Politika Halcom CA

Javni del notranjih pravil Halcom CA

za kvalificirana digitalna potrdila za časovni žig

CPName: Halcom CA TSA 1

Politika za Kvalificirana digitalna potrdila za časovni žig
CPOID:1.3.6.1.4.1.5939.14.1.1

Dokument je veljaven od: 01.07.2017

Pregled predhodnih izdaj:

Izdaja	št.dokumenta in prilog	Opis spremembe	Avtor	Datum zadnje spremembe
1	400085-35-1/17	Začetna izdaja	L. Ribičič	22.6.2017
2				
3				
4				
5				

Kazalo vsebine

1. UVOD

(1) Halcom CA je najstarejši in tudi največji ponudnik storitev zaupanja v Sloveniji, ki za izvajanje svojih storitev na področju elektronskega podpisovanja, elektronskega žigosanja, elektronskega časovnega žigosanja, validacije in drugih storitev uporablja najvarnejše tehnologije, vključno z uporabo varnih nosilcev podatkov in varnega oblaka.

(2) Ta politika je javni del notranjih pravil Halcom CA za kvalificirana digitalna potrdila za časovni žig za ponudnike storitev zaupanja.

(3) Oblika in vsebina te politike je usklajena z uredbo eIDAS, mednarodnim priporočilom IETF RFC in evropskimi standardi ETSI in drugimi.

1.1. Pregled

(1) Ta politika predstavlja nedeljivo celoto splošnih pravil delovanja ponudnika storitev zaupanja Halcom CA glede izdaje kvalificiranih digitalnih potrdil, ureja namen, delovanje in metodologijo upravljanja kvalificiranih digitalnih potrdil ter varnostne zahteve, ki jih morajo izpolnjevati ponudnik storitev zaupanja Halcom CA, imetniki potrdil, tretje osebe, ki se zanašajo na ta potrdila, ter odgovornost vseh naštetih oseb.

(2) Halcom CA je ponudnik storitev zaupanja, ki izdaja in upravlja s kvalificiranimi digitalnimi potrdili za časovni žig. Ponudnik storitev zaupanja Halcom CA deluje v okviru Halcom d.d.

(3) Halcom CA izdaja kvalificirana digitalna potrdila za časovni žig z enim parom ključev.

(4) Vse določbe te politike glede ravnanja Halcom CA so ustrezno prenesene in podrobneje določene v javno objavljenih pravilih poslovanja ponudnika storitev zaupanja (CPS) ter opredeljene v določbah zaupnih notranje pravil ponudnika storitev zaupanja, ki opredeljujejo infrastrukturo, določila glede osebja Halcom CA (pristojnosti, naloge, pooblastila in zahtevani pogoji posameznih članov osebja), fizično varovanje (dostop do prostorov, ravnanje s strojno in programsko opremo), programsko varovanje (varnostne nastavitve strežnikov, varnostne kopije,...) in notranji nadzor (kontrola fizičnih dostopov, pooblastil,...).

(5) Halcom CA izdaja potrdila in opravlja druge dejavnosti ponudnika storitev zaupanja v skladu z veljavnim pravnim redom Republike Slovenije in Evropske unije, ter v skladu z uredbo eIDAS, tehničnimi zahtevami ETSI, standardom IETF RFC in družino standardov ISO/IEC ter drugih sorodnih standardov.

(6) Seznam prijavnih služb, ki omogočajo pridobitev kvalificiranih digitalnih potrdil za poslovne subjekte, Halcom CA objavi na svetovnem spletu.

1.2. Identifikacijski podatki politike

(1) Oznaka te politike delovanja Halcom CA TSA 1 je:

CPOID:1.3.6.1.4.1.5939.14.1.1

1.3. Subjekti

1.3.1 Ponudnik storitev zaupanja Halcom CA

Halcom CA je ponudnik storitev zaupanja, ki izdaja in upravlja s kvalificiranimi digitalnimi potrdili za časovni žig. Ponudnik storitev zaupanja Halcom CA deluje v okviru Halcom d.d.

1.3.2 Prijavna služba Halcom CA

(1) Prijavna služba za ponudnika storitev zaupanja izvaja naslednje naloge:

1. preverjanje istovetnosti poslovnega subjekta in drugih, za upravljanje kvalificiranih digitalnih potrdil, pomembnih podatkov,
2. sprejemanje zahtevkov za pridobitev potrdil,
3. sprejemanje zahtevkov za preklic potrdil,
4. izdajanje potrebne dokumentacije poslovnim subjektom, imetnikom oz. bodočim imetnikom,
5. posredovanje zahtevkov in ostalih podatkov na varen način ponudniku storitev zaupanja Halcom CA.

(2) Ponudnik storitev zaupanja Halcom CA lahko poleg svoje prijavne službe za opravljanje nalog prijavne službe pooblasti tudi druge organizacije v poslovnem in javnem sektorju. Vsako takšno organizacijo ponudnik storitev zaupanja Halcom CA pogodbeno zaveže k izpolnjevanju strogih varnostnih pogojev v skladu z veljavnimi evropskim in slovenskimi predpisi ter mednarodnimi, evropskimi in slovenskimi standardi in priporočili ter politikami, pravili poslovanja in notranjimi pravili Halcom CA.

1.3.3 Naročniki in imetniki potrdil

(1) Imetnik potrdila, ki je naprava ponudnika storitev zaupanja, uporablja svoje, od ponudnika storitev zaupanja dodeljene, podatke (par ključev) za časovni žig in kvalificirana digitalna potrdila za povezavo tega z imetnikom.

(2) Naročnik potrdila je poslovni subjekt - ponudnik storitev zaupanja, ki ima glede na naravo potrdil vse pravice naročnika in imetnika po tej politiki.

1.3.4 Tretje osebe

(1) Tretje osebe so osebe, ki se zanašajo na izdana potrdila in druge storitve ponudnika storitev zaupanja Halcom CA, in so lahko fizične osebe ali poslovni subjekti.

(2) Tretje osebe se morajo ravnati po navodilih ponudnika storitev zaupanja Halcom CA in morajo vedno preveriti veljavnost potrdila, namen uporabe potrdila, čas veljavnosti potrdila itd. Podrobnejše obveznosti in odgovornosti tretjih oseb so navedene v razd. 4.5.2. in 9.6.4.

(3) Tretje osebe niso nujno tudi imetniki potrdil ponudnika storitev zaupanja Halcom CA ali digitalnih potrdil drugih ponudnikov storitev zaupanja.

1.4. Namen uporabe

Halcom CA upravlja (izdaja in preverja, preklicuje, podaljšuje, hrani, objavlja) s kvalificiranimi digitalnimi potrdili za časovni žig (v nadaljevanju potrdila), ki so namenjena ponudnikov storitev zaupanja.

1.4.1 Pravilna uporaba potrdil in ključev

Potrdila so namenjena ponudnikom storitev časovnega žigosanja.

1.4.2 Nedovoljena uporaba

(1) Prepovedna je uporaba potrdila, izdanih v skladu s to politiko, v nasprotju z določili te politike ali veljavnih predpisov ali izven obsega dovoljene uporabe, določene v prejšnjem razdelku.

(2) Potrdila niso namenjena nadaljnji prodaji.

1.5. Upravljanje politike

1.5.1 Upravljavec politik

(1) S to in drugimi svojimi politikami upravlja ponudnik storitev zaupanja Halcom CA, ki deluje v sklopu Halcom d.d.

(2) Naslov upravljavca:

Halcom d.d.
Tržaška 118
1000 LJUBLJANA
Slovenija

1.5.2 Pooblaščene kontaktne osebe

(1) Za vprašanja v zvezi s to politiko se lahko obrnete na pooblaščene osebe ponudnika storitev zaupanja, ki so dosegljive na spodnjem naslovu in spodaj navedenih telefonskih številkah.

(2) Naslov Halcom CA:

Halcom CA
Tržaška 118
1000 LJUBLJANA
Slovenija
Tel.: (+386) 01 200 34 86
Fax: (+386) 01 200 33 60
E-pošta: ca@halcom.si

1.5.3 Odgovorna oseba glede skladnosti delovanja ponudnika storitev zaupanja Halcom CA s politiko

Za skladnost delovanja ponudnika storitev zaupanja Halcom CA s to politiko so skladno s svojimi pristojnostmi odgovorne pooblaščene osebe ponudnika storitev zaupanja.

1.5.4 Postopek za sprejem nove politike

(1) Vsak predlog nove politike je pred potrditvijo glavnega izvršnega direktorja Halcom d.d. z namenom zagotavljanja zakonitosti, varnosti in kakovosti podvržen tako tehnološkemu kot tudi pravnemu pregledu.

(2) Ponudnik storitev zaupanja lahko za posamezna določila veljavne politike izda dopolnitve, kot je to določeno v razdelku 9.12.

1.6. Okrajšave in izrazi

1.6.1 Okrajšave

CA	Ponudnik storitev zaupanja, ki izdaja potrdila (angl.: Certificate Authority ali Certificate Agency).
CPName	Ime politike delovanja ponudnika storitev zaupanja (angl.: Certification Policy Name), enolično povezano z mednarodno številko politike delovanja CPOID (angl.: Certification Policy Object Identifier).
CPOID	Mednarodna številka, ki enolično določa politiko delovanja (angl.: Certification Policy Object IDentifier).
CRL	Certificate Revocation List – seznam preklicanih digitalnih potrdil.
DN	Enolično razločevalno ime (prim. opredelitev razločevalnega imena) (angl.: Distinguished Name).
CP	Politika ponudnika storitev zaupanja (angl. Certificate Policy). Politika ureja namen, delovanje in metodologijo upravljanja storitve ter odgovornosti in varnostne zahteve, ki jih morajo izpolnjevati ponudnik storitev zaupanja, imetniki potrdil (uporabniki storitev) in tretje osebe, ki se zanašajo na ta potrdila/storitev.
CPS	CPS (angl. Certification Practice Statement) predstavlja splošna pravila delovanja ponudnika storitev zaupanja.
LDAP	Leightweight Directory Access Protocol je protokol, ki določa dostop do imenika in je specificiran po IETF (Internet Engineering Task Force) priporočilu IETF RFC 3494:.
S/MIME	Secure Multipurpose Internet Mail Extensions
SSL	Secure Sockets Layer
TLS	Transport Layer Security
PKI	Public Key Infrastructure je infrastruktura javnih ključev.
UTC	Koordinirani univerzalni čas – mednarodni standard za merjenje časa, kii temelji na atomski uri; Ang.: Coordinated Universal Time

1.6.2 Izrazi

Imenik potrdil	Imenik potrdil po priporočilu X.500, kjer so shranjena potrdila po priporočilu X.509 ver. 3, do katerih je možen dostop po protokolu LDAP.
Identifikacija	Identifikacija pomeni postopek uporabe identifikacijskih podatkov osebe v fizični ali elektronski obliki, ki enolično predstavljajo bodisi fizično ali pravno osebo bodisi fizično osebo, ki zastopa pravno osebo.
Ponudnik storitev zaupanja	Fizična ali pravna oseba, ki izdaja potrdila ali opravlja druge storitve zaupanja (angl.: Trust Service provider - TSP).

Prijavna služba	Služba ali oseba, ki sprejema vloge za potrdila in prevzema identificiranje in preverjanje istovetnosti bodočih imetnikov v imenu ponudnika storitev zaupanja potrdil (angl.: Registration Authority - RA).
Razločevalno ime	Enolično ime v potrdilu (prim. opredelitev DN), ki nedvoumno in enolično definira uporabnika v strukturi imenika.
Časovni žig	Časovni žig (ang. Time stamp) je elektronsko podpisano kvalificirano potrdilo ponudnika storitev zaupanja, s katerim se zagotovi povezljivost elektronskih dokumentom z datumom in časom, do sekunde natančno, v katerem so bili ti elektronsko podpisani. Glede izdajanja časovnega žiga veljajo primerljive zakonske zahteve kot glede izdajanja kvalificiranih digitalnih potrdil.

2. OBJAVE INFORMACIJ IN JAVNI IMENIK POTRDIL

2.1. Zbirka dokumentov

(1) Ponudnik storitev zaupanja Halcom CA vse v zvezi s svojim delovanjem, obvestila imetnikom in tretjim osebam ter druge pomembne dokumente javno objavi na spletnih straneh Halcom CA na naslovu http://www.halcom.si (povzetki bistvenih sestavin tudi v angleškem jeziku).

(2) Dokumenti, ki so javno dostopni, so:

- politika uporabe storitev zaupanja (CP),
- pravila delovanja ponudnika storitev zaupanja (CPS)
- naročilnice in druge pogodbe za storitve ponudnika storitev zaupanja,
- navodila za varno uporabo digitalnih potrdil,
- informacije o veljavnih predpisih in standardih v zvezi z delovanjem ponudnika storitev zaupanja ter
- ostale informacije v zvezi z delovanjem Halcom CA.

(3) Javno pa niso dostopni dokumenti, ki predstavljajo zaupni del notranjih pravil ponudnika storitev zaupanja Halcom CA.

2.2. Imenik potrdil

(1) Nove politike so objavljene v skladu z navedbo v razdelku 9.10.

(2) Vsa potrdila ponudnika storitev zaupanja temeljijo na standardu X.509 in so objavljena v centralnem imeniku na strežniku ldap.halcom.si, ki je v skrbništvu HALCOM CA. Zaradi varstva podatkov je javno dostopen le register preklicanih potrdil, ki je del imenika.

(3) Preklicana potrdila se v registru preklicanih potrdil objavijo takoj (podrobno o tem v razd. 4.9.8.), ostale javno dostopne informacije oz. dokumenti pa se objavijo po potrebi.

(4) Dostop do imenika izdanih potrdil je omogočen le pooblaščenim uporabnikom, ki preverjajo večje število izdanih potrdil.

2.3. Pogostnost objav

(1) Nova politika se objavi takoj po sprejemu.

(2) Halcom CA poskrbi, da se potrdila objavijo v javnem imeniku takoj po njihovi izdaji.

(3) Spisek preklicanih potrdil se osveži takoj po preklicu potrdila v javnem imeniku preklicanih potrdil Halcom CA. Z nekajminutnim zamikom se ta osvežitev prenese tudi na spletne strani.

(4) Javno dostopne informacije oz. dokumenti (razen zgoraj navedenih) se objavijo po potrebi.

2.4. Upravljanje dostopa do zbirke dokumentov

(1) Centralni imenik je dostopen na strežniku ldap.halcom.si, TCP vratih 389 po protokolu LDAP. Javno dostopen je le register preklicanih potrdil, ki je del imenika.

(2) Z ustreznimi tehničnimi ukrepi informacijske varnosti Halcom CA zagotavlja kontrole, ki preprečujejo nepooblaščeno dodajanje, spreminjanje ali brisanje podatkov v javnem imeniku potrdil.

3. ISTOVETNOST IMETNIKOV POTRDIL

3.1. Dodelitev imen

Razločevalna imena, ki jih vsebuje potrdilo, nedvoumno in enolično definirajo imetnika potrdila, razen če je drugače zahtevano bodisi s to politiko bodisi z vsebino kvalificiranega digitalnega potrdila.

3.1.1 Razločevalna imena

(1) Skladno z IETF RFC 5280 vsebuje vsako potrdilo podatke o imetniku ter ponudniku storitev zaupanja v obliki razločevalnega imena. Razločevalno ime je oblikovano skladno z IETF RFC 5280 in standardom X501.

(2) Ponudnik storitev zaupanja potrdila je v izdanem potrdilu naveden v polju Izdajatelj, angl. Issuer. Osnovni podatki o poslovnem subjektu in imetniku, ki jih vsebuje razločevalno ime potrdil za poslovne subjekte, so v izdanem potrdilu navedeni v polju Imetnik angl. Subject.

(3) Serijsko številko, ki jo prav tako vsebuje razločevalno ime, določi ponudnik storitev zaupanja Halcom CA. (več v razd. 3.1.5.)

Vrsta potrdila	Naziv polja	Razločevalno ime
Korensko (Root) potrdilo ponudnika storitev zaupanja Halcom CA	Izdajatelj, angl. Issuer in Imetnik, angl. Subject	C= SI O= Halcom d.d. 2.5.4.97 = VATSI-43353126 CN= Halcom Root Certificate Authority
Vmesno/podrejeno (Intermediate) potrdilo ponudnika storitev zaupanja Halcom CA	Izdajatelj, angl. Issuer	C= SI O= Halcom d.d. 2.5.4.97 = VATSI-43353126 CN= Halcom Root Certificate Authority
	Imetnik, angl. Subject	C= SI O= Halcom d.d. 2.5.4.97= VATSI-43353126 CN= Halcom CA TSA 1
Kvalificirano digitalno potrdilo uporabnika	Izdajatelj, angl. Issuer	C= SI O= Halcom d.d.

		2.5.4.97= VATSI-43353126 CN= Halcom CA TSA 1
	Imetnik, angl. Subject	C= SI O= <naziv poslovnega subjekta> 2.5.4.97=VAT<dvomestna ISO oznaka države>-<davčna št. poslovnega subjekta> in/ali 1.3.6.1.4.1.5939.2.3= <davčna št. poslovnega subjekta> OU= TSA CN=<naziv servisa časovnega žigosanja> E = <e-pošta>

3.1.2 Zahteve pri tvorbi razločevalnega imena

(1) Oznaka poslovnega subjekta, ki je v skladu z določili razd. 3.1.1 vključena v razločevalno ime, mora izpolnjevati naslednje zahteve:

- mora biti enolično, registrirano v poslovnem ali drugem uradnem registru,
- mora biti pomensko povezano z imetnikom oz. poslovnim subjektom,
- največja dolžina je lahko dvainštirideset (42) znakov.

(2) Halcom CA si pridržuje pravico za zavrnitev firme, naziva ali oznake poslovnega subjekta, če ugotovi:

- da je le-to neprimerno oz. žaljivo,
- da je zavajajoče za tretje stranke oz. že pripada neki drugi pravni ali fizični osebi,
- da je v nasprotju z veljavnimi predpisi.

3.1.3 Uporaba anonimnih imen ali psevdonimov

Uporaba anonimnih imen ali psevdonimov ni dovoljena.

3.1.4 Pravila za interpretacijo razločevalnih imen

(1) Podatki o imetniku potrdila v razločevalnem imenu vsebujejo črke angleške abecede, preostali znaki pa se pretvorijo po spodnjem pravilu:

Znak	Pretvorba
Č	C
Ć	C
Đ	DJ
Š	S
Ž	Z
Ü	UE
Ö	OE
Ø	OE
ß	SS
Ñ	N
Ŕ	RZ

(2) Z ustrezno kombinacijo črk ponudnik storitev zaupanja zagotovi uporabo drugih nepredvidenih znakov.

3.1.5 Enoličnost razločevalnih imen

Razločevalna imena so enolična za vsako izdano potrdilo in nedvoumno in enolično identificirajo

imetnika v strukturi imenika.

3.1.6 Zaščite imen oz. znamk

(1) Poslovni subjekti oz. imetniki ne smejo zahtevati nazivov državnih organov ali organov lokalnih skupnosti, imen, označb, blagovnih znamk ali drugih elementov intelektualne lastnine, ki bi pripadale tretjim osebam in bi bile s tem kršene pravice intelektualne lastnine ali druge pravice tretjih oseb ali določbe veljavnih predpisov.

(2) Morebitne spore rešujeta izključno prizadeta stran in imetnik potrdila.

(3) Odgovornost v zvezi z uporabo imen oz. zaščitenih znamk je izključno na strani poslovnega subjekta. Ponudnik storitev zaupanja Halcom CA ni dolžan preverjati in/ali na to opozoriti imetnika oz. poslovnega subjekta.

3.2. Preverjanje istovetnosti imetnikov ob prvi izdaji potrdila

3.2.1 Metoda za posedovanje pripadnosti zasebnega ključa

Dokazovanje o posedovanju zasebnega ključa, ki pripada javnemu ključu v potrdilu, je zagotovljeno z varnimi postopki pred in ob prevzemu potrdila ter standardom PKCS#10.

3.2.2 Preverjanje istovetnosti organizacije

(1) Podatki o poslovnem subjektu so navedeni v razločevalnem imenu, glej razd. 3.1.1 in 3.1.2.

(2) Za pravilnost podatkov jamči zakoniti zastopnik poslovnega subjekta s podpisom na dokumentaciji za pridobitev potrdila.

(3) Ponudnik storitev zaupanja Halcom CA pri ustreznih službah, uradnih evidencah ali s pomočjo uradno potrjene dokumentacije preveri pravilnost podatkov poslovnega subjekta in istovetnost odgovorne osebe.

3.2.3 Preverjanje istovetnosti imetnika

(1) Imetnik potrdila je poslovni subjekt –ponudnik storitev zaupanja za svoje naprave.

(3) Poslovni subjekt se zavezuje, da bodo upravljalci potrdil izpolnjevali vse določbe Politike Halcom CA in veljavne predpise.

3.2.4 Nepreverjeni podatki v potrdilih

Halcom CA ne preverja pravilnosti in delovanja naslova e-pošte imetnika potrdila.

3.2.5 Preverjanje pooblastil zaposlenih za pridobitev potrdil

Zakoniti zastopnik poslovnega subjekta s podpisom na dokumentaciji za pridobitev potrdila jamči, da želi za poslovni subjekt pridobiti ustrezno potrdilo.

3.2.6 Medsebojno priznavanje

(1) Ponudnik storitev zaupanja Halcom CA ni dolžan pogodbeno sodelovati ali jamčiti za druge

ponudnike storitev zaupanja tudi, če ima drugi ponudnik status kvalificiranega ponudnika storitev zaupanja.

(2) Ponudnik storitev zaupanja Halcom CA zagotavlja, da bo izvajal medsebojno priznavanje izključno po podpisu pisne pogodbe z drugimi ponudnik storitev zaupanja, ki pa morajo izpolnjevati raven varnostnih zahtev, ki je primerljiva ali višja, kot jo predpiše ponudnik storitev zaupanja Halcom CA.

(3) Če ni zagotovljena zunanja in neodvisna presoja skladnosti, pooblaščene osebe ponudnika storitev zaupanja Halcom CA pregledajo notranja pravila drugega ponudnika storitev zaupanja ter njegovo izpolnjevanje varnostnih zahtev.

(4) Stroške potrebne infrastrukture, ki jo zahteva ponudnik storitev zaupanja Halcom CA za medsebojno priznavanje, krije drugi ponudnik storitev zaupanja.

3.3. Preverjanje imetnikov za ponovno izdajo potrdila

3.3.1 Preverjanje imetnikov pri podaljšanju potrdil

Istovetnost imetnikov pri ponovni izdaji potrdila se preverja:

- na prijavni službi ponudnika storitev zaupanja Halcom CA,
- na podlagi že izdanega veljavnega kvalificiranega digitalnega potrdila, ki ga je izdal kvalificiran ponudnik storitev zaupanja, pri čemer ponudnik storitev zaupanja Halcom CA preveri podatke fizične osebe ali poslovnega subjekta v ustreznih registrih.

3.3.2 Preverjanje imetnikov za ponovno pridobitev potrdila po preklicu

Preverjanje imetnikov poteka skladno z določili iz razd. 3.2.3.

3.4. Preverjanje istovetnosti ob zahtevi za preklic

(1) Zahtevek za preklic potrdila poslovni subjekt odda:

- osebno na prijavno službo, kjer pooblaščene osebe preverijo istovetnost zakonitega zastopnika,
- elektronsko, vendar mora biti zahtevek digitalno podpisan z kvalificiranim digitalnim potrdilom, s tem pa izkazana tudi istovetnost prosilca,
- če imetnik potrdila prek telefona, elektronske pošte ali FAX-a zahteva preklic potrdila, ponudnik storitev zaupanja Halcom CA odredi suspenz potrdila. Šele na podlagi pisne zahteve za preklic potrdila, pa se dejansko izvede preklic potrdila.

(2) Podroben postopek za preklic: razd. 4.9.3.

4. UPRAVLJANJE S POTRDILI

4.1. Pridobitev potrdila

4.1.1 Kdo lahko pridobi potrdilo

Bodoči imetniki potrdil izdanih po tej politiki so poslovni subjekti - ponudniki storitev zaupanja za svoje naprave.

4.1.2 Postopek bodočega imetnika za pridobitev potrdila in odgovornosti

(1) Potrdilo se izda na podlagi podpisane pogodbe s poslovnim subjektom – ponudnikom storitev zaupanja in pravilno izpolnjene in podpisane naročilnice izdajo potrdila za časovni žig (v nadaljevanju naročilnice) s strani zakonitega zastopnika poslovnega subjekta. Vlogo zakoniti zastopnik odda prijavni službi Halcom CA, ter poravna finančne obveznosti v zvezi z izdajo potrdila. Naročilnice za izdajo digitalnega potrdila so na voljo pri prijavni službi Halcom CA.

(2) Zakoniti zastopnik poslovnega subjekta poda vlogo v pisni obliki.

(3) Pred izdajo naročilnice Halcom CA poslovni subjekt seznani s to politiko in splošnimi pravili delovanja ponudnika storitev zaupanja Halcom CA.

(4) Halcom CA si pridružuje pravico do zavrnitve vloge za izdajo potrdila brez posebne pisne obrazložitve zaradi pomanjkljivih podatkov, dokumentacije ali previsokega tveganja za varnost ali zakonitost delovanja.

4.2. Postopek ob sprejemu zahtevka za pridobitev potrdila

4.2.1 Preverjanje istovetnosti bodočega imetnika

(1) Potrdilo se izda na osnovi podpisane pogodbe in pravilno izpolnjene in podpisane naročilnice za izdajo potrdila za časovni žig (v nadaljevanju naročilnica) s strani zakonitega zastopnika poslovnega subjekta. Vlogo zakoniti zastopnik odda prijavni službi Halcom CA, ter poravna finančne obveznosti v zvezi z izdajo potrdila. Naročilnice za izdajo digitalnega potrdila so na voljo pri prijavni službi Halcom CA.

(2) Zakoniti zastopnik poslovnega subjekta poda vlogo v pisni obliki.

(3) Pred izdajo potrdila Halcom CA poslovni subjekt seznani s to politiko in splošnimi pravili delovanja ponudnika storitev zaupanja Halcom CA.

(4) Halcom CA si pridružuje pravico do zavrnitve vloge za izdajo potrdila brez posebne pisne obrazložitve zaradi pomanjkljivih podatkov, dokumentacije ali previsokega tveganja za varnost ali zakonitost delovanja.

4.2.2 Odobritev/zavrnitev zahtevka

(1) Pooblaščene osebe ponudnika storitev zaupanja Halcom CA naročilnico za pridobitev potrdila odobrijo oz. v primeru nepravilnih ali pomanjkljivih podatkov ali neizpolnjevanja obveznosti zavrnejo, o čemer je poslovni subjekt nemudoma obveščen osebno ali po e-pošti.

(2) V primeru odobritve ponudnik storitev zaupanja Halcom CA pred izdajo potrdila obvesti bodočega imetnika v skladu z veljavnimi predpisi.

4.2.3 Čas za izdajo potrdila

Halcom CA na podlagi podpisane pogodbe in odobrene naročilnice, pridobljenega elektronskega zahtevka (ang. »certificate request«) in poravnanih finančnih obveznosti v zvezi z izdajo potrdila izda potrdilo najkasneje v petih (5) delovnih dneh od prejetega plačila.

4.3. Izdaja potrdila

4.3.1 Postopek ponudnika storitev zaupanja Halcom CA

(1) Proizvodni postopek za potrdila in za par ključev je sestavljen iz jasno ločenih delov (ali funkcij), z njihovimi ustrezno ločenimi podsistemi:

1. podpis pogodbe
2. obravnava vloge za izdajo potrdila,
3. pridobitev elektronskega zahtevka (ang. »certificate request«),
4. preverjanje in potrditev izdaje potrdila,
5. pooseblјanje in izdaja potrdila,
6. posredovanje potrdila imetniku.

(2) Vsi opisani postopki so zasnovani tako, da jih ne more opraviti posamezna oseba sama.

4.3.2 Obvestilo imetnika o izdaji

Glej prejšnji razdelek.

4.4. Prevzem potrdila

4.4.1 Postopek prevzema potrdila

(1) Poslovni subjekt v strojnem varnostnem modulu (ang. HSM- hardware security module) sproži generacijo ključev in določi geslo za zaščito le-teh.

(2) Halcom CA na podlagi prejetega elektronskega zahtevka (»certificate request«) izdela potrdilo in ga posreduje poslovnemu subjektu.

(3) Poslovni subjekt s pomočjo prej omenjenega gesla kreira strežniško potrdilo s pripadajočim parom ključev.

(4) Pooblaščena oseba poslovnega subjekta mora ob prevzemu potrdila nemudoma preveriti podatke v potrdilu in ob morebitnih napakah ali problemih takoj obvestiti Halcom CA.

4.4.2 Objava potrdila

Postopek je opisan v 2. razdelku

4.4.3 Obvestilo ponudnika storitev zaupanja o izdaji potrdila tretjim osebam

Ponudnik storitev zaupanja Halcom CA o izdaji posameznega potrdila imetnikom potrdila ne obvešča tretjih oseb.

4.5. Obveznosti in odgovornosti uporabnikov glede uporabe potrdil

4.5.1 Obveznosti imetnika potrdila

(1) Imetnik oziroma bodoči imetnik potrdila je dolžan:

- seznaniti se in ravnati v skladu s politiko pred izdajo potrdila,
- ravnati v skladu s politiko in ostalimi veljavnimi predpisi,
- po prevzemu potrdila preveriti podatke v potrdilu in ob morebitnih napakah ali

problemih takoj obvestiti Halcom CA oziroma zahtevati preklic potrdila,
- spremljati vsa obvestila Halcom CA in ravnati v skladu z njimi,
- v skladu z obvestili ustrezno posodabljati potrebno strojno in programsko opremo za varno delo s potrdili,
- nemudoma sporočiti Halcom CA vse spremembe, ki so povezane s potrdilom,
- zahtevati preklic potrdila, če je bil zasebni ključ ogrožen na način, ki vpliva na zanesljivost uporabe, ali če obstaja nevarnost zlorabe,
- uporabljati potrdilo za namen, določen v potrdilu (glej razdelek 7.1.), in na način, ki je določen s politiko Halcom CA.

(2) Imetnik oziroma bodoči imetnik potrdila je glede varovanja zasebnega ključa dolžan tudi:
- podatke za prevzem potrdila skrbno varovati pred nepooblaščenimi osebami,
- hraniti zasebni ključ in potrdilo na način in na sredstvih za varno hranjenje zasebnih ključev v skladu z obvestili in priporočili Halcom CA,
- zasebni ključ in vse druge zaupne podatke ščititi s primernim geslom v skladu s priporočili Halcom CA ali na drug način tako, da ima dostop do njih samo imetnik,
- skrbno varovati gesla za zaščito zasebnega ključa,
- po preteku veljavnosti oz. preklicu potrdila ravnati v skladu z obvestili Halcom CA.

4.5.2 Obveznosti za tretje osebe

(1) Tretja oseba, ki se zanaša na potrdilo, mora:
- ravnati in uporabljati potrdila v skladu in namenom s politiko in ostalimi veljavnimi predpisi,
- skrbno proučiti vse možnosti tveganja in odgovornosti pri uporabi potrdil in določiti politiko za način uporabe,
- obvestiti Halcom CA, če izve, da so bili zasebni ključi imetnika potrdila, na katerega se zanaša, ogroženi na način, ki vpliva na zanesljivost uporabe, ali če obstaja nevarnost zlorabe, ali če so se spremenili podatki, navedeni v potrdilu,
- se zanašati na potrdilo samo za namen, določen v potrdilu (glej razd.6.1.7.) na način, ki je določen s politiko,
- v času uporabe potrdila preveriti, če potrdilo ni v registru preklicanih potrdil,
- v času uporabe potrdila preveriti, če je bilo digitalno potrdilo kreirano z ustreznim namenom potrdila,
- v času uporabe potrdila preveriti podpis potrdila ponudnika storitev zaupanja Halcom CA, ki je objavljen v tej politiki in tudi na spletnih straneh Halcom,
- upoštevati druge določbe, v kolikor je s ponudnikom storitev zaupanja Halcom CA sklenila dogovor o uporabi potrdil.

(2) Tretja oseba mora za preverjanje veljavnosti podpisa oz. druge kriptografske operacije uporabljati programsko in strojno opremo, s katero lahko na verodostojen način preveri vse zgoraj navedene zahteve za varno uporabo potrdil.

4.6. Ponovna izdaja potrdila

Ponovna izdaja potrdila poteka na enak način kot prva pridobitev potrdila (glej razd. 4.1).

4.6.1 Okoliščine, ki terjajo ponovno izdajo potrdila

Pred potekom veljavnosti digitalnega potrdila si z zahtevkom za ponovno izdajo imetniki potrdil zagotovijo kontinuiteto uporabe digitalnega potrdila. Zahtevek za novo izdajo pa je mogoče

vložiti tudi po poteku veljavnosti digitalnega potrdila.

4.6.2 Osebe, ki lahko zahtevajo ponovno izdajo potrdila

Ponovno izdajo potrdila lahko zahteva zakoniti zastopnik poslovnega subjekta.

4.6.3 Postopek obravnave prošenj za ponovno izdajo potrdila

Postopek je enak postopku pri prvem naročilu potrdila (glej razd. 4.2).

4.6.4 Obvestilo imetniku o novo izdanem potrdilu

Glej razd. 4.3.1.

4.6.5 Postopek prevzema novo izdanega potrdila

Glej razd. 4.4.1.

4.6.6 Objava novo izdanega potrdila

Postopek je opisan v 2. razdelku.

4.6.7 Obvestilo ponudnika storitev zaupanja o izdaji potrdila tretjim osebam

Ponudnik storitev zaupanja Halcom CA o izdaji posameznega potrdila imetnikom potrdila ne obvešča tretjih oseb.

4.7. Regeneriranje ključev

4.7.1 Razlogi za regeneracijo

Ni podprto.

4.7.2 Kdo zahteva regeneracijo

Ni podprto.

4.7.3 Postopek za izdajo zahtevka za regeneracijo

Ni podprt.

4.7.4 Obvestilo imetniku potrdila o novo izdanem potrdilu

Ni podprto.

4.7.5 Postopek prevzema

Ni podprt.

4.7.6 Objava potrdila ponudnika storitev zaupanja z novim parom ključev

Ni podprta.

4.7.7 Obvestilo ponudnika storitev zaupanja o izdaji potrdila tretjim osebam

Ni podprto.

4.8. Sprememba potrdila

(1) V primeru spremembe podatkov, ki vplivajo na veljavnost razločevalnega imena oz. drugih podatkov v potrdilu, je potrebno potrdilo preklicati.

(2) Za pridobitev novega potrdila je potrebno ponoviti postopek za pridobitev novega potrdila, kot je naveden v razdelku 4.1.

4.8.1 Okoliščina za spremembo potrdila

Ni podprta.

4.8.2 Kdo zahteva spremembo

Ni podprto.

4.8.3 Postopek ob zahtevku za spremembo

Ni podprt.

4.8.4 Obvestilo o izdaji novega potrdila

Ni podprto.

4.8.5 Prevzem spremenjenega potrdila

Ni podprt.

4.8.6 Objava spremenjenega potrdila

Ni podprta.

4.8.7 Obvestilo drugih subjektov o spremembi

Ni podprto.

4.9. Preklic in suspenz potrdila

(1) Preklic potrdila lahko poslovni subjekt zahteva kadarkoli, mora pa ga zahtevati v primeru:

- spremembe razločevalnega imena (DN),
- ko poslovni subjekt ali imetnik potrdila zamenja ključne podatke, povezane s potrdilom (naziv storitve, poslovnega subjekta in podobno),
- ko se ugotovi ali sumi, da je prišlo do razkritja ključa ali zlorabe potrdila,
- nadomestitvi potrdila z drugim potrdilom (npr. ob izgubi gesel za dostop do potrdila in podobno).

(2) Halcom CA lahko prekliče potrdilo tudi brez zahteve imetnika v primerih iz prvega odstavka ali na podlagi zahteve pristojnega sodišča, prekrškovnih ali upravnih organov.

(3) Preklic potrdila je mogoč 24 ur dnevno. Natančna navodila za preklic potrdila so objavljena na spletnih straneh Halcom CA.

(4) Halcom CA bo na podlagi pravilne zahteve za preklic potrdila potrdilo preklical najkasneje v štirih (4) urah. V primeru nastanka nepredvidljivih okoliščin bo Halcom CA izjemoma preklical potrdilo najkasneje v 8 (osmih) urah po prejemu pravilne zahteve za preklic potrdila. V tem času bo preklicano potrdilo v imeniku označeno kot preklicano in dodano v register preklicanih potrdil. Če bo imetnik potrdila Halcom CA posredoval nepravilno zahtevo za preklic potrdila, mu bo poslano opozorilo o nepravilni zahtevi za preklic potrdila in bo seznanjen z navodili za vložitev pravilne zahteve za preklic.

4.9.1 Razlogi za preklic

(1) Preklic potrdila mora poslovni subjekt zahtevati v primeru:
- če je bil zasebni ključ imetnika potrdila ogrožen na način, ki vpliva na zanesljivost uporabe,
- če obstaja nevarnost zlorabe zasebnega ključa ali potrdila imetnika,
- če so se spremenili oz. so napačni ključni podatki, navedeni v potrdilu.

(2) Ponudnik storitev zaupanja Halcom CA prekliče potrdilo tudi brez zahteve imetnika takoj, ko izve:
- da je podatek v potrdilu napačen ali je bilo potrdilo izdano na podlagi napačnih podatkov,
- da je prišlo do napake pri preverjanju istovetnosti podatkov na prijavni službi,
- da so se spremenile druge okoliščine, ki vplivajo na veljavnost potrdila,
- za neizpolnjevanje obveznosti imetnika,
- da niso poravnani morebitni stroški za upravljanje digitalnih potrdil,
- da je bila infrastruktura ponudnika storitev zaupanja ogrožena na način, ki vpliva na zanesljivost potrdila,
- da je bil zasebni ključ imetnika potrdila ogrožen na način, ki vpliva na zanesljivost uporabe,
- da bo Halcom CA prenehal z izdajanjem potrdil ali da je bilo ponudniku storitev zaupanja prepovedano upravljanje s potrdili in njegove dejavnosti ni prevzel drug ponudnik storitev zaupanja,
- da je preklic odredilo pristojno sodišče, prekrškovni ali upravni organ.

4.9.2 Kdo zahteva preklic

Preklic potrdila lahko zahteva:
- pooblaščena oseba ponudnika storitev zaupanja Halcom CA,
- zakoniti zastopnik poslovnega subjekta,
- imetnik (skrbnik potrdila za časovni žig),
- pristojno sodišče, prekrškovni ali upravni organ.

4.9.3 Postopki za preklic

(1) Preklic lahko zakoniti zastopnik poslovnega subjekta ali imetnik zahteva:
- osebno v času uradnih ur na prijavni službi,
- elektronsko štiriindvajset (24) ur na dan vse dni v letu, če gre za možnost zlorabe ali nezanesljivosti potrdila, sicer v času, ki po veljavni zakonodaji velja za poslovni čas državnih organov,
- po faksu štiriindvajset (24) ur na dan vse dni v letu, če gre za možnost zlorabe ali nezanesljivosti potrdila, sicer v času, ki po veljavni zakonodaji velja za poslovni čas državnih organov,

(2) Če se preklic zahteva:
- osebno, je potrebno izpolniti ustrezen zahtevek za preklic potrdila ter ga oddati na prijavno službo,
- elektronsko, mora imetnik poslati na Halcom CA elektronsko sporočilo z zahtevkom za preklic, ki mora biti digitalno podpisan z zaupanja vrednim potrdilom za njegovo preverjanje,
- po faksu, mora imetnik izpolniti ustrezen zahtevek za preklic potrdila ter ga poslati po FAX-u na ustrezno dežurno FAX št. (glej razd. 1.3.1.) in naknadno priporočeno poslati po pošti ali oddati na prijavno službo,
- če imetnik potrdila prek telefona, elektronske pošte ali FAX-a zahteva preklic potrdila, ponudnik storitev zaupanja Halcom CA odredi suspenz potrdila. Šele na podlagi pisne zahteve za preklic potrdila, pa se dejansko izvede preklic potrdila.

(4) O datumu ter času preklica, vložniku zahtevka za preklic ter vzrokih za preklic morata biti vedno obveščena poslovni subjekt ali imetnik.

(5) Sodišča, prekrškovni in upravni organi, ki tudi lahko zahtevajo preklic, storijo to skladno z zakoni, ki urejajo postopek pred njimi (kazenski postopek, pravdni postopek, splošni upravni postopek in drugi).

4.9.4 Čas za izdajo zahtevka za preklic

Preklic je potrebno zahtevati nemudoma, če gre za možnost zlorabe ali nezanesljivosti ipd. nujne primere. V ostalih primerih se preklic lahko zahteva prvi delovni dan v času, ki velja za čas uradnih ur na prijavnih službah (glej naslednji razdelek).

4.9.5 Čas od prejetega zahtevka za preklic do izvedbe preklica

(1) Ponudnik storitev zaupanja Halcom CA po prejemu veljavne zahteve za preklic:
- najkasneje v štirih (4) urah prekliče potrdilo, če gre za preklic zaradi nevarnosti zlorabe ali nezanesljivosti ipd.,
- sicer pa prvi delovni dan po prejetju zahtevka za preklic.

(2) Po preklicu je tako potrdilo takoj dodano v register preklicanih potrdil.

4.9.6 Zahteve po preverjanju registra preklicanih potrdil za tretje osebe

(1) Pred uporabo morajo tretje osebe, ki se zanašajo na potrdilo, preveriti najnovejši objavljeni register preklicanih potrdil. Zaradi verodostojnosti in celovitosti je vedno potrebno preveriti tudi verodostojnost tega registra, ki je digitalno podpisan s strani Halcom CA.

(2) Tretja oseba mora za vsako uporabljeno digitalno potrdilo izvesti popoln postopek preverjanja verige zaupanja v skladu z evropskimi in mednarodnimi standardi in priporočili.

4.9.7 Pogostnost objave registra preklicanih potrdil

Register preklicanih potrdil se osvežuje (za dostop do registra glej razd. 7.2.3):

- po vsakem preklicu potrdila,
- enkrat dnevno, če ni novih zapisov oz. sprememb v registru preklicanih potrdil, in sicer približno štiriindvajset (24) ur po zadnjem osveževanju.

4.9.8 Čas objave registra preklicanih potrdil

Objava novega registra preklicanih potrdil se izvede:

- v javnem imeniku na strežniku ldap://ldap.halcom.si takoj (največ 5 sekund),
- na spletni strani http://domina.halcom.si/crls pa z zakasnitvijo največ desetih (10) minut.

4.9.9 Sprotno preverjanje statusa potrdil

Podprt je protokol za sprotno preverjanje statusa potrdil (OCSP) v skladu z evropskimi in mednarodnimi standardi in priporočili (glej razd. 7.3).

4.9.10 Zahteve za sprotno preverjanje statusa potrdil

Tretje osebe morajo ob uporabi potrdila vedno preveriti, ali je potrdilo, na katerega se zanašajo, preklicano.

4.9.11 Drugi načini za dostop do statusa potrdil

Niso podprti.

4.9.12 Posebne zahteve pri zlorabi zasebnega ključa

Niso določene.

4.9.13 Razlogi za suspenz

(1) Če imetnik potrdila telefonsko, elektronsko ali po FAX-u zahteva preklic potrdila, se do prejema originala pisne zahteve potrdilo začasno suspendira.

(2) Če imetnik potrdila, tretje ali druge osebe, državni ali sorodni organi oziroma ponudnik storitev zaupanja sam, izrazi sum, da se v zvezi s potrdilom ravna v nasprotju s to politiko oziroma veljavnimi predpisi, se potrdilo začasno suspendira do dokončne odločitve.

4.9.14 Kdo zahteva suspenz

Glej razd. 4.9.13.

4.9.15 Postopek za suspenz

Glej razd. 4.9.13.

4.9.16 Čas suspenza

Glej razd. 4.9.13.

4.10. Preverjanje statusa potrdil

4.10.1 Dostop za preverjanje

(1) Register preklicanih potrdil je javno objavljen na strežniku ldap://ldap.halcom.si/ po protokolu LDAP in na http://domina.halcom.si/crls po protokolu HTTP.

(2) Sprotno preverjanje statusa potrdila je dostopno na naslovu http://ocsp.halcom.si.

(3) Podrobnosti o objavi in dostopu so v razdelku 7.2 in 7.3.

4.10.2 Razpoložljivost

Preverjanje statusa potrdil je stalno na razpolago štiriindvajset (24) ur vse dni v letu.

4.10.3 Druge informacije za preverjanje statusa

Niso predpisane.

4.11. Prekinitev razmerja med imetnikom in ponudnikom storitev zaupanja

Razmerje med imetnikom oz. poslovnim subjektom in ponudnikom storitev zaupanja Halcom CA se prekine, če/ob:

- imetnikovo potrdilo preteče in ga le-ta ne podaljša,
- je potrdilo preklicano, imetnik pa ne zaprosi za novega,
- nespoštovanju ali prenehanju pogodbenega razmerja.

4.12. Odkrivanje kopije ključev za dešifriranje

4.12.1 Razlogi za odkrivanje kopije ključev za dešifriranje

Ni podprto.

4.12.2 Kdo zahteva odkrivanje kopije ključev za dešifriranje

Ni podprto.

4.12.3 Postopek ob zahtevku za odkrivanje kopije ključev za dešifriranje

Ni podprto.

5. UPRAVLJANJE IN VARNOSTNI NADZOR INFRASTRUKTURE

(1) Halcom CA načrtuje in izvaja vse varnostne ukrepe v skladu z družino standardov ISO/IEC 27000 in s FIPS 140-2 nivo 3 ter s tehničnimi zahtevami ETSI.

(2) Oprema Halcom CA je postavljena v posebnih, ločenih prostorih in je zavarovana z večnivojskim sistemom fizičnega in protivlomnega tehničnega varovanja. Oprema je varovana proti nepooblaščenemu dostopu. Prav tako je zavarovana in zaščitena s protipožarnim sistemom, s sistemom proti izlitju vode, sistemom za prezračevanje in večnivojskim sistemom neprekinjenega napajanja.

(3) Halcom CA shranjuje rezervne in distribucijske nosilce podatkov tako, da je v največji meri preprečena izguba, vdor ali nepooblaščena uporaba ali spreminjanje shranjenih informacij. Tako za obnovitev podatkov kot za arhiviranje pomembnih informacij so zagotovljene rezervne

kopije, ki so shranjene na drugem mestu, kot je shranjena programska oprema za upravljanje s potrdili, za zagotovitev ponovnega delovanja v primerih, ko bi bili uničeni podatki na osnovni lokaciji.

(4) Podroben opis infrastrukture Halcom CA, operativno delovanje, postopki upravljanja z infrastrukturo ter nadzor nad varnostno politiko njegovega delovanja je določen z njegovimi notranjimi pravili.

5.1. Fizično varovanje

(1) Oprema ponudnika storitev zaupanja je varovana z večnivojskim sistemom fizičnega in elektronskega varovanja.

(2) Varovanje infrastrukture ponudnika storitev zaupanja se izvaja v skladu s priporočili stroke za najvišji nivo varovanja.

(3) Celoten opis infrastrukture ponudnika storitev zaupanja in postopki upravljanja ter varovanje le-te so določeni z notranjimi pravili ponudnika storitev zaupanja.

5.1.1 Lokacija in zgradba ponudnika storitev zaupanja

(1) Oprema ponudnika storitev zaupanja na Halcom CA je postavljena v posebnih, varovanih, ločenih prostorih.

(2) Zavarovana je z večnivojskim sistemom fizičnega in elektronskega varovanja.

(3) Podrobna določila so v notranjih pravilih ponudnika storitev zaupanja Halcom CA.

5.1.2 Fizični dostop do infrastrukture ponudnika storitev zaupanja

(1) Dostop do infrastrukture ponudnika storitev zaupanja je omogočen samo pooblaščenim osebam ponudnika storitev zaupanja skladno z njihovimi nalogami in pooblastili, glej razd. 5.2.1.

(2) Vsi dostopi so varovani v skladu z zakonodajo in priporočili.

(3) Podrobna določila so v notranjih pravilih ponudnika storitev zaupanja Halcom CA.

5.1.3 Napajanje in prezračevanje

(1) Infrastruktura ponudnika storitev zaupanja ima zagotovljeno neprekinjeno napajanje in ustrezne klimatske sisteme.

(2) Podrobno o tem je določeno v notranjih pravilih ponudnika storitev zaupanja Halcom CA.

5.1.4 Zaščita pred poplavo

(1) Infrastruktura ponudnika storitev zaupanja ni izpostavljena nevarnosti poplav, razen v primeru višje sile.

(2) Podrobno o tem je določeno v notranjih pravilih ponudnika storitev zaupanja Halcom CA.

5.1.5 Zaščita pred požari

(1) Prostori ponudnika storitev zaupanja so varovani pred morebitnim izbruhom požara.

(2) Podrobno o tem je določeno v notranjih pravilih ponudnika storitev zaupanja Halcom CA.

5.1.6 Hramba nosilcev podatkov

(1) Nosilci podatkov, bodisi v papirnati ali elektronski obliki, se hranijo varno v zaščitenih objektih.

(2) Varnostne kopije programske opreme in šifriranih baz ponudnika storitev zaupanja Halcom CA se redno obnavljajo in shranjujejo v dveh ločenih in fizično varovanih prostorih, na različnih lokacijah.

5.1.7 Odstranjevanje odpadkov

(1) Halcom CA zagotavlja varno odstranjevanje in uničevanje dokumentov v fizični in elektronski obliki.

(2) Odstranjevanje odpadkov izvaja posebna komisija v skladu z notranjimi pravili ponudnika storitev zaupanja Halcom CA.

(3) Podrobno o tem je določeno v Splošnih pravilih delovanja in notranjimi pravili ponudnika storitev zaupanja Halcom CA.

5.1.8 Hramba na oddaljeni lokaciji

Glej razd. 5.1.6.

5.2. Organizacijska struktura ponudnika storitev zaupanja

5.2.1 Organizacijske skupine

(1) Operativno, organizacijsko in strokovno pravilno delovanje ponudnika storitev zaupanja Halcom CA vodi pooblaščenec za notranji nadzor, ki je odgovoren za upravljanje potrdil.

(2) Med pooblaščene osebe ponudnika storitev zaupanja Halcom CA spadajo zaposleni pri ponudniku storitev zaupanja Halcom CA.

(3) Zaposleni pri ponudniku storitev zaupanja na Halcom CA so razporejeni v štiri organizacijske skupine, ki pokrivajo naslednja vsebinska področja:
- upravljanje z informacijskim sistemom,
- upravljanje s potrdili,
- varovanje in kontrola,
- regulativno.

Organizacijska skupina	Vloga	Osnovne naloge	Število oseb
Upravljanje z informacijskim sistemom	Glavni sistemski administrator	• Priprava začetne konfiguracije sistema, • Začetna nastavitev parametrov novih podrejenih ponudnikov storitev zaupanja • Postavitev začetne konfiguracije omrežja	2

		• Priprava nosilcev podatkov za zasilni ponovni start sistema v primeru katastrofalne izgube sistema • Varno shranjevanje in distribucija kopij in nadgradenj na ločeno lokacijo	
	Sistemski administrator	• Upravljanje postopkov za izdajo potrdil • Pomoč podrejenim ponudnikom storitev zaupanja • Pooblaščanje podrejenih ponudnikov storitev zaupanja • Dostop do protokola podpisovanja potrdil • Varno shranjevanje in distribucija kopij in nadgradenj na ločeno lokacijo	2
Upravljanje s potrdili	Sistemski operater 1	• Priprava sistemskih kopij, nadgradnja in obnovitev programske opreme, varno shranjevanje in distribucija kopij in nadgradenj Administrativne funkcije povezane z vzdrževanjem • Izvajanje arhiviranja zahtevanih sistemskih zapisov • Izpis kod PIN • Dnevni pregled sistema	2
	Operater za avtorizacijo	• Potrjevanje izdaje potrdil in proženje gesel	2
	Operater za potrdila	• Predpoosebljanje varnih pametnih kartic • Priprava potrdil (obdelava podpisanih zahtev za potrdila) • Poosebljanje (izdelava potrdil, zapis na varni nosilec, tiskanje imetnikovih podatkov na varni nosilec) • Distribucija potrdil	2
	Operater za kode	• Distribucija kod PIN kod	2
	Uslužbenec za prijavo	• Identifikacija imetnikov potrdil	2
	Uslužbenec za preklic	• Priprava zahtev za preklic • Preklic potrdil	2
Varovanje in kontrola	Varnostni administrator	• Določanje varnostnih pravil in nadzor njihovega upoštevanja • Pregledovanje sistemske dokumentacije in kontrolnih dnevnikov za nadzor dela • Osebno sodelovanje in pomoč pri letni inventuri dokumentacije podrejenih ponudnikov storitev zaupanja	2
	Pooblaščenec za notranji nadzor	• Nadzor varnostnih pravil in njihovega upoštevanja • Nadzor sistemske dokumentacije in kontrolnih dnevnikov za nadzor dela	2
Regulativno	Pooblaščenec za zasebnost in regulatorno skladnost	• Samostojno in neodvisno usmerjanje, presoja varovanja zasebnosti in varstva osebnih podatkov	1

		• Zagotavljanje skladnosti z veljavnimi evropskimi in slovenskimi predpisi, mednarodnimi standardi in priporočili • Strokovna pomoč poslovodstvu in zaposlenim pri operativnem izvajanju ukrepov varovanja zasebnosti in zagotavljanja regulatorne skladnosti	

5.2.2 Število oseb za posamezne naloge

(1) Operativne delovne vloge so načrtovane tako, da v največji možni meri preprečujejo možnosti zlorab in so razdeljene med posamezne, organizacijske skupine:

Organizacijska skupina: Upravljanje z informacijskim sistemom
Vloga: glavni sistemski administrator
Število oseb: 2
Naloge:
1. Priprava začetne konfiguracije sistema, vključno z varnim zagonom in ustavitvijo delovanja sistema
2. Začetna nastavitev parametrov novih podrejenih ponudnikov storitev zaupanja
3. Postavitev začetne konfiguracije omrežja
4. Priprava nosilcev podatkov za zasilni ponovni start sistema v primeru katastrofalne izgube sistema
5. Varno shranjevanje in distribucija kopij in nadgradenj na ločeno lokacijo

Organizacijska skupina: Upravljanje z informacijskim sistemom
Vloga: sistemski administrator
Število oseb: 2
Naloge:
1. Upravljanje postopkov za izdajo potrdil
2. Pomoč podrejenim ponudnikom storitev zaupanja
3. Pooblaščanje podrejenih ponudnikov storitev zaupanja
4. Dostop do protokola podpisovanja potrdil
5. Varno shranjevanje in distribucija kopij in nadgradenj na ločeno lokacijo

Organizacijska skupina: Upravljanje s potrdili
Vloga: sistemski operater 1
Število oseb: 2
Naloge:
1. Priprava sistemskih kopij, nadgradnja in obnovitev programske opreme, varno shranjevanje in distribucija kopij in nadgradenj na ločeno lokacijo
2. Administrativne funkcije, ki so povezane z vzdrževanjem baze podatkov ponudnika storitev zaupanja in ki pomagajo pri raziskavah odstopanj od pravil
3. Spremembe imena strežnika in/ali omrežnega naslova
4. Izvajanje arhiviranja zahtevanih sistemskih zapisov
5. Izpis kod PIN
6. Dnevni pregled sistema

Organizacijska skupina: Upravljanje s potrdili
Vloga: operater za avtorizacijo
Število oseb: 2
Naloge:
1. Potrjevanje izdaje potrdil in proženje gesel

Organizacijska skupina: Upravljanje s potrdili
Vloga: operater za potrdila
Število oseb: 2
Naloge:
1. Predpoosebljanje varnih nosilcev
2. Priprava potrdil (obdelava podpisanih zahtev za potrdila)
3. Poosebljanje (izdelava potrdil, zapis na varni nosilec, tiskanje imetnikovih podatkov na varni nosilec)
4. Distribucija potrdil

Organizacijska skupina: Upravljanje s potrdili
Vloga: operater za kode
Število oseb: 2
Naloge:
1. Distribucija kod PIN

Organizacijska skupina: Upravljanje s potrdili
Vloga: uslužbenec za prijavo
Število oseb: 2
Naloge:
1. Identifikacija imetnikov potrdil

Organizacijska skupina: Upravljanje s potrdili
Vloga: uslužbenec za preklic
Število oseb: 2
Naloge:
1. Priprava zahtev za preklic
2. Preklic potrdil

Organizacijska skupina: Varovanje in kontrola
Vloga: varnostni administrator
Število oseb: 2
Naloge:
1. Določanje varnostnih pravil in nadzor njihovega upoštevanja
2. Pregledovanje sistemske dokumentacije in kontrolnih dnevnikov za nadzor dela
3. Osebno sodelovanje in pomoč pri letni inventuri dokumentacije podrejenih ponudnikov storitev zaupanja

Organizacijska skupina: Varovanje in kontrola
Vloga: pooblaščenec za notranji nadzor
Število oseb: 2
Naloge:
1. Nadzor varnostnih pravil in njihovega upoštevanja
2. Nadzor sistemske dokumentacije in kontrolnih dnevnikov za nadzor dela

Organizacijska skupina: Regulativno
Vloga: pooblaščenec za zasebnost in regulatorno skladnost
Število oseb: 1
Naloge:
1. samostojno in neodvisno usmerjanje, presoja varovanja zasebnosti in varstva osebnih

podatkov
2. zagotavljanje skladnosti z veljavnimi evropskimi in slovenskimi predpisi, mednarodnimi standardi in priporočili
3. strokovna pomoč poslovodstvu in zaposlenim pri operativnem izvajanju ukrepov varovanja zasebnosti in zagotavljanja regulatorne skladnosti

(2) Navedeno je minimalno število zaposlenih za posamezne vloge.

5.2.3 Izkazovanje istovetnosti za opravljanje posameznih nalog

Izkazovanje istovetnosti in pravice dostopov za opravljanje posameznih nalog skladno z vlogo posamezne organizacijske skupine kot tudi za opravljanje nalog prijavne službe je zagotovljena z varnostnimi mehanizmi in kontrolnimi postopki v skladu z notranjimi pravili ponudnika storitev zaupanja Halcom CA.

5.2.4 Nezdružljivost nalog

Za vsako vlogo je v notranjih pravilih Halcom CA natančno določeno, s katero sme oz. ne sme biti združljiva. Za nekatere je potrebna prisotnost vsaj dveh za to pooblaščenih oseb. V primeru nepredvidene odsotnosti določenih zaposlenih njihove vloge prevzamejo drugi zaposleni, če to po notranjih pravilih ni nezdružljivo.

5.3. Nadzor nad osebjem

(1) Operativno, organizacijsko in strokovno pravilno delovanje ponudnika storitev zaupanja Halcom CA vodi pooblaščenec za notranji nadzor, ki ne opravljajo nalog v zvezi z upravljanjem potrdil.

(2) pooblaščenec za notranji nadzor nadzoruje delo Halcom CA. Pooblaščenec za notranji nadzor v primeru odkritih pomanjkljivosti odredi ustrezne ukrepe za odpravo teh pomanjkljivosti, ki jih je Halcom CA dolžan izvesti, ter nadzoruje izvedbo odrejenih ukrepov.

5.3.1 Potrebne kvalifikacije in izkušnje osebja

Halcom CA zaposluje zanesljivo in strokovno usposobljeno osebje, ki preverjeno ni bilo kaznovano za kakršnokoli kaznivo dejanje. Vse osebje se redno usposablja in pridobiva dodatna znanja s svojega strokovnega področja.

5.3.2 Primernost osebja

Osebje ponudnika storitev zaupanja ima skladno z zahtevami veljavnih predpisov ter tehničnih standardov in priporočil ustrezne kvalifikacije in izkušnje.

5.3.3 Dodatno usposabljanje osebja

Osebam, ki opravljajo naloge zgoraj navedenih organizacijskih skupin in naloge prijavne službe, se zagotavlja vso potrebno usposabljanje.

5.3.4 Zahteve za redna usposabljanja

Osebje se usposablja glede na potrebe oz. novosti v zvezi z delovanjem infrastrukture ponudnika storitev zaupanja Halcom CA.

5.3.5 Menjava nalog

Ni predpisana.

5.3.6 Sankcije

Sankcije v primeru nepooblaščenega ali malomarnega izvajanja nalog se za pooblaščene osebe ponudnika storitev zaupanja izvajajo skladno z veljavnimi predpisi in notranjimi pravili ponudnika storitev zaupanja Halcom CA.

5.3.7 Zahteve za zunanje izvajalce

Za morebitne zunanje izvajalce veljajo enake zahteve kot za pooblaščene osebe ponudnika storitev zaupanja Halcom CA.

5.3.8 Dostop osebja do dokumentacije

Pooblaščenim osebam ponudnika storitev zaupanja je na voljo vsa potrebna dokumentacija skladno z njihovimi zadolžitvami in nalogami.

5.4. Varnostni pregledi sistema

5.4.1 Vrste dnevnikov

(1) Ponudnik storitev zaupanja Halcom CA redno preverja in evidentira vse, kar pomembno vpliva na:

- varnost infrastrukture,
- nemoteno delovanje vseh varnostnih sistemov in
- ali je v vmesnem času prišlo do vdora ali poskusa vdora nepooblaščenih oseb do opreme ali podatkov.

(2) Podrobni podatki o tem so skladno z Uredbo določeni v notranjih pravilih ponudnika storitev zaupanja Halcom CA.

5.4.2 Pogostnost pregledov dnevnikov

Ponudnik storitev zaupanja Halcom CA opravlja varnostne preglede svoje infrastrukture oz. dnevnikov dnevno.

5.4.3 Čas hrambe dnevnikov

Dnevniki se hranijo vsaj sedem (7) let po njihovem nastanku, če poseben zakon ne določa daljšega roka.

5.4.4 Zaščita dnevnikov

Dnevniki so varovani v skladu z varnostnimi mehanizmi, ki zagotavljajo najvišji nivo varnosti.

5.4.5 Varnostne kopije dnevnikov

Varnostne kopije dnevnikov se izvajajo dnevno.

5.4.6 Zbiranje podatkov za dnevnike

Podatki se zbirajo bodisi avtomatsko ali pa ročno, odvisno od vrste podatkov.

5.4.7 Obveščanje povzročitelja dogodka

Povzročitelja dogodkov ni potrebno obveščati.

5.4.8 Ocena ranljivosti sistema

(1) Analiza dnevnikov in nadzor nad izvajanjem vseh postopkov se izvaja redno s strani pooblaščenih oseb ponudnika storitev zaupanja ali pa samodejno z drugimi varnostnimi mehanizmi na vseh infromacijsko-komunikacijskih napravah ponudnika storitev zaupanja.

(2) Ocena ranljivosti se izvaja na podlagi analize dnevnikov, varnostnih dogodkov in drugih pomembnih podatkov.

5.5. Dolgoročna hramba podatkov

5.5.1 Vrste dolgoročno hranjenih podatkov

Ponudnik storitev zaupanja Halcom CA v skladu z določili veljavnih predpisov hrani naslednje gradivo:

- dnevnike,
- zapisnike,
- vsa dokazila o opravljenem preverjanju istovetnosti imetnikov oz. poslovnih subjektov,
- vse zahtevke,
- potrdila in register preklicanih potrdil,
- politike delovanja,
- objave in obvestila ponudnika storitev zaupanja Halcom CA ter
- druge dokumente v skladu z veljavnimi predpisi.

5.5.2 Rok hrambe

(1) Dolgoročno hranjeni podatki v zvezi s ključi in digitalnimi potrdili se hranijo vsaj sedem (7) let po poteku potrdila, na katerega se podatek nanaša, če poseben zakon ne določa daljšega roka.

(2) Ostali dolgoročno hranjeni podatki se hranijo vsaj sedem (7) let po njihovem nastanku, če poseben zakon ne določa daljšega roka.

5.5.3 Zaščita dolgoročno hranjenih podatkov

(1) Dolgoročno hranjeni podatki so varno shranjeni.

(2) Podrobnejša ureditev je v skladu z veljavnimi predpisi, standardi in priporočili določena v Splošnih pravilih delovanja in notranjih pravilih ponudnika storitev zaupanja Halcom CA.

5.5.4 Varnostna kopija dolgoročno hranjenih podatkov

(1) Kopija dolgoročno hranjenih podatkov se varno hrani.

(2) Podrobnejša ureditev je v skladu z veljavnimi predpisi, standardi in priporočili določena v Splošnih pravilih delovanja in notranjih pravilih ponudnika storitev zaupanja Halcom CA.

5.5.5 Zahteva po časovnem žigosanju

Ni predpisano.

5.5.6 Način zbiranja podatkov

(1) Podatki se zbirajo na način, skladen z vrsto dokumenta.

(2) Podrobnejša ureditev je v skladu z veljavnimi predpisi, standardi in priporočili določena v Splošnih pravilih delovanja in notranjih pravilih ponudnika storitev zaupanja Halcom CA.

5.5.7 Postopek za dostop do dolgoročno hranjenih podatkov in njihova verifikacija

(1) Dostop do dolgoročno hranjenih podatkov je možen samo pooblaščenim osebam.

(2) Podrobnejša ureditev je v skladu z veljavnimi predpisi, standardi in priporočili določena v Splošnih pravilih delovanja in notranjih pravilih ponudnika storitev zaupanja Halcom CA.

5.6. Sprememba javnega ključa ponudnika storitev zaupanja Halcom CA

V primeru novega izdanega lastnega potrdila ponudnika storitev zaupanja Halcom CA se postopek objavi na spletnih straneh ponudnika storitev zaupanja Halcom CA.

5.7. Okrevalni načrt

5.7.1 Postopek v primeru vdorov in zlorabe

Podrobnejša ureditev je v skladu z veljavnimi predpisi, standardi in priporočili določena v Splošnih pravilih delovanja in notranjih pravilih ponudnika storitev zaupanja Halcom CA.

5.7.2 Postopek v primeru okvare programske opreme, podatkov

Podrobnejša ureditev je v skladu z veljavnimi predpisi, standardi in priporočili določena v Splošnih pravilih delovanja in notranjih pravilih ponudnika storitev zaupanja Halcom CA.

5.7.3 Postopek v primeru ogroženega zasebnega ključa ponudnika storitev zaupanja Halcom CA

Podrobnejša ureditev je v skladu z veljavnimi predpisi, standardi in priporočili določena v Splošnih pravilih delovanja in notranjih pravilih ponudnika storitev zaupanja Halcom CA.

5.7.4 Okrevalni načrt

Zagotovljena je podvojenost kritičnih sistemov in shranjevanje podatkov na geografsko oddaljenih lokacijah. Podrobnejša ureditev je v skladu z veljavnimi predpisi, standardi in priporočili določena v Splošnih pravilih delovanja in notranjih pravilih ponudnika storitev zaupanja Halcom CA.

5.8. Prenehanje delovanja Halcom CA

Podrobnejša ureditev je v skladu z veljavnimi predpisi, standardi in priporočili določena v Splošnih pravilih delovanja in notranjih pravilih ponudnika storitev zaupanja Halcom CA.

6. TEHNIČNE VARNOSTNE ZAHTEVE

6.1. Generiranje in namestitev ključev

6.1.1 Generiranje ključev

(1) Par ključev ponudnika storitev zaupanja Halcom CA za podpisovanje in preverjanje veljavnosti podpisa je bil ustvarjen po najvišjih varnostnih standardih, v varnem okolju ponudnika storitev zaupanja Halcom CA.

(2) Pari ključev imetnikov kvalificiranih potrdil za časovni žig se generirajo v strojnem varnostnem modulu, pri imetniku.

6.1.2 Dostava zasebnega ključa imetnikom

(1) Zasebni ključi potrdil za časovni žig se ne prenašajo, saj se generirajo v strojnem varnostnem modulu, pri imetniku.

6.1.3 Dostava javnega ključa ponudniku storitev zaupanja

Pri potrdilih za časovni žig se ključi generirajo pri imetniku, v strojnem varnostnem modulu. PKCS#10 zahtevek za izdajo potrdila (angl. »certificate request«) pa se prenese iz uporabnikovega strojnega varnostnega modula do ponudnika storitev zaupanja preko zaščitene omrežne povezave.

6.1.4 Dostava javnega ključa ponudnika storitev zaupanja

Potrdilo z javnim ključem ponudnika storitev zaupanja Halcom CA je imetniku dostavljeno oz. tretjim osebam dostopno:

- v javnem imeniku ldap://ldap.halcom.si po protokolu LDAP (glej razdelek 2.3),
- v obliki PEM na naslovu http://www.halcom.si/si/produkti/digitalno-potrdilo/politike-in-dokumenti/, pri čemer mora dodatno preveriti verodostojnost potrdila.

6.1.5 Dolžina ključev

Potrdilo	Dolžina ključa po RSA [bit]
Korensko (Root) potrdilo ponudnika storitev zaupanja Halcom CA	Najmanj 2048
Vmesno/podrejeno (Intermediate) potrdilo ponudnika storitev zaupanja Halcom CA	Najmanj 2048
Kvalificirano digitalno potrdilo uporabnika	Najmanj 2048

6.1.6 Generiranje in kakovost parametrov javnih ključev

Kvaliteta parametrov ključa ponudnika storitev zaupanja Halcom CA je zagotovljena s strani proizvajalca programske opreme z uporabo kvalitetnih generatorjev naključnih števil (angl. random number generator).

6.1.7 Namen ključev in potrdil

(1) Namen uporabe ključev oz. potrdil je v skladu z X.509 v.3 določen v potrdilu v polju uporaba ključa (angl. Key Usage) in razširjena uporaba ključa (angl. Enhanced Key Usage).

(2) Za podpis potrdil in registra preklicanih potrdil je namenjen zasebni ključ ponudnika storitev zaupanja Halcom CA, za preverjanje veljavnosti podpisapa javni ključ v potrdilu ponudnika storitev zaupanja.

(3) Profil potrdil je podan v razdelku 7.1.

6.2. Zaščita zasebnega ključa

6.2.1 Standardi za kriptografski modul

Zasebni ključ ponudnika storitev zaupanja HALCOM CA je zaščiten v kriptografskem modulu, ki je certificiran v skladu s FIPS 140-2 nivo 3 in/ali Common Criteria EAL4+.

6.2.2 Nadzor zasebnega ključa s strani pooblaščenih oseb

Določila glede dostopa do zasebnega ključa ponudnika storitev zaupanja Halcom CA so v skladu z veljavnimi predpisi in Splošnimi pravili delovanja določena v notranjih pravilih ponudnika storitev zaupanja Halcom CA.

6.2.3 Odkrivanje kopije zasebnega ključa

Določila glede odkrivanja zasebnega ključa ponudnika storitev zaupanja Halcom CA so v skladu z veljavnimi predpisi in Splošnimi pravili delovanja določena v notranjih pravilih ponudnika storitev zaupanja Halcom CA.

6.2.4 Varnostna kopija zasebnega ključa

Določila glede varnostnega kopiranja zasebnega ključa ponudnika storitev zaupanja Halcom CA so v skladu z veljavnimi predpisi in Splošnimi pravili delovanja določena v notranjih pravilih ponudnika storitev zaupanja Halcom CA.

6.2.5 Arhiviranje zasebnega ključa

(1) Zasebne ključe Halcom CA lahko kopirajo in hranijo samo pooblaščene osebe ponudnika storitev zaupanja Halcom CA. Varnostne kopije ključev se hranijo z enako stopnjo zaščite kot ključi v uporabi.

(2) Podrobnejša določila kopiranja zasebnega ključa ponudnika storitev zaupanja Halcom CA so v skladu z veljavnimi predpisi in Splošnimi pravili delovanja določena v notranjih pravilih ponudnika storitev zaupanja Halcom CA.

6.2.6 Prenos zasebnega ključa iz/v kriptografski modul

Zasebni ključi pri potrdilih za časovni žig se ne prenašajo, saj se ustvarijo pri imetniku.

6.2.7 Hramba zasebnega ključa v kriptografskem modulu

(1) Zasebni ključ ponudnik storitev zaupanja HALCOM CA hrani v kriptografskem modulu, ki je certificiran v skladu s FIPS 140-2 nivo 3 in/ali Common Criteria EAL4+.

(2) Zasebni ključi uporabnikov potrdil za časovni žig se ustvarijo in hranijo pri imetniku.

6.2.8 Postopek za aktiviranje zasebnega ključa

(1) Postopek za aktiviranje zasebnega ključa ponudnika storitev zaupanja Halcom CA poteka na varen način skladno z določili notranjih pravil ponudnika storitev zaupanja Halcom CA.

(2) Postopek za aktiviranje zasebnega ključa imetnikov poteka skladno z določili notranjih pravil ponudnika storitev zaupanja za časovno žigosanje.

6.2.9 Postopek za deaktiviranje zasebnega ključa

Postopek za deaktiviranje zasebnega ključa ponudnika storitev zaupanja Halcom CA poteka na varen način skladno z določili notranjih pravil ponudnika storitev zaupanja Halcom CA.

6.2.10 Postopek za uničenje zasebnega ključa

(1) Postopek za uničenje zasebnega ključa ponudnika storitev zaupanja Halcom CA poteka na varen način skladno z določili notranjih pravil ponudnika storitev zaupanja Halcom CA in navodili proizvajalca strojnega varnostnega modula. Zasebni ključ se uniči tako, da ga ni mogoče restavrirati.

(2) Uničenje zasebnih ključev na strani imetnikov je v pristojnosti imetnikov. Uporabiti morajo ustrezne aplikacije za varno brisanje potrdil.

6.2.11 Lastnosti kriptografskega modula

Strojni varnostni moduli ustrezajo standardom, podanim v razd. 6.2.1.

6.3. Ostali aspekti upravljanja ključev

6.3.1 Arhiviranje javnega ključa

Ponudnik storitev zaupanja Halcom CA arhivira svoj javni ključ in javne ključe imetnikov, kot je podano v razdelku 5.5.

6.3.2 Obdobje veljavnosti za javne in zasebne ključe

(1) Veljavnost potrdil je razvidna iz spodnje razpredelnice.

Tip potrdila	Potrdilo	Ključ	Veljavnost
Potrdilo za časovni žig	par ključev za časovno žigosanje	Zasebni ključ	5 let
		Javni ključ	5 let

(2) Halcom CA lahko v posebnih primerih za posamezno potrdilo določi tudi drugačen rok veljavnosti potrdila.

6.4. Gesla za dostop do potrdil oz. ključev

6.4.1 Generiranje gesel

Imetniki potrdil sami določijo geslo, s katerim zaščitijo dostop do svojih zasebnih ključev.

6.4.2 Zaščita gesel

Imetniki potrdil za časovni žig sami določijo geslo, s katerim zaščitijo dostop do svojih zasebnih ključev. Halcom CA priporoča, da se geslo za dostop do zasebnega ključa ne shranjuje oz. se shrani na varno mesto in da ima do njega dostop le imetnik.

6.4.3 Drugi aspekti gesel

Niso predpisani.

6.5. Varnostne zahteve za informacijsko-komunikacijsko opremo ponudnika storitev zaupanja

6.5.1 Specifične tehnične varnostne zahteve

Podrobnejša ureditev je v skladu z veljavnimi predpisi, standardi in priporočili določena v Splošnih pravilih delovanja in notranjih pravilih ponudnika storitev zaupanja Halcom CA.

6.5.2 Nivo varnostne zaščite

Podrobnejša ureditev je v skladu z veljavnimi predpisi, standardi in priporočili določena v Splošnih pravilih delovanja in notranjih pravilih ponudnika storitev zaupanja Halcom CA.

6.6. Tehnični nadzor življenjskega cikla ponudnika storitev zaupanja

6.6.1 Nadzor razvoja sistema

Halcom CA uporablja programsko in strojno opremo, ki je certificirana v skladu s FIPS 140-2 nivo 3 in/ali Common Criteria EAL4+.

6.6.2 Upravljanje varnosti

Podrobnejša ureditev je v skladu z veljavnimi predpisi, standardi in priporočili določena v Splošnih pravilih delovanja in notranjimi pravili ponudnika storitev zaupanja Halcom CA.

6.6.3 Nadzor življenjskega cikla

Podrobne tehnične zahteve so določene v Splošnih pravilih delovanja in notranjih pravilih ponudnika storitev zaupanja Halcom CA.

6.7. Varnostna kontrola omrežja

Podrobnejša ureditev je v skladu z veljavnimi predpisi, standardi in priporočili določena v Splošnih pravilih delovanja in notranjih pravilih ponudnika storitev zaupanja Halcom CA.

6.8. Časovno žigosanje

Ni predpisano.

7. PROFIL POTRDIL IN REGISTRA PREKLICANIH POTRDIL

7.1. Profil potrdil

(1) Na podlagi te politike Halcom CA izdaja potrdila za časovni žig za poslovne subjekte – ponudnike storitev zaupanja.

(2) Vsa potrdila vključujejo podatke, ki so skladno z uredbo eIDAS določena za kvalificirana potrdila.

(3) Potrdila ponudnika storitev zaupanja Halcom CA sledijo standardu X.509.

7.1.1 Različica potrdil

Vsa potrdila ponudnika storitev zaupanja Halcom CA sledijo standardu X.509, in sicer različici 3.

7.1.2 Profil potrdil z razširitvami

(1) Profil korenskega (root) potrdila - Halcom Root Certificate Authority.

Nazivi polja	Vrednost oz. pomen
Osnovna polja v potrdilu	
Različica, angl. Version	V3
Identifikacijska oznaka potrdila, angl. Serial Number	enolična interna številka potrdila
Algoritem za podpis, angl. Signature algorithm	Sha256RSA (OID 1.2.840.113549.1.1.11)
Izdajatelj, angl. Issuer	CN = Halcom Root Certificate Authority 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Veljavnost, angl. Validity	Valid from: <10.6.2016 07:07:50 GMT > Valid to: <10.6.2036 07:07:50 GMT >
Imetnik, angl. Subject	CN = Halcom Root Certificate Authority 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Algoritem za javni ključ, angl. Subject Public Key Algorithm	rsaEncryption (OID 1.2.840.113549.1.1.1)
Javni ključ, angl. Public Key (... bits)	modul, eksponent,...
Imetnikov javni ključ, ki pripada ustreznemu paru ključev, šifriran z alg. RSA, angl. RSA Public Key	dolžina ključa 2048 bitov
Razširitve X.509v3	
Uporaba ključa, OID 2.5.29.15, angl. Key Usage	Certificate Signing, Off-line CRL Signing, CRL Signing
Identifikator imetnikovega ključa, OID 2.5.29.14, angl. Subject Key Identifier	42 ae a6 43 c7 98 28 b0
Osnovne omejitve, OID 2.5.29.19, angl. Basic Constraints	Subject Type=CA Path Length Constraint=None

Dodatna identifikacija (ni del digitalnega potrdila)	
razpoznavni odtis potrdila-SHA1 angl. Certificate Fingerprint – SHA1	Razpoznavni odtis potrdila po SHA1

(2) Profil vmesnega/podrejena (intermediate) potrdila – Halcom CA TSA 1

Nazivi polja	Vrednost oz. pomen
Osnovna polja v potrdilu	
Različica, angl. Version	V3
Identifikacijska oznaka potrdila, angl. Serial Number	enolična interna številka potrdila
Algoritem za podpis, angl. Signature algorithm	Sha256RSA (1.2.840.113549.1.1.11)
Izdajatelj, angl. Issuer	CN = Halcom Root Certificate Authority 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Veljavnost, angl. Validity	Valid from: <22.04.2017 08:00:00 GMT > Valid to: <22.04.2027 08:00:00 GMT >
Imetnik, angl. Subject	CN = Halcom CA TSA 1 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Algoritem za javni ključ, angl. Subject Public Key Algorithm	rsaEncryption (OID 1.2.840.113549.1.1.1)
Javni ključ, angl. Public Key (... bits)	modul, eksponent,...
Imetnikov javni ključ, ki pripada ustreznemu paru ključev, šifriran z alg. RSA, angl. RSA Public Key	dolžina ključa je 2048 bitov
Razširitve X.509v3	
Objava registra preklicanih potrdil, OID 2.5.29.31, angl. CRL Distribution Points	URL=ldap://ldap.halcom.si/cn=Halcom%20Root%20Certificate%20Authority,o=Halcom,c=SI?certificaterevocationlist;binary URL=http://domina.halcom.si/crls/halcom_root_certificate_authority.crl
Uporaba ključa, OID 2.5.29.15, angl. Key Usage	Certificate Signing, Off-line CRL Signing, CRL Signing
Identifikator ključa ponudnika storitev zaupanja, OID 2.5.29.35, angl. Authority Key Identifier	KeyID=42 ae a6 43 c7 98 28 b0
Identifikator imetnikovega ključa, OID 2.5.29.14, angl. Subject Key Identifier	43 8f 8b 56 9f 44 1e d7
Osnovne omejitve, OID 2.5.29.19, angl. Basic Constraints	Subject Type=CA Path Length Constraint=None
Dodatna identifikacija (ni del digitalnega potrdila)	
razpoznavni odtis potrdila-SHA1 angl. Certificate Fingerprint – SHA1	Razpoznavni odtis potrdila po SHA1

(3) Profil potrdil končnih uporabnikov

Nazivi polja	Vrednost oz. pomen

Osnovna polja v potrdilu	
Različica, angl. Version	V3
Identifikacijska oznaka potrdila, angl. Serial Number	enolična interna številka potrdila
Algoritem za podpis, angl. Signature algorithm	Sha256RSA (OID 1.2.840.113549.1.1.11)
Izdajatelj, angl. Issuer	CN = Halcom CA TSA 1 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Veljavnost, angl. Validity	Valid from: <pričetek veljavnosti po GMT> Valid to: <konec veljavnosti po GMT>
Imetnik, angl. Subject	razločevalno ime imetnika, glej razd. 3.1.1.
Algoritem za javni ključ, angl. Subject Public Key Algorithm	rsaEncryption (OID 1.2.840.113549.1.1.1)
Javni ključ, angl. Public Key (... bits)	modul, eksponent,...
Imetnikov javni ključ, ki pripada ustreznemu paru ključev, šifriran z alg. RSA, angl. RSA Public Key	dolžina ključa je min 2048 bitov, glej razd. 6.1.5.
Razširitve X.509v3	
Objava registra preklicanih potrdil, OID 2.5.29.31, angl. CRL Distribution Points	URI:ldap://ldap.halcom.si/cn=Halcom%20CA%20TSA%201,o=Halcom,c=SI?certificaterevocationlist;binary URL=http://domina.halcom.si/crls/halcom_ca_TSA_1.crl
Uporaba ključa, OID 2.5.29.15, angl. Key Usage	Digital Signature
Razširjena uporaba ključa angl. Enhanced Key Usage	Time Stamping (1.3.6.1.5.5.7.3.8)
Identifikator ključa ponudnika storitev zaupanja, OID 2.5.29.35, angl. Authority Key Identifier	KeyID=43 8f 8b 56 9f 44 1e d7

(4) Polje rezširjena uporaba ključa (angl. Enhanced Key Usage) je označeno kot kritično (angl. critical).

(5) Imetnik ima lahko več veljavnih potrdil za časovni žig.

7.1.2.1 Zahteve za elektronski naslov

Niso predpisane.

7.1.3 Identifikacijske oznake algoritmov

(1) Potrdila, ki jih izdaja Halcom CA, so s strani ponudnika storitev zaupanja podpisana z algoritmom, določenim v polju signature algorithm: vrednost »sha256RSA, identifikacijska oznaka: OID 1.2.840.113549.1.1.11.

(2) Celoten nabor algoritmov, formatov podatkov in protokolov je na razpolago pri pooblaščenih osebah ponudnika storitev zaupanja Halcom CA.

7.1.4 Oblika razločevalnih imen

Glej razd. 3.1.1.

7.1.5 Omejitve glede imen

Omejitve glede imen (polje v potrdilu angl. nameConstraints) niso predpisane.

7.1.6 Označba politike potrdila

Glej razd. 7.1.2.

7.1.7 Omejitve uporabe

Omejitve uporabe (polje v potrdilu angl. usage policy constraints extension) niso predpisane.

7.1.8 Sintaksa in pomen označb politike potrdil

V potrdilih, ki jih izdaja ponudnik storitev zaupanja Halcom CA, se uporablja specifični podatek policyQualifiers, ki se obravnava v skladu IETF RFC in ETSI standardom.

7.1.9 Pomen bistvenih dodatkov politike

Ni podprto.

7.2. Profil registra preklicanih potrdil

(1) Register preklicanih potrdil Halcom CA je seznam preklicanih potrdil (CRL) in se nahaja v veji:

CN= Halcom CA TSA 1
O = Halcom
C = SI

(2) Register preklicanih potrdil se osvežuje po vsakem preklicu potrdila oziroma najmanj enkrat dnevno, če ni novih zapisov oz. sprememb v registru preklicanih potrdil (24 ur po zadnjem osveževanju).

(3) Register preklicanih potrdil vsebuje enolično interno serijsko številko preklicanega potrdila ter čas in datum preklica.

7.2.1 Različica

(1) Register preklicanih potrdil ustreza priporočilu ITU-T za X.509 (2005) in ISO/IEC 9594-8:2014.

(2) Register preklicanih potrdil je stalno dostopen v javnem imeniku potrdil (glej razdelek 2.3):

- po protokolu LDAP in
- po protokolu HTTP.

7.2.2 Vsebina registra in razširitve

(1) Register preklicanih potrdil poleg ostalih podatkov v skladu s priporočilom X.509 vsebuje (osnovna polja in razširitve so podrobneje prikazana v tabeli spodaj):

- identifikacijske oznake preklicanih potrdil in

- čas in datum preklica.

(2) Korenski (Root) register preklicanih potrdil (CRL vmesnih/podrejenih oz. intermediate potrdil)

Naziv polja	Vrednost oz. pomen
Osnovna polja v CRL	
Različica, angl. Version	V2
Algoritem za podpis, angl. Signature Algorithm	Sha256RSA
Podpis ponudnika storitev zaupanja, angl. Signature	podpis Halcom CA
Razločevalno ime ponudnika storitev zaupanja, angl. Issuer	CN = Halcom Root Certificate Authority 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Čas izdaje CRL, angl. thisUpdate	Effective date: <čas izdaje po GMT>
Čas izdaje naslednjega CRL, angl. nextUpdate	Next Update: <čas naslednje izdaje po GMT>
identifikacijske oznake preklicanih potrdil in čas preklica, angl. revokedCertificate	Serial Number: <identifikacijska oznaka preklicanega dig. potrdila> Revocation Date: <čas preklica po GMT>
Razširitve X.509v2 CRL	
Številka VRL list Angl. CRL number	Zaporedna številka CRL liste
identifikator ključa ponudnika storitev zaupanja, angl. Authority Key Identifier (OID 2.5.29.35)	KeyID=42 ae a6 43 c7 98 28 b0
angl. issuerAltName (OID 2.5.28.18)	se ne uporablja
angl. deltaCRLindicator (OID 2.5.29.27)	se ne uporablja
angl. issuingDistribuitionPoint (OID 2.5.29.28)	se ne uporablja

(3) Vmesni/podrejeni (Intermediate) register preklicanih potrdil (CRL uporabniških potrdil)

Naziv polja	Vrednost oz. pomen
Osnovna polja v CRL	
Različica, angl. Version	V2
Algoritem za podpis, angl. Signature Algorithm	Sha256RSA
Podpis ponudnika storitev zaupanja, angl. Signature	podpis Halcom CA
Razločevalno ime ponudnika storitev zaupanja, angl. Issuer	CN = Halcom CA TSA 1 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Čas izdaje CRL, angl. thisUpdate	Effective date: <čas izdaje po GMT>
Čas izdaje naslednjega CRL, angl. nextUpdate	Next Update: <čas naslednje izdaje po GMT>
identifikacijske oznake preklicanih potrdil in čas preklica, angl. revokedCertificate	Serial Number: <identifikacijska oznaka preklicanega dig. potrdila> Revocation Date: <čas preklica po GMT>
Razširitve X.509v2 CRL	
Številka VRL list Angl. CRL number	Zaporedna številka CRL liste

identifikator ključa ponudnika storitev zaupanja, angl. Authority Key Identifier (OID 2.5.29.35)	KeyID= 43 8f 8b 56 9f 44 1e d7
angl. issuerAltName (OID 2.5.28.18)	se ne uporablja
angl. deltaCRLindicator (OID 2.5.29.27)	se ne uporablja
angl. issuingDistribuitionPoint (OID 2.5.29.28)	se ne uporablja

7.2.3 Objava registra preklicanih potrdil

Halcom CA objavlja register v javnem imeniku na strežniku ldap://ldap.halcom.si po protokolu LDAP in http://domina.halcom.si/crls po protokolu HTTP.

7.3. Profil sprotnega preverjanja statusa potrdil

(1) Sprotno preverjanje statusa digitalnih potrdil je dostopno na naslovu http://ocsp.halcom.si

(2) Profil sporočil OCSP (zahtevek/odgovor) storitve za sprotno preverjanje statusa potrdil je v skladu s priporočilom IETF RFC.

7.3.1 Verzija sprotnega preverjanja statusa

Ponudnik storitev zaupanja Halcom CA uporablja sporočila OCSP verzije 1 v skladu s priporočilom IETF RFC.

7.3.2 Profil sprotnega preverjanje statusa

Sporočila OCSP (zahtevek/odgovor) storitve za sprotno preverjanje statusa potrdil podpirajo razširitev Nonce, ki ni označena kot kritična.

8. NADZOR

(1) Pri Halcom CA deluje pooblaščenec za notranji nadzor in z ustreznimi tehnološkimi in pravnimi znanji, ki ne opravljajo nalog v zvezi z upravljanjem potrdil.

(2) Pooblaščenec za notranji nadzor nadzoruje delo Halcom CA. Pooblaščenec za notranji nadzor v primeru odkritih pomanjkljivosti odredi ustrezne ukrepe za odpravo teh pomanjkljivosti, ki jih je Halcom CA dolžan izvesti, ter nadzoruje izvedbo odrejenih ukrepov.

(3) Halcom CA je enkrat letno podvržen zunanji neodvisni presoj, ki jo izvaja Akreditirani organ.

8.1. Pogostnost nadzora

(1) Pooblaščenec za notranji nadzor opravi nadzor najmanj enkrat letno.

(2) Pooblaščenec za zunanji nazdor za ISO 9001 in ISO 27001 opravi nadzor enkrat letno. Pooblaščenec za zunanji nadzor nad delovanjem v skladu z ETSI standardi opravi nadzor enkrat na dve leti .

(3) Vsi relevantni ETSI standardi so na voljo na spletni strani Halcom CA.

8.2. Vrsta in usposobljenost nadzora

(1) Pooblaščenec za notranji nadzor ima ustrezna tehnološka in pravna znanja.

(2) Pooblaščenec za zunanji nadzor ima ustrezna tehnološka in pravna znanja.

8.3. Neodvisnost nadzora

(1) Pooblaščenec za notranji nadzor ne opravlja nalog v zvezi z upravljanjem potrdil.

(2) Pooblaščenec za zunanji nadzor ne opravlja nalog v zvezi z upravljanjem potrdil.

8.4. Področja nadzora

Področja nadzora so določena v notranjih pravilih ponudnika storitev zaupanja Halcom CA.

8.5. Ukrepi ponudnika storitev zaupanja

V primeru ugotovljenih pomanjkljivosti ali napak pooblaščenec za notranji/zunanji nadzor odredi ustrezne ukrepe za odpravo teh pomanjkljivosti, ki jih je Halcom CA dolžan izvesti, ter nadzoruje izvedbo odrejenih ukrepov. Podrobno je izvajanje ukrepov določeno v notranjih pravilih ponudnika storitev zaupanja Halcom CA.

8.6. Objava rezultatov nadzora

Rezultati izvedbe nadzorov se hranijo pri ponudniku storitev zaupanja Halcom CA.

9. FINANČNE IN OSTALE PRAVNE ZADEVE

9.1. Cenik

Cenik je del pogodbe s ponudnikom storitev zaupanja.

9.1.1 Cena izdaje potrdil in podaljšanja

Cena izdaje potrdil in podaljšanja je določena s pogodbo.

9.1.2 Cena dostopa do potrdil

Dostop do javnega imenika potrdil je brezplačen, razen če se stranki dogovorita drugače.

9.1.3 Cena dostopa do statusa potrdila in registra preklicanih potrdil

Register preklicanih potrdil je brezplačno dostopen vsem osebam.

9.1.4 Cene drugih storitev

Cene drugih storitev, opreme in infrastrukture so določene z veljavnim cenikom ali pogodbo.

9.1.5 Povrnitev stroškov

Ni predpisana.

9.2. Finančna odgovornost

9.2.1 Zavarovalniško kritje

Halcom CA ima ustrezno zavarovano svojo odgovornost. Podrobnejše informacije so objavljene na spletnih straneh.

9.2.2 Drugo kritje

Ni predpisano.

9.2.3 Zavarovanje imetnikov

Ni predpisano.

9.3. Varovanje poslovnih podatkov

9.3.1 Varovani podatki

(1) Ponudnik storitev zaupanja Halcom CA ravna zaupno z naslednjimi podatki:

- z vsemi zahtevki za pridobitev potrdila ali druge storitve,
- vse morebitne zaupne podatke v zvezi s finančnimi obveznostmi,
- vse morebitne zaupne podatke, ki so predmet medsebojne pogodbe s tretjimi osebami ter
- vse ostale zadeve, ki so v skladu z Uredbo zavedene v notranjih pravilih delovanja ponudnika storitev zaupanja Halcom CA.

(2) Z vsemi morebitnimi zaupnimi podatki o poslovnih subjektih, imetnikih in tretjih osebah, ki so nujno potrebni za storitve upravljanja s potrdili, ponudnik storitev zaupanja Halcom CA ravna v skladu z veljavno zakonodajo.

9.3.2 Nevarovani podatki

Ponudnik storitev zaupanja Halcom CA javno objavlja samo take poslovne podatke, ki v skladu z veljavno zakonodajo niso zaupne narave (osebni podatki, poslovne skrivnosti in podobno).

9.3.3 Odgovornost glede varovanja

(1) Halcom CA ne prevzema nobene odgovornosti za vsebino podatkov imetnika potrdila, in sicer tudi v primeru, da je imetnik ali tretja oseba spoštoval vse veljavne predpise, vsa določila te politike in drugih pravil Halcom CA oziroma upošteval vsa njegova navodila.

(2) Halcom CA ne prevzema nobene odgovornosti za posledice, ki nastanejo, ker imetnik potrdila ni ravnal v skladu z varnostnimi zahtevami iz točke 4.5.1 te politike.

9.4. Varovanje osebnih podatkov

9.4.1 Načrt varovanja osebnih podatkov

Halcom CA skrbno varuje osebne podatke skladno z evropskimi in slovenskimi veljavnimi predpisi, mednarodnimi standardi in priporočili, izvaja redne pisne ocene učinkov ter zagotavlja vgrajeno in privzeto zasebnost. Pri Halcom d.d. deluje pooblaščenec za zasebnost kot uradna oseba za varstvo podatkov.

9.4.2 Varovani osebni podatki

(1) Varovani podatki so vsi osebni podatki, ki jih ponudnik storitev zaupanja Halcom CA pridobi na zahtevkih za svoje storitve ali v ustreznih registrih za dokazovanje istovetnosti imetnika ali tekom izvajanja storitev zaupanja.

(2) Podatki v potrdilih in registru preklicanih potrdil so zaradi narave uporabe potrdil in določb veljavnih predpisov in standardov dostopni tretjim osebam, ki se zanašajo na potrdila ali preverjajo njihovo veljavnost.

9.4.3 Nevarovani osebni podatki

Drugih morebitnih nevarovanih osebnih podatkov, razen teh, ki so navedeni v potrdilu in registru preklicanih potrdil, ni.

9.4.4 Odgovornost glede varovanja osebnih podatkov

Ponudnik storitev zaupanja Halcom CA je za varstvo podatkov odgovoren v skladu z veljavnimi predpisi o varstvu podatkov in določili internega Pravilnika o varstvu podatkov.

9.4.5 Pooblastilo glede uporabe osebnih podatkov

Imetnik pooblasti ponudnika storitev zaupanja Halcom CA za uporabo osebnih podatkov na zahtevku za pridobitev potrdila, posebni pisni privolitvi za obdelavo osebnih podatkov ali za druge primere kasneje v drugi pisni obliki.

9.4.6 Posredovanje osebnih podatkov

(1) Ponudnik storitev zaupanja Halcom CA ne posreduje drugih podatkov o imetnikih potrdil, ki niso navedeni v potrdilu, razen če se določeni podatki posebej zahtevajo za izvajanje specifičnih storitev oz. aplikacij, povezanih s potrdili, ter je ponudnika storitev zaupanja Halcom CA imetnik pooblastil za to (glej prejšnji razdelek), ali na zahtevo pristojnega sodišča, prekrškovnega, organa pregona, upravnega organa ali druge pooblaščene osebe. Vsako takšno zahtevo Halcom CA skrbno preveri ter posreduje podatke samo v nujnem obsegu, določenem z veljavnimi predpisi.

(2) Podatki se posredujejo brez pisne privolitve samo v primerih, če tako določajo veljavni evropski ali slovenski predpisi z zakonsko močjo.

9.4.7 Druga določila glede varovanja osebnih podatkov

Niso predpisana.

9.5. Določbe glede pravic intelektualne lastnine

(1) Določbe glede avtorskih, sorodnih in drugih pravic intelektualne lastnine:

- na zasebnem ključu pripadajo vse pravice poslovnemu subjektu oz. imetniku potrdila,
- na javnih ključih, vseh podatkih na potrdilu, na imeniku potrdil in registru preklicanih potrdil ter na tej politiki pripadajo vse pravice Halcom CA.

9.6. Obveznosti in odgovornosti

9.6.1 Obveznosti in odgovornosti ponudnika storitev zaupanja Halcom CA

1) Ponudnik storitev zaupanja Halcom CA je dolžan:
- delovati v skladu s svojimi notranjimi pravili in ostalimi veljavnimi predpisi in zakonodajo,
- delovati v skladu z mednarodnimi priporočili,
- objavljati vse pomembne dokumente, ki določajo njegovo delovanje (politike delovanja, zahtevke, cenik, navodila za varno uporabo kvalificiranih digitalnih potrdil ipd.),
- objavljati na svojih spletnih straneh vse informacije o tistih spremembah glede dejavnosti ponudnika storitev zaupanja, ki kakorkoli vplivajo na imetnike potrdil in tretje osebe,
- zagotoviti delovanje prijavnih služb v skladu z določili HALCOM CA in ostalimi veljavnimi predpisi,
- spoštovati določila glede varnega ravnanja z osebnimi, poslovnimi in zaupnimi podatki o ponudniku storitev zaupanja, imetnikih potrdil ali tretjimi osebami,
- preklicati potrdilo in objaviti preklicano potrdilo v registru preklicanih potrdil, ko ugotovi, da so podani razlogi po tej politiki ali drugih veljavnih predpisih,
- izdajati kvalificirana digitalna potrdila v skladu s to politiko in ostalimi predpisi ter priporočili.

(2) Ponudnik storitev zaupanja Halcom CA je dolžan:
- zagotoviti pravilnost podatkov izdanih potrdil,
- zagotoviti pravilnost objave registra preklicanih potrdil,
- zagotoviti enoličnost razločevalnih imen,
- zagotoviti primerno fizično varnost prostorov in dostopov do samih prostorov ponudnika storitev zaupanja,
- kot dober gospodar skrbeti za nemoteno delovanje in čim večjo razpoložljivost storitve,
- kot dober gospodar skrbeti za čim večjo dostopnost storitev,
- kot dober gospodar skrbeti za nemoteno delovanje vseh ostalih spremljajočih storitev,
- poskušati odpraviti nastale probleme po najboljših močeh in v najkrajšem času,
- skrbeti za optimizacijo strojne in programske opreme in
- obveščati uporabnike o pomembnih zadevah ter
- izpolnjevati vse druge zahteve v skladu s to politiko.

(3) Ponudnik storitev zaupanja Halcom CA zagotavlja čim večjo dostopnost svojih storitev, in sicer vse dni v letu, pri čemer pa se ne upošteva naslednje primere:
- načrtovane in vnaprej napovedane tehnične ali servisne posege na infrastrukturi,
- nenačrtovane tehnične ali servisne posege na infrastrukturi kot posledica nepredvidenih okvar,
- tehnične ali servisne posege zaradi okvare infrastrukture izven pristojnosti ponudnika storitev zaupanja Halcom CA in
- nedostopnost kot posledica višje sile ali izrednih dogodkov.

(4) Vzdrževalna dela ali nadgradnje infrastrukture mora ponudnik storitev zaupanja Halcom CA najaviti vsaj tri (3) dni pred pričetkom del.

(5) Ponudnik storitev zaupanja Halcom CA je odgovoren za vse navedbe v tem dokumentu in za izvajanje vseh določil iz te politike.

(6) Ostale obveznosti oz. odgovornosti ponudnika storitev zaupanja Halcom CA so določene z morebitnim medsebojnim dogovorom s tretjo osebo.

9.6.2 Obveznost in odgovornost prijavne službe

(1) Prijavna služba je dolžna:
- preverjati istovetnost imetnikov oz. bodočih imetnikov,
- sprejemati zahtevke za storitve Halcom CA,
- preverjati zahtevke,
- izdajati potrebno dokumentacijo poslovnim subjektom, imetnikom oz. bodočim imetnikom.

(2) Prijavna služba je odgovorna za izvajanje vseh določil iz te politike in drugih zahtev, ki jih dogovorita s ponudnikom storitev zaupanja Halcom CA.

9.6.3 Obveznosti in odgovornost imetnika potrdila

(1) Poslovni subjekt odgovarja za:
- nastalo škodo v primeru zlorabe potrdila od prijave preklica do preklica,
- vsako škodo, ki je bodisi posredno ali neposredno povzročena zato, ker je bila omogočena uporaba oz. zloraba imetnikovega potrdila s strani nepooblaščenih oseb,
- vsako drugo škodo, ki izvira iz neupoštevanja določil te politike in drugih obvestil Halcom CA ter veljavnih predpisov.

(2) Obveznosti imetnikov so glede uporabe potrdil določena v razd. 4.5.1.

9.6.4 Obveznosti in odgovornost tretjih oseb

(1) Ob prvi uporabi potrdil Halcom CA po tej politiki mora tretja oseba, ki se zanaša na potrdilo, skrbno prebrati to politiko in od tedaj redno spremljati vsa obvestila Halcom CA.

(2) Tretja oseba mora vedno v času uporabe potrdila natančno preveriti, če potrdilo ni v registru preklicanih potrdil.

(3) Če potrdilo vsebuje podatke o tretji osebi, je ta dolžna zahtevati preklic potrdila, če izve, da je bil zasebni ključ ogrožen na način, ki vpliva na zanesljivost uporabe, ali če obstaja nevarnost zlorabe, ali če so se spremenili podatki, ki so navedeni v potrdilu.

(4) Tretja oseba se lahko do preklica potrdila zanese na takšno potrdilo.

(5) Tretja oseba lahko kadarkoli zahteva vse informacije glede veljavnosti kateregakoli izdanega potrdila, glede določb te politike ter glede obvestil Halcom CA.

9.6.5 Obveznosti in odgovornost drugih oseb

Ni predpisano.

9.7. Omejitev odgovornosti

Ponudnik storitev zaupanja Halcom CA ni odgovoren za škodo, ki bi nastala zaradi:
- uporabe potrdil za namen in na način, ki ni izrecno predviden v tej politiki,
- nepravilnega ali pomanjkljivega varovanja gesel ali zasebnih ključev imetnikov, izdajanja zaupnih podatkov ali ključev tretjim osebam in neodgovornega ravnanja imetnika,

- zlorabe oz. vdora v informacijski sistem imetnika potrdila in s tem do podatkov o potrdilih s strani nepooblaščenih oseb,
- nedelovanja ali slabega delovanja informacijske infrastrukture imetnika potrdila ali tretjih oseb,
- nepreverjanja podatkov in veljavnosti potrdil v registru preklicanih potrdil,
- nepreverjanja časa veljavnosti potrdila,
- ravnanja imetnika potrdila ali tretje osebe v nasprotju z obvestili Halcom CA, politiko in drugimi predpisi,
- omogočene uporabe oz. zlorabe imetnikovega potrdila nepooblaščenim osebam,
- izdanega potrdila z napačnimi podatki in neverodostojnimi podatki ali drugih dejanj imetnika ali ponudnika storitev zaupanja,
- uporabe potrdil ter veljavnosti potrdil ob spremembah podatkov iz potrdila, elektronskih naslovov ali spremembah imen imetnikov,
- izpada infrastrukture, ki ni v domeni upravljanja ponudnika storitev zaupanja Halcom CA,
- podatkov, ki se šifrirajo ali podpisujejo z uporabo potrdil,
- ravnanja imetnikov pri uporabi potrdil, in sicer tudi v primeru, če je imetnik ali tretja oseba spoštoval vsa določila te politike, obvestila Halcom CA ali druge veljavne predpise,
- uporabe in zanesljivosti delovanja strojne in programske opreme imetnikov potrdil.

9.8. Omejitev glede uporabe

Potrdila so namenjena le časovnemu žigosanju.

9.9. Poravnava škode

Za škodo odgovarja stranka, ki je le-to povzročila zaradi neupoštevanja določil iz te politike in veljavne zakonodaje.

9.10. Veljavnost politike

(1) Halcom CA si pridržuje pravico do spremembe politike delovanja in nadgradnje infrastrukture brez predhodnega obveščanja imetnikov potrdil. Veljavna potrdila pri tem ostanejo v veljavi do konca preteka veljavnosti in zanje še naprej velja tista politika delovanja, ki je veljala ob njihovi izdaji. Za vsa potrdila, izdana po začetku veljavnosti nove politike, velja nova politika.

(2) Ta politika začne veljati z dnem, ko jo sprejme Halcom CA.

9.10.1 Čas veljavnosti

(1) Nova verzija oz. spremembe politike ponudnika storitev zaupanja Halcom CA se osem (8) dni pred veljavo predhodno objavi na spletnih straneh ponudnika storitev zaupanja Halcom CA, pod novo identifikacijsko številko (CP_{OID}) in označenim datumom začetka njene veljavnosti.

(2) Konec veljavnosti politike ni določen in povezan z veljavnostjo potrdil, izdanih na podlagi politike.

9.10.2 Konec veljavnosti politike

(1) Ob objavi nove politike ostanejo za vsa potrdila, izdana na podlagi te politike, v veljavi tista

določila, ki se smiselno ne morejo nadomestiti z ustreznimi določili po novi politiki (na primer postopek, ki določa način, po katerem je bilo to potrdilo izdano ipd.).

(2) Ponudnik storitev zaupanja lahko za posamezna določila veljavne politike izda dopolnitve, kot je to določeno v razdelku 9.12.

9.10.3 Učinek poteka veljavnosti politike

(1) Ob izdaji nove politike se vsa kvalificirana digitalna potrdila izdana po tem datumu obravnavajo po novi politiki.

(2) Nova politika ne vpliva na veljavnost potrdil, ki so bila izdana po prejšnjih politikah. Taka potrdila ostanejo v veljavi do konca preteka veljavnosti, pri čemer se, kjer je to možno, obravnavajo po novi politiki.

9.11. Komuniciranje med subjekti

(1) Kontaktni podatki ponudnika storitev zaupanja so objavljeni na spletnih straneh in podani v razd. 1.3.1.

(2) Kontaktni podatki imetnikov so podani v zahtevkih v zvezi s potrdili.

(3) Kontaktni podatki tretjih oseb so podani v morebitnem medsebojnem dogovoru med tretjo osebo in ponudnikom storitev zaupanja Halcom CA.

9.12. Spremembe in dopolnitve

9.12.1 Postopek za sprejem sprememb in dopolnitev

(1) Spremembe ali dopolnitve k tej politiki lahko ponudnik storitev zaupanja objavi v obliki sprememb in dopolnitev tej politiki, kadar ne gre za bistvene spremembe v delovanju ponudnika storitev zaupanja.

(2) Dopolnitve se sprejmejo po enakem postopku kot politika.

(3) Če spremembe in dopolnitve bistveno vplivajo na delovanje ponudnika storitev zaupanja, se o tem obvesti pristojno ministrstvo po enakem postopku, kot to velja za politiko.

(4) Način za označevanje dopolnitev določi ponudnik storitev zaupanja Halcom CA.

9.12.2 Veljavnost in objava sprememb in dopolnitev

(1) Ponudnik storitev zaupanja Halcom CA določi pričetek in konec veljavnosti sprememb in dopolnitev.

(2) Spremembe in dopolnitve se osem (8) dni pred pričetkom veljavnosti objavijo na spletnih straneh Halcom CA.

9.12.3 Sprememba identifikacijske številke politike

Če sprejete spremembe in dopolnitve vplivajo na uporabo potrdil, potem lahko ponudnik storitev zaupanja Halcom CA določi novo identifikacijsko oznako politike (CP_{OID}) oz. sprememb in dopolnitev.

9.13. Postopek v primeru sporov

(1) Vse pritožbe imetnikov potrdil rešuje pooblaščenec za zasebnost in regulatorno skladnost.

(2) Morebitne spore med imetnikom potrdila ali tretjo osebo in Halcom CA rešuje stvarno pristojno sodišče v Ljubljani.

9.14. Veljavna zakonodaja

Za odločanje o tej politiki se uporablja pravo Evropske unije in Republike Slovenije.

9.15. Skladnost z veljavno zakonodajo

(1) Nadzor nad skladnostjo delovanja ponudnika storitev zaupanja Halcom CA z veljavnimi predpisi izvaja pristojni inšpektorat in akreditirani organi za ugotavljanje skladnosti.

(2) Akreditiran organ za ugotavljanje skladnosti ponudnika storitev zaupanja Halcom CA revidira najmanj vsakih 24 mesecev. Namen revizije je potrditi, ali ponudnik kvalificiranih storitev zaupanja in kvalificirane storitve zaupanja, ki jih zagotavlja, izpolnjujejo zakonske zahteve.

(3) Notranje preverjanje skladnosti delovanja izvajajo pooblaščene osebe v okviru ponudnika storitev zaupanja Halcom CA.

9.16. Splošne določbe

(1) Z ostalimi subjekti ponudnik storitev zaupanja Halcom CA lahko sklene medsebojne dogovore, če to določa veljavna zakonodaja oz. drugi predpisi.

(2) Če katerakoli od določb te politike je ali postane neveljavna, to ne vpliva na ostale določbe. Neveljavna določba se nadomesti z veljavno, ki mora čimbolj ustrezati namenu, ki ga je želela doseči neveljavna določba

9.17. Druge določbe

Niso predpisane.

Kraj in datum:
Ljubljana, 22.06.2017

Glavni izvršni direktor
Marko Valjavec