnicima i trećim licima

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

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

### 6.1.5 Dužine ključeva

Sertifikat	Dužina ključa prema RSA [bit]
Sertifikat pružaoca usluga od poverenja HALCOM BG CA (root)	Najmanje 2048
Intermediate (podređeni) sertifikat pružaoca usluga od poverenja HALCOM BG CA	Najmanje 2048
Kvalifikovani sertifikat za korisnike	Najmanje 2048

### 6.1.6 Generisanje kriptografskih parametara i provera kvaliteta

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

### 6.1.7 Moguće „Key Usage” opcije - svrha ključeva i sertifikata

- (1) Namena upotrebe asimetričnih ključeva, odnosno 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*).
- (2) Elektronsko potpisivanje sertifikata i registra opozvanih sertifikata se vrši privatnim ključem pružaoca usluga od poverenja HALCOM BG CA, dok se za verifikaciju pomenutih potpisa koristi javni ključ iz kvalifikovanog elektronskog sertifikata pružaoca usluga od poverenja. U tom smislu, *keyUsage* ekstenzija u sertifikatu pružaoca usluga od poverenja sadrži odgovarajuće vrednosti.
- (3) Profili kvalifikovanih elektronskih sertifikata koje izdaje pružalac usluga od poverenja HALCOM BG CA su navedeni u poglavlju 7.1

## **6.2. ZAŠTITA PRIVATNOG KLJUČA I TEHNIČKE KONTROLE KRIPTOGRAFSKOG MODULA**

### **6.2.1 Standardi i kontrole kriptografskog hardverskog modula**

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

### **6.2.2 Kontrola privatnog ključa od strane ovlašćenih osoba**

Odredbe vezane za aktivaciju privatnog ključa pružaoca usluga od poverenja HALCOM BG CA definisane su u internim pravilima rada pružaoca usluga od poverenja HALCOM BG CA.

### **6.2.3 Otkrivanje kopije privatnog ključa**

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

### **6.2.4 Backup ključeva HALCOM BG CA pružaoca usluga od poverenja**

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

### **6.2.5 Arhiviranje privatnog ključa**

- (1) Kopije privatnih ključeva HALCOM BG CA mogu se kopirati i čuvati samo do strane ovlašćenih osoba pružaoca usluga od poverenja HALCOM BG CA. Sigurne kopije privatnih ključeva čuvaju se sa istim nivoom zaštite kao i ključevi koji su u upotrebi.
- (2) Precizniji uslovi kopiranja privatnih ključeva pružaoca usluga od poverenja HALCOM BG CA u skladu je sa važećim propisima i Opštim pravilima poslovanja kao i internim pravilima poslovanja pružaoca usluga od poverenja HALCOM BG CA.

### **6.2.6 Transfer privatnog ključa na hardverski kriptografski modul**

- (1) Privatni par ključeva pružaoca usluga od poverenja se generiše u HSM uređaju. Detaljnije odredbe vezane za prenos privatnog ključa HALCOM BG CA definisane su u internim pravilima rada pružaoca usluga od poverenja HALCOM BG CA.
- (2) Privatni par ključeva za vlasnike sertifikata se generišu u smart kartici/USB ključu i ne mogu se pročitati sa smart kartice/USB ključa, kao takvi se naknadno dostavljaju vlasniku sertifikata.

### **6.2.7 Čuvanje privatnog ključa na hardverskom kriptografskom modulu**

- (1) Privatni ključ pružaoca usluga od poverenja HALCOM BG CA se čuva u kriptografskom modulu, koje je sertifikovan u skladu sa FIPS PUB 140-2 nivo 3 i/ili Common Criteria EAL4+.
- (2) Privatni ključevi korisnika:
  - Napredni sertifikati se generišu i čuvaju na bezbednom medijumu

### 6.2.8 Metoda aktivacije privatnog ključa

- (1) Postupak aktivacije privatnog ključa pružaoca usluga od poverenja i procedura distribuirane odgovornosti u vezi tog postupka su definisane u internim pravilima rada pružaoca usluga od poverenja.
- (2) HALCOM BG CA preporučuje upotrebu programskog okruženja, koji prilikom odjave ili nakon isteka nekog vremena, onemogućiti pristup njihovom privatnom ključu bez unosa odgovarajuće lozinke.

### 6.2.9 Metoda deaktiviranja privatnog ključa

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

### 6.2.10 Metoda uništavanja privatnog ključa

- (1) Postupak za uništavanje privatnog ključa pružaoca usluga od poverenja HALCOM BG CA vrši se bezbednim načinom u skladu sa odredbama internih pravila rada HALCOM BG CA i uputstva proizvođača bezbednog kriptografskog uređaja. Privatni ključ se uništava na takav način da ga nije moguće ponovo koristiti.
- (2) Uništenje privatnih ključeva korisnika, je u nadležnosti vlasnika sertifikata. Mogu koristiti odgovarajuće aplikacije za sigurno brisanje sertifikata.

### 6.2.11 Karakteristike kriptografskih hardverskih modula

Bezbedni kriptografski uređajodgovaraju standardima navedenim u poglavlju 6.2.1.

## 6.3. NEKI DRUGI ASPEKTI UPRAVLJANJA PAROM KLJUČEVA

### 6.3.1 Arhiviranje javnog ključa

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

### 6.3.2 Periodi validnosti kvalifikovanog elektronskog sertifikata i privatnog ključa

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

Tip sertifikata	Ključ	Važenje
Root sertifikat HALCOM BG CA	Privatni ključ	20 godina
	Javni ključ	20 godina
Intermediate sertifikat HALCOM BG CA FL e-signature	Privatni ključ	10 godina
	Javni ključ	10 godina
Sertifikat za korisnike	Privatni ključ	3 godine
	Javni ključ	3 godine

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

## **6.4. AKTIVACIONI PODACI**

### **6.4.1 Generisanje i instalacija aktivacionih podataka**

- (1) Za potrebe pristupa privatnim ključevima vlasnika sertifikata koriste se PIN/PUK kodovi za pristup karticama koji se generišu u HALCOM BG CA.
- (2) PIN/PUK kod za smart karticu/USB ključ generiše se i štampa na specijalnim PIN/PUK kovertama u okviru pružaoca usluga od poverenja HALCOM BG CA.
- (3) Vlasnik je u obavezi da promeni PIN kod pre prve upotrebe sertifikata, a nakon toga, po savetu pružaoca usluga od poverenja, potrebno je da ga menja jednom mesečno.

### **6.4.2 Zaštita aktivacionih podataka**

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

### **6.4.3 Drugi aspekti u vezi aktivacionih podataka**

Ovo poglavlje nije primenljivo u okviru ove CP.

## **6.5. BEZBEDNOSNE KONTROLE RAČUNARA**

### **6.5.1 Specifični zahtevi za bezbednost računara**

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

### **6.5.2 Nivo bezbednosti**

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

## **6.6. ŽIVOTNI CIKLUS TEHNIČKIH BEZBEDNOSNIH KONTROLA**

### **6.6.1 Kontrole sistemskog razvoja**

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

### **6.6.2 Kontrole upravljanja bezbednošću**

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

### 6.6.3 Životni ciklus bezbednosnih kontrola

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

## 6.7. MREŽNE BEZBEDNOSNE KONTROLE

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

## 6.8. VREMENSKI PEČAT

Ovo poglavlje nije primenljivo u okviru ove CP.

## 7. PROFIL KVALIFIKOVANOG SERTIFIKATA CRL I OCSP

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

### 7.1. PROFILI KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA

- (1) Na osnovu ove politike pružanja usluge, pružalac usluga od poverenja HALCOM BG CA izdaje kvalifikovane elektronske sertifikate za fizička lica.
- (2) Kvalifikovani elektronski sertifikati koje izdaje pružalac usluga od poverenja HALCOM BG CA zadovoljavaju standard X.509.

#### 7.1.1 Broj verzije

Svi kvalifikovani elektronski sertifikati koje izdaje pružalac usluga od poverenja HALCOM BG CA zadovoljavaju standard X.509, i to verziju 3.

#### 7.1.2 Ekstenzije u sertifikatu

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

Nazivi polja	Vrednost odnosno značenje
<b>Osnovna polja u sertifikatima</b>	
Varijanta engl. Version	V3
Identifikaciona oznaka kvalifikovanih elektronskih sertifikata engl. <i>Serial Number</i>	6e 95 f3 d2 71 f5 e5 6b

Algoritam za potpis, engl. <i>Signature algorithm</i>	Sha256RSA (OID 1.2.840.113549.1.1.11 )
Izdavalac engl. <i>Issuer</i>	CN = Halcom BG Root CA 2.5.4.97 = VATRS-102193722 2.5.4.97 = MB:RS-17419722 O = Halcom a.d. Beograd C = RS
Valjanost, engl. <i>Validity</i>	Valid from: <16.10.2018 10:00:00 GMT> Valid to: <16.10.2038 10:00:00 GMT>
Vlasnik, engl. <i>Subject</i>	CN = Halcom BG Root CA 2.5.4.97 = VATRS-102193722 2.5.4.97 = MB:RS-17419722 O = Halcom a.d. Beograd C = RS
Algoritam za javni ključ, engl. <i>Subject Public Key Algorithm</i>	rsaEncryption (OID 1.2.840.113549.1.1.1)
Javni ključ, engl. <i>Public Key (... bits)</i>	30 82 01 0a 02 82 01 01 00 e6 cf d3 da 3b c5 9d e3 ac 77 31 73 2a e7 f5 89 7f 5c 36 ed 58 8b 63 19 61 17 5c 3e 29 e5 af 58 c4 6e 08 41 2f 37 dd 3a e3 ab c5 3e 45 c8 6a f4 19 3a d8 54 a6 01 23 83 0b e5 97 65 ae 60 09 e4 a9 d2 1a 6b 3e 18 3a 92 e5 6f 09 5d bd 14 e4 7b 64 46 15 b7 d2 27 09 38 4b 5b 3d 46 2f 7a cd c0 a2 57 1d 05 93 6a 54 9b 43 0e c0 cf 07 f7 e2 98 82 b6 32 c6 a0 27 67 dc a7 b9 ae 18 ff a5 b2 aa 25 64 ce 15 18 e8 14 18 89 7b b9 b6 8c 4f 78 0e 7c c2 a2 94 b0 e6 78 9a 7c be d0 c0 0e aa f0 f5 90 74 ea e1 ee 25 12 34 cf ec be 48 45 01 58 36 9c 03 24 b4 90 3d a1 3b 29 86 87 a3 6d fd 2d f9 87 cd af e7 3d 87 53 1e 4c e0 d0 b0 62 c4 6e 3b 9b 35 f5 e0 cb d0 04 92 35 34 c6 3f 9e 31 9d b6 de 4d c3 fc bb b3 20 fe 6a d7 8a e2 a5 68 76 eb 81 4c be be 29 4c 88 64 a1 8a 47 f8 61 d1 83 02 03 01 00 01
Vlasnikov javni ključ koji pripada odgovarajućem paru, ključeva, šifriran alg. RSA, engl. <i>RSA Public Key</i>	dužina ključa je 2048 bitova
<b>Ekstenzije u okviru X.509v3 standarda</b>	
korišćenje ključa, OID 2.5.29.15, engl. <i>Key Usage</i>	Certificate Signing, Off-line CRL Signing, CRL Signing
Identifikator ključa vlasnika, OID 2.5.29.14, engl. <i>Subject Key Identifier</i>	identifikator ključa vlasnika  49 2c 22 39 ad 8d a4 e0

Osnovna ograničenja, OID 2.5.29.19, engl. <i>Basic Constraints</i>	Subject Type=CA Path Length Constraint=None
Dodatna identifikacija (nije deo kvalifikovanih elektronskih sertifikata)	
Prepoznavan otisak kvalifikovanih elektronskih sertifikata -SHA1 engl. <i>Certificate Fingerprint - SHA1</i>	89 8f cb b2 fe 5b 82 d2 ec ad 5b a5 ac 28 f5 6f ef 20 8f

(2) Halcom BG CA FL e-signature

Nazivi polja	Vrednost odnosno značenje
<b>Osnovna polja u kvalifikovanom elektronskom sertifikatu</b>	
Varijanta engl. <i>Version</i>	V3
Identifikaciona oznaka kvalifikovanih elektronskih sertifikata engl. <i>Serial Number</i>	15 c3 7f 32 64 ab 09 b2
Algoritam za potpis, engl. <i>Signature algorithm</i>	Sha256RSA (1.2.840.113549.1.1.11)
Izdavalac engl. <i>Issuer</i>	CN = Halcom BG Root CA 2.5.4.97 = VATRS-102193722 2.5.4.97 = MB:RS-17419722 O = Halcom a.d. Beograd C = RS
Valjanost, engl. <i>Validity</i>	Valid from: <16.10.2018 11:00:00 GMT> Valid to: <16.10.2028 11:00:00 GMT>
Vlasnik, engl. <i>Subject</i>	CN = Halcom BG CA FL e-signature 2.5.4.97 = VATRS-102193722 2.5.4.97 = MB:RS-17419722 O = Halcom a.d. Beograd C = RS
Algoritam za javni ključ, engl. <i>Subject Public Key Algorithm</i>	rsaEncryption (OID 1.2.840.113549.1.1.1)

Javni ključ, engl. <i>Public Key (... bits)</i>	30 82 01 0a 02 82 01 01 00 9e 5c 25 e4 54 73 d0 a4 88 be 9b 1d 64 05 ab f0 95 11 af 97 f1 3b 72 e5 ad 6c 1e e4 47 4f b5 1e 07 ec df 8f 41 84 fb 1e 99 36 5f 0a a7 9a 0e 9c 38 1f 31 ae ba 21 22 b5 74 ae 18 aa b5 8d f1 35 aa a5 7f 28 09 7b 94 f3 a3 00 08 1c 7f cd e4 af 83 4f c9 bd 53 28 8b ae 91 f3 61 b9 c4 ec f6 90 85 49 1f f8 cc f1 dc cf fa bc 49 6d 79 4f 61 91 d2 d1 25 2d 51 22 ff e1 4a 19 20 7d 5d 42 8c 58 0e ec 5c 4c 86 39 90 4b bb 1a 98 e1 06 2e 04 b4 ea d0 50 b2 a1 88 1a 6d ee 4d 93 63 17 98 d9 ce 57 1d f4 ad 16 ec 31 40 b4 94 c1 ad a0 9e 37 3e c1 b3 91 68 ea 79 70 a4 22 d9 04 53 da 74 d5 97 0d 60 ba 6c 16 5f ed 51 35 91 f9 32 3b cc 47 80 41 de 2d cc ff 0b 5f 9b c2 41 e2 71 e6 5f aa 3a 78 a2 0d af 37 b3 28 3e 5b 7c 65 f3 92 e3 bf 0d 4b d6 87 a2 f8 a5 67 98 c2 e3 ea 91 3a 47 fe 11 02 03 01 00 01
Vlasnikov javni ključ koji pripada odgovarajućem paru, ključeva, šifriran alg. RSA, engl. <i>RSA Public Key</i>	<i>dužina ključa je 2048 bitova,</i>
<b>Ekstenzije u okviru X.509v3 standarda</b>	
Objava registra opozvanih kvalifikovanih elektronskih sertifikata, OID 2.5.29.31,  engl. <i>CRL Distribution Points</i>	URL= <a href="ldap://ldap.halcom.rs/cn=Halcom%20BG%20Root%20CA,o=Halcom%20a.d.%20Beograd,c=RS?certificaterevocationlist;binary">ldap://ldap.halcom.rs/cn=Halcom%20BG%20Root%20CA,o=Halcom%20a.d.%20Beograd,c=RS?certificaterevocationlist;binary</a>  URL= <a href="http://domina.halcom.rs/crls/Halcom_BG_Root_CA.crl">http://domina.halcom.rs/crls/Halcom_BG_Root_CA.crl</a>
korišćenje ključa, OID 2.5.29.15, engl. <i>Key Usage</i>	Certificate Signing, Off-line CRL Signing, CRL Signing
Prošireno korišćenje, OID 2.5.29.37, engl. <i>Enhanced Key Usage</i>	/
Identifikator ključa pružaoca usluga od poverenja, OID 2.5.29.35, engl. <i>Authority Key Identifier</i>	KeyID=49 2c 22 39 ad 8d a4 e0
Identifikator ključa vlasnika, OID 2.5.29.14, engl. <i>Subject Key Identifier</i>	4d b5 23 f3 ff f4 0a 62



Politika, u nadležnosti koje je sertifikat izdat, sa URL adresom CPS-a , OID 2.5.29.32, engl. certificatePolicies	Certificate Policy: Policy Identifier=All issuance policies [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier:  <a href="http://www.halcom.rs/UserFiles/File/CPS_HalcomCA.pdf">http://www.halcom.rs/UserFiles/File/CPS_HalcomCA.pdf</a>
Osnovna ograničenja, OID 2.5.29.19, engl. <i>Basic Constraints</i>	Subject Type=CA Path Length Constraint=None
Dodatna identifikacija (nije deo kvalifikovanog elektronskog sertifikata)	
Prepoznatljiv otisak kvalifikovanih elektronskih sertifikata-SHA1 engl. <i>Certificate Fingerprint - SHA1</i>	ac 35 11 e3 66 fd cd b7 2a ea e1 b3 78 25 78 cc d1 42 91 7e

(3) Profil sertifikata krajnjih korisnika HALCOM BG CA FL e-signature

Nazivi polja	Vrednost odnosno značenje
<b>Osnovna polja u sertifikatima</b>	
Varijanta engl. <i>Version</i>	V3
Identifikaciona oznaka kvalifikovanog elektronskog sertifikata engl. <i>Serial Number</i>	Jedinstven interni broj kvalifikovanih elektronskih sertifikata
Algoritam za potpis, engl. <i>Signature algorithm</i>	Sha256RSA (1.2.840.113549.1.1.11)
Izdavalac engl. <i>Issuer</i>	CN = Halcom BG CA FL e-signature 2.5.4.97 = VATRS-102193722 2.5.4.97 = MB:RS-17419722 O = Halcom a.d. Beograd C = RS
Valjanost, engl. <i>Validity</i>	Valid from: <početak validnosti prema GMT> Valid to: <kraj validnosti prema GMT>
Vlasnik, engl. <i>Subject</i>	Jedinstveno ime, pogledati poglavlje 3.1.1.
Algoritam za javni ključ, engl. <i>Subject Public Key Algorithm</i>	rsaEncryption (OID 1.2.840.113549.1.1.1)
Javni ključ, engl. <i>Public Key (... bits)</i>	modulus, eksponent,...

Vlasnikov javni ključ koji pripada odgovarajućem paru, ključeva, šifriran alg. RSA, engl. <i>RSA Public Key</i>	dužina ključa je min 2048 bitova, pogledaj poglavlje 6.1.5.
<b>Ekstenzije u okviru X.509v3 standarda</b>	
Objava registra opozvanih kvalifikovanih elektronskih sertifikata, OID 2.5.29.31, engl. <i>CRL Distribution Points</i>	<p>URL=ldap://ldap.halcom.rs/cn=Halcom%20BG%20CA%20FL%20e-signature,o=Halcom%20a.d.%20Beograd,c=RS?certificaterevocationlist;binary</p> <p>URL=http://domina.halcom.rs/crls/Halcom_BG_CA_FL_e-signature.crl</p>
Politika, u nadležnosti koje je sertifikat izdat, sa URL adresom CPS-a , OID 2.5.29.32, engl. <i>certificatePolicies</i>	<p>[1]Certificate Policy:          Policy Identifier=1.3.6.1.4.1.5939.11.2.4          [1,1]Policy Qualifier Info:          Policy Qualifier Id=CPS          Qualifier:</p> <p><a href="http://www.halcom.rs/UserFiles/File/CPS_HalcomCA.pdf">http://www.halcom.rs/UserFiles/File/CPS_HalcomCA.pdf</a></p> <p>[2]Certificate Policy:          Policy Identifier=0.4.0.194112.1.2</p>
korišćenje ključa, OID 2.5.29.15, engl. <i>Key Usage</i>	Napredni sertifikati: Digital Signature, Non Repudiation, Key Encipherment
Identifikator ključa pružaoca usluga od poverenja, OID 2.5.29.35, engl. <i>Authority Key Identifier</i>	KeyID=4d b5 23 f3 ff f4 0a 62

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

### 7.1.2.1. Zahtevi sa elektronskom adresom

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

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

(2) Ne postoje druga ograničenja u elektronskoj adresi.

### 7.1.3 Identifikacione oznake kriptografskih algoritama

(1) Sertifikati, koje izdaje HALCOM BG CA, potpisana su primenom kriptografskog algoritma, određenim u polju signature algorithm: vrednost "sha256RSA, identifikaciona oznaka: OID1.2.840.113549.1.1.11".

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

#### 7.1.4 Forme imena

Pogledati poglavlje 3.1.1.

#### 7.1.5 Ograničenja imena

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

#### 7.1.6 Objektni identifikator

Pogledati poglavlje 7.1.2.

#### 7.1.7 Ograničenja upotrebe

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

#### 7.1.8 Sintaksa i semantika „Policy Qualifier“-sa

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

#### 7.1.9 Značenje bitnih dodataka politike

Nije podržano u okviru ove CP.

## 7.2. PROFIL REGISTRA OPOZVANIH SERTIFIKATA (CRL)

(1) Registar opozvanih sertifikata (CRL) izdaje pružalac usluga od poverenja HALCOM BG CA sa karakterističnim imenom:

- Registar opozvanih intermediate/podređenih sertifikata  
CN= Halcom BG Root CA  
O = Halcom a.d. Beograd  
C = RS
- Registar opozvanih sertifikata za e-potpis fizičkih lica  
CN= HALCOM BG CA FL e-signature  
O = Halcom a.d. Beograd  
C =RS

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

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

#### 7.2.1 Broj verzije

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

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

- LDAP protokola i
- HTTP protokola.

### 7.2.2 CRL i CRL entry ekstenzije

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

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

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

Naziv polja	Vrednost odnosno značenje
<b>Osnovna polja u CRL</b>	
Verzija, engl. <i>Version</i>	V2
Algoritam za digitalni potpis CRL, engl. <i>Signature Algorithm</i>	Sha256RSA
Potpis pružaoca usluga od poverenja, engl. <i>Signature</i>	potpis HALCOM BG CA
Jedinstveno ime pružaoca usluga od poverenja engl. <i>Issuer</i>	CN = Halcom BG Root CA 2.5.4.97 = VATRS-102193722 2.5.4.97 = MB:RS-17419722 O = Halcom a.d. Beograd C = RS
Vreme izdavanja CRL, engl. <i>thisUpdate</i>	Effective date: <vreme izdavanja prema GMT>
Vreme izdavanja sledeće CRL, engl. <i>nextUpdate</i>	Next Update: <vreme izdavanja sledeće CRL prema GMT>
Identifikacione oznake (serijski brojevi) opozvanih kvalifikovanih elektronskih sertifikata i vreme opoziva, engl. <i>revokedCertificate</i>	Serial Number: <identifikaciona oznaka (serijski broj) opozvanog kvalifikovanog elektronskog kvalifikovanih elektronskih sertifikata> Revocation Date: <vreme opoziva prema GMT>
<b>Ekstenzije X.509v2 CRL</b>	
Redni broj CRL engl. <i>CRL number</i>	Redni broj izdatog registra opozvanih kvalifikovanih elektronskih sertifikata
Identifikator ključa pružaoca usluga od poverenja, engl. <i>Authority Key Identifier (OID 2.5.29.35)</i>	KeyID=49 2c 22 39 ad 8d a4 e0
engl. <i>issuerAltName (OID 2.5.28.18)</i>	Ne upotrebljava se
engl. <i>deltaCRLIndicator (OID 2.5.29.27)</i>	Ne upotrebljava se
engl. <i>issuingDistributionPoint (OID 2.5.29.28)</i>	Ne upotrebljava se

(3) Intermediate/podređenih registar opozvanih sertifikata HALCOM BG CA FL e-signature (CRL sertifikata krajnjih korisnika)

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>	Sha256RSA
Potpis pružaoca usluga od poverenja, engl. <i>Signature</i>	potpis HALCOM BG CA
Jedinstveno ime pružaoca usluga od poverenja engl. <i>Issuer</i>	CN = Halcom BG CA FL e-signature 2.5.4.97 = VATRS-102193722 2.5.4.97 = MB:RS-17419722 O = Halcom a.d. Beograd C = RS
Vreme izdavanja CRL, engl. <i>thisUpdate</i>	Effective date: <vreme izdavanja prema GMT>
Vreme izdavanja sledeće CRL, engl. <i>nextUpdate</i>	Next Update: <vreme izdavanja sledeće CRL prema GMT>
Identifikacione oznake (serijski brojevi) opozvanih kvalifikovanih elektronskih sertifikata i vreme opoziva, engl. <i>revokedCertificate</i>	Serial Number: <identifikaciona oznaka (serijski broj) opozvanog kvalifikovanog elektronskog kvalifikovanih elektronskih sertifikata> Revocation Date: <vreme opoziva prema GMT>
Ekstenzije X.509v2 CRL	
redni broj CRL engl. <i>CRL number</i>	Redni broj izdatog registra opozvanih kvalifikovanih elektronskih sertifikata
identifikator ključa pružaoca usluga od poverenja, engl. <i>Authority Key Identifier (OID 2.5.29.35)</i>	KeyID=4d b5 23 f3 ff f4 0a 62
angl. issuerAltName (OID 2.5.28.18)	Ne upotrebljava se
angl. deltaCRLIndicator (OID 2.5.29.27)	Ne upotrebljava se
angl. issuingDistributionPoint (OID 2.5.29.28)	Ne upotrebljava se

(4) Opozvani kvalifikovani elektronski sertifikati kojima je istekla validnost, mogu se brisati iz CRL nakon isteka važnosti.

### 7.2.3 Objava registra opozvanih sertifikata

HALCOM BG CA objavljuje registre u javnom direktorijumu na serveru ldap://ldap.halcom.rs po protokolu LDAP i <http://domina.halcom.rs/crls> po protokolu HTTP.

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

- (1) Stalna provera statusa elektronskih sertifikata dostupna je na <http://ocsp.halcom.rs>.
- (2) Profil OCSP poruke (zahtev/odgovor) za proveru statusa u realnom vremenu je u skladu sa preporukom IETF RFC.

### 7.3.1 Broj verzije

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

### 7.3.2 OCSP ekstenzije

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

## 8. PROVERA USKLAĐENOSTI I DRUGA OCENJIVANJA

- (1) U okviru pružaoca usluga od poverenja HALCOM BG CA postoji jedinica za unutrašnju kontrolu i usklađenost koju čine stručnjaci sa odgovarajućim tehnološkim i pravnim znanjima, a koji ne vrše zadatke vezane za upravljanje kvalifikovanim elektronskim sertifikatima.
- (2) Sistem evidentičar nadzire rad HALCOM BG CA. U slučaju otkrivenih nedostataka definiše odgovarajuće mere za uklanjanje tih nedostataka, koje je pružalac usluga od poverenja HALCOM BG CA dužno da sprovede, i nadzire sprovođenje definisanih mera.
- (3) Sistem evidentičari vrše nadzor rada pružaoca usluga od poverenja najmanje jedanput u godini.

### 8.1. FREKVENCIJA ILI USLOVI OCENJIVANJA

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

### 8.2. IDENTITET/KVALIFIKACIJE PROCENJIVAČA

- (1) Sistem evidentičari i usklađenost čine stručnjaci sa odgovarajućim tehnološkim i pravnim znanjima.
- (2) Poverenik za eksternu kontrolu ima odgovarajuća tehnološka i pravna znanja.

### 8.3. ODNOS OCENJIVAČA PREMA OCENJIVANOM ENTITETU - NEZAVISNOST NADZORA

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

### 8.4. PODRUČJA NADZORA

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

## **8.5. AKTIVNOSTI PREDUZETE KAO REZULTAT UTVRĐENIH NEDOSTATAKA**

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

## **8.6. OBJAVLJIVANJE REZULTATA NADZORA**

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

## **9. DRUGI POSLOVNI I PRAVNI ASPEKTI**

### **9.1. CENE**

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

#### **9.1.1 Cene izdavanja ili obnove kvalifikovanih elektronskih sertifikata**

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

#### **9.1.2 Cena pristupa sertifikatima**

Ovo poglavlje nije primenljivo u okviru ove CP.

#### **9.1.3 Cena pristupa informacijama o statusu kvalifikovanih elektronskih sertifikata i registru opozvanih sertifikata**

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

#### **9.1.4 Cene za druge servise**

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

#### **9.1.5 Povratak troškova**

Ovo poglavlje nije primenljivo u okviru ove CP.

## **9.2. FINANSIJSKA ODGOVORNOST**

### **9.2.1 Pokrivenost osiguranjem**

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

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

### **9.2.2 Druga dobra**

Ovo poglavlje nije primenljivo u okviru ove CP.

### **9.2.3 Osiguranje ili garancijska pokrivenost za krajnje korisnike**

Ovo poglavlje nije primenljivo u okviru ove CP.

## **9.3 POVERLJIVOST POSLOVNIH INFORMACIJA**

### **9.3.1 Opseg poverljivih informacija**

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

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

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

### **9.3.2 Informacije koje nisu u opsegu poverljivih informacija**

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

### **9.3.3 Odgovornost za zaštitu poverljivih informacija**

- (1) Pružalac usluga od poverenja HALCOM BG CA ne preuzima nikakve odgovornosti za sadržaj podataka koje vlasnik kvalifikovanog elektronskog sertifikata elektronski šifruje ili potpisuje. Takođe, pružalac usluga od poverenja ne preuzima nikakve odgovornosti za pitanja da li su vlasnik ili treće lice poštovali sve važeće propise, sve odredbe politike pružanja usluga i drugih pravila pružaoca usluga od poverenja HALCOM BG CA, odnosno vodili računa o svim objavljenim uputstvima.
- (2) Pružalac usluga od poverenja HALCOM BG CA ne preuzima nikakve odgovornosti za posledice do kojih dolazi ukoliko vlasnik kvalifikovanog elektronskog sertifikata nije postupao u skladu sa sigurnosnim zahtevima iz poglavlja 4.5.1 ovog CP dokumenta.

## **9.4. PRIVATNOST LIČNIH PODATAKA**

### **9.4.1 Plan privatnosti**

- (1) HALCOM BG CA pridržava se pravila zaštite privatnosti ličnih podataka i pravila poverljivosti kako je propisano u ovom dokumentu, kao i u odgovarajućim zakonskim dokumentima.
- (2) Sa svim ličnim i poverljivim podacima o vlasnicima kvalifikovanih elektronskih sertifikata koji su nužno potrebni za usluge upravljanja kvalifikovanim elektronskim sertifikatima, pružalac usluga od poverenja HALCOM BG CA postupa u skladu sa važećim zakonodavstvom.



#### **9.4.2 Informacije koje se tretiraju kao privatne**

- (1) Pružalac usluga od poverenja HALCOM BG CA tretira privatnim sve informacije koje se odnose na korisnike kvalifikovanih elektronskih sertifikata.
- (2) Poverljivi podaci koji se čuvaju su svi lični podaci koje HALCOM BG CA prikupi u okviru zahteva za svoje usluge ili u odgovarajućim registrima za dokazivanje identiteta vlasnika. Podaci u sertifikatima i registru opozvanih sertifikata su zbog prirode upotrebe sertifikata, važećih pravila i standarda dostupni trećima licima koja se oslanjaju na sertifikate ili proveravaju njihovu validnost.

#### **9.4.3 Informacije koje se ne smatraju privatnim**

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

#### **9.4.4 Odgovornost za zaštitu privatnih informacija**

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

#### **9.4.5 Obaveštenje i saglasnost za korišćenje privatnih informacija**

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

#### **9.4.6 Otkrivanje informacija shodno pravnim i administrativnim procesima**

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

#### **9.4.7 Druge okolnosti za otkrivanje informacija**

Ovo poglavlje nije primenljivo u okviru ove CP.

### **9.5. 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 ovom politici pružanja usluga od poverenja pripadaju pružaocu usluga od poverenja HALCOM BG CA.

## 9.6. PREDSTAVLJANJA I GARANCIJE

### 9.6.1 HALCOM BG CA predstavljanja i garancije

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

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

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

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

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

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

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

- (5) Pružalac usluga od poverenja HALCOM BG CA je odgovorno za sve navode u ovom dokumentu i za sprovođenje svih odredaba iz ove politike pružanja usluga od poverenja.
- (6) Ostale obaveze odnosno odgovornosti HALCOM BG CA definisane su mogućim međusobnim dogovorom sa korisnicima ili trećim licima.

### **9.6.2 Obaveze i odgovornosti registracionih tela**

- (1) Registraciona tela i prijavna služba je obavezna da:
  - proveri identitet vlasnika ili budućih vlasnika,
  - primi zahteve za usluge HALCOM BG CA,
  - proveri zahtev,
  - izda potrebnu dokumentaciju fizičkim licima, vlasnicima ili budućim vlasnicima,
  - dostavi zahteve i druge podatke na siguran način u HALCOM BG CA.
- (2) Registraciono telo je odgovorno za sprovođenje svih odredbi iz ove politike pružanja usluga od poverenja i drugih zahteva koje dogovori sa pružaocem usluga od poverenja HALCOM BG CA.

### **9.6.3 Obaveze i odgovornosti vlasnika sertifikata**

- (1) 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 privatnog ključa od strane neovlašćenih lica,
  - svaku drugu štetu koja nastane iz nepoštovanja odredbi ove politike pružanja usluga od poverenja i drugih dokumenata pružaoca usluga od poverenja HALCOM BG CA, kao i važećih propisa,
- (2) Obaveze vlasnika sertifikata su, vezano za korišćenje sertifikata, definisane u poglavlju 4.5.1.

### **9.6.4 Obaveze i odgovornosti trećih lica**

- (1) Nakon prve upotrebe sertifikata, treća strana koja se oslanja na sertifikat mora pažljivo pročitati politiku i od tada redovno pratiti sva obaveštenja od HALCOM BG CA.
- (2) Treća strana mora redovno proveravati da sertifikat nije u registru opozvanih sertifikata.
- (3) Ako sertifikat sadrži informacije o trećoj strani, obavezan je da zatraži opoziv sertifikata ako sazna, da je privatni ključ ugrožen na način koji utiče na pouzdanost korišćenja ili postoji rizik od zloupotrebe ili ako su se podaci promenili.
- (4) Treća strana se može osloniti na takav sertifikat do opoziva sertifikata.
- (5) Treća strana može u svako doba zatražiti bilo koju informaciju o važnosti izdatog sertifikata, odredbe politike ili obaveštenja HALCOM BG CA.

### **9.6.5 Obaveze i odgovornosti drugih lica**

Ovo poglavlje nije primenljivo u okviru ove CP.

## **9.7. OGRANIČENJE ODGOVORNOSTI**

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

- korišćenje sertifikata za namene i na način koji nije izričito predviđen u ovoj politici pružanja usluga od poverenja,
- 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,
- ne postupanja 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 pružalac usluge od poverenja HALCOM BG CA, ovom politikom pružanja usluga od poverenja i drugim propisima,
- omogućenog korišćenja odnosno zloupotrebe vlasnikovog sertifikata od strane neovlašćenih lica,
- izdatog sertifikata sa pogrešnim podacima, ili drugim radnjama vlasnika sertifikata ukoliko vlasnik sertifikata nije po prijemu prijavio grešku, u skladu sa tačkom 4.5.1.,
- korišćenja sertifikata koji nisu validni, uz promenu podataka iz sertifikata, elektronskih adresa ili promena imena vlasnika,
- ispada infrastrukture koja nije u domenu upravljanja pružaoca usluga od poverenja HALCOM BG CA,
- podataka koji se šifruju ili potpisuju korišćenjem kvalifikovanih elektronskih sertifikata,
- upotrebe i pouzdanosti rada mašinske i programske opreme vlasnika sertifikata.

## 9.8. OGRANIČENJE U UPOTREBI

Ovo poglavlje nije primenljivo u okviru ove CP.

## 9.9. ODŠTETE

Za štetu je odgovorna stranka koja je istu prouzrokovala zbog nepoštovanja odredaba iz ove politike pružanja usluga od poverenja i važećeg zakonodavstva.

## 9.10. PERIOD VAŽENJA I KRAJ VALIDNOSTI OVE POLITIKE

- (1) Pružalac usluga od poverenja HALCOM BG CA zadržava pravo da izmeni politiku pružanja usluga od poverenja 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 pružanja usluga od poverenja koja je važila u vreme njihovog izdavanja. Za sve sertifikate izdate nakon početka validnosti nove politike pružanja usluga od poverenja, važi nova politika.
- (2) Ova politika pružanja usluga od poverenja stupa na snagu onoga dana kada je odobrena i objavljena od strane pružaoca usluga od poverenja HALCOM BG CA.

### 9.10.1 Važnost

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

### 9.10.2 Kraj validnosti

- (1) Kraj validnosti politike pružanja usluga od poverenja nije određen niti je povezan sa periodom validnosti sertifikata izdatih na osnovu ove politike pružanja usluga od poverenja.
- (2) Prilikom objavljivanja nove politike pružanja usluga od poverenja, za sve sertifikate izdate po osnovu te politike pružanja usluga od poverenja, ostaju validne one odredbe koje smisaono ne mogu da se nadomeste odgovarajućim odredbama nove politike (na primer postupak koji određuje način na koji je bio izdat taj sertifikat, i sl.).
- (3) Pružalac usluga od poverenja može za pojedinačne odredbe validne politike pružanja usluga od poverenja da objavi amandmane kao što je to navedeno u poglavlju 9.12.

### 9.10.3 Efekat završetka i ponovnog rada

- (1) Prilikom objavljivanja nove politike, svi kvalifikovani elektronski sertifikati izdati nakon tog datuma se procesiraju prema novoj politici.
- (2) Nova politika ne utiče na validnost sertifikata koji su bili izdati prema prethodnim politikama. Takvi kvalifikovani elektronski sertifikati ostaju važeći do isteka validnosti pri čemu se, gde god je to moguće procesiraju i/ili tretiraju prema novoj politici pružanja usluga od poverenja.

## 9.11. POJEDINAČNA OBAVEŠTENJA I KOMUNIKACIJA SA UČESNICIMA

- (1) Kontaktni podaci pružaoca usluga od poverenja objavljeni su na web stranicama istog i navedeni u poglavlju 1.3.1.
- (2) Kontaktni podaci vlasnika sertifikata dostavljeni su u narudžbenicama vezanim za sertifikate.
- (3) Kontaktni podaci trećih lica dostavljeni su u mogućem međusobnom dogovoru između trećeg lica i pružaoca usluga od poverenja HALCOM BG CA.

## 9.12. ISPRAVKE, MODIFIKACIJE I DOPUNE

### 9.12.1 Procedure za ispravku, modifikaciju ili dopune

- (1) Promene ili dopune ove politike pružanja usluga od poverenja pružalac usluga od poverenja može da objavi u obliku promena ili dopuna ovoj politici ako se ne radi o suštinskim promenama operativnog rada pružaoca usluga od poverenja HALCOM BG CA.
- (2) Dopune se usvajaju i prihvataju istim postupkom kao i sama politika.
- (3) Ako promene i dopune suštinski utiču na operativni rad pružaoca usluga od poverenja, o tome se obaveštava nadležno ministarstvo istim postupkom kao što to važi i za samu politiku.
- (4) Način za označavanje amandmana definiše pružalac usluga od poverenja HALCOM BG CA.

### **9.12.2 Mehanizam i period obaveštavanja**

- (1) Pružalac usluga od poverenja HALCOM BG CA definiše početak i kraj validnosti promena i dopuna.
- (2) Promene i dopune se objave osam (8) dana pre početka validnosti na web stranicama HALCOM BG CA.

### **9.12.3 Promena identifikacionog broja politike pružanja usluga od poverenja**

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

## **9.13. ODREDBE REŠAVANJA SPOROVA**

- (1) Sve pritužbe vlasnika sertifikata rešavaju sistem evidentičari i zakonsku regulativu.
- (2) Moguće sporove između vlasnika sertifikata ili trećeg lica i pružaoca usluga od poverenja HALCOM BG CA rešava nadležni sud.

## **9.14. VAŽEĆE ZAKONODAVSTVO**

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

## **9.15. USKLAĐENOST SA VAŽEĆIM ZAKONODAVSTVOM**

- (1) Nadzor nad usklađenošću operativnog rada pružaoca usluga od poverenja HALCOM BG CA sa važećim zakonodavstvom i propisima sprovodi nadležna služba ili akreditovani organ.
- (2) Akreditovani organ za ocenjivanje usaglašenosti za HALCOM BG CA sprovode reviziju usaglašenosti najmanje na svaka 24 meseca. Svrha revizije je da potvrdi da li je pružalac usluge od poverenja ispunjava zakonske uslove.
- (3) Interne provere usaglašenosti rada sprovode ovlašćena lica u okviru HALCOM BG CA.

## **9.16. OPŠTE ODREDBE**

- (1) Sa ostalim subjektima pružalac usluga od poverenja može da sklopi međusobne dogovore ako tako definiše važeće zakonodavstvo, odnosno drugi propisi.
- (2) Ako bilo koja odredba ove politike bude ili postane nevažna, to neće uticati na druge odredbe. Nevažna odredba zameniće se važećom.

## **9.17. DRUGE ODREDBE**

Ovo poglavlje nije primenljivo u okviru ove CP.

direktor Halcom a.d. Beograd,

Aleksandar Spremić