Pripravil(a): Luka RIBIČIČ

Številka dokumenta: 400085-8-10/17

Politika Halcom CA: Splošna pravila delovanja - CPS

Izdaja: 10

Politika Halcom CA

Splošna pravila delovanja - CPS (Certificate Practise Statement)

Dokument je veljaven od: 15.6.2024

Izdaja	št. dokumenta in prilog	Opis spremembe	Avtor	Datum zadnje spremembe
1	400085-8-1/17	Začetna izdaja	L. Ribičič	3.1.2011
2	4000851-8-2/17	Dopolnitve EIDAS	L. Ribičič	24.4.2017
3	400085-8-3/17	Letni pregled dokumenta – ni sprememb	S. Lazić	1.6.2018
4	400085-8-4/17	Letni pregled dokumenta, nova celostna podoba, dopolnitev za potrdila v oblaku	L. Ribičič	24.5.2019
5	400085-8-5/17	Dopolnitev identifikatorjev, osnovni kapital, identifikacija, distribucija kod	S. Lazić	29.4.2020
6	400085-8-6/17	Dopolnitev profila potrdil končnih uporabnikov (Non Repudiation)	S. Lazić	3.2.2021
7	400085-8-7/17	Letni pregled dokumenta, dopolnitev postopka pri izdaji potrdil in razločevalnega imena	S. Lazić	21.5.2021
8	400085-8-8/17	Letni pregled dokumenta, odstranili fax, dopolnitev veljavnosti potrdila v oblaku	S. Lazić	13.4.2022
9	400085-8-9/17	Letni pregled dokumenta, nova vmesna potrdila, čas in rok hrambe	S. Lazić	23.5.2023
10	400085-8-10/17	Letni pregled dokumenta, EŠEI	L. Ribičič	22.5.2024

Kazalo vsebine

1. UVOD

(1) Ta dokument predstavlja Splošna pravila delovanja (v nadaljevanju: CPS (angl. Certificate Practise Statement)) ponudnika storitev zaupanja na področju elektronskega podpisovanja, elektronskega žigosanja, elektronskega časovnega žigosanja, validacije in drugih storitev.

(2) 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.

(3) Vse določbe CPS glede ravnanja Halcom CA so ustrezno prenesene in podrobneje opredeljene v določbah notranjih pravil. To so dokumenti zaupne narave, ki opredeljujejo infrastrukturo, določila glede osebja Halcom CA (pristojnosti, naloge, pooblastila in zahtevani pogoji, ki jih morajo izpolnjevati posamezni člani 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,...).

1.1. Pregled

(1) CPS predstavlja splošna pravila delovanja ponudnika storitev zaupanja HALCOM CA za izdajo potrdil, ureja namen, delovanje in metodologijo upravljanja s potrdili ter varnostne zahteve, ki jih morajo izpolnjevati ponudnik storitev zaupanja HALCOM CA, imetniki in tretje osebe, ki se zanašajo na ta potrdila, ter odgovornost vseh naštetih oseb.

(2) Halcom CA je ponudnik naslednjih storitev:

- Kvalificirana potrdila za elektronske podpise,
- kvalificirana storitev potrjevanja veljavnosti elektronskih podpisov,
- kvalificirana storitev hrambe elektronskih podpisov,
- kvalificirani potrdila za elektronske žige,
- kvalificirana storitev potrjevanja veljavnosti elektronskih žigov,
- kvalificirana storitev hrambe elektronskih žigov,
- kvalificirani elektronski časovni žig,
- kvalificirana potrdila za avtentikacijo spletišč.

(3) Ponudnik storitev zaupanja Halcom CA deluje v okviru Halcom d.d.

(4) Halcom CA izdaja:

- Kvalificirana digitalna potrdila za elektronsko podpisovanje,
- kvalificirana digitalna potrdila za elektronsko žigosanje,

- kvalificirana digitalna potrdila za avtentikacijo spletišč in
- kvalificirana digitalna potrdila za časovno žigosanje.

(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 potrdil, Halcom CA objavi na svetovnem spletu.

1.1.1 Osnovni dokumenti ponudnika storitev zaupanja Halcom CA

Podrobnejša pravila, pogoji ter pravice in obveznosti glede delovanja ponudnika storitev zaupanja Halcom CA so opisani v sledečih javnih dokumentih:

- Politika Halcom CA za kvalificirana digitalna potrdila za poslovne subjekte,
- Politika Halcom CA za kvalificirana digitalna potrdila za fizične osebe,
- Politika Halcom CA za kvalificirana digitalna potrdila za avtentikacijo spletišč,
- Politika Halcom CA za kvalificirano časovno žigosanje,
- Splošna pravila delovanja.

1.1.2 Povezave osnovnih dokumentov ponudnika storitev zaupanja Halcom CA

(1) Politika definira zahteve poslovanja ponudnika storitev zaupanja, CPS pa operativne procese za izpolnitev teh zahtev. Splošna pravila delovanja (CPS) definirajo način, kako ponudnik storitev zaupanja zagotavlja tehnične, organizacijske in procesne zahteve poslovanja, ki so definirane v politiki Halcom CA.

(2) Politika je v primerjavi s CPS bolj splošen dokument. CPS predstavlja podrobnejši opis načina poslovanja ponudnika storitev zaupanja Halcom CA, poslovnih in operativnih procesov izdajanja in upravljanja s potrdili.

(3) Politika je definirana neodvisno od specifične operativne enote ponudnika storitev zaupanja, splošna pravila delovanja pa predstavljajo podroben opis organizacijske strukture in operativnih procesov ponudnika storitev zaupanja Halcom CA.

1.1.3 Standardi

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 s tehničnimi zahtevami ETSI, standardom IETF RFC in družino standardov ISO/IEC ter drugih sorodnih standardov.

1.1.4 Notranja pravila Halcom CA

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

(2) Notranja pravila so zaupni dokumenti in predstavljajo poslovno skrivnost ponudnika storitev zaupanja Halcom CA.

(3) Notranja pravila vsebujejo podrobne odredbe o:

- Sistemu fizične kontrole vstopov v prostore Halcom CA,
- sistemu logične kontrole pristopov računalniškim omrežjem Halcom CA,
- sistemu za varovanje privatnih ključev Halcom CA,
- sistemu distribuirane odgovornosti pri aktivaciji privatnih ključev Halcom CA,
- postopkih in osebju, ki sodeluje pri izvajanju storitev zaupanja,
- postopkih v nepredvidljivih okoliščinah (požar, poplava, potres, vdor v prostore ali informacijski sistem ponudnika storitev zaupanja).

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

1.2. Ponudnik storitev zaupanja Halcom CA

Halcom CA je odgovoren za izdajo naslednjih kvalificiranih digitalnih potrdil:

- Halcom Root Certificate Authority (korensko potrdilo Halcom CA)
- Halcom CA PO e-signature 1 (vmesno/podrejeno potrdilo za Kvalificirana digitalna potrdila za poslovne subjekte),
- Halcom CA PO e-signature 2 (vmesno/podrejeno potrdilo za Kvalificirana digitalna potrdila za poslovne subjekte),
- Halcom CA FO e-signature 1 (vmesno/podrejeno potrdilo za Kvalificirana digitalna potrdila za fizične osebe),
- Halcom CA FO e-signature 2 (vmesno/podrejeno potrdilo za Kvalificirana digitalna potrdila za fizične osebe),
- Halcom CA PO e-seal 1 (vmesno/podrejeno potrdilo za Kvalificirana digitalna potrdila za elektronske žige)
- Halcom CA PO e-seal 2 (vmesno/podrejeno potrdilo za Kvalificirana digitalna potrdila za elektronske žige)
- Halcom CA web 1 (vmesno/podrejeno potrdilo za Kvalificirana digitalna potrdila za avtentikacijo spletišč)
- Halcom CA TSA 1 (vmesno/podrejeno potrdilo za Kvalificirane časovne žige)
- Uporabniška potrdila:

    1. Fizične osebe:

- Potrdila za elektronsko podpisovanje,
- potrdila za avtenikacijo spletišč.

2. Poslovni subjekti:

    1. Potrdila za elektronsko podpisovanje (pooblaščenci poslovnih subjektov),
    2. potrdila za avtenikacijo spletišč,
    3. potrdila za elektronsko žigosanje.

1.3. Subjekti

1.3.1 Ponudnik storitev zaupanja Halcom CA

Halcom CA je ponudnik storitev zaupanja, ki izdaja in upravlja s potrdili za elektronsko podpisovanje, elektronsko žigosanje, elektronsko časovno žigosanje, validacijo in druge storitve. 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 fizične osebe, poslovnih subjektov, pooblaščenca poslovnih subjektov in drugih, za upravljanje potrdil, pomembnih podatkov,
- sprejemanje zahtevkov za pridobitev potrdil,
- sprejemanje zahtevkov za preklic potrdil,
- izdajanje potrebne dokumentacije 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, splošnimi pravili delovanja in notranjimi pravili Halcom CA.

(3) Ponudnik storitev zaupanja Halcom CA ima vzpostavljeno geografsko razpršeno prijavno službo, kar bodočim imetnikom omogoča enostavno prijavo v domačem ali bližnjem kraju. Informacije o lokacijah prijavne službe so dostopne na spletnih straneh ponudnika storitev zaupanja Halcom CA.

1.3.3 Naročniki in imetniki potrdil

(1) Naročnik/imetnik potrdila je lahko fizična oseba ali poslovni subjekt (odvisno od vrste potrdila).

Storitev	Izdajatelj	Naročnik	Imetnik

Potrdila za poslovne subjekte (e-podpis)	Halcom CA PO e-signature 1	Poslovni subjekt	Fizična oseba
Potrdila za poslovne subjekte (e-podpis)	Halcom CA PO e-signature 2	Poslovni subjekt	Fizična oseba
Potrdila za elektronske žige	Halcom CA PO e-seal 1	Poslovni subjekt	Naprava oz. strežnik
Potrdila za elektronske žige	Halcom CA PO e-seal 2	Poslovni subjekt	Naprava oz. strežnik
Potrdila za avtentikacijo spletišč	Halcom CA web 1	Poslovni subjekt ali fizična oseba	Strežnik
Potrdila za fizične osebe	Halcom CA FO e-signature 1	Fizična oseba	Fizična oseba
Potrdila za fizične osebe	Halcom CA FO e-signature 2	Fizična oseba	Fizična oseba
Potrdila za elektronske časovne žige	Halcom CA TSA 1	Ponudnik storitve zaupanja	Naprava oz. strežnik

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 ali pravne osebe.

(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 potrdili za elektronsko podpisovanje, elektronsko žigosanje, avtentikacijo spletišč in časovno žigosanje. Potrdila so namenjena fizičnim osebam in poslovnim subjektom.

1.4.1 Pravilna uporaba potrdil in ključev

(1) Potrdila za elektronsko podpisovanje/žigosanje so namenjena podpisovanju/žigosanju enostranskih ali medsebojnih komunikacij imetnikov potrdil ter za uporabo v različnih aplikacijah in za različne namene, ki se pojavljajo na tržišču. Med drugim se lahko potrdila uporabljajo v namenih kot so npr.:

1) identifikacija imetnika,

2) izkazovanje istovetnosti imetnika,

3) podpisovanje dokumentov v elektronski obliki,

4) šifriranje in dešifriranje dokumentov v elektronski obliki.

(2) Elektronski podpis/žig se lahko uporablja v aplikacijah kot so npr.:

1) elektronsko oz. mobilno bančništvo,
2) aplikacije e-uprave ali m-uprave,
3) aplikacije e-zdravstva ali m-zdravstva,
4) podpisovanje/žigosanje elektronskih ali mobilnih obrazcev,
5) varno poslovanje z organi in organizacijami javnega sektorja ter z drugimi pravnimi ali fizičnimi osebami,
6) druge aplikacije oziroma storitve, v katerih se zahteva uporaba potrdila,
7) kontrola dostopa.

(3) Potrdila za avtentikacijo spletišč so namenjena:

1) identifikacija spletišča,
2) izkazovanje istovetnosti spletišča,
3) kontroli dostopa,
4) vzpostavitvi varnih povezav.

(4) Varni 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:

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

1.4.2 Nedovoljena uporaba

(1) Prepovedana je uporaba potrdil, izdanih v skladu s politikami, v nasprotju z določili politik ali veljavnih predpisov ali izven obsega dovoljene uporabe, določene v prejšnjem razdelku.

(2) Potrdila niso namenjena nadaljnji prodaji.

1.5. Upravljanje z dokumenti

1.5.1 Upravljavec dokumentov

(1) S CPS 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 splošnimi pravili delovanja in politikami 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.com
E-pošta za preklic : ca_preklici@halcom.si

1.5.3 Odgovorna oseba glede skladnosti delovanja ponudnika storitev zaupanja Halcom CA z dokumenti

Za skladnost delovanja ponudnika storitev zaupanja Halcom CA s CPS in politikami so skladno s svojimi pristojnostmi odgovorne pooblaščene osebe ponudnika storitev zaupanja.

1.5.4 Postopek za sprejem dokumentov

(1) Vsak predlog novega CPS 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 izda dopolnitve, kot je to določeno v razdelku 9.12.

1.6. Okrajšave in izrazi

1.6.1 Okrajšave

CA	Ponundnik 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).

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.
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).
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.
EŠEI	Enotna številka elektronske identifikacije

1.6.2 Izrazi

Ponudnik storitev zaupanja	Fizična ali pravna oseba, ki izdaja potrdila ali opravlja druge storitve zaupanja (angl.: Trust Service provider - TSP).
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.

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.com/ (povzetki bistvenih sestavin tudi v angleškem jeziku).

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

- cenik,
- politika uporabe storitev zaupanja (CP),
- splošna pravila delovanja ponudnika storitev zaupanja (CPS),
- naročilnice in druge pogodbe za storitve ponudnik 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) CPS in 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) CPS ali nove politike se objavi najkasneje naslednji delovni dan po sprejemu.

(2) Halcom CA poskrbi, da se potrdila objavijo v centralnem imeniku takoj (največ 5 sekund) po njihovi izdaji.

(3) Spisek preklicanih potrdil se osveži takoj (največ 5 sekund) 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 fizične osebe ali 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.).

(4) Halcom CA lahko skladno z eIDAS Uredbo ter ETSI standardi pri tvorbi razločevalnega imena tujih fizičnih oseb in/ali tujih poslovnih subjektov uporabi tudi druge semantične identifikatorje fizičnih oseb in poslovnih subjektov, kot so "PNO", »IDC« ali »PAS« in ISO 3161-1 oznaka države za identifikacijo na podlagi nacionalne matične številke ali številke potnega lista ali osebne izkaznice za fizične osebe, za poslovne subjekte pa "NTR" in ISO 3161-1 oznaka države za identifikacijo na podlagi identifikatorja iz nacionalnega registra poslovnih subjektov ali lokalna oznaka (dva znaka v skladu z lokalno opredelitvijo v določeni državi, ki se šteje za primerno za nacionalno in evropsko raven).

(5) Za kvalificirana potrdila za namen identifikacije ponudnikov plačilnih storitev se v skladu s prvim odstavkom 34. člena Delegirane uredbe Komisije (EU) 2018/389 z dne 27. novembra 2017 o dopolnitvi Direktive (EU) 2015/2366 Evropskega parlamenta in Sveta glede regulativnih tehničnih standardov za močno avtentikacijo strank ter skupnih in varnih odprtih standardov komunikacije (RTS SCA) uporablja semantičen identifikator »PSD« z ISO 3161-1 oznako države, vlogo ponudnika plačilnih plačil, naziv pristojnega organa (NCA), kjer je ponudnik plačilnih storitev registriran in registracijsko številko ponudnika plačilnih storitev, ki je navedena v uradnih evidencah tega organa.

(6) Ponudnik storitev zaupanja Halcom CA lahko pri izdaji kvalificiranega digitalnega potrdila v polje Imetnik (angl. Subject) doda tudi atribut 1.3.6.1.4.1.5939.2.9, ki predstavlja vrsto potrdila (npr. označuje, da gre za kvalificirano digitalno potrdilo v oblaku, na pametni kartici ali ključu USB ipd.).

- Potrdila ponudnika storitev zaupanja Halcom CA:

Vrsta potrdila	Naziv polja	Razločevalno ime
Korensko potrdilo	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 potrdilo za poslovne subjekte	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 PO e-signature 1 ali CN= Halcom CA PO e-signature 2
	Izdajatelj, angl. *Issuer* in	C= SI O= Halcom d.d.

Vmesno/podrejeno potrdilo za fizične osebe		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 FO e-signature 1 ali CN= Halcom CA FO e-signature 2
Vmesno/podrejeno potrdilo za elektronske žige	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 PO e-seal 1 ali CN= Halcom CA PO e-seal 2
Vmesno/podrejeno za avtentikacijo spletišč	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 web 1
Vmesno/podrejeno za časovno žigosanje	Izdajatelj, angl. *Issuer*	C= SI O= Halcom d.d. 2.5.4.97 = VATSI-43353126 CN= Halcom Root Certificate Authority
	Imetnik,	C= SI

	angl. *Subject*	O= Halcom d.d. 2.5.4.97= VATSI-43353126 CN= Halcom CA TSA 1

- Potrdila končnih uporabnikov

Vrsta potrdila	Naziv polja	Razločevalno ime
Potrdilo za poslovne subjekte (e-podpis)	Izdajatelj, angl. *Issuer*	C= SI O= Halcom d.d. 2.5.4.97= VATSI-43353126 CN= Halcom CA PO e-signature 1 ali CN= Halcom CA PO e-signature 2
	Imetnik, angl. *Subject*	C= SI O= <naziv poslovnega subjekta> 2.5.4.97=<VATSI- davčna št. poslovnega subjekta> in/ali 1.3.6.1.4.1.5939.2.3= <davčna št. poslovnega subjekta> CN=<ime in priimek> SN= <priimek> G= <ime> SERIALNUMBER=<TINSI-davčna št. imetnika> in/ali 1.3.6.1.4.1.5939.2.2= <davčna št. imetnika> E= <elektronska pošta>
Potrdilo za fizične osebe (e-podpis)	Izdajatelj, angl. *Issuer*	C= SI O= Halcom d.d. 2.5.4.97= VATSI-43353126 CN= Halcom CA FO e-signature 1 ali CN= Halcom CA FO e-signature 2
	Imetnik, angl. *Subject*	C= SI CN=<ime in priimek>

		SN= <priimek> G= <ime> SERIALNUMBER=<TINSI-davčna št. imetnika> in/ali 1.3.6.1.4.1.5939.2.2= <davčna št. imetnika> E= <elektronska pošta>
Potrdilo za elektronske žige	Izdajatelj, angl. *Issuer*	C= SI O= Halcom d.d. 2.5.4.97= VATSI-43353126 CN= Halcom CA PO e-seal 1 ali CN= Halcom CA PO e-seal 2
	Imetnik, angl. *Subject*	C= SI O= <naziv poslovnega subjekta> 2.5.4.97=<VATSI- davčna št. poslovnega subjekta> in/ali 1.3.6.1.4.1.5939.2.3= <davčna št. poslovnega subjekta> CN=< naziv informacijskega sistema ali oddelka > E= <elektronska pošta>
Potrdilo za avtentikacijo spletišč	Izdajatelj, angl. *Issuer*	C= SI O= Halcom d.d. 2.5.4.97= VATSI-43353126 CN= Halcom CA web 1
	Imetnik, angl. *Subject*	C= SI O= <naziv poslovnega subjekta> 2.5.4.97=<VATSI- davčna št. poslovnega subjekta> in/ali 1.3.6.1.4.1.5939.2.3= <davčna št. poslovnega subjekta> OU= server certificates CN=<ime spletišča in domena> SN= <domena>

		G= <ime spletišča> E = <e-pošta>
Potrdilo za 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*	C= SI O= <naziv poslovnega subjekta oz. ponudnika storitev zaupanja> 2.5.4.97=<VATSI- davčna št. poslovnega subjekta> in/ali 1.3.6.1.4.1.5939.2.3= <davčna št. poslovnega subjekta> CN=<ime potrdila oz. servisa za časovno žigosanje> E= <elektronska pošta>

3.1.2 Zahteve pri tvorbi razločevalnega imena

(1) Oznaka fizične ali pravne osebe, ki je v skladu z določili razdelka 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) V primeru potrdila za strežnik mora biti za ime strežnika navedeno polno domensko ime (angl. fully qualified domain name).

(3) 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 bodočih imetnikov ob prvi izdaji potrdila

Istovetnost bodočih imetnikov pri prvi izdaji potrdila se preverja na prijavni službi ponudnika storitev zaupanja ali neposredno pri ponudniku storitev zaupanja Halcom CA. Halcom CA pred izdajo potrdila preveri podatke bodočega imetnika in poslovnega subjekta v ustreznih registrih.

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 razdelek 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.

(4) Ponudnik storitev zaupanja Halcom CA na podlagi vloge za potrdilo za avtentikacijo spletišč pri pooblaščenem registrarju domen preveri lastništvo domene, katero je pooblaščena oseba poslovnega subjekta navedla na zahtevku.

3.2.3 Preverjanje istovetnosti imetnika

(1) Prijavna služba ponudnika storitev zaupanja Halcom CA nesporno ugotovi istovetnost imetnikov potrdil v skladu z veljavnimi predpisi (uradni dokument s sliko) ali posreduje podatke o imetnikih iz svojih podatkovnih zbirk, pridobljenih po postopku, ki ga prijavna služba uporablja za druge namene in skladno z veljavnimi predpisi zagotavlja enakovredno raven zanesljivosti.

(2) Poslovni subjekt se kot delodajalec oziroma pooblastitelj imetnikov potrdil zavezuje, da bodo pooblaščenci izpolnjevali vse določbe Politike Halcom CA in veljavne predpise.

(3) Ponudnik storitev zaupanja Halcom CA preveri osebne podatke imetnika v ustreznih registrih, če ni z veljavnimi predpisi določeno drugače.

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 in/ali določeno osebo, ki je zaposlena ali opravlja naloge za ta 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 storitev zaupanja status kvalificiranega ponudnika storitev zaupanja ali ponudnika storitev zaupanja kvalificiranih digitalnih potrdil.

(2) Ponudnik storitev zaupanja Halcom CA zagotavlja, da bo izvajal medsebojno priznavanje izključno po podpisu pisne pogodbe z drugimi ponudniki 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 drugega ponudnika storitev zaupanja, pooblaščene osebe 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 ponudnik storitev zaupanja, pri čemer ponudnik storitev zaupanja Halcom CA preveri podatke poslovnega subjekta in imetnika v ustreznih registrih.

3.3.2 Preverjanje imetnikov za ponovno pridobitev potrdila po preklicu

Preverjanje imetnikov poteka skladno z določili iz razdelka 3.2.3.

3.4. Preverjanje istovetnosti ob zahtevi za preklic

(1) Zahtevek za preklic potrdila poslovni subjekt ali imetnik odda:

- osebno na prijavno službo, kjer pooblaščene osebe preverijo istovetnost prosilca,
- elektronsko, vendar mora biti zahtevek digitalno podpisan s kvalificiranim potrdilom, s tem pa izkazana tudi istovetnost prosilca,
- če imetnik potrdila prek telefona ali elektronske pošte 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 : razdelek 4.9.3.

4. UPRAVLJANJE S POTRDILI

4.1. Pridobitev potrdila

4.1.1 Kdo lahko pridobi potrdilo

(1) Bodoči imetniki potrdil so fizične osebe, pooblaščenci poslovnih subjektov ali poslovni subjekti za svoje naprave.

(2) Za pridobitev potrdila morajo biti izpolnjeni naslednji pogoji:

- izpolnjena in osebno oddana naročilnica ali pogodba v prijavni službi,

- identifikacijske obveznosti,
- finančne obveznosti.

(3) Bodočemu imetniku se potrdil ne izda, če je poslovni subjekt ali pooblaščenec uvrščen na seznam oseb, proti katerem so uveljavljeni omejevalni ukrepi (sankcije) Združenih narodov, Evropske unije, Republike Slovenije, Združenega kraljestva, Kanade, Avstralije ali Združenih držav Amerike.

4.1.2 Postopek bodočega imetnika za pridobitev potrdila in odgovornosti

(1) Kvalificirana potrdila za pooblaščence poslovnih subjektov:

1) Potrdilo se izda na osnovi pravilno izpolnjene in podpisane naročilnice s strani zakonitega zastopnika poslovnega subjekta in bodočega imetnika potrdila. 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 prijavnih službah Halcom CA in na spletni strani Halcom CA. Cenik storitev je javno objavljen na spletnih straneh Halcom CA.

2) S podpisom naročilnice zakoniti zastopnik tudi pooblašča pooblaščeno osebo poslovnega subjekta (imetnika digitalnega potrdila), da lahko v imenu in za račun poslovnega subjekta veljavno varno elektronsko podpiše zahtevo za podaljšanje obstoječega digitalnega potrdila ali izdajo novega z enakimi podatki v skladu s takrat veljavno politiko in cenikom ponudnika storitev zaupanja Halcom CA, vendar samo pod pogojem, da je varen elektronski podpis mogoče preveriti.

3) Zakoniti zastopnik poslovnega subjekta poda vlogo v pisni obliki.

4) Pred izdajo naročilnice Halcom CA poslovni subjekt in bodočega imetnika seznani s politiko in splošnimi pravili delovanja ponudnika storitev zaupanja Halcom CA.

5) Pred izdajo naročilnice Halcom CA bodočega imetnika seznani s CPS, politiko in delovanjem ponudnik storitev zaupanja Halcom CA.

(2) Kvalificirana potrdila za fizične osebe:

1) Potrdilo se izda na osnovi pravilno izpolnjenega in podpisanega zahtevka za izdajo potrdila s strani bodočega imetnika potrdila. Vlogo bodoči imetnik potrdila odda prijavni službi Halcom CA, ter poravna finančne obveznosti v zvezi z izdajo potrdila. Zahtevki za izdajo digitalnega potrdila so na voljo pri prijavnih službah Halcom CA in na spletni strani Halcom CA. Cenik storitev je javno objavljen na spletnih straneh Halcom CA.

2) Bodoči imetnik potrdila poda vlogo v pisni obliki.

3) Pred izdajo naročilnice Halcom CA bodočega imetnika seznani s CPS, politiko in obvestilom delovanjem ponudnika storitev zaupanja Halcom CA.

(3) Kvalificirana potrdila za elektronske žige:

1) Potrdilo se izda na osnovi pravilno izpolnjene in podpisane naročilnice izdajo potrdila (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 prijavnih službah Halcom CA in na spletni strani Halcom CA. Cenik storitev je javno objavljen na spletnih straneh Halcom CA.

2) S podpisom naročilnice zakoniti zastopnik dovoljuje elektronsko podaljšanje obstoječega digitalnega potrdila ali izdajo novega z enakimi podatki v skladu s takrat veljavno politiko in cenikom ponudnika storitev zaupanja Halcom CA, vendar samo pod pogojem, da je kvalificiran elektronski žig in s tem istovetnost naročnika (poslovnega subjekta) mogoče preveriti.

3) Zakoniti zastopnik poslovnega subjekta poda vlogo v pisni obliki.

4) Pred izdajo naročilnice Halcom CA bodočega imetnika seznani s CPS, politiko in delovanjem ponudnika storitev zaupanja Halcom CA.

(4) Kvalificirana potrdila za avtentikacijo spletišč:

1) Potrdilo se izda na osnovi pravilno izpolnjene in podpisane naročilnice izdajo potrdila za avtentikacijo spletišč (v nadaljevanju naročilnice) s strani imetnika spletišča (fizična oseba ali zakoniti zastopnik poslovnega subjekta). Vlogo imetnik spletišča odda prijavni službi Halcom CA, ter poravna finančne obveznosti v zvezi z izdajo potrdila. Naročilnice za izdajo digitalnega potrdila so na voljo pri prijavnih službah Halcom CA in na spletni strani Halcom CA. Cenik storitev je javno objavljen na spletnih straneh Halcom CA.

2) Imetnik spletišča poda vlogo v pisni obliki.

3) Pred izdajo naročilnice Halcom CA bodočega imetnika seznani s CPS, politiko in delovanjem ponudnika storitev zaupanja Halcom CA.

(5) Kvalificirana potrdila za časovno žigosanje:

1) Potrdila za časovno žigosanje so namenjena le ponudnikom storitev zaupanja.

2) Ponudnik storitev zaupanja Halcom CA ni dolžan pogodbeno sodelovati z drugimi ponudniki storitev zaupanja tudi, če ima drugi ponudnik storitev zaupanja status kvalificiranega ponudnika storitev.

3) Ponudnik storitev zaupanja Halcom CA zagotavlja, da bo potrdilo izdal izključno po podpisu pisne pogodbe z drugim ponudnikom storitev zaupanja, ki pa mora izpolnjevati raven varnostnih zahtev, ki je primerljiva ali višja, kot jo predpiše ponudnik storitev zaupanja Halcom CA.

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

5) Pred izdajo naročilnice Halcom CA bodočega imetnika seznani s CPS, politiko in delovanjem ponudnika storitev zaupanja Halcom CA.

(6) 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) Pooblaščena oseba prijavne službe preveri istovetnost zakonitega zastopnika in/ali imetnika z veljavnim osebnim dokumentom s sliko ob obisku prijavne službe ali preko kurirske službe ob vročitvi potrdila.

(2) Prijavna služba ponudnika storitev zaupanja Halcom CA lahko posreduje podatke tudi iz svojih podatkovnih zbirk, pridobljenih po postopku, ki ga prijavna služba uporablja za druge namene in skladno z veljavnimi predpisi zagotavlja enakovredno raven zanesljivosti.

(3) Pooblaščene osebe so dolžne preveriti istovetnost poslovnega subjekta in/ali bodočega imetnika oz. vse tiste podatke, ki so navedeni v zahtevku in so dostopni v uradnih evidencah oz. drugih uradnih veljavnih dokumentih.

(4) Prijavne službe preverijo izpolnjene vloge in sprejemajo originalno dokumentacijo ter jo na varen način posredujejo na Halcom CA.

4.2.2 Odobritev/zavrnitev zahtevka

(1) Pooblaščene osebe ponudnik 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 oz. bodoči imetnik 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 odobrene naročilnice ali pogodbe in poravnanih finančnih obveznosti v zvezi z izdajo potrdila izda potrdilo najkasneje v petih delovnih (5) dneh od prejetega plačila.

4.3. Izdaja potrdila

4.3.1 Postopek ponudnika storitev zaupanja Halcom CA

(1) Proizvodnji postopek izdaje potrdila je odvisen od vrste potrdila:

- Napredna kvalificirana potrdila

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

  1. predpoosebljanje varnega nosilca (generiranje ključev na kartici, izbira gesla za zaščito potrdila),

  2. pridobitev elektronske vloge za izdajo potrdila,

3. obravnava vloge za izdajo potrdila,
4. priprava potrdila,
5. pooseblјanje varnega nosilca (izdaja in zapis potrdila, tiskanje imetnikovih podatkov),
6. tiskanje osebnega gesla (kode PIN - le v primeru pošiljanja s priporočeno pošto),
7. posredovanje potrdila in osebnega gesla (kode PIN) ter obvestila imetniku.

Potrdilo na varnem nosilcu in pripadajoče osebno geslo (kodo PIN) se imetniku posreduje s priporočeno pošto, v dveh ločenih pošiljkah, v razmaku enega delovnega dne. Osebno geslo (koda PIN) se imetniku lahko posreduje tudi po drugem varnem kanalu (preko posebnega spletišča, kjer se imetnik identificira preko posebne povezave, prejete preko elektronske pošte, in še enim podatkom, ki je znan imetniku (npr. številka osebnega dokumenta, davčna številka imetnika, zadnje štiri številke ali CVV koda plačilne ali kreditne kartice ali podobno)). Izjemoma lahko pošiljki pooblaščene osebe prijavne službe imetniku predajo tudi osebno.

- Kvalificirana potrdila v oblaku

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

1. obravnava vloge za izdajo potrdila,
2. priprava potrdila in registracijske ter aktivacijske kode,
3. posredovanje registracijske in aktivacijske kode ter obvestila imetniku,
4. generiranje ključev na varnem nosilcu v oblaku in izdaja potrdila.

Registracijska in aktivacijska koda se imetniku posredujeta po dveh ločenih kanalih, ena po elektronski pošti, druga pa po drugem varnem kanalu (varen spletni portal dostopen s kvalificiranim potrdilom, osebna vročitev po klasični pošti ali preko posebnega spletišča, kjer se imetnik identificira preko posebne povezave, prejete preko elektronskega sporočila, in še enim podatkom, ki je znan imetniku (npr. številka osebnega dokumenta, davčna številka imetnika, zadnje štiri številke ali CVV koda plačilne ali kreditne kartice ali podobno)). Izjemoma lahko eno od navedenih kod pooblaščena oseba prijavne službe Halcom CA imetniku preda tudi osebno.

- Standardno kvalificirano digitalno potrdilo:

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

1. obravnava vloge za izdajo potrdila,
2. priprava potrdila in referenčne ter avtorizacijske kode,
3. posredovanje referenčne in avtorizacijske kode ter obvestila imetniku,

4. prevzem potrdila.

Referenčna koda se imetniku posreduje z elektronsko pošto, avtorizacijska koda pa priporočeno po pošti. Izjemoma lahko avtorizacijsko kodo pooblaščena oseba prijavne službe Halcom CA imetniku preda tudi osebno.

- Kvalificirana potrdila za avtentikacijo spletišč in informacijske sisteme

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

  1. obravnava vloge za izdajo potrdila,
  2. pridobitev elektronskega zahtevka (ang. »certificate request«),
  3. poosebljanje in izdaja potrdila,
  4. posredovanje potrdila imetniku.

- Kvalificirana potrdila za časovne žige

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

  1. pregled varnostnih zahtev in notranjih pravil drugega ponudnika storitev zaupanja,
  2. obravnava in podpis pogodbe za izdajo potrdila,
  3. pridobitev elektronskega zahtevka (ang. »certificate request«),
  4. priprava potrdila,
  5. poosebljanje potrdila,
  6. posredovanje potrdila ponudnika storitev zaupanja.

(2) Naročnik in imetnik praviloma nista ista oseba kot Halcom CA ali prijavna služba Halcom CA. Če prijavna služba Halcom CA naroča potrdilo zase ali za svoje pooblaščene zaposlene, takšno naročilo dodatno, skrbno preveri osebje Halcom CA.

(3) Če Halcom CA naroči potrdilo zase ali za svoje pooblaščene osebe izdajo vseh takih potrdil dodatno skrbno preverita pooblaščenec za notranji nadzor in pooblaščenec za regulatorno skladnost.

(4) Postopki so zasnovani tako, da jih ne more opraviti posamezna oseba sama.

(5) Ponudnik storitev zaupanja Halcom CA lahko za določene naloge (npr. tiskanje imetnikovih podatkov, izpis kod PIN, dostava in podobno) na podlagi pisne pogodbe pooblasti preverjene zunanje izvajalce, ki jih redno nadzoruje in za katere odgovarja, kot bi naloge opravljal sam.

4.3.2 Obvestilo imetnika o izdaji

Glej prejšnji razdelek.

4.4. Prevzem potrdila

4.4.1 Postopek prevzema potrdila

(1) Postopek prevzema potrdila je odvisen od vrste potrdila:

- Napredna potrdila

  Pri naprednih potrdilih prevzem potrdila ni potreben, saj bodoči imetnik potrdilo na varnem nosilcu in pripadajočo osebno geslo (kodo PIN) prejme priporočeno po pošti, po drugem varnem kanalu oz. mu ga izjemoma lahko vroči pooblaščena oseba Halcom CA, glej razdelek 4.3.1.

- Potrdila v oblaku

  Pri potrdilih v oblaku prevzem potrdila ni potreben, saj le-tega po pooblastilu imetnika varno hrani ponudnik storitev zaupanja Halcom CA. Uporabniku se posreduje le kode za dostop do varnega oblaka, glej razd. 4.3.1.

- Standardna potrdila

  Pri standardnih potrdilih bodoči imetnik skladno z navodili potrdilo prevzame s pomočjo Halcom CA programske opreme za prevzem digitalnega potrdila. Uporabniku se posreduje le kode za prevzem standardnega potrdil, glej razd. 4.3.1.

- Potrdila za avtentikacijo spletišč, informacijske sisteme in časovni žig

  Pri potrdilih za avtentikacijo spletišč, informacijske sisteme in časovni žig poslovni subjekt lokalno sproži generacijo ključev in določi geslo za zaščito le-teh. Ponudnik storitev zaupanja Halcom CA na podlagi prejetega elektronskega zahtevka (»certificate request«) izdela potrdilo in ga posreduje poslovnemu subjektu, ki s pomočjo prej omenjenega gesla kreira potrdilo s pripadajočim parom ključev.

(2) Imetnik potrdila oz. poslovni subjekt mora ob prevzemu potrdila nemudoma preveriti podatke v potrdilu in ob morebitnih napakah ali problemih takoj obvestiti ponudnika storitev zaupanja Halcom CA.

4.4.2 Objava potrdila

Postopek je opisan v 2. razdelku.

4.4.3 Obvestilo CA o izdaji potrdila tretjim osebam

Ponudnik storitev zaupanja Halcom CA o izdaji posameznega potrdila imetnikom potrdila ne obvešča tretjih oseb. Prijavna služba lahko pridobi podatek o izdaji potrdil, za katere je sprejela vloge za izdajo.

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 oziroma aktivaciji 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,
- zahtevati preklic potrdila v oblaku ob izgubi ali kraji mobilnega telefona, ali če obstaja nevarnost zlorabe le-tega,
- 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 oziroma aktivacijo 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 oziroma dostop do 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 bil digitalni podpis/žig kreiran v času veljavnosti in 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/žiga 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

(1) Podaljševanje veljavnosti potrdila je mogoče samo na prošnjo imetnika potrdila.

(2) Po preteku veljavnosti naprednega potrdila mora imetnik po enkratnem (1x) podaljšanju ponovno zaprositi za izdajo potrdila.

(3) Imetnik potrdila lahko pred iztekom veljavnosti potrdila po elektronski poti zaprosi za izdajo novega digitalnega potrdila, ki ga podpiše s še veljavnim potrdilom.

(4) Ponovna izdaja potrdila za časovno žigosanje in avtentikacijo spletišč 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 elektronskim 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 podaljšanje izdajo potrdila

Podaljševanje veljavnosti potrdila je mogoče samo na prošnjo imetnika potrdila.

4.6.3 Postopek obravnave prošenj za ponovno izdajo potrdila

Postopek zagotavlja, da je poslovni subjekt in/ali fizična oseba, ki zaprosi za ponovno izdajo potrdila brez spremembe javnega ključa dejansko imetnik potrdila.

4.6.4 Obvestilo imetniku o novo izdanem potrdilu

Glej razdelek 4.3.2.

4.6.5 Postopek prevzema novo izdanega potrdila

Glej razdelek 4.4.1.

4.6.6 Objava novo izdanega potrdila

Postopek je opisan v 2. razdelku.

4.6.7 Obvestilo CA o izdaji potrdila drugim subjektom

Halcom CA o izdaji posameznega potrdila imetnikom potrdila ne obvešča podjetij in drugih organizacij.

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 ponudnik storitev zaupanja z novima paroma 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 ali imetnik potrdila zahteva kadarkoli, mora pa ga zahtevati v primeru:

1) Spremembe razločevalnega imena (DN),
2) ko poslovni subjekt ali imetnik potrdila zamenja ključne podatke, povezane s potrdilom (ime ali priimek, naziv poslovnega subjekta, elektronski naslov, zaposlitev in podobno),
3) ko se ugotovi ali sumi, da je prišlo bodisi do razkritja ključa za podpisovanje bodisi do zlorabe potrdila,
4) nadomestitvi potrdila z drugim potrdilom (npr. ob izgubi potrdila ali varnega nosilca, izgubi gesel za dostop do podatkov na kartici in podobno).

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

(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 osmih (8) 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 ali imetnik 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 ponudnik 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.

(3) Imetnik digitalnega potrdila lahko zahteva v roku trideset (30) dni od izdaje ponovno generiranje osebnega gesla (kode PIN) za napredna potrdila oziroma referenčne ter avtorizacijske kode za standardna potrdila ali registracijske ter aktivacijske kode za potrdila v oblaku v primeru, če je e-dostopne podatke zgolj pozabil ter pod civilno in kazensko odgovornostjo jamči, da ne obstaja možnost, da je/bi bil zasebni ključ ogrožen na način, ki vpliva na zanesljivost uporabe in da ne obstaja nevarnost zlorabe zasebnega ključa ali potrdila imetnika.

4.9.2 Kdo zahteva preklic

Preklic potrdila lahko zahteva:

- pooblaščena oseba ponudnik storitev zaupanja Halcom CA,
- zakoniti zastopnik poslovnega subjekta,
- imetnik,
- 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.

(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/žigosan z zaupanja vrednim potrdilom za njegovo preverjanje.
- če imetnik potrdila prek telefona ali elektronske pošte 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.

(3) O datumu ter času preklica mora biti vedno obveščen poslovni subjekt ali imetnik. Ponudnik storitev zaupanja, na podlagi pisne zahteve poslovnega subjekta ali imetnika, posreduje tudi dodatne informacije o preklicu (podatke o vložniku zahtevka za preklic, vzroku za preklic ipd.).

(4) 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).

(5) Določbe v zvezi s preklicem se smiselno uporabljajo tudi za postopke v zvezi z ponovnim generiranjem kode PIN za napredna potrdila oziroma referenčne ter avtorizacijske kode za standardna potrdila in registracijske ter aktivacijske kode za potrdila v oblaku.

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 (največ 5 sekund) dodano v register preklicanih potrdil.

4.9.6 Zahteve po preverjanju registra preklicanih potrdil za tretje osebe

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.

4.9.7 Pogostnost objave registra preklicanih potrdil

Register preklicanih potrdil se osvežuje (za dostop do registra glej razdelek 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

(1) 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.

(2) Ponudnik storitev zaupanja Halcom CA zagotavlja čim večjo dostopnost svojih storitev, in sicer vse dni v letu, pri čemer pa se ne upošteva nepredvidenih okoliščin. Halcom CA bo v primeru nepredvidenih okvar in nenačrtovanih tehničnih ali servisnih posegov na infrastrukturi objavil register preklicanih potrdil najkasneje v 8 (osmih) urah. V primeru nastanka nepredvidljivih okoliščin kot posledica višje sile ali izrednih dogodkov bo Halcom CA izjemoma objavil register preklicanih potrdil najkasneje v 24 urah, vendar še pred potekom zadnjega veljavnega registra preklicanih potrdil.

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). Sprotno preverjanje statusa potrdil (OCSP) lahko deluje z zakasnitvijo največ ene (1) minute od objave novega registra.

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 ali elektronsko zahteva preklic potrdila, se do prejema originala pisne zahteve potrdilo začasno suspendira.

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

4.9.14 Kdo zahteva suspenz

Glej razdelek 4.9.13.

4.9.15 Postopek za suspenz

Glej razdelek 4.9.13.

4.9.16 Čas suspenza

Glej razdelek 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

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

(2) Ponudnik storitev zaupanja Halcom CA zagotavlja čim večjo dostopnost svojih storitev, in sicer vse dni v letu, pri čemer pa se ne upošteva nepredvidenih okoliščin. Halcom CA bo v primeru nepredvidenih okvar in nenačrtovanih tehničnih ali servisnih posegov na infrastrukturi ponovno omogočil preverjanje statusa potrdil najkasneje v 8 (osmih) urah. V primeru nastanka nepredvidljivih okoliščin kot posledica višje sile ali izrednih dogodkov bo Halcom CA izjemoma omogočil preverjanje statusa potrdil najkasneje v 24 urah, vendar še pred potekom zadnjega veljavnega registra preklicanih potrdil.

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 se prekine, če:

- imetnikovo potrdilo preteče in ga le-ta ne podaljša,
- je potrdilo preklicano, imetnik pa ne zaprosi za novega.

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 več nivojskim 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 več nivojskim 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 razdelek 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 notranjih pravilih ponudnika storitev zaupanja Halcom CA.

5.1.8 Hramba na oddaljeni lokaciji

Glej razdelek 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 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, • pomoč podrejenim ponudnikom storitev zaupanja, • pooblaščanje podrejenih ponudnikov storitev zaupanja, • dostop do protokola	2

		podpisovanja potrdil, • varno shranjevanje in distribucija kopij in nadgradenj na ločeno lokacijo.	
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 nosilcev, • 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	2

		dnevnikov za nadzor dela, • osebno sodelovanje in pomoč pri letni inventuri dokumentacije podrejenih ponudnikov storitev zaupanja.	
	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.

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 v skladu z Uredbo 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 v skladu z Uredbo določene v notranjih pravilih ponudnika storitev zaupanja.

5.4.5 Varnostne kopije dnevnikov

(1) Varnostne kopije dnevnikov se izvajajo dnevno.

(2) Podrobnosti so v skladu z Uredbo 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 v skladu z Uredbo 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 v skladu z Uredbo 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 imetnikov oz. poslovnih subjektov,
- vse zahtevke,
- 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

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. 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 podpisov je bil ustvarjen po najvišjih varnostnih standardih, v varnem okolju ponudnika storitev zaupanja Halcom CA.

(2) Ključi imetnikov se generirajo odvisno od vrste potrdila v skladu s spodnjo tabelo.

Tip potrdila	Ključ	Ključ se generira
Korensko in vmesna potrdila Halcom CA	Par ključev	v strojnem varnostnem modulu ponudnika storitev zaupanja
Napredno potrdilo	Dva para ključev	na varnem nosilcu, pri ponudniku storitev zaupanja Halcom CA
Standardno potrdilo	Par ključev	pri imetniku potrdila
Potrdilo v oblaku	Par ključev	v strojnem varnostnem modulu ponudnika storitev zaupanja
Potrdilo za informacijske sisteme	Par ključev	v varnem okolju imetnika potrdila
Potrdilo za avtentikacijo spletišč	Par ključev	v varnem okolju imetnika potrdila

Potrdilo za časovni žig	Par ključev	v strojnem varnostnem modulu ponudnika storitev zaupanja

6.1.2 Dostava zasebnega ključa imetnikom

Način varnega prenosa zasebnega ključa je podan v spodnji tabeli.

Tip potrdila	Ključ	Dostava
Korensko in vmesna potrdila Halcom CA	Zasebni ključ	ni prenosa
Napredno potrdilo	Zasebna ključa	prenos varnega nosilca poteka priporočeno po pošti
Standardno potrdilo	Zasebni ključ	ni prenosa
Potrdilo v oblaku	Zasebni ključ	ni prenosa
Potrdilo za informacijske sisteme	Zasebni ključ	ni prenosa
Potrdilo za avtentikacijo spletišč	Zasebni ključ	ni prenosa
Potrdilo za časovni žig	Zasebni ključ	ni prenosa

6.1.3 Dostava javnega ključa ponudnik storitev zaupanja potrdil

(1) Pri naprednih potrdilih se ključi generirajo na varnem nosilcu, v varnem okolju ponudnika storitev zaupanja Halcom CA.

(2) Pri potrdilih v oblaku se ključi generirajo v strojnem varnostnem modulu, v varnem okolju ponudnika storitev zaupanja Halcom CA.

(3) Pri potrdilih za informacijske sisteme in avtentikacijo spletišč se ključi generirajo pri imetniku. PKCS#10 zahtevek za izdajo potrdila (angl. »certificate request«) pa se prenese iz uporabnikovega računalnika do ponudnika storitev zaupanja preko zaščitene omrežne povezave.

(4) Pri standardnih potrdilih se ključi generirajo pri imetniku. PKCS#10 zahtevek za izdajo potrdila (angl. »certificate request«) in izdaja potrdila pa poteka preko Halcom CA programske opreme za prevzem digitalnega potrdila.

(5) Pri potrdilih za časovne žige se ključi generirajo v strojnem varnostnem modulu pri ponudniku storitev zaupanja. PKCS#10 zahtevek za izdajo potrdila (angl. »certificate request«) pa se prenese 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://domina.halcom.si/crls, 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
Vmesna (Intermediate) potrdila ponudnika storitev zaupanja Halcom CA	Najmanj 2048
Uporabniška potrdila	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. *keyUsage)* in *razširjena uporaba ključa* (angl. *extended keyUsage).*

(2) Za podpis potrdil in registra preklicanih potrdil je namenjen zasebni ključ ponudnika storitev zaupanja Halcom CA, za preverjanje veljavnosti podpisa pa 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

(1) Zasebni ključi pri naprednih potrdilih se ustvarijo v varnem nosilcu s katerim se naknadno prenesejo imetniku potrdila.

(2) Zasebni ključi pri potrdilih v oblaku se ustvarijo in hranijo v kriptografskem modulu, ki je certificiran v skladu s FIPS 140-2 nivo 3 in/ali Common Criteria EAL4+.

(3) Zasebni ključi ostalih potrdil se ustvarijo in hranijo pri imetniku.

6.2.7 Hramba zasebnega ključa v kriptografskem modulu

(1) Zasebni ključ ponudnika 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:

- naprednih potrdil se ustvarijo in hranijo na varnem nosilcu,
- potrdil v oblaku se ustvarijo in hranijo v kriptografskem modulu,
- standardnih potrdilih se ustvarijo in hranijo pri imetniku,
- potrdil za informacijske sisteme se ustvarijo in hranijo pri imetniku,
- potrdil za avtentikacijo spletišč sisteme se ustvarijo in hranijo pri imetniku,
- potrdil za časovni žig se ustvarijo in hranijo v kriptografskem modulu.

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) Halcom CA imetnikom priporoča uporabo programskega okolja, ki ob odjavi ali po določenem pretečenem času onemogoči dostop do njihovega zasebnega ključa brez vnosa ustreznega gesla.

(3) Imetnik potrdila za podpisovanje v oblaku lahko uporabi storitev kvalificiranega elektronskega podpisa v oblaku. V takem primeru imetnik ali v njegovem imenu drug pošiljatelj posreduje na varen način ponudniku storitev zaupanja Halcom CA elektronski dokument, ki naj se kvalificirano elektronsko podpiše. Imetnik zatem na varen način preko mobilne naprave in z uporabo s strani ponudnika storitev zaupanja Halcom CA predpisanega varnega postopka (uporaba PIN in mobilnih varnostnih postopkov) odobri kvalificiran elektronski podpis v oblaku. Na podlagi odobritve imetnika ponudnik storitev zaupanja Halcom CA uporabi zasebni ključ imetnika v oblaku in kvalificirano elektronsko podpiše dokument ter podpisan dokument dostavi imetniku ali drugemu pošiljatelju dokumenta.

(4) Zaradi varstva zaupnosti elektronskih dokumentov imetnika, lahko imetnik ob naročilu potrdila izrecno pisno zahteva, da ponudnik storitev zaupanja Halcom CA pri podpisovanju v oblaku, kot je opisano v prejšnjem odstavku, ne zahteva prejema celotnega dokumenta za kvalificiran elektronski podpis v oblaku, temveč zgolj zgoščene vrednosti (angl. hash value) takšnega dokumenta in imetniku ali drugemu pošiljatelju posreduje zgolj kvalificiran elektronski podpis. Halcom CA v takšnem primeru ne zagotavlja preverjanja izračuna zgoščene vrednosti ali drugih varnostnih mehanizmov glede elektronskega dokumenta ter je odgovornost v celoti na strani imetnika.

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 pravili 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 pravili 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.

(3) Zasebni ključ potrdila v oblaku se po poteku veljavnosti potrdila samodejno uniči. Zasebni ključ potrdila v oblaku lahko na zahtevo imetnika potrdila Halcom CA uniči tudi pred iztekom veljavnosti. Zasebni ključ se uniči tako, da ga ni mogoče restavrirati.

6.2.11 Lastnosti kriptografskega modula

Strojni varnostni modulu 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 je odvisna od vrste potrdila.

Tip potrdila	Ključ	Veljavnost
Korensko potrdilo	Zasebni ključ	20 let
	Javni ključ	20 let
Vmesno (podrejeno) potrdilo	Zasebni ključ	10 let
	Javni ključ	10 let
Napredno potrdilo	Zasebni ključ	3 leta
	Javni ključ	3 leta
Standardno potrdilo	Zasebni ključ	3 leta
	Javni ključ	3 leta
Potrdilo v oblaku	Zasebni ključ	1 - 3 leta
	Javni ključ	1 - 3 leta
Potrdilo za informacijske sisteme	Zasebni ključ	3 leta
	Javni ključ	3 leta
Potrdilo za avtentikacijo spletišč	Zasebni ključ	1-3 leta
	Javni ključ	1-3 leta
Potrdilo za časovni žig	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

(1) Napredno potrdilo

Številka (koda PIN) za uporabo naprednega potrdila in številka za odklepanje varnega nosilca (koda PUK) se ustvarita na strani Halcom CA. Osebno številko mora imetnik pred prvo uporabo potrdila spremeniti.

(2) Potrdilo v oblaku

Registracijska in aktivacijska koda za potrdila v oblaku se ustvarita na strani Halcom CA. V procesu aktivacije si uporabnik nastavi svojo osebno številko (kodo PIN) za dostop do potrdila v oblaku.

(3) Standardno potrdilo, potrdilo za informacijske sisteme in avtentikacijo spletišč

Imetniki standardnih potrdil, potrdil za informacijske sisteme in avtentikacijo spletišč sami določijo geslo, s katerim zaščitijo dostop do svojih zasebnih ključev. Halcom CA priporoča uporabo varnih gesel:

- mešano uporaba velikih in malih črk, števil in posebnih znakov,
- dolžine vsaj 8 znakov,
- odsvetuje se uporabo besed, ki so zapisane v slovarjih.

6.4.2 Zaščita gesel

(1) Napredno potrdilo

Osebno geslo za uporabo naprednega potrdila (koda PIN) in geslo za odklepanje varnega nosilca (koda PUK) se kreirata varno pri ponudniku storitev zaupanja Halcom CA. Halcom CA posreduje oba gesla imetniku potrdila priporočeno po pošti ali preko drugega varnega kanala oz. ju izjemoma preda tudi osebno. Halcom CA priporoča, da se obe gesli hrani na varnem mestu do katerega ima dostop le imetnik.

(2) Potrdilo v oblaku

Registracijska in aktivacijska koda za potrdila v oblaku se ustvarita varno pri ponudniku storitev zaupanja Halcom CA. Kodi se imetniku posredujeta po dveh ločenih kanalih, ena po elektronski pošti, druga pa po drugem varnem kanalu (varen spletni portal dostopen s kvalificiranim potrdilom, osebna vročitev po klasični pošti ali drug soroden varen način). Izjemoma lahko eno od navedenih kod pooblaščena oseba prijavne službe Halcom CA imetniku preda tudi osebno. Kodi sta namenjeni le aktivaciji dostopa do potrdila v oblaku, med katero si uporabnik sam nastavi svojo osebno številko (kodo PIN).

(3) Standardno potrdilo

Referenčna in avtorizacijska koda za prevzem standardnega potrdila se ustvarita varno pri ponudniku storitev zaupanja Halcom CA. V procesu prevzema potrdila si uporabnik sam določi geslo, s katerim zaščiti 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.

(4) Potrdilo za informacijske sisteme in avtentikacijo spletišč

Imetniki potrdil za informacijske sisteme 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 računalniško 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 notranjih pravilih ponudnika storitev zaupanja Halcom CA.

6.6.3 Nadzor življenjskega cikla

Podrobne tehnične zahteve so določene v 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 CPS in politik Halcom CA izdaja potrdila:

- napredna potrdila,
- potrdila v oblaku,
- standardna potrdila,

- potrdila za informacijske sisteme,
- potrdila za avtentikacijo spletišč in
- potrdila za časovni žig.

(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

Podatki v potrdilih so navedeni spodaj.

(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 vmesnih/podrejenih (intermediate) potrdil:

- Halcom CA PO e-signature 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: <15.6.2016 10:34:13 GMT > Valid to: <15.6.2026 10:34:13 GMT >
Imetnik, angl. Subject	CN = Halcom CA PO e-signature 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	40 f6 95 20 9b 79 c2 09
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

- Halcom CA PO e-signature 2

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: <03.04.2023 07:00:00 GMT > Valid to: <03.04.2033 07:00:00 GMT >
Imetnik, angl. Subject	CN = Halcom CA PO e-signature 2 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 3072 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 4d 32 75 16 03 c9 75
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

- Halcom CA FO e-signature 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: <15.6.2016 10:34:15 GMT > Valid to: <15.6.2026 10:34:15 GMT >

Imetnik, angl. Subject	CN = Halcom CA FO e-signature 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 2048 bitov
Razširitve X.509v3	
Objava registra preklicanih potrdil, OID 2.5.29.31, angl. CRL Distribution Points	URI: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	48 fb 3b 13 99 c3 4e ce
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

- Halcom CA FO e-signature 2

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: <03.04.2023 07:00:00 GMT > Valid to: <03.04.2033 07:00:00 GMT >
Imetnik, angl. Subject	CN = Halcom CA FO e-signature 2 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 3072 bitov
Razširitve X.509v3	
Objava registra preklicanih potrdil, OID 2.5.29.31, angl. CRL Distribution Points	URI: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	48 c4 27 a6 6f 6e f0 2e
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

- Halcom CA PO e-seal 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: <22.4.2017 08:00:00 GMT > Valid to: <22.4.2027 08:00:00 GMT >
Imetnik, angl. Subject	CN = Halcom CA PO e-seal 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	49 48 76 50 77 0a b1 0c
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

- Halcom CA PO e-seal 2

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: <03.04.2023 07:00:00 GMT > Valid to: <03.04.2033 07:00:00 GMT >
Imetnik, angl. Subject	CN = Halcom CA PO e-seal 2 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 3072 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	47 35 c8 bc 61 e2 5d 9e

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

- Halcom CA web 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: <22.4.2017 08:00:00 GMT > Valid to: <22.4.2027 08:00:00 GMT >
Imetnik, angl. Subject	CN = Halcom CA web 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	48 42 0b 17 ed ae 9e 70
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

- 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: <22.4.2017 08:00:00 GMT > Valid to: <22.4.2027 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

- Halcom CA PO e-signature 1 in Halcom CA PO e-signature 2

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 PO e-signature 1 ali CN = Halcom CA PO e-signature 2 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%20PO%20e-signature%201,o=Halcom,c=SI?certificaterevocationlist;binary URL=http://domina.halcom.si/crls/halcom_ca_po_ e-signature_1.crl ali URI:ldap://ldap.halcom.si/cn=Halcom%20CA%20PO%20e-signature%202,o=Halcom,c=SI?certificaterevocationlist;binary URL=http://domina.halcom.si/crls/halcom_ca_po_ e-signature_2.crl
Uporaba ključa, OID 2.5.29.15, angl. Key Usage	Napredna potrdila: Digital Signature, Non Repudiation, Key Encipherment Potrdila v oblaku: Digital Signature, Non Repudiation
Identifikator ključa ponudnika storitev zaupanja, OID 2.5.29.35, angl. Authority Key Identifier	KeyID=40 f6 95 20 9b 79 c2 09 ali KeyID=43 4d 32 75 16 03 c9 75
EŠEI	enotna številka elektronske identifikacije (glej razdelek 7.1.2.1)

- Halcom CA FO e-signature 1 in Halcom CA FO e-signature 2

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 FO e-signature 1 ali CN = Halcom CA FO e-signature 2 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%20FO%20e-signature%201,o=Halcom,c=SI?certificaterevocationlist;binary URL=http://domina.halcom.si/crls/halcom_ca_fo_e-signature_1.crl ali URI:ldap://ldap.halcom.si/cn=Halcom%20CA%20FO%20e-signature%202,o=Halcom,c=SI?certificaterevocationlist;binary URL=http://domina.halcom.si/crls/halcom_ca_fo_e-signature_2.crl
Uporaba ključa, OID 2.5.29.15, angl. Key Usage	Napredna potrdila: Digital Signature, Non Repudiation, Key Encipherment Standardna potrdila: Digital Signature, Non Repudiation, Key Encipherment Potrdila v oblaku: Digital Signature, Non Repudiation

Identifikator ključa ponudnika storitev zaupanja, OID 2.5.29.35, angl. Authority Key Identifier	KeyID=48 fb 3b 13 99 c3 4e ce ali KeyID= 48 c4 27 a6 6f 6e f0 2e
EŠEI	enotna številka elektronske identifikacije (glej razdelek 7.1.2.1)

- Halcom CA PO e-seal 1 in Halcom CA PO e-seal 2

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 PO e-seal 1 ali CN = Halcom CA PO e-seal 2 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%20PO%20e-seal%201,o=Halcom,c=SI?certificaterevocationlist;binary URL=http://domina.halcom.si/crls/halcom_ca_po_ e-seal_1.crl ali URI:ldap://ldap.halcom.si/cn=Halcom%20CA%20PO%20e-seal%202,o=Halcom,c=SI?certificaterevocationlist;binary URL=http://domina.halcom.si/crls/halcom_ca_po_ e-seal_2.crl
Uporaba ključa, OID 2.5.29.15, angl. Key Usage	Digital Signature, Non Repudiation, Key Encipherment
Identifikator ključa ponudnika storitev zaupanja, OID 2.5.29.35, angl. Authority Key Identifier	KeyID= 49 48 76 50 77 0a b1 0c Ali KeyID= 47 35 c8 bc 61 e2 5d 9e
EŠEI	enotna številka elektronske identifikacije (glej razdelek 7.1.2.1)

- Halcom CA web 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 (OID 1.2.840.113549.1.1.11)

Izdajatelj, angl. Issuer	CN = Halcom CA web 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%20web%201,o=Halcom,c=SI?certificaterevocationlist;binary URL=http://domina.halcom.si/crls/halcom_ca_web_1.crl
Uporaba ključa, OID 2.5.29.15, angl. Key Usage	Digital Signature, Key Encipherment
Identifikator ključa ponudnika storitev zaupanja, OID 2.5.29.35, angl. Authority Key Identifier	KeyID= 48 42 0b 17 ed ae 9e 70
EŠEI	enotna številka elektronske identifikacije (glej razdelek 7.1.2.1)

- 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 (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, Key Encipherment
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 *namen uporabe* (angl. *Key Usage*) je označeno kot kritično (angl. *critical*).

(5) Imetnik potrdila za elektronsko podpisovanje ima lahko eno samo veljavno istovrstno potrdilo, razen v času šestdeset (60) dni pred potekom veljavnosti tega potrdila, ko lahko imetnik pridobi novo potrdilo.

(6) Imetnik potrdila za elektronsko žigosanje, informacijske sisteme, avtentikacijo spletišč in časovni žig, ima lahko več veljavnih potrdil.

7.1.2.1 Enotna številka elektronske identifikacije

V skladu s 24. členom Zakona o elektronski identifikaciji in storitvah zaupanja (Uradni list RS, št. 121/21 in 189/21 – ZDU-1M), 52. členom Uredbe o določitvi sredstev elektronske identifikacije in uporabi centralne storitve za spletno prijavo in elektronski podpis (Uradni list RS, št. 29/22) se Enotna številka elektronske identifikacije (EŠEI) imetnika v kvalificirano potrdilo za elektronski podpis, elektronski žig ali avtentikacijo spletišč zapiše kot zasebna razširitev kvalificiranega potrdila. Slednje se zapiše kot samostojno razširitveno polje, zapisano v ASN.1 notaciji:

SEQUENCE :
OBJECT_IDENTIFIER : '1.3.6.1.4.1.58536.1.1.1.1.1' <OID razširitve za vrednost EŠEI fizične osebe>
OCTET_STRING :
IA5String : 'xxxxxxxxxxxx' <vrednost>

SEQUENCE :
OBJECT_IDENTIFIER : '1.3.6.1.4.1.58536.1.1.1.1.2' <OID razširitve za vrednost EŠEI poslovnega subjekta>
OCTET_STRING :
IA5String : 'xxxxxxxxxxxx' <vrednost>

7.1.2.2 Zahteve za elektronski naslov

(1) Halcom CA si pridržuje pravico za zavrnitev zahtevka za pridobitev potrdila, če ugotovi, da je elektronski naslov:

- neprimeren oz. žaljiv,
- da je zavajajoč za tretje stranke,
- je v nasprotju z veljavnimi predpisi in standardi.

(2) Druge omejitve glede elektronskih 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 razdelek 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 razdelek 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) Registri preklicanih potrdil Halcom CA je seznami preklicanih potrdil (CRL) in se nahajajo v vejah:

- Register preklicanih vmesnih/podrejenih potrdil:

  CN= Halcom Root Certificate Authority

  O = Halcom

  C = SI
- Register preklicanih potrdil za e-podpis poslovnih subjektov:

  CN= Halcom CA PO e-signature 1 ali CN= Halcom CA PO e-signature 2

  O = Halcom

  C = SI
- Register preklicanih potrdil za e-podpis fizičnih oseb:

  CN= Halcom CA FO e-signature 1 ali CN= Halcom CA FO e-signature 2

  O = Halcom

  C = SI
- Register preklicanih potrdil za e-žig poslovnih subjektov:

  CN= Halcom CA PO e-seal 1 ali CN= Halcom CA PO e-seal 2

  O = Halcom

  C = SI
- Register preklicanih potrdil za avtentikacijo spletišč:

  CN= Halcom CA web 1

  O = Halcom

  C = SI

- Register preklicanih potrdil za časovno žigosanje:

  CN= Halcom CA TSA 1

  O = Halcom

  C = SI

(2) Register preklicanih vmesnih/podrejenih potrdil se osvežuje najmanj enkrat letno, ostali registri preklicanih potrdil pa se osvežujejo po vsakem preklicu potrdila oziroma najmanj enkrat dnevno, če ni novih zapisov oz. sprememb v registrih preklicanih potrdil (24 ur po zadnjem osveževanju).

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

7.2.1 Različica

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

(2) Registri preklicanih potrdil so stalno dostopni 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)

- Halcom CA PO e-signature 1 ali Halcom CA PO e-signature 2

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 PO e-signature 1 ali CN = Halcom CA PO e-signature 2 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= 40 f6 95 20 9b 79 c2 09 ali KeyID= 43 4d 32 75 16 03 c9 75
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

- Halcom CA FO e-signature 1 ali Halcom CA FO e-signature 2

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 FO e-signature 1 ali CN = Halcom CA FO e-signature 2 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= 48 fb 3b 13 99 c3 4e ce Ali KeyID= 48 c4 27 a6 6f 6e f0 2e
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

- Halcom CA PO e-seal 1 ali Halcom CA PO e-seal 2

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 PO e-seal 1 ali CN = Halcom CA PO e-seal 2 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=49 48 76 50 77 0a b1 0c ali KeyID= 47 35 c8 bc 61 e2 5d 9e
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

- Halcom CA web 1

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 web 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=48 42 0b 17 ed ae 9e 70
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

- Halcom CA TSA 1

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 registre 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 preverjanje 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. 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.

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

8.1. 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.

(3) Pooblaščenec za zunanji nadzor nad delovanjem v skladu z ETSI standardi opravi nadzor enkrat letno.

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

Halcom CA določi cenik uporabe potrdil, svojih storitev, potrebne opreme in infrastrukture ter cenik objavi na svojih spletnih straneh.

9.1.1 Cena izdaje potrdil in podaljšanja

Cena izdaje potrdil in podaljšanja je določena z veljavnim cenikom.

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.

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 ponudnika storitev zaupanja Halcom CA.

(2) Z vsemi morebitnimi zaupnimi podatki o 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.

9.3.3 Odgovornost glede varovanja

(1) Halcom CA ne prevzema nobene odgovornosti za vsebino podatkov, ki jih imetnik potrdila elektronsko šifrira ali podpisuje, in sicer tudi v primeru, da je imetnik ali tretja oseba spoštoval vse veljavne predpise, vsa določila 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 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

Določbe glede avtorskih, sorodnih in drugih pravic intelektualne lastnine:

- na zasebnem ključu pripadajo vse pravice 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 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,
- posredovati zahtevke in ostale podatke na varen način na 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.

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 CPS, politike in drugih obvestil Halcom CA ter veljavnih predpisov.

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

9.6.4 Obveznosti in odgovornost tretjih oseb

(1) Ob prvi uporabi potrdil Halcom CA mora tretja oseba, ki se zanaša na potrdilo, skrbno prebrati 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 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,
- ne preverjanja podatkov in veljavnosti potrdil v registru preklicanih potrdil,
- ne preverjanja 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,
- napak pri izračunu zgoščene vrednosti (angl. hash value), preverjanju te vrednosti ali drugih varnostnih postopkih glede elektronskega dokumenta, ki se podpisuje, če je imetnik zahteval podpis v oblaku zgolj na podlagi zgoščene vrednosti in brez predložitve celotnega elektronskega dokumenta ponudniku storitev zaupanja Halcom CA.

9.8. Omejitev glede uporabe

Ni predpisano.

9.9. Poravnava škode

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

9.10. Veljavnost CPS

(1) Halcom CA si pridržuje pravico do spremembe CPS in nadgradnje infrastrukture brez

predhodnega obveščanja imetnikov potrdil.

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

9.10.1 Čas veljavnosti

Novo verzijo oz. spremembe CPS se osem (8) dni pred veljavo predhodno objavi na spletnih straneh ponudnika storitev zaupanja Halcom CA z označenim datumom začetka veljavnosti CPS.

9.10.2 Konec veljavnosti CPS

(1) Ob objavi nove CPS ter politik ostanejo za vsa potrdila, izdana na podlagi politik, v veljavi tista določila, ki se smiselno ne morejo nadomestiti z ustreznimi določili po novih politikah (na primer postopek, ki določa način, po katerem je bilo to potrdilo izdano ipd.).

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

9.10.3 Učinek poteka veljavnosti CPS

(1) Veljavnost potrdil urejajo politike.

(2) Nov CPS in s tem nova politika ne vpliva na veljavnost potrdil, ki so bila izdana po prejšnjih politikah. Taka potrdila ostanejo v veljavi do 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 razdelku 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 CPS lahko ponudnik storitev zaupanja objavi v obliki sprememb in dopolnitev CPS, kadar ne gre za bistvene spremembe v delovanju ponudnika storitev zaupanja.

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

(3) Način za označevanje sprememb in 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.

9.13. 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 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 veljavno zakonodajo in 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, 22.5.2024

Glavni izvršni direktor:
Tomi Šefman