Pripravil(a): Luka RIBIČIČ

Številka dokumenta: 400085-7-7/17

Politika Halcom CA : Javni del notranjih pravil za storitev EU kvalificiranega časovnega žigosanja,

Izdaja: 03

Politika Halcom CA

Javni del notranjih pravil Halcom CA TS 5

za storitev EU kvalificiranega časovnega žigosanja

CPName (RFC 3161, SHA-256): Halcom CA TS RFC 2
CPName (DSS XML, SHA-256): Halcom CA TS DSS 2

Politika za EU kvalificirano časovno žigosanje
CPOID (RFC 3161, SHA-256): 1.3.6.1.4.1.5939.3.1.2.5
CPOID (DSS XML, SHA-256): 1.3.6.1.4.1.5939.3.2.2.5

Dokument je veljaven od: 15.6.2023

Izdaja	št. dokumenta in prilog	Opis spremembe	Avtor	Datum zadnje spremembe
1	400085-7-5/17	Začetna izdaja, novo potrdilo za časovno žigosanje	L. Ribičič	24.5.2021
2	400085-7-6/17	Letni pregled, odstranili fax	S. Lazić	21.4.2022
3	400085-7-7/17	Letni pregled, čas in rok shrambe	S. Lazić	23.5.2023

Kazalo vsebine

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 kvalificirane časovne žige za fizične osebe in poslovne subjekte (pravne osebe, samostojne podjetnike in druge fizične osebe registrirane za opravljanje dejavnosti).

(3) Oblika in vsebina te politike je usklajena z uredbo eIDAS, mednarodnim priporočilom 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 časovnih žigov, ureja namen, delovanje in metodologijo upravljanja kvalificiranih časovnih žigov ter varnostne zahteve, ki jih morajo izpolnjevati ponudnik storitev zaupanja Halcom CA, uporabniki časovnega žigosanja in tretje osebe, ki se zanašajo na te časovne žige, ter odgovornost vseh naštetih oseb.

(2) Halcom CA je ponudnik storitev zaupanja, ki izdaja in upravlja s kvalificiranimi časovnimi žigi. Ponudnik storitev zaupanja Halcom CA deluje v okviru Halcom d.d.

(3) 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 notranjih 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,...).

(4) Halcom CA izdaja potrdila za časovne žige, časovne žige 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.

1.2. Identifikacijski podatki politike

(1) Storitev časovnega žigosanja ponudnika storitev zaupanja Halcom CA predstavljajo naslednji podatki:

- Korensko (Root) potrdilo ponudnika storitev zaupanja Halcom CA:

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:

C= SI, O= Halcom d.d., 2.5.4.97= VATSI-43353126, CN= Halcom CA TSA 1

- Kvalificirano digitalno potrdilo za elektronsko časovno žigosanje Halcom CA:

  C=SI, O= Halcom d.d., 1.3.6.1.4.1.5939.2.3 = 43353126, 2.5.4.97= VATSI-43353126, CN=Halcom CA TS 5

1. Za RFC 3161 časovne žige in zgostitveno funkcijo SHA-256:
   - CPName Halcom CA TS RFC 2
   - CPOID 1.3.6.1.4.1.5939.3.1.2.5
2. Za OASIS DSS XML časovne žige in zgostitveno funkcijo SHA-256:
   - CPName Halcom CA TS DSS 2
   - CPOID 1.3.6.1.4.1.5939.3.2.2.5

(2) Obe politiki za časovno žigosanje ponudnika storitev zaupanja Halcom CA podpirajo BTSP - a best practices time-stamp policy.

1.3. Subjekti

1.3.1 Ponudnik storitev zaupanja Halcom CA

(1) Halcom CA je ponudnik storitev zaupanja, ki izdaja in upravlja s kvalificiranimi časovnimi žigi. Ponudnik storitev zaupanja Halcom CA lahko upravlja več različnih enot za časovno žigosanje (angl. TSU - Time-Stamping Unit), preko katerih ponuja servis oziroma storitev časovnega žigosanja (angl. TSP - Time-stamping service).

(2) 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:

- preverjanje istovetnosti poslovnega subjekta in drugih, za upravljanje kvalificiranih časovnih žigov, pomembnih podatkov,
- sprejemanje pogodb za vklop storitve varnega časovnega žigosanja,
- sprejemanje pogodb za izklop storitve varnega časovnega žigosanja,
- izdajanje potrebne dokumentacije poslovnim subjektom, imetnikom oz. bodočim imetnikom,
- 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 evropskimi 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 uporabniki storitve

(1) Uporabnik storitve časovnega žigosanja je naprava fizične osebe ali poslovnega subjekta.

(2) Uporabnik časovnega žiga mora izpolnjevati vse zahteve iz te politike in veljavnih predpisov.

(3) Naročnik storitve časovnega žigosanja je fizična oseba ali poslovni subjekt.

1.3.4 Tretje osebe

(1) Tretje osebe so osebe, ki se zanašajo na časovne žige ponudnika storitev zaupanja Halcom CA, in so lahko fizične osebe ali poslovni subjekti.

(2) Ob prvi uporabi časovnih žigov Halcom CA po tej politiki mora tretja oseba, ki se zanaša na časovni žig, skrbno prebrati to politiko in od tedaj redno spremljati vsa obvestila Halcom CA.

1.4. Namen uporabe

Halcom CA izdaja in dodeljuje časovne žige, ki so namenjeni uporabi pri storitvah v povezavi s kvalificiranimi digitalnimi potrdili za preverjanje veljavnosti elektronskega podpisa ali drugih storitvah, kjer se podatkom v elektronski obliki dodaja varni časovni žig.

1.4.1 Pravilna uporaba časovnih žigov

(1) Namen časovnih žigov je na kriptografsko varen način zagotavljati povezljivost elektronsko podpisanih dokumentov in drugih elektronskih podatkov z datumom in časom, v katerem so bili elektronski dokumenti ali podatki elektronsko podpisani. Z varnim časovnim žigom se zagotovi tudi, da je bilo digitalno potrdilo veljavno v času elektronskega podpisa dokumenta.

(2) Časovni žigi se uporabljajo v različnih aplikacijah in za različne namene, ki se pojavljajo na tržišču. Med drugim se časovni žigi uporabljajo v aplikacijah in namenih kot so:

- elektronsko bančništvo,
- elektronska hramba podatkov, dokumentarnega ali arhivskega gradiva,
- aplikacije e-uprave,
- druge aplikacije, kjer je treba zagotoviti povezljivost določenega dejanja ali dejstva s točnim časovnim virom.

(3) Za uporabo časovnega žiga Halcom CA mora imeti uporabnik programsko opremo, ki omogoča

časovno žigosanje. Preko nje uporabnik ponudniku storitev zaupanja Halcom CA posreduje zgostitveno vrednost elektronskih podatkov ali elektronskega dokumenta, katerega želi časovno žigosati. Zgostitvena vrednost je »povzetek« dokumenta fiksne dolžine, katero ponudnik storitve časovnega žigosanja Halcom CA digitalno podpiše s svojim zasebnim ključem, pred tem pa ji doda podatke o točnem času podpisa. S tem je zagotovljeno, da so žigosani elektronski podatki ali elektronski dokument nastali pred tem časom.

1.4.2 Nedovoljena uporaba

(1) Prepovedna je uporaba potrdil, 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) Časovni žigi niso namenjeni 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.

Dunajska cesta 123

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

Dunajska cesta 123

1000 LJUBLJANA

Slovenija

Tel.: (+386) 01 200 34 86

E-pošta: ca@halcom.si

E-pošta za preklic : ca_preklici@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 7.12.

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.
NTP	Protokol za sinhronizacijo časa; Ang.: Network Time Protocol
TSP	Protokol za izdajanje časovnih žigov; Ang.: Time-Stamping Protocol
TSA	Time-Stamping Authority je ponudnik storitve zaupanja (angl.: Trust Service provider – TSP), ki uporablja eno ali več enot časovnega žigosanja.
TSS	Time-Stamping Service je servis, ki izdaja časovne žige.
TSU	Time-Stamping Unit je enota za časovno žigosanje, ki uporablja nabor strojne in programske opreme z enim aktivnim ključem za časovno žigosanje.
UTC	Koordinirani univerzalni čas – mednarodni standard za merjenje časa, ki 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 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.com.

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

- cenik,
- politika uporabe storitev zaupanja (CP),
- pravila delovanja ponudnika storitev zaupanja (CPS),
- naročilnice in druge pogodbe za storitve ponudnika storitev zaupanja,
- 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) Potrdila ponudnika storitev zaupanja Halcom CA za časovno žigosanje temeljijo na standardu X.509 in so objavljena na spletnih straneh Halcom CA ter v centralnem imeniku na strežniku ldap.halcom.si. Del centralnega imenika je tudi register preklicanih potrdil.

(3) Preklicana potrdila ponudnika storitev zaupanja 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.

2.3. Pogostnost objav

(1) Nova politika se objavi najkasneje naslednji delovni dan po sprejemu.

(2) Halcom CA poskrbi, da se potrdila ponudnika storitev zaupanja objavijo na spletnih strani in v javnem imeniku takoj (največ 5 sekund) po njihovi izdaji.

(3) Spisek preklicanih potrdil se osveži takoj (največ 5 sekund) po preklicu potrdila v 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) Javni imenik je dostopen na strežniku ldap.halcom.si, TCP vratih 389 po protokolu LDAP.

(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 PONUDNIKA STORITEV ZAUPANJA

Imetnik potrdila za časovno žigosanje je ponudnik storitve zaupanja Halcom CA ali drug zunanji ponudnik storitve zaupanja, ki ga Halcom CA pogodbeno zaveže k izpolnjevanju strogih varnostnih pogojev.

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 Razločevalno ime

(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 X.501.

(2) Ponudnik storitev zaupanja potrdila Halcom CA je v izdanem potrdilu naveden v polju Izdajatelj, angl. Issuer. Osnovni podatki imetnika, ki jih vsebuje razločevalno ime potrdil za časovno žigosanje, so v izdanem potrdilu navedeni v polju Imetnik angl. Subject.

(3) Ponudnik storitve zaupanja Halcom CA je za storitev časovnega žigosanja oblikoval svoje lastno potrdilo, ki je namenjeno elektronskemu podpisovanju časovnih žigov.

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 za elektronsko časovno žigosanje	Izdajatelj, angl. Issuer	C= SI O= Halcom d.d. 2.5.4.97= VATSI-43353126 CN= Halcom CA TSA 1
	Imetnik, angl. Subject	E = ca@halcom.si CN = Halcom CA TS 5 OU = TSA 2.5.4.97 = VATSI-43353126 1.3.6.1.4.1.5939.2.3 = 43353126 O = Halcom d.d. C = SI

3.1.2 Profil potrdila

(1) Profil potrdila za kvalificirano elektronsko časovno žigosanje Halcom CA TS 5.

Nazivi polja Osnovna polja v potrdilu	Vrednost oz. pomen
Različica, angl. Version	V3
Identifikacijska oznaka potrdila, angl. Serial Number	12 08 75
Algoritem za podpis, angl. Signature algorithm	Sha256RSA (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: <24. 05. 2021 08:47:50 GMT> Valid to: <24. 05. 2026 08:47:50 GMT>
Imetnik, angl. Subject	E = ca@halcom.si CN = Halcom CA TS 5 OU = TSA 2.5.4.97 = VATSI-43353126 1.3.6.1.4.1.5939.2.3 = 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	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=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
Identifikator ključa ponudnika storitev zaupanja, OID 2.5.29.35, angl. Authority Key Identifier	KeyID=43 8f 8b 56 9f 44 1e d7
Identifikator imetnikovega ključa, OID 2.5.29.14, angl. Subject Key Identifier	41 85 c9 4b 78 1a 4a 67
Osnovne omejitve, OID 2.5.29.19, angl. Basic Constraints	Subject Type=End Entity Path Length Constraint=None
Razširjena uporaba ključa, angl. Enhanced Key Usage	Time Stamping (1.3.6.1.5.5.7.3.8)
Dodatna identifikacija (ni del digitalnega potrdila)	
Razpoznavni odtis potrdila-SHA1 angl. Certificate Fingerprint – SHA1	Razpoznavni odtis potrdila po SHA1

(2) 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).

(3) Polje razširjena uporaba ključa (angl. Enhanced Key Usage) je označeno kot kritično (angl. critical).

4 ČASOVNO ŽIGOSANJE

4.1. Servis časovnega žigosanja in pridobitev časovnih žigov

4.1.1 Naročilo na storitev časovnega žigosanja

(1) Bodoči uporabnik storitve časovnega žigosanja ponudnika storitev zaupanja Halcom CA se na storitev prijavi z oddajo in podpisom pogodbe za vklop storitve časovnega žigosanja ponudnika storitev zaupanja Halcom CA.

(2) Bodoči uporabnik lahko v pogodbi poleg osebnih podatkov in podatkov o poslovnem subjektu, navede tudi podatke o kvalificiranem digitalnem potrdilu, ki ga bo uporabljal za dostop do servisa varnega časovnega žigosanja ponudnika storitev zaupanja Halcom CA.

(3) Kvalificirano digitalno potrdilo za dostop do časovnega žigosanja lahko izda tudi ponudnik

storitev zaupanja Halcom CA v skladu s takrat veljavno politiko in cenikom ponudnika storitev zaupanja Halcom CA.

(4) S podpisom pogodbe za storitev časovnega žigosanja ponudnika storitev zaupanja Halcom CA se uporabnik zavezuje, da bo spoštoval vse dogovorjene finančne obveznosti ter pogoje in zahteve ponudnika storitev zaupanja Halcom CA iz te politike, pogodbe in določila veljavnih predpisov ter zakonodaje.

4.1.2 Postopek izdaje časovnega žiga

(1) Uporabnik storitve časovnega žigosanja ponudnika storitev zaupanja Halcom CA strežniku za žigosanje posreduje zahtevek za žigosanje preko varne povezave SSL oziroma TLS. Uporabnik (fizična oseba ali informacijski sistem) se na strežnik prijavi s svojim kvalificiranim digitalnim potrdilom (glej razd. 4.1.1).

(2) Programska oprema za izdajo časovnega žiga ponudnika storitev zaupanja Halcom CA samodejno preveri, ali je uporabnik storitve registriran za uporabo storitve časovnega žigosanja po ustrezni politiki ponudnika storitev zaupanja Halcom CA za izdajo časovnega žiga.

(3) Zahtevek za časovno žigosanje se v programski opremi ponudnika storitev zaupanja Halcom CA preveri, tako da vsebuje pravilne podatke in zgostitveno vrednost pravilne vrste in dolžine glede na uporabljeno politiko časovnega žigosanja.

(4) Preverjeni zahtevek za časovno žigosanje se vpiše v dnevnik zahtevkov za žigosanje.

(5) Za zgostitveno vrednost dokumenta iz zahtevka se izdela nov časovni žig ponudnika storitev zaupanja Halcom CA, ki vsebuje vse podatke časovnega žiga (glej razd. 4.1.3) in je digitalno podpisan v varovani strojni opremi v varnem okolju ponudnika storitev zaupanja z namenskim zasebnim ključem za časovno žigosanje.

(6) Časovni žig ponudnika storitev zaupanja Halcom CA se zapiše v dnevnik izdanih časovnih žigov in se posreduje uporabniku, ki je zahtevek za žigosanje poslal.

4.1.3 Varni časovni žig

(1) Časovni žigi, ki jih izdaja ponudnik storitev zaupanja Halcom CA, so izdani na varen način in vsebujejo točen čas nastanka žiga.

(2) Oblika časovnega žiga je v skladu z mednarodnim standardom IETF RFC 3161 in IETF RFC 5816, kadar gre za binarne časovne žige, in standardom OASIS Digital Signature Service (DSS Core specification) kadar gre za časovne žige v obliki XML.

(3) Časovni žigi ponudnika storitev zaupanja Halcom CA vsebujejo naslednje podatke:

- oznako CP_{OID} politike, po kateri je bil žig izdan,
- enolično serijsko številko, ki ga razlikuje od vseh ostalih časovnih žigov, izdanih pri ponudniku storitev zaupanja Halcom CA,
- čas nastanka žiga, ki je na varen način sledljivo usklajen z enim od uradnih UTC laboratorijev

na svetu, seznam katerih določa organizacija Bureau International des Poids et Mesures (BIPM),

- natančnost ure, ki določa čas nastanka posameznega časovnega žiga, omejene s to politiko,
- oznaka algoritma in zgostitveno vrednost podatkov, ki se časovno žigosajo,
- oznaka ponudnika storitev zaupanja Halcom CA, država, kjer se ponudnik storitve nahaja (SI) ter oznaka logične enote, ki je časovni žig izdala (glej razd. 3.1),
- ostale podatke, ki jih predpiše ponudnik storitev zaupanja Halcom CA.

(4) Programska oprema za izdajo časovnih žigov ponudnika storitev zaupanja Halcom CA ima vgrajene metode in postopke za ugotavljanje odstopanja lokalne ure od ure UTC laboratorija, ki v primeru prevelikega odstopanja preprečijo izdajo časovnih žigov.

(5) Časovni žigi ponudnika storitev zaupanja Halcom CA se podpisujejo s ključem, ki se uporablja izključno za namene časovnega žigosanja.

4.2. Upravljanje s ključi za varno časovno žigosanje

4.2.1 Generiranje ključev

(1) Par ključev ponudnika storitev zaupanja Halcom CA za izdajo varnih časovnih žigov se generira v varnem okolju ponudnika storitev zaupanja ob prisotnosti osebja ponudnika storitev zaupanja po posebnem postopku generiranja ključev pod vsaj dvojnim nadzorom.

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

(3) Algoritem za generiranje ključev, dolžina ključev ter algoritem za podpisovanje podatkov so v skladu z evropskimi in mednarodnimi standardi in priporočili.

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

4.2.2 Izdaja potrdila za časovno žigosanje

(1) Potrdilo ponudnika storitev zaupanja Halcom CA za izdajo varnih časovnih žigov se generira v varnem okolju ponudnika storitev zaupanja Halcom CA ob prisotnosti osebja ponudnika storitev zaupanja po posebnem postopku pod vsaj dvojnim nadzorom.

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

4.2.3 Veljavnost digitalnega potrdila za časovno žigosanje

(1) Veljavnost potrdila ponudnika storitev zaupanja Halcom CA za časovno žigosanje je skladno s politiko ponudnika storitev zaupanja Halcom CA za izdajo kvalificiranih digitalnih potrdil pet (5) let.

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

4.2.4 Ponovna izdaja potrdila in regeneracija ključev

(1) Programska in strojna oprema za izdajo časovnih žigov ter postopki ponudnika storitev zaupanja Halcom CA imajo vgrajene varovala in mehanizme, ki preprečujejo uporabo zasebnih ključev po poteku njihove časovne veljavnosti.

(2) Novi ključi ponudnika storitev zaupanja Halcom CA za izdajo časovnih žigov se izdelajo ter aktivirajo v skladu z veljavno politiko ponudnika storitev zaupanja Halcom CA še pred potekom časovne veljavnosti starih ključev.

4.2.5 Uničenje ključev

Postopek za uničenje zasebnega ključa ponudnika storitev zaupanja Halcom CA za časovno žigosanje 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.

4.3 Preklic in suspenz potrdila za časovno žigosanje

4.3.1 Razlogi za preklic

Preklic potrdila se izvede v primeru:

- če je bil zasebni ključ potrdila ogrožen na način, ki vpliva na zanesljivost uporabe,
- če obstaja nevarnost zlorabe zasebnega ključa ali potrdila,
- če so se spremenili oz. so napačni ključni podatki, navedeni v potrdilu,
- da je prišlo do napake pri preverjanju istovetnosti podatkov na prijavni službi,
- da so se spremenile druge okoliščine, ki vplivajo na veljavnost potrdila,
- da je bila infrastruktura ponudnika storitev zaupanja ogrožena na način, ki vpliva na zanesljivost potrdila,
- da bo ponudnik storitve Halcom CA prenehal z izdajanjem časovnih žigov ali da je bilo ponudniku storitev zaupanja prepovedano upravljanje s potrdili in časovnimi žigi ter njegove dejavnosti ni prevzel drug ponudnik storitev zaupanja,
- da je preklic odredilo pristojno sodišče, prekrškovni ali upravni organ.

4.3.2 Kdo zahteva preklic

Preklic potrdila lahko zahteva:

- pooblaščena oseba ponudnika storitev zaupanja,
- pristojno sodišče, prekrškovni ali upravni organ.

4.3.3 Postopki za preklic

(1) Preklic potrdila se izvede v skladu z notranjimi pravili ponudnika storitev zaupanja Halcom CA.

(2) 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).

4.3.4 Čas za izdajo zahtevka za preklic

Preklic je potrebno izvesti nemudoma, če gre za primer zlorabe ali nezanesljivosti ipd. nujne primere.

4.3.5 Čas izvedbe preklica

(1) Ponudnik storitev zaupanja Halcom CA prekliče potrdilo:

- najkasneje v štirih (4) urah, če gre za preklic zaradi zlorabe ali nezanesljivosti ipd.

(2) Po preklicu je tako potrdilo takoj (največ pet (5) sekund) dodano v register preklicanih potrdil.

4.3.6 Zahteve po preverjanju registra preklicanih potrdil za tretje osebe

Pred uporabo morajo tretje osebe, ki se zanašajo na časovne žige, 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.

4.3.7 Pogostnost objave registra preklicanih potrdil

Register preklicanih potrdil se osvežuje:

- 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.

4.3.8 Čas objave registra preklicanih potrdil

Objava novega registra preklicanih potrdil se izvede:

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

4.3.9 Sprotno preverjanje statusa potrdil OCSP

Ni podprto.

4.4 Sinhronizacija ure s časovnim virom

(1) Referenčna ura, ki se uporablja za določanje časa nastanka časovnih žigov ponudnika storitev zaupanja Halcom CA, se redno na varen način po protokolu NTP z obojestransko avtentikacijo usklajuje z uro enega od uradno priznanih UTC laboratorijev s seznama organizacije Bureau

International des Poids et Mesures (BIPM).

(2) Referenčna ura, ki se uporablja za določanje časa nastanka časovnih žigov ponudnika storitev zaupanja Halcom CA, se nahaja v elektronsko in fizično varovanih prostorih ponudnika storitev zaupanja Halcom CA, do katerih ima dostop le pooblaščeno osebje ponudnika storitev zaupanja Halcom CA.

(3) Programska oprema za nadzor referenčne ure ponudnika storitev zaupanja Halcom CA izklopi sistem za izdajo časovnih žigov v primeru, da zazna odstopanje referenčne ure od ure UTC laboratorija, ki presega v tej politiki deklarirano natančnost izdanih časovnih žigov ponudnika storitev zaupanja Halcom CA v velikosti +/- 1 sekunde.

(4) Referenčna ura, ki se uporablja za določanje časa nastanka časovnih žigov ponudnika storitev zaupanja Halcom CA, skrbi za upoštevanje prestopne sekunde (angl. »leap second«), kot jo določi ustrezna mednarodna meroslovna organizacija.

4.5 Šifrirni algoritmi, formati podatkov in protokoli

(1) Halcom CA uporablja:

- za podpisovanje varnega časovnega žiga algoritem RSA s parom ključev dolžine 2048 bitov,
- za šifriranje podatkov algoritme Triple DES in AES,
- zgostitveni algoritem SHA-256,
- za sinhronizacijo ure protokol NTP v4 z IFF autokey obojestransko avtentikacijo,
- format potrdila ponudnika storitev zaupanja Halcom CA sledijo standardu X.509, in sicer različici 3,
- format varnega časovnega žiga ustreza priporočilu IETF RFC 3161 in IETF RFC 5816 ter standardu OASIS Digital Signature service (DSS Core specification),
- register preklicanih potrdil ustreza priporočilu ITU-T za X.509 (2005) in ISO/IEC

  9594-8:2014,
- protokol LDAP ustreza priporočilu IETF RFC.

(2) Celoten nabor algoritmov, formatov podatkov in protokolov je na razpolago pri Halcom CA.

5 UPRAVLJANJE IN VARNOSTNI NADZOR INFRASTRUKTURE

(1) Halcom CA načrtuje in izvaja vse varnostne ukrepe v skladu z družino standardov ISO/IEC 27000, FIPS 140-2 nivo 3 in/ali Common Criteria EAL4+ 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 več nivojskim 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 več nivojskim 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 notranjih pravilih ponudnika storitev zaupanja Halcom CA.

5.1.8 Hramba na oddaljeni lokaciji

Glej razd. 5.1.6.

5.2. Organizacijska struktura ponudnika storitev zaupanja

(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 in
- prijavne službe.

(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, • priprava nosilcev podatkov za zasilni ponovni start sistema v primeru katastrofalne izgube sistema, • varno shranjevanje in distribucija kopij in nadgradenj na ločeno lokacijo.	2
	Sistemski administrator	• Upravljanje postopkov za izdajo potrdil in žigov, • pomoč podrejenim ponudnikom storitev zaupanja, • pooblaščanje podrejenih ponudnikov storitev zaupanja, • dostop do protokola podpisovanja potrdil in časovnega žigosanja, • 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	2

		povezane z vzdrževanjem, • izvajanje arhiviranja zahtevanih sistemskih zapisov, • izpis kod PIN, • dnevni pregled sistema.	
	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
	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, • 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.	1

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 in žigov.

2. Pomoč podrejenim ponudnikom storitev zaupanja.

3. Pooblaščanje podrejenih ponudnikov storitev zaupanja.

4. Dostop do protokola podpisovanja potrdil in časovnega žigosanja.

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: 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 ali žigov.

(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 določeni v notranjih pravilih ponudnika storitev zaupanja Halcom CA.

5.4.2 Pogostost 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 deset (10) let po njihovem nastanku, če poseben zakon ne določa daljšega roka.

5.4.4 Zaščita dnevnikov

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

(2) Podrobnosti so določene v notranjih pravilih ponudnika storitev zaupanja.

5.4.5 Varnostne kopije dnevnikov

(1) Varnostne kopije dnevnikov se izvajajo dnevno.

(2) Podrobnosti določene v notranjih pravilih ponudnika storitev zaupanja.

5.4.6 Zbiranje podatkov za dnevnike

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

(2) Podrobnosti so določene v notranjih pravilih ponudnika storitev zaupanja.

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 avtomatsko z drugimi varnostnimi mehanizmi na vseh informacijsko-komunikacijskih napravah v pristojnosti ponudnika storitev zaupanja.

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

(3) Podrobnosti so določene v notranjih pravilih ponudnika storitev zaupanja.

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,
- vse zahtevke ali pogodbe,

- potrdila in register preklicanih potrdil,
- politike delovanja,
- CPS,
- 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 deset (10) let po poteku potrdila, na katerega se podatek nanaša, če poseben zakon ne določa daljšega roka.

(2) Ostali dolgoročno hranjeni podatki se hranijo vsaj deset (10) 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 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 notranjih pravilih ponudnika storitev zaupanja Halcom CA.

5.5.5 Zahteva po časovnem žigosanju dokumentov

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 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 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 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 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 notranjih pravilih ponudnika storitev zaupanja Halcom CA.

5.7.4 Okrevalni načrt

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

6. 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.

6.1. Pogostnost nadzora

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

(2) Pooblaščenec za zunanji nadzor 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.

6.2. 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.

6.3. 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.

6.4. Področja nadzora

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

6.5. 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.

6.6. Objava rezultatov nadzora

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

7. FINANČNE IN OSTALE PRAVNE ZADEVE

7.1. Cenik

Halcom CA določi cenik storitev časovnega žiga in drugih svojih storitev ter cenik objavi na svojih spletnih straneh.

7.1.1 Cena izdaje časovnih žigov

Cena je določena v skladu s cenikom storitev ali pogodbo z uporabnikom.

7.1.2 Cena dostopa do potrdil

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

7.1.3 Cena dostopa do statusa potrdila in registra preklicanih potrdil

Register preklicanih potrdil je brezplačno dostopen vsem osebam.

7.1.4 Cene drugih storitev

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

7.1.5 Povrnitev stroškov

Ni predpisana.

7.2. Finančna odgovornost

7.2.1 Zavarovalniško kritje

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

7.2.2 Drugo kritje

Ni predpisano.

7.2.3 Zavarovanje imetnikov

Ni predpisano.

7.3. Varovanje poslovnih podatkov

7.3.1 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 zavedene v notranjih pravilih ponudnika storitev zaupanja Halcom CA.

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

7.3.2 Nevarovani podatki

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

7.3.3 Odgovornost glede varovanja

(1) Halcom CA je zavezan delovati in izdajati časovne žige v skladu s to politiko, z notranjimi pravili, ter z drugimi predpisi, na katere se ta politika sklicuje.

(2) Halcom CA ne prevzema nobene odgovornosti za podatke, ki jih naročnik časovnega žiga elektronsko šifrira, podpisuje ali varno časovno žigosa. Halcom CA ne prevzema odgovornosti za te

podatke 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.

(3) Halcom CA ne prevzema nobene odgovornosti za posledice, ki nastanejo, ker uporabnik varnega časovnega žiga ni ravnal v skladu z varnostnimi zahtevami te politike.

7.4. Varovanje osebnih podatkov

7.4.1 Načrt varovanja osebnih podatkov

Z vsemi osebnimi in zaupnimi podatki o imetnikih potrdil, ki so nujno potrebni za storitve upravljanja s časovnimi žigi, ponudnik storitev zaupanja Halcom CA ravna v skladu z veljavno zakonodajo.

7.4.2 Varovani osebni podatki

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.

7.4.3 Nevarovani osebni podatki

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

7.4.4 Odgovornost glede varovanja osebnih podatkov

Ponudnik storitev zaupanja Halcom CA je odgovoren v skladu z veljavnimi predpisi o varstvu podatkov.

7.4.5 Pooblastilo glede uporabe osebnih podatkov

Ni predpisano.

7.4.6 Posredovanje osebnih podatkov

(1) Ponudnik storitev zaupanja Halcom CA ne posreduje drugih podatkov o uporabnikih, razen če se določeni podatki posebej zahtevajo za izvajanje specifičnih storitev oz. aplikacij, povezanih s časovnimi žigi, ter je ponudnika storitev zaupanja Halcom CA imetnik pooblastil za to, ali na zahtevo pristojnega sodišča, prekrškovnega ali upravnega organa.

(2) Podatki se posredujejo tudi brez pisne privolitve, če to določa zakonodaja oz. veljavni predpisi.

7.4.7 Druga določila glede varovanja osebnih podatkov

Niso predpisana.

7.5. Določbe glede pravic intelektualne lastnine

Vse avtorske, sorodne in druge pravice na časovnem žigu in na drugih ključih ter vseh ostalih podatkih pripadajo Halcom CA.

7.6. Obveznosti in odgovornosti

7.6.1 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 ipd.),
- objavljati na svojih spletnih straneh vse informacije o tistih spremembah glede dejavnosti ponudnika storitev zaupanja, ki kakorkoli vplivajo na uporabnike časovnega žiga in tretje osebe,
- zagotoviti delovanje prijavnih služb v skladu z določili Halcom CA in ostalimi veljavnimi predpisi,
- spoštovati določila glede varnega ravnanja z osebnimi 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,
- izdati časovni žig v skladu s to politiko in ostalimi predpisi ter priporočili.

(2) Ponudnik storitev zaupanja Halcom CA je dolžan:

- 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.

7.6.2 Obveznost in odgovornost prijavne službe

(1) Prijavna služba je dolžna:

- preverjati istovetnost poslovnega subjekta in drugih, za upravljanje kvalificiranih časovnih žigov, pomembnih podatkov,
- sprejemati pogodbe za vklop storitve varnega časovnega žigosanja,
- sprejemati pogodbe za izklop storitve varnega časovnega žigosanja,
- izdajati potrebne dokumentacije poslovnim subjektom, imetnikom oz. bodočim imetnikom,
- posredovati pogodbe in ostale podatke na varen način ponudniku storitev zaupanja Halcom CA.

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

7.6.3 Obveznosti in odgovornost imetnika potrdila

(1) Uporabnik oziroma bodoči uporabnik časovnega žiga je dolžan:

- skrbno prebrati to politiko pred podpisom pogodbe za časovni žig ter spremljati vsa obvestila Halcom CA in ravnati v skladu z njimi,
- spremljati razvoj tehnologije oziroma obvestila Halcom CA in ravnati v skladu s priporočili Halcom CA glede zanesljive uporabe časovnih žigov.

(2) Uporabnik časovnega žiga mora izpolnjevati vse zahteve iz te politike in veljavnih predpisov.

(3) Uporabnik časovnega žiga lahko kadarkoli zahteva vse informacije glede veljavnosti časovnega žiga, glede določb te politike ter glede obvestil Halcom CA.

7.6.4 Obveznosti in odgovornost tretjih oseb

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

(2) Tretje osebe, ki se zanašajo na varni časovni žig, morajo:

- preveriti pravilnost zapisa varnega časovnega žiga,
- preveriti veljavnosti časovnega žiga in veljavnost lastnega digitalnega potrdila Halcom CA, s katerim so elektronsko podpisani javni ključi časovnih žigov,
- seznaniti se s to politiko,
- upoštevati morebitne omejitve pri uporabi časovnih žigov, določene s to politiko.

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

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

7.6.5 Obveznosti in odgovornost drugih oseb

Ni predpisano.

7.7. Omejitev odgovornosti

(1) HALCOM-CA ne prevzema nobene odgovornosti za podatke, ki jih naročnik varnega časovnega žiga elektronsko šifrira, podpisuje ali varno časovno žigosa. Halcom CA ne prevzema odgovornosti za te podatke 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 uporabnik varnega časovnega žiga ni ravnal v skladu z varnostnimi zahtevami.

7.8. Omejitev glede uporabe

Ni predpisano.

7.7. Poravnava škode

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

7.10. Veljavnost politike

(1) Halcom CA si pridržuje pravico do spremembe politike delovanja in nadgradnje infrastrukture brez predhodnega obveščanja imetnikov potrdil. Izdani časovni žigi pri tem ostanejo v veljavi in zanje še naprej velja tista politika delovanja, ki je veljala ob njihovi izdaji. Za vsak časovni žig, izdan

po začetku veljavnosti nove politike, velja nova politika.

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

7.10.1 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 časovnih žigov, izdanih na podlagi politike.

7.10.2 Konec veljavnosti politike

(1) Ob objavi nove politike ostanejo za vse časovne žige, izdane 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 bil časovni žig izdan ipd.).

(2) Ponudnik storitev zaupanja lahko za posamezna določila veljavne politike izda dopolnitve, kot je to določeno v razdelku 7.12.

7.10.3 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 časovnih žigov, ki so bili izdani po prejšnjih politikah. Taki časovni žigi ostanejo v veljavi, pri čemer se, kjer je to možno, obravnavajo po novi politiki.

7.11. Komuniciranje med subjekti

(1) Kontaktni podatki ponudnika storitev zaupanja so objavljeni na spletnih straneh in podani v razd. 1.5.2.

(2) Kontaktni podatki uporabnikov so podani v pogodbi.

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

7.12. Spremembe in dopolnitve

7.12.1 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.

7.12.2 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.

7.12.3 Sprememba identifikacijske številke politike

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

7.13. Postopek v primeru sporov

(1) Vse pritožbe uporabnikov 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.

7.14. Veljavna zakonodaja

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

7.15. 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.

7.16. 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.

7.17. Druge določbe

Niso predpisane.

Kraj in datum:
Ljubljana, 26.5.2023

Glavni izvršni direktor:
Tomi Šefman