

Pripravl(a): Luka RIBIČIČ

Številka dokumenta: 400085-4-10/17

Politika Halcom CA: Javni del notranjih pravil za EU korenska in vmesna/podrejena potrdila

Izdaja: 10

Politika Halcom CA

Javni del notranjih pravil Halcom CA
za EU korenska in vmesna/podrejena potrdila

CPName: Halcom Root Certificate Authority

Politika za EU korenska in vmesna/podrejena potrdila

Generacija 1: CPOID:1.3.6.1.4.1.5939.13.1.1

Generacija 2: CPOID:1.3.6.1.4.1.5939.13.2.1

Generacija 3: CPOID:1.3.6.1.4.1.5939.13.3.1

Dokument je veljaven od: 15. 6. 2026

Izdaja	št. dokumenta in prilog	Opis spremembe	Avtor	Datum zadnje spremembe
1	400085-4-1/17	Začetna izdaja	L. Ribičič	17.6.2016
2	400085-4-2/17	Dopolnitve EIDAS	L. Ribičič	24.4.2017
3	400085-4-3/17	Letni pregled dokumenta – ni sprememb	S. Lazič	1.6.2018
4	400085-4-4/17	Letni pregled dokumenta, nova celostna podoba	L. Ribičič	24.5.2019
5	400085-4-5/17	Letni pregled dokumenta, popravljen osnovni kapital	L. Ribičič	26.1.2021
6	400085-4-6/17	Letni pregled dokumenta	S. Lazič	21.5.2021
7	400085-4-7/17	Letni pregled dokumenta, odstranili fax	S. Lazič	13.4.2022
8	400085-4-8/17	Letni pregled dokumenta, čas in rok hrambe	S. Lazič	23.5.2023
9	400085-4-9/17	Dodana nova (G2) struktura Halcom CA	L. Ribičič	23.5.2025
10	400085-4-10/17	Dodana nova (G3) struktura Halcom CA	L. Ribičič	23.5.2026

Kazalo vsebine

1. UVOD	12
1.1. Pregled.....	12
1.2. Identifikacijski podatki politike	12
1.3. Subjekti.....	13
1.3.1 Ponudnik storitev zaupanja Halcom CA.....	13
1.3.2 Prijavna služba Halcom CA.....	13
1.3.3 Naročniki in imetniki potrdil	13
1.3.4 Tretje osebe	13
1.4. Namen uporabe	13
1.4.1 Pravilna uporaba potrdil in ključev	13
1.4.2 Nedovoljena uporaba.....	13
1.5. Upravljanje politike	13
1.5.1 Upravljaivec politik.....	13
1.5.2 Pooblaščen kontaktne osebe	14
1.5.3 Odgovorna oseba glede skladnosti delovanja ponudnika storitev zaupanja Halcom CA s politiko.....	14
1.5.4 Postopek za sprejem nove politike.....	14
1.6. Okrajšave in izrazi	14
1.6.1 Okrajšave.....	14
1.6.2 Izrazi.....	15
2. OBJAVE INFORMACIJ IN JAVNI IMENIK POTRDIL... 16	
2.1. Zbirka dokumentov	16
2.2. Imenik potrdil.....	17
2.3. Pogostnost objav.....	17
2.4. Upravljanje dostopa do zbirke dokumentov	17
3. ISTOVETNOST IMETNIKOV POTRDIL	17
3.1. Dodelitev imen.....	17
3.1.1 Razločevalna imena.....	17

3.1.2	Zahteve pri tvorbi razločevalnega imena	19
3.1.3	Uporaba anonimnih imen ali psevdonimov	19
3.1.4	Pravila za interpretacijo razločevalnih imen	19
3.1.5	Enoličnost razločevalnih imen	19
3.1.6	Zaščite imen oz. znamk	19
3.2.	Preverjanje istovetnosti imetnikov ob prvi izdaji potrdila	19
3.2.1	Metoda za posedovanje pripadnosti zasebnega ključa	19
3.2.2	Preverjanje istovetnosti organizacije	20
3.2.3	Preverjanje istovetnosti imetnika	20
3.2.4	Nepreverjeni podatki v potrdilih	20
3.2.5	Preverjanje pooblastil zaposlenih za pridobitev potrdil	20
3.2.6	Medsebojno priznavanje	20
3.3.	Preverjanje imetnikov za ponovno izdajo potrdila	20
3.3.1	Preverjanje imetnikov pri podaljšanju potrdil	20
3.3.2	Preverjanje imetnikov za ponovno pridobitev potrdila po preklicu	20
3.4.	Preverjanje istovetnosti ob zahtevi za preklic	20
4.	UPRAVLJANJE S POTRDILI	21
4.1.	Pridobitev potrdila	21
4.1.1	Kdo lahko pridobi potrdilo	21
4.1.2	Postopek bodočega imetnika za pridobitev potrdila in odgovornosti	21
4.2.	Postopek ob sprejemu zahtevka za pridobitev potrdila	21
4.2.1	Preverjanje istovetnosti bodočega imetnika	21
4.2.2	Odobritev/zavrnitev zahtevka	21
4.2.3	Čas za izdajo potrdila	21
4.3.	Izdaja potrdila	21
4.3.1	Postopek ponudnika storitev zaupanja Halcom CA	21
4.3.2	Obvestilo imetnika o izdaji	21
4.4.	Prevzem potrdila	21
4.4.1	Postopek prevzema potrdila	21
4.4.2	Objava potrdila	22
4.4.3	Obvestilo ponudnika storitev zaupanja o izdaji potrdila tretjim osebam	22
4.5.	Obveznosti in odgovornosti uporabnikov glede uporabe potrdil	22

4.5.1 Obveznosti imetnika potrdila.....	22
4.5.2 Obveznosti za tretje osebe.....	23
4.6. Ponovna izdaja potrdila	23
4.6.1 Okoliščine, ki terjajo ponovno izdajo potrdila	23
4.6.2 Osebe, ki lahko zahtevajo ponovno izdajo potrdila	23
4.6.3 Postopek obravnave prošenj za ponovno izdajo potrdila	23
4.6.4 Obvestilo imetniku o novo izdanem potrdilu.....	23
4.6.5 Postopek prevzema novo izdanega potrdila.....	23
4.6.6 Objava novo izdanega potrdila.....	24
4.6.7 Obvestilo ponudnika storitev zaupanja o izdaji potrdila tretjim osebam.....	24
4.7. Regeneriranje ključev	24
4.7.1 Razlogi za regeneracijo.....	24
4.7.2 Kdo zahteva regeneracijo	24
4.7.3 Postopek za izdajo zahtevka za regeneracijo.....	24
4.7.4 Obvestilo imetniku potrdila o novo izdanem potrdilu	24
4.7.5 Postopek prevzema	24
4.7.6 Objava potrdila ponudnika storitev zaupanja z novima paroma ključev.....	24
4.7.7 Obvestilo ponudnika storitev zaupanja o izdaji potrdila tretjim osebam.....	24
4.8. Sprememba potrdila	24
4.8.1 Okoliščina za spremembo potrdila	24
4.8.2 Kdo zahteva spremembo	24
4.8.3 Postopek ob zahtevku za spremembo.....	25
4.8.4 Obvestilo o izdaji novega potrdila.....	25
4.8.5 Prevzem spremenjenega potrdila	25
4.8.6 Objava spremenjenega potrdila.....	25
4.8.7 Obvestilo drugih subjektov o spremembi.....	25
4.9. Preklic in suspenz potrdila	25
4.9.1 Razlogi za preklic.....	25
4.9.2 Kdo zahteva preklic	26
4.9.3 Postopki za preklic.....	26
4.9.4 Čas za izdajo zahtevka za preklic	27
4.9.5 Čas od prejetega zahtevka za preklic do izvedbe preklica.....	27
4.9.6 Zahteve po preverjanju registra preklicanih potrdil za tretje osebe	27

4.9.7 Pogostnost objave registra preklicanih potrdil.....	27
4.9.8 Čas objave registra preklicanih potrdil.....	27
4.9.9 Sprotno preverjanje statusa potrdil.....	27
4.9.10 Zahteve za sprotno preverjanje statusa potrdil.....	28
4.9.11 Drugi načini za dostop do statusa potrdil.....	28
4.9.12 Posebne zahteve pri zlorabi zasebnega ključa.....	28
4.9.13 Razlogi za suspenz.....	28
4.9.14 Kdo zahteva suspenz.....	28
4.9.15 Postopek za suspenz.....	28
4.9.16 Čas suspenza.....	28
4.10. Preverjanje statusa potrdil.....	28
4.10.1 Dostop za preverjanje.....	28
4.10.2 Razpoložljivost.....	28
4.10.3 Druge informacije za preverjanje statusa.....	29
4.11. Prekinitev razmerja med imetnikom in ponudnikom storitev zaupanja.....	29
4.12. Odkrivanje kopije ključev za dešifriranje.....	29
4.12.1 Razlogi za odkrivanje kopije ključev za dešifriranje.....	29
4.12.2 Kdo zahteva odkrivanje kopije ključev za dešifriranje.....	29
4.12.3 Postopek ob zahtevku za odkrivanje kopije ključev za dešifriranje.....	29
5. UPRAVLJANJE IN VARNOSTNI NADZOR INFRASTRUKTURE.....	29
5.1. Fizično varovanje.....	30
5.1.1 Lokacija in zgradba ponudnika storitev zaupanja.....	30
5.1.2 Fizični dostop do infrastrukture ponudnika storitev zaupanja.....	30
5.1.3 Napajanje in prezračevanje.....	30
5.1.4 Zaščita pred poplavo.....	30
5.1.5 Zaščita pred požari.....	30
5.1.6 Hramba nosilcev podatkov.....	31
5.1.7 Odstranjevanje odpadkov.....	31
5.1.8 Hramba na oddaljeni lokaciji.....	31
5.2. Organizacijska struktura ponudnika storitev zaupanja.....	31

5.2.1 Organizacijske skupine.....	31
5.2.2 Število oseb za posamezne naloge	33
5.2.3 Izkazovanje istovetnosti za opravljanje posameznih nalog	36
5.2.4 Nezdržljivost nalog.....	36
5.3. Nadzor nad osebjem.....	36
5.3.1 Potrebne kvalifikacije in izkušnje osebja	37
5.3.2 Primernost osebja	37
5.3.3 Dodatno usposabljanje osebja.....	37
5.3.4 Zahteve za redna usposabljanja	37
5.3.5 Menjava nalog	37
5.3.6 Sankcije	37
5.3.7 Zahteve za zunanje izvajalce.....	37
5.3.8 Dostop osebja do dokumentacije.....	37
5.4. Varnostni pregledi sistema	37
5.4.1 Vrste dnevnikov.....	37
5.4.2 Pogostnost pregledov dnevnikov.....	38
5.4.3 Čas hrambe dnevnikov.....	38
5.4.4 Zaščita dnevnikov	38
5.4.5 Varnostne kopije dnevnikov.....	38
5.4.6 Zbiranje podatkov za dnevnike	38
5.4.7 Obveščanje povzročitelja dogodka.....	38
5.4.8 Ocena ranljivosti sistema.....	38
5.5. Dolgoročna hramba podatkov.....	38
5.5.1 Vrste dolgoročno hranjenih podatkov.....	38
5.5.2 Rok hrambe.....	39
5.5.3 Zaščita dolgoročno hranjenih podatkov	39
5.5.4 Varnostna kopija dolgoročno hranjenih podatkov	39
5.5.5 Zahteva po časovnem žigosanju.....	39
5.5.6 Način zbiranja podatkov	39
5.5.7 Postopek za dostop do dolgoročno hranjenih podatkov in njihova verifikacija	39
5.6. Sprememba javnega ključa ponudnika storitev zaupanja Halcom CA 40	
5.7. Okrevalni načrt	40

5.7.1	Postopek v primeru vdorov in zlorabe	40
5.7.2	Postopek v primeru okvare programske opreme, podatkov	40
5.7.3	Postopek v primeru ogroženega zasebnega ključa ponudnika storitev zaupanja Halcom CA	40
5.7.4	Okrevalni načrt	40
5.8.	Prenehanje delovanja Halcom CA	40
6.	TEHNIČNE VARNOSTNE ZAHTEVE	40
6.1.	Generiranje in namestitvev ključev	40
6.1.1	Generiranje ključev	40
6.1.2	Dostava zasebnega ključa imetnikom	40
6.1.3	Dostava javnega ključa ponudniku storitev zaupanja	41
6.1.4	Dostava javnega ključa ponudnika storitev zaupanja	41
6.1.5	Dolžina ključev	41
6.1.6	Generiranje in kakovost parametrov javnih ključev	41
6.1.7	Namen ključev in potrdil	41
6.2.	Zaščita zasebnega ključa	41
6.2.1	Standardi za kriptografski modul	41
6.2.2	Nadzor zasebnega ključa s strani pooblaščenih oseb	42
6.2.3	Odkrivanje kopije zasebnega ključa	42
6.2.4	Varnostna kopija zasebnega ključa	42
6.2.5	Arhiviranje zasebnega ključa	42
6.2.6	Prenos zasebnega ključa iz/v kriptografski modul	42
6.2.7	Hramba zasebnega ključa v kriptografskem modulu	42
6.2.8	Postopek za aktiviranje zasebnega ključa	42
6.2.9	Postopek za deaktiviranje zasebnega ključa	43
6.2.10	Postopek za uničenje zasebnega ključa	43
6.2.11	Lastnosti kriptografskega modula	43
6.3.	Ostali aspekti upravljanja ključev	43
6.3.1	Arhiviranje javnega ključa	43
6.3.2	Obdobje veljavnosti za javne in zasebne ključe	43
6.4.	Gesla za dostop do potrdil oz. ključev	43
6.4.1	Generiranje gesel	43
6.4.2	Zaščita gesel	44

6.4.3 Drugi aspekti gesel	44
6.5. Varnostne zahteve za informacijsko-komunikacijsko opremo ponudnika storitev zaupanja	44
6.5.1 Specifične tehnične varnostne zahteve	44
6.5.2 Nivo varnostne zaščite	44
6.6. Tehnični nadzor življenjskega cikla ponudnika storitev zaupanja	44
6.6.1 Nadzor razvoja sistema	44
6.6.2 Upravljanje varnosti	44
6.6.3 Nadzor življenjskega cikla	44
6.7. Varnostna kontrola omrežja	44
6.8. Časovno žigosanje	44
7. PROFIL POTRDIL IN REGISTRA PREKLICANIH POTRDIL	45
7.1. Profil potrdil	45
7.1.1 Različica potrdil	45
7.1.2 Profil potrdil z razširitvami	45
7.1.2.1 Zahteve za elektronski naslov	47
7.1.3 Identifikacijske oznake algoritmov	47
7.1.4 Oblika razločevalnih imen	48
7.1.5 Omejitve glede imen	48
7.1.6 Označba politike potrdila	48
7.1.7 Omejitve uporabe	48
7.1.8 Sintaksa in pomen označb politike potrdil	48
7.1.9 Pomen bistvenih dodatkov politike	48
7.2. Profil registra preklicanih potrdil	48
7.2.1 Različica	49
7.2.2 Vsebina registra in razširitve	49
7.2.3 Objava registra preklicanih potrdil	50
7.3. Profil sprotnega preverjanja statusa potrdil	50
7.3.1 Verzija sprotnega preverjanja statusa	50
7.3.2 Profil sprotnega preverjanja statusa	50

8. NADZOR.....	50
8.1. Pogostnost nadzora	50
8.2. Vrsta in usposobljenost nadzora.....	51
8.3. Neodvisnost nadzora	51
8.4. Področja nadzora.....	51
8.5. Ukrepi ponudnika storitev zaupanja	51
8.6. Objava rezultatov nadzora.....	51
9. FINANČNE IN OSTALE PRAVNE ZADEVE	51
9.1. Cenik	51
9.1.1 Cena izdaje potrdil in podaljšanja.....	51
9.1.2 Cena dostopa do potrdil.....	51
9.1.3 Cena dostopa do statusa potrdila in registra preklicanih potrdil	51
9.1.4 Cene drugih storitev	52
9.1.5 Povrnitev stroškov	52
9.2. Finančna odgovornost	52
9.2.1 Zavarovalniško kritje	52
9.2.2 Drugo kritje	52
9.2.3 Zavarovanje imetnikov.....	52
9.3. Varovanje poslovnih podatkov.....	52
9.3.1 Varovani podatki	52
9.3.2 Nevarovani podatki	52
9.3.3 Odgovornost glede varovanja.....	52
9.4. Varovanje osebnih podatkov.....	53
9.4.1 Načrt varovanja osebnih podatkov.....	53
9.4.2 Varovani osebni podatki	53
9.4.3 Nevarovani osebni podatki.....	53
9.4.4 Odgovornost glede varovanja osebnih podatkov	53
9.4.5 Pooblastilo glede uporabe osebnih podatkov	53
9.4.6 Posredovanje osebnih podatkov	53
9.4.7 Druga določila glede varovanja osebnih podatkov.....	53
9.5. Določbe glede pravic intelektualne lastnine	54

9.6.	Obveznosti in odgovornosti.....	54
9.6.1	Obveznosti in odgovornosti ponudnika storitev zaupanja Halcom CA.....	54
9.6.2	Obveznost in odgovornost prijavne službe.....	55
9.6.3	Obveznosti in odgovornost imetnika potrdila	55
9.6.4	Obveznosti in odgovornost tretjih oseb.....	55
9.6.5	Obveznosti in odgovornost drugih oseb.....	56
9.7.	Omejitev odgovornosti	56
9.8.	Omejitev glede uporabe.....	56
9.9.	Poravnava škode	57
9.10.	Veljavnost politike	57
9.10.1	Čas veljavnosti.....	57
9.10.2	Konec veljavnosti politike	57
9.10.3	Učinek poteka veljavnosti politike	57
9.11.	Komuniciranje med subjekti.....	57
9.12.	Spremembe in dopolnitve	58
9.12.1	Postopek za sprejem sprememb in dopolnitev	58
9.12.2	Veljavnost in objava sprememb in dopolnitev	58
9.12.3	Sprememba identifikacijske številke politike	58
9.13.	Postopek v primeru sporov	58
9.14.	Veljavna zakonodaja	58
9.15.	Skladnost z veljavno zakonodajo.....	58
9.16.	Splošne določbe	59
9.17.	Druge določbe	59

1. UVOD

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

(2) Ta politika je javni del notranjih pravil Halcom CA za korenska (angl. »root«) in vmesna/podrejena (angl. »intermediate«) potrdila.

(3) Oblika in vsebina te politike je usklajena z uredbo eIDAS, uredbo eIDAS 2.0, mednarodnim priporočilom IETF RFC in evropskimi standardi ETSI in drugimi.

1.1. Pregled

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

(2) Halcom CA je ponudnik storitev zaupanja s kvalificiranim statusom. Ponudnik storitev zaupanja Halcom CA deluje v okviru Halcom d.d.

(3) Halcom CA izdaja korenska in vmesna/podrejena potrdila z najmanj enim parom ključev in z obvezno uporabo varnega nosilca oz. strojnega varnostnega modula.

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

(5) Halcom CA izdaja potrdila in opravlja druge dejavnosti ponudnika storitev zaupanja v skladu z veljavnim pravnim redom Republike Slovenije in Evropske unije, ter v skladu z uredbo eIDAS, uredbo eIDAS 2.0, tehničnimi zahtevami ETSI, standardom IETF RFC in družino standardov ISO/IEC ter drugih sorodnih standardov.

1.2. Identifikacijski podatki politike

Oznaka te politike delovanja je:

- Za korensko potrdilo generacije 1 (v nadaljevanju G1): CPOID: 1.3.6.1.4.1.5939.13.1.1
- Za korensko potrdilo generacije 2 (v nadaljevanju G2): CPOID: 1.3.6.1.4.1.5939.13.2.1

- Za korensko potrdilo generacije 3 (v nadaljevanju G3): CPOID: 1.3.6.1.4.1.5939.13.3.1

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

Ni podprto.

1.3.3 Naročniki in imetniki potrdil

Naročnik in imetnik potrdila je ponudnik storitev zaupanja, ki uporablja v njih navedene zasebne ključe izključno za izdajanje oziroma podpisovanje potrdil za elektronski podpis, elektronski žig, avtentikacijo spletišč in izdajo elektronskih časovnih žigov.

1.3.4 Tretje osebe

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

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

1.4. Namen uporabe

Halcom CA upravlja (izdaja in preverja, preklicuje, hrani, objavlja) s korenskimi potrdili za izdajanje oziroma podpisovanje vmesnih/podrejenih potrdil za elektronski podpis, elektronski žig, avtentikacijo spletišč in časovni žig ter za izdajo časovnih žigov.

1.4.1 Pravilna uporaba potrdil in ključev

Potrdila in ključi so namenjeni za elektronsko podpisovanje digitalnih potrdil in registra preklicanih potrdil (zasebni ključ) oziroma za preverjanje veljavnosti teh podpisov (javni ključ).

1.4.2 Nedovoljena uporaba

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

(2) Potrdila niso namenjena nadaljnji prodaji.

1.5. Upravljanje politike

1.5.1 Upravljalavec politik

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

(2) Naslov upravljavca: Halcom d.d.
Dunajska cesta 123
1000 LJUBLJANA
Slovenija

1.5.2 Pooblaščne kontaktne osebe

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

(2) Naslov Halcom CA: Halcom CA
Dunajska cesta 123
1000 LJUBLJANA
Slovenija
Tel.: (+386) 01 200 34 86
E-pošta: ca@halcom.si
E-pošta za preklic : ca_preklici@halcom.si

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

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

1.5.4 Postopek za sprejem nove politike

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

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

1.6. Okrajšave in izrazi

1.6.1 Okrajšave

CA	Ponudnik storitev zaupanja, ki izdaja potrdila (angl.: Certificate Authority ali Certificate Agency).
----	---

CPName	Ime politike delovanja ponudnika storitev zaupanja (angl.: Certification Policy Name), enolično povezano z mednarodno številko politike delovanja CPOID (angl.: Certification Policy Object Identifier).
CPOID	Mednarodna številka, ki enolično določa politiko delovanja (angl.: Certification Policy Object Identifier).
CRL	Certificate Revocation List – seznam preklicanih digitalnih potrdil.
DN	Enolično razločevalno ime (prim. opredelitev razločevalnega imena) (angl.: Distinguished Name).
CP	Politika ponudnika storitev zaupanja (angl. Certificate Policy). Politika ureja namen, delovanje in metodologijo upravljanja storitve ter odgovornosti in varnostne zahteve, ki jih morajo izpolnjevati ponudnik storitev zaupanja, imetniki potrdil (uporabniki storitev) in tretje osebe, ki se zanašajo na ta potrdila/storitev.
CPS	CPS (angl. Certification Practice Statement) predstavlja splošna pravila delovanja ponudnika storitev zaupanja.
LDAP	Leightweight Directory Access Protocol je protokol, ki določa dostop do imenika in je specificiran po IETF (Internet Engineering Task Force) priporočilu IETF RFC 3494:.
S/MIME	Secure Multipurpose Internet Mail Extensions
SSL	Secure Sockets Layer
TLS	Transport Layer Security
PKI	Public Key Infrastructure je infrastruktura javnih ključev.
EŠEI	Enotna številka elektronske identifikacije
HSM	Strojni varnostni modulu (angl. Hardware Security Module).
G1 oz. G2	Prva oz. druga generacija korenskega in podrejenih potrdil Halcom CA.
QCert for ESig/ ESeal	Kvalificirano digitalno potrdilo izdano na varnem mediju (angl. QSCD – Qualified signature creation device). Halcom CA lahko potrdilo izda na pametni kartici, pametnem ključu USB ali v oblaku (HSM). Potrdilo je namenjeno kvalificiranemu elektronskemu podpisu/žigu (angl. Qualified electronic signature/seal).
Cert for ESig/ ESeal	Kvalificirano digitalno potrdilo izdano v datoteki, ki je namenjeno naprednemu elektronskemu podpisu/žigu (angl. Advanced electronic signature/seal).
OT potrdilo	OT potrdilo (angl. One Time Certificate) je potrdilo s kratko veljavnostjo, ki je namenjeno enkratnemu podpisu dokumenta ali skupka dokumentov.

1.6.2 Izrazi

Imenik potrdil	Imenik potrdil po priporočilu X.500, kjer so shranjena potrdila po priporočilu X.509 ver. 3, do katerih je možen dostop po protokolu LDAP. Po tej politiki je ponudnik storitev zaupanja edini mogoči imetnik potrdila.
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). Po tej politiki ni predvidene prijavnne službe.
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.si> (povzetki bistvenih sestavin tudi v angleškem jeziku).

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

- cenik,
- politika uporabe storitev zaupanja (CP),
- pravila delovanja ponudnika storitev zaupanja (CPS)
- naročilnice in druge pogodbe za storitve 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) Nove politike so objavljene v skladu z navedbo v razdelku 9.10.

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

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

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

2.3. Pogostnost objav

(1) Nova politika se objavi takoj po sprejemu.

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

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

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

2.4. Upravljanje dostopa do zbirke dokumentov

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

(2) Z ustreznimi tehničnimi ukrepi informacijske varnosti Halcom CA zagotavlja kontrole, ki preprečujejo nepooblaščen 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 imetniku, ki jih vsebuje razločevalno ime potrdil, so v izdanem potrdilu navedeni v polju Imetnik angl. Subject.

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

Vrsta potrdila	Naziv polja	Razločevalno ime	Generacija
Korensko (Root) potrdilo ponudnika storitev zaupanja Halcom CA	Izdajatelj, angl. Issuer in Imetnik, angl. Subject	C= SI O= Halcom d.d. 2.5.4.97 = VATSI-43353126 CN= Halcom Root Certificate Authority	G1
	Izdajatelj, angl. Issuer in Imetnik, angl. Subject	C= SI O= Halcom d.d. 2.5.4.97 = VATSI-43353126 CN= Halcom Root CA G2	G2
	Izdajatelj, angl. Issuer in Imetnik, angl. Subject	C= SI O= Halcom d.d. 2.5.4.97 = VATSI-43353126 CN= Halcom Root CA G3	G3
Vmesno/podrejeno (Intermediate) potrdilo imetnika - ponudnika storitev zaupanja	Izdajatelj, angl. Issuer	C= SI O= Halcom d.d. 2.5.4.97 = VATSI-43353126 CN= Halcom Root Certificate Authority	G1
	Imetnik, angl. Subject	C= SI O= Halcom d.d. 2.5.4.97 = VAT<dvomestna ISO oznaka države>-<davčna št. poslovnega subjekta> CN= <oznaka podrejenega potrdila>	
Vmesno/podrejeno (Intermediate) potrdilo imetnika - ponudnika storitev zaupanja	Izdajatelj, angl. Issuer	C= SI O= Halcom d.d. 2.5.4.97 = VATSI-43353126 CN= Halcom Root CA G2	G2
	Imetnik, angl. Subject	C= SI O= Halcom d.d. 2.5.4.97= VAT<dvomestna ISO oznaka države>-<davčna št. poslovnega subjekta> CN= <oznaka podrejenega potrdila>	
	Izdajatelj,	C= SI	

Vmesno/podrejeno (Intermediate) potrdilo imetnika - ponudnika storitev zaupanja	angl. Issuer	O= Halcom d.d. 2.5.4.97 = VATSI-43353126 CN= Halcom Root CA G3	G3
	Imetnik, angl. Subject	C= SI O= Halcom d.d. 2.5.4.97= VAT<dvomestna ISO oznaka države>-<davčna št. poslovnega subjekta> CN= <oznaka podrejenega potrdila>	

(4) Ponudnik storitev zaupanja Halcom CA lahko za razločevalno ime imetniških potrdil uporabi dodatna polja, če je to potrebno.

3.1.2 Zahteve pri tvorbi razločevalnega imena

Oznaka imetnika potrdila, ki je v skladu z določili razd. 3.1.1 vključena v razločevalno ime, mora izpolnjevati naslednje zahteve:

- mora biti enolično,
- mora biti pomensko povezano z imetnikom,
- največja dolžina je lahko dvainštirideset (42) znakov.

3.1.3 Uporaba anonimnih imen ali psevdonimov

Uporaba anonimnih imen ali psevdonimov ni dovoljena.

3.1.4 Pravila za interpretacijo razločevalnih imen

Podatki o imetniku potrdila v razločevalnem imenu vsebujejo znake iz kodne tabele UTF-8.

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) 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.

3.2. Preverjanje istovetnosti imetnikov ob prvi izdaji potrdila

3.2.1 Metoda za posedovanje pripadnosti zasebnega ključa

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

3.2.2 Preverjanje istovetnosti organizacije

Preverjanje izvedejo pooblaščen osebe Halcom CA skladno z notranjimi pravili ali pogodbo z drugim ponudnikom storitev zaupanja.

3.2.3 Preverjanje istovetnosti imetnika

Preverjanje izvedejo pooblaščen osebe Halcom CA skladno z notranjimi pravili ali pogodbo z drugim ponudnikom storitev zaupanja.

3.2.4 Nепreverjeni podatki v potrdilih

Ni nepreverjenih podatkov.

3.2.5 Preverjanje pooblastil zaposlenih za pridobitev potrdil

Ni predpisano.

3.2.6 Medsebojno priznavanje

(1) Ponudnik storitev zaupanja Halcom CA ni dolžan pogodbeno sodelovati ali jamčiti za druge ponudnike storitev zaupanja tudi, če ima drugi ponudnik status kvalificiranega ponudnika storitev zaupanja.

(2) Ponudnik storitev zaupanja Halcom CA zagotavlja, da bo izvajal medsebojno priznavanje izključno po podpisu pisne pogodbe z drugimi 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, pooblaščen 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

Ni podprto.

3.3.2 Preverjanje imetnikov za ponovno pridobitev potrdila po preklicu

Ni podprto.

3.4. Preverjanje istovetnosti ob zahtevi za preklic

Preverjanje izvedejo pooblaščen osebe Halcom CA skladno z notranjimi pravili ali pogodbo z drugim ponudnikom storitev zaupanja.

4. UPRAVLJANJE S POTRDILI

4.1. Pridobitev potrdila

4.1.1 Kdo lahko pridobi potrdilo

Bodoči imetniki potrdil izdanih po tej politiki so Halcom CA ali drugi ponudniki storitev zaupanja.

4.1.2 Postopek bodočega imetnika za pridobitev potrdila in odgovornosti

Potrdilo se izda na osnovi odobritve pooblaščen osebe Halcom CA skladno z notranjimi pravili ali pogodbo z drugim ponudnikom storitev zaupanja.

4.2. Postopek ob sprejemu zahtevka za pridobitev potrdila

4.2.1 Preverjanje istovetnosti bodočega imetnika

Preverjanje izvedejo pooblaščen osebe Halcom CA skladno z notranjimi pravili ali pogodbo z drugim ponudnikom storitev zaupanja.

4.2.2 Odobritev/zavrnitev zahtevka

Pooblaščen osebe ponudnika storitev zaupanja Halcom CA naročilnico za pridobitev potrdila odobrijo oz. v primeru nepravilnih ali pomanjkljivih podatkov ali neizpolnjevanja obveznosti zavrnejo.

4.2.3 Čas za izdajo potrdila

Halcom CA izda potrdilo najkasneje v petih (5) delovnih dneh od odobritve.

4.3. Izdaja potrdila

4.3.1 Postopek ponudnika storitev zaupanja Halcom CA

(1) Proizvodni postopek se izvede skladno z notranjimi pravili ali pogodbo z drugim ponudnikom storitev zaupanja.

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

4.3.2 Obvestilo imetnika o izdaji

Glej prejšnji razdelek.

4.4. Prevzem potrdila

4.4.1 Postopek prevzema potrdila

(1) Postopek prevzema se izvede skladno z notranjimi pravili ali pogodbo z drugim ponudnikom storitev zaupanja.

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

4.4.2 Objava potrdila

Postopek je opisan v 2. razdelku.

4.4.3 Obvestilo ponudnika storitev zaupanja o izdaji potrdila tretjim osebam

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

4.5. Obveznosti in odgovornosti uporabnikov glede uporabe potrdil

4.5.1 Obveznosti imetnika potrdila

(1) Imetnik oziroma bodoči imetnik potrdila je dolžan:

- seznaniti se in ravnati v skladu s politiko pred izdajo potrdila,
- ravnati v skladu s politiko in ostalimi veljavnimi predpisi,
- po prevzemu 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,
- 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 preučiti 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 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 CA oz. drugih ponudnikov storitev zaupanja,
- upoštevati druge določbe, v kolikor je s ponudnikom storitev zaupanja Halcom CA sklenila dogovor o uporabi potrdil.

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

4.6. Ponovna izdaja potrdila

Ni podprto.

4.6.1 Okoliščine, ki terjajo ponovno izdajo potrdila

Ni predpisano.

4.6.2 Osebe, ki lahko zahtevajo ponovno izdajo potrdila

Ni predpisano.

4.6.3 Postopek obravnave prošenj za ponovno izdajo potrdila

Ni predpisano.

4.6.4 Obvestilo imetniku o novo izdanem potrdilu

Glej razd. 4.3.2.

4.6.5 Postopek prevzema novo izdanega potrdila

Ni predpisano.

4.6.6 Objava novo izdanega potrdila

Ni predpisano.

4.6.7 Obvestilo ponudnika storitev zaupanja o izdaji potrdila tretjim osebam

Ni predpisano.

4.7. Regeneriranje ključev

4.7.1 Razlogi za regeneracijo

Ni podprto.

4.7.2 Kdo zahteva regeneracijo

Ni podprto.

4.7.3 Postopek za izdajo zahtevka za regeneracijo

Ni podprt.

4.7.4 Obvestilo imetniku potrdila o novo izdanem potrdilu

Ni podprto.

4.7.5 Postopek prevzema

Ni podprt.

4.7.6 Objava potrdila ponudnika storitev zaupanja z 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 imetnik potrdila zahteva kadarkoli, mora pa ga zahtevati v primeru:

- spremembe razločevalnega imena (DN),
- ko imetnik potrdila zamenja ključne podatke, povezane s potrdilom (naziv),
- ko se ugotovi ali sumi, da je prišlo bodisi do razkritja ključa za podpisovanje bodisi do zlorabe potrdila,
- nadomestitvi potrdila z drugim potrdilom.

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

(3) Preklic potrdila je mogoč štiriindvajset (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 imetnik zahtevati v primeru:

- če je bil zasebni ključ imetnika potrđila ogrožen na način, ki vpliva na zanesljivost uporabe,
- če obstaja nevarnost zlorabe zasebnega ključa ali potrđila imetnika,
- če so se spremenili oz. so napačni ključni podatki, navedeni v potrđilu.

(2) Ponudnik storitev zaupanja Halcom CA prekliče potrđilo tudi brez zahteve imetnika takoj, ko izve:

- da je podatek v potrđilu napačen ali je bilo potrđilo izdano na podlagi napačnih podatkov,
- da so se spremenile druge okoliščine, ki vplivajo na veljavnost potrđila,
- za neizpolnjevanje obveznosti imetnika,
- da niso poravnani morebitni stroški za upravljanje digitalnih potrđil,
- da je bila infrastruktura ponudnika storitev zaupanja ogrožena na način, ki vpliva na zanesljivost potrđila,
- da je bil zasebni ključ imetnika potrđila ogrožen na način, ki vpliva na zanesljivost uporabe,
- da bo Halcom CA prenehal z izdajanjem potrđil ali da je bilo ponudniku storitev zaupanja prepovedano upravljanje s potrđili in njegove dejavnosti ni prevzel drug ponudnik storitev zaupanja,
- da je preklic odredilo pristojno sodišče, prekrškovni ali upravni organ.

4.9.2 Kdo zahteva preklic

Preklic potrđila lahko zahteva:

- ponudnik storitev zaupanja Halcom CA,
- imetnik (drug ponudnik storitev zaupanja),
- pristojno sodišče, prekrškovni ali upravni organ.

4.9.3 Postopki za preklic

(1) Preklic lahko imetnik zahteva:

- osebno v času uradnih ur na Halcom CA,
- elektronsko štiriindvajset (24) ur na dan vse dni v letu, če gre za možnost zlorabe ali nezanesljivosti potrđila, sicer v času, ki po veljavni zakonodaji velja za poslovni čas državnih organov,
- na drug način določen s pogodbo z imetnikom - drugim ponudnikom storitev zaupanja.

(2) O datumu ter času preklica, vložniku zahtevka za preklic ter vzrokih za preklic morata biti vedno obveščeni imetnik.

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

4.9.4 Čas za izdajo zahtevka za preklic

Preklic je potrebno zahtevati nemudoma, če gre za možnost zlorabe ali nezanesljivosti ipd. nujne primere. V ostalih primerih se preklic lahko zahteva naslednji delovni dan.

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 preklične potrdilo, če gre za preklic zaradi nevarnosti zlorabe ali nezanesljivosti ipd.,
- sicer pa prvi delovni dan po prejetju zahtevka za preklic.

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

4.9.6 Zahteve po preverjanju registra preklicanih potrdil za tretje osebe

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

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

4.9.7 Pogostnost objave registra preklicanih potrdil

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

- po vsakem preklicu potrdila,
- najmanj enkrat letno, če ni novih zapisov oz. sprememb v registru preklicanih potrdil.

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 pet (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 osmih (8) urah. V primeru nastanka nepredvidljivih okoliščin kot posledica višje sile ali izrednih dogodkov bo Halcom CA izjemoma objavil register preklicanih potrdil najkasneje v štiriindvajsetih (24) urah, vendar še pred potekom zadnjega veljavnega registra preklicanih potrdil.

4.9.9 Sprotno preverjanje statusa potrdil

(1) Sprotno preverjanje statusa (OCSP) korenskega potrdila ni podprt.

(2) Podprt je protokol za sprotno preverjanje statusa podrejenih potrdil 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

Ni podprto.

4.9.14 Kdo zahteva suspenz

Ni podprto.

4.9.15 Postopek za suspenz

Ni podprto.

4.9.16 Čas suspenza

Ni podprto.

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 podrejenih potrdil 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 osmih (8) urah. V primeru nastanka

nepredvidljivih okoliščin kot posledica višje sile ali izrednih dogodkov bo Halcom CA izjemoma omogočil preverjanje statusa potrdil najkasneje v štiriindvajsetih (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 in ponudnikom storitev zaupanja Halcom CA 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 Common Criteria EAL4+ ter s tehničnimi zahtevami ETSI.

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

(3) Halcom CA shranjuje rezervne in distribucijske nosilce podatkov tako, da je v največji meri preprečena izguba, vdor ali nepooblaščen uporaba ali spreminjanje shranjenih informacij. Tako za obnovitev podatkov kot za arhiviranje pomembnih informacij so zagotovljene rezervne kopije, ki so shranjene na drugem mestu, kot je shranjena programska oprema za upravljanje s potrdili, za zagotovitev ponovnega delovanja v primerih, ko bi bili uničeni podatki na osnovni lokaciji.

(4) Podroben opis infrastrukture Halcom CA, operativno delovanje, postopki upravljanja z

infrastrukturo ter nadzor nad varnostno politiko njegovega delovanja je določen z njegovimi notranjimi pravili.

5.1. Fizično varovanje

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

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

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

5.1.1 Lokacija in zgradba ponudnika storitev zaupanja

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

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

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

5.1.2 Fizični dostop do infrastrukture ponudnika storitev zaupanja

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

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

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

5.1.3 Napajanje in prezračevanje

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

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

5.1.4 Zaščita pred poplavo

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

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

5.1.5 Zaščita pred požari

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

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

5.1.6 Hramba nosilcev podatkov

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

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

5.1.7 Odstranjevanje odpadkov

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

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

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

5.1.8 Hramba na oddaljeni lokaciji

Glej razd. 5.1.6.

5.2. Organizacijska struktura ponudnika storitev zaupanja

5.2.1 Organizacijske skupine

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

(2) Med pooblaščen osebe ponudnika storitev zaupanja Halcom CA spadajo:

- zaposleni pri ponudniku storitev zaupanja Halcom CA in
- prijavnne 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	<ul style="list-style-type: none"> • Priprava začetne konfiguracije sistema, • začetna nastavitve parametrov 	2

		<p>novih podrejenih ponudnikov storitev zaupanja,</p> <ul style="list-style-type: none"> • postavitve 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. 	
	Sistemi administrator	<ul style="list-style-type: none"> • Upravljanje postopkov za izdajo potrdil, • pomoč podrejenim ponudnikom storitev zaupanja, • pooblaščenje podrejenih ponudnikov storitev zaupanja, • dostop do protokola podpisovanja potrdil, • varno shranjevanje in distribucija kopij in nadgradenj na ločeno lokacijo. 	2
Upravljanje s potrdili	Sistemi operater 1	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Potrjevanje izdaje potrdil in proženje gesel. 	2
	Operater za potrdila	<ul style="list-style-type: none"> • Predpoosebljanje varnih pametnih kartic • priprava potrdil (obdelava podpisanih zahtev za potrdila), • poosebljanje (izdelava potrdil, zapis na varni nosilec, tiskanje imetnikovih podatkov na varni nosilec), • distribucija potrdil. 	2
	Operater za kode	<ul style="list-style-type: none"> • Distribucija kod PIN. 	2

	Uslužbenec za prijavo	<ul style="list-style-type: none"> Identifikacija imetnikov potrdil. 	2
	Uslužbenec za preklic	<ul style="list-style-type: none"> Priprava zahtev za preklic, preklic potrdil. 	2
Varovanje in kontrola	Varnostni administrator	<ul style="list-style-type: none"> Določanje varnostnih pravil in nadzor njihovega upoštevanja, pregledovanje systemske dokumentacije in kontrolnih dnevnikov za nadzor dela, osebno sodelovanje in pomoč pri letni inventuri dokumentacije podrejenih ponudnikov storitev zaupanja. 	2
	Pooblaščenec za notranji nadzor	<ul style="list-style-type: none"> Nadzor varnostnih pravil in njihovega upoštevanja, nadzor systemske dokumentacije in kontrolnih dnevnikov za nadzor dela. 	2
Regulativno	Pooblaščenec za zasebnost in regulatorno skladnost	<ul style="list-style-type: none"> 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 systemski administrator

Število oseb: 2

Naloge:

- Priprava začetne konfiguracije sistema, vključno z varnim zagonom in ustavitvijo delovanja sistema.
- Začetna nastavitve 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. Pooblaščenje 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 prošenje 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 systemske 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 prijavnne službe je zagotovljena z varnostnimi mehanizmi in kontrolnimi postopki v skladu z notranjimi pravili ponudnika storitev zaupanja Halcom CA.

5.2.4 Nezdržljivost 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 nezdržljivo.

5.3. Nadzor nad osebjem

(1) Operativno, organizacijsko in strokovno pravilno delovanje ponudnika storitev zaupanja Halcom CA nadzira pooblaščenec za notranji nadzor, ki ne opravlja 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 prijavnih služb, 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 pooblaščen 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 pooblaščen osebe ponudnika storitev zaupanja Halcom CA.

5.3.8 Dostop osebja do dokumentacije

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

5.4. Varnostni pregledi sistema

5.4.1 Vrste dnevnikov

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

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

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

5.4.2 Pogostnost pregledov dnevnikov

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

5.4.3 Čas hrambe dnevnikov

Dnevniki se hranijo vsaj deset (10) let po njihovem nastanku, če poseben zakon ne določa daljšega roka.

5.4.4 Zaščita dnevnikov

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

5.4.5 Varnostne kopije dnevnikov

Varnostne kopije dnevnikov se izvajajo dnevno.

5.4.6 Zbiranje podatkov za dnevnike

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

5.4.7 Obveščanje povzročitelja dogodka

Povzročitelja dogodkov ni potrebno obveščati.

5.4.8 Ocena ranljivosti sistema

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

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

5.5. Dolgoročna hramba podatkov

5.5.1 Vrste dolgoročno hranjenih podatkov

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

- dnevnike,
- zapisnike,
- vsa dokazila o opravljenem preverjanju istovetnosti imetnikov,
- 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 Splošnih pravilih delovanja in notranjih pravilih ponudnika storitev zaupanja Halcom CA.

5.5.4 Varnostna kopija dolgoročno hranjenih podatkov

(1) Kopija dolgoročno hranjenih podatkov se varno hrani.

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

5.5.5 Zahteva po časovnem žigosanju

Ni predpisano.

5.5.6 Način zbiranja podatkov

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

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

5.5.7 Postopek za dostop do dolgoročno hranjenih podatkov in njihova verifikacija

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

(2) Podrobnejša ureditev je v skladu z veljavnimi predpisi, standardi in priporočili določena v

Splošnih pravilih delovanja in notranjih pravilih ponudnika storitev zaupanja Halcom CA.

5.6. Sprememba javnega ključa ponudnika storitev zaupanja Halcom CA

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

5.7. Okrevalni načrt

5.7.1 Postopek v primeru vdorov in zlorabe

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

5.7.2 Postopek v primeru okvare programske opreme, podatkov

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

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

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

5.7.4 Okrevalni načrt

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

5.8. Prenehanje delovanja Halcom CA

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

6. TEHNIČNE VARNOSTNE ZAHTEVE

6.1. Generiranje in namestitvev ključev

6.1.1 Generiranje ključev

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

(2) Imetnikov par ključev se generira na strojnem varnostnem modulu pri imetniku.

6.1.2 Dostava zasebnega ključa imetnikom

Imetnikov zasebni ključ se generira pri imetniku in se ne prenaša.

6.1.3 Dostava javnega ključa ponudniku storitev zaupanja

Ključni se generirajo v strojnem varnostnem modulu imetnika, PKCS#10 zahtevke za izdajo potrdila (angl. »certificate request«) pa se prenese iz imetnikovega sistema do ponudnika storitev zaupanja preko zaščitene omrežne povezave.

6.1.4 Dostava javnega ključa ponudnika storitev zaupanja

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

- v javnem imeniku <ldap://ldap.halcom.si> po protokolu LDAP (glej razdelek 2.3),
- v obliki PEM na naslovu <https://www.halcom.com/sl/halcom-ca/politike-in-dokumenti/> pri čemer mora dodatno preveriti verodostojnost potrdila.

6.1.5 Dolžina ključev

Potrdilo	Dolžina ključa po RSA [bit]
Korensko (Root) potrdilo ponudnika storitev zaupanja Halcom CA	G1 - Najmanj 2048 G2 - Najmanj 4096 G3 - Najmanj 4096
Vmesna/podrejena (Intermediate) potrdila	G1 - Najmanj 2048 G2 - Najmanj 4096 G3 - Najmanj 4096

6.1.6 Generiranje in kakovost parametrov javnih ključev

Kvaliteta parametrov ključa ponudnika storitev zaupanja Halcom CA je zagotovljena s strani proizvajalca strojne in 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 strojnem varnostnem modulu, ki je certificiran v skladu s 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 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 pooblašcene 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 ključ korenskega potrdila se ustvari v strojnem varnostnem modulu in se prenaša le z namenom izdelave varnostne kopije zasebnega ključa.
- (2) Zasebni ključi imetnikov - ponudnikov storitev zaupanja se ustvarijo in hranijo v strojnem varnostnem modulu imetnika in se ne prenašajo.

6.2.7 Hramba zasebnega ključa v kriptografskem modulu

- (1) Zasebni ključ ponudnik storitev zaupanja HALCOM CA hrani v strojnem varnostnem modulu, ki je certificiran v skladu s Common Criteria EAL4+.
- (2) Zasebni ključi imetnikov - ponudnikov storitev zaupanja se ustvarijo in hranijo v strojnem varnostnem 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) Imetniki morajo zagotoviti varno aktiviranje svojega zasebnega ključa.

6.2.9 Postopek za deaktiviranje zasebnega ključa

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

(2) Imetniki morajo uporabljati tako programsko opremo, ki ob zaustavitvi delovanja deaktivira zasebni ključ.

6.2.10 Postopek za uničenje zasebnega ključa

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

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

6.2.11 Lastnosti kriptografskega modula

Strojni varnostni modul ustreza 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 potrdila je razvidna iz spodnje razpredelnice.

Tip potrdila	Potrdilo	Ključ	Veljavnost
Korensko potrdilo	par ključev za digitalno podpisovanje/ preverjanje veljavnosti podpisa	Zasebni ključ za podpisovanje	20 let
		Javni ključ za preverjanje veljavnosti podpisa	20 let

(2) Veljavnost podrejenih potrdil je predvidoma deset (10) let, največ pa do poteka veljavnosti korenskega potrdila Halcom CA, ki je podrejeno potrdilo izdal.

6.4. Gesla za dostop do potrdil oz. ključev

6.4.1 Generiranje gesel

(1) Pooblaščen osebe ponudnika storitev zaupanja Halcom CA za dostop do zasebnega ključa korenskih in podrejenih potrdil Halcom CA uporabljajo pametne kartice in osebne številke (kode PIN), s katerimi ravnajo v skladu z notranjimi pravili ponudnika storitev zaupanja Halcom CA.

(2) Pametne kartice in osebne številke (kode PIN) za dostop do korenskih in podrejenih potrdil se ustvarijo v varnem okolju ponudnika storitev zaupanja Halcom CA.

6.4.2 Zaščita gesel

Gesla (kode PIN) pooblaščenih oseb za dostop do zasebnih ključev korenskih in podrejenih potrdil se shranijo v skladu z notranjimi pravili ponudnika storitev zaupanja Halcom CA.

6.4.3 Drugi aspekti gesel

Niso predpisani.

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

6.5.1 Specifične tehnične varnostne zahteve

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

6.5.2 Nivo varnostne zaščite

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

6.6. Tehnični nadzor življenjskega cikla ponudnika storitev zaupanja

6.6.1 Nadzor razvoja sistema

Halcom CA uporablja programsko in strojno opremo, ki je certificirana v skladu s 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 Splošnih pravilih delovanja in notranjih pravilih ponudnika storitev zaupanja Halcom CA.

6.7. Varnostna kontrola omrežja

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

6.8. Časovno žigosanje

Ni predpisano.

7. PROFIL POTRDIL IN REGISTRA PREKLICANIH POTRDIL

7.1. Profil potrdil

(1) Na podlagi te politike Halcom CA izdaja lastna korenska in podrejena potrdila ali podrejena potrdila imetnikov - ponudnikov storitev zaupanja.

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

7.1.1 Različica potrdil

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

7.1.2 Profil potrdil z razširitvami

(1) Profil korenskih (root) potrdill

Nazivi polja	Vrednost oz. pomen
Osnovna polja v potrdilu	
Različica, angl. Version	V3
Identifikacijska oznaka potrdila, angl. Serial Number	G1: 0cdf9b
	G2: 6fb450b4a6bbeebb983055e81d53c040
	G3: 7539c53f6170763fb3c445b870ef6174
Algoritem za podpis, angl. Signature algorithm	G1: Sha256RSA
	G2: RSASSA-PSS
	G3: RSASSA-PSS
Izdajatelj, angl. Issuer	G1: C=SI, O=Halcom d.d., 2.5.4.97 = VATSI-43353126 CN=Halcom Root Certificate Authority
	G2: C=SI, O=Halcom d.d., 2.5.4.97 = VATSI-43353126 CN=Halcom Root CA G2
	G3: C=SI, O=Halcom d.d., 2.5.4.97 = VATSI-43353126 CN=Halcom Root CA G3
Veljavnost, angl. Validity	G1: Valid from: <10.6.2016 07:07:50 GMT > Valid to: <10.6.2036 07:07:50 GMT >
	G2: Valid from: < 19.3. 2025 09:00:00 GMT> Valid to: <19.3.2045 09:00:00 GMT>
	G2: Valid from: < 19.3. 2026 10:00:00 GMT> Valid to: <19.3.2045 10:00:00 GMT>
Imetnik, angl. Subject	G1: C=SI, O=Halcom d.d., 2.5.4.97 = VATSI-43353126 CN=Halcom Root Certificate Authority
	G2: C=SI, O=Halcom d.d., 2.5.4.97 = VATSI-43353126 CN=Halcom Root CA G2
	G3: C=SI, O=Halcom d.d., 2.5.4.97 = VATSI-43353126 CN=Halcom Root CA G3
	G1: RSA

ključ, angl. Subject Public Key Algorithm	G2: RSASSA-PSS G3: RSA
Javni ključ, angl. Public Key (... bits)	modul, eksponent,...
Imetnikov javni ključ, ki pripada ustreznemu paru ključev, šifriran z alg. RSA ali RSASSA-PSS, angl. Public Key	G1: dolžina ključa je najmanj 2048 bitov
	G2: dolžina ključa je najmanj 4096 bitov
	G3: dolžina ključa je najmanj 4096 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	G1: 42aea643c79828b0
	G2: 4e14b2790896f4b6
	G3: 4ba6657603985167
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

Nazivi polja	Vrednost oz. pomen
Osnovna polja v potrdilu	
Različica, angl. Version	V3
Identifikacijska oznaka potrdila, angl. Serial Number	G1: 0cdf9b
	G2: 6fb450b4a6bbeebb983055e81d53c040
	G2: 7539c53f6170763fb3c445b870ef6174
Algoritem za podpis, angl. Signature algorithm	G1: Sha256RSA
	G2: RSASSA-PSS
	G3: RSASSA-PSS
Izdajatelj, angl. Issuer	G1: C=SI, O=Halcom d.d., 2.5.4.97 = VATSI-43353126 CN=Halcom Root Certificate Authority
	G2: C=SI, O=Halcom d.d., 2.5.4.97 = VATSI-43353126 CN=Halcom Root CA G2
	G3: C=SI, O=Halcom d.d., 2.5.4.97 = VATSI-43353126 CN=Halcom Root CA G3
Veljavnost, angl. Validity	Valid from: <pričetek veljavnosti po GMT> Valid to: <konec veljavnosti po GMT>
Imetnik, angl. Subject	razločevalno ime imetnika, glej 3.1.1.
	G1: RSA

Algoritem za javni ključ, angl. Subject Public Key Algorithm	G2: RSASSA-PSS G3: RSA
Javni ključ, angl. Public Key (... bits)	modul, eksponent,...
Imetnikov javni ključ, ki pripada ustreznemu paru ključev, šifriran z alg. RSA ali RSASSA-PSS, angl. Public Key	dolžina ključa, glej razd. 6.1.5.
Razširitve X.509v3	
Objava registra preklicanih potrdil, OID 2.5.29.31, angl. CRL Distribution Points	enolična URI registra preklicanih potrdil
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	G1: KeyID=42aea643c79828b0
	G2: KeyID=4e14b2790896f4b6
	G3: KeyID=4ba6657603985167
Identifikator imetnikovega ključa, OID 2.5.29.14, angl. Subject Key Identifier	enoličen identifikator ključa imetnika
Osnovne omejitve, OID 2.5.29.19, angl. Basic Constraints	Subject Type=CA Path Length Constraint=None
Dotatna identifikacija (ni del digitalnega potrdila)	
razpoznavni odtis potrdila-SHA1 angl. Certificate Fingerprint – SHA1	Razpoznavni odtis potrdila po SHA1

(4) Polje Namen uporabe (angl. Key Usage) ter polje Osnovne omejitve (angl. Basic Constraints) sta označeni kot kritično (angl. critical).

7.1.2.1 Zahteve za elektronski naslov

Ni predpisano.

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:

- G1: sha256RSA, identifikacijska oznaka: OID 1.2.840.113549.1.1.11 ali

- G2: RSASSA-PSS, identifikacijska oznaka: OID 1.2.840.113549.1.1.10.
- G3: RSASSA-PSS, identifikacijska oznaka: OID 1.2.840.113549.1.1.10.

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

7.1.4 Oblika razločevalnih imen

Glej razd. 3.1.1.

7.1.5 Omejitve glede imen

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

7.1.6 Označba politike potrdila

Glej razd. 7.1.2.

7.1.7 Omejitve uporabe

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

7.1.8 Sintaksa in pomen označb politike potrdil

Glej razd. 7.1.2.

7.1.9 Pomen bistvenih dodatkov politike

Ni podprto.

7.2. Profil registra preklicanih potrdil

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

- G1:
 - CN= Halcom Root Certificate Authority
 - O = Halcom
 - C = SI
- G2:
 - CN= Halcom Root CA G2
 - O = Halcom
 - C = SI
- G3:
 - CN= Halcom Root CA G3
 - O = Halcom
 - C = SI

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

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

7.2.1 Različica

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

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

- po protokolu LDAP in
- po protokolu HTTP.

7.2.2 Vsebina registra in razširitve

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

- identifikacijske oznake preklicanih potrdil in
- čas in datum preklica.

Korenski 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	G1: Sha256RSA
	G2: RSASSA-PSS
	G3: RSASSA-PSS
Podpis ponudnika storitev zaupanja, angl. Signature	podpis Halcom CA
Razločevalno ime ponudnika storitev zaupanja, angl. Issuer	G1: C=SI, O=Halcom d.d., 2.5.4.97 = VATSI-43353126 CN=Halcom Root Certificate Authority
	G2: C=SI, O=Halcom d.d., 2.5.4.97 = VATSI-43353126 CN=Halcom Root CA G2
	G3: C=SI, O=Halcom d.d., 2.5.4.97 = VATSI-43353126 CN=Halcom Root CA G3
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)	G1: KeyID= 42aea643c79828b0
	G2: KeyID=4e14b2790896f4b6
	G3: KeyID=4ba6657603985167
angl. issuerAltName (OID 2.5.28.18)	se ne uporablja
angl. deltaCRLindicator (OID 2.5.29.27)	se ne uporablja
angl. issuingDistributionPoint (OID 2.5.29.28)	se ne uporablja

7.2.3 Objava registra preklicanih potrdil

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

7.3. Profil sprotnega preverjanja statusa potrdil

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

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

7.3.1 Verzija sprotnega preverjanja statusa

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

7.3.2 Profil sprotnega preverjanja statusa

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

8. NADZOR

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

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

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

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.

Pooblaščenec za zunanji nadzor nad delovanjem v skladu z ETSI standardi opravi nadzor enkrat na dve leti.

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

8.2. Vrsta in usposobljenost nadzora

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

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

8.3. Neodvisnost nadzora

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

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

8.4. Področja nadzora

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

8.5. Ukrepi ponudnika storitev zaupanja

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

8.6. Objava rezultatov nadzora

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

9. FINANČNE IN OSTALE PRAVNE ZADEVE

9.1. Cenik

V skladu s pogodbo z imetnikom – ponudnikom storitev zaupanja.

9.1.1 Cena izdaje potrdil in podaljšanja

V skladu s pogodbo z imetnikom – ponudnikom storitev zaupanja.

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

V skladu s pogodbo z imetnikom – ponudnikom storitev zaupanja.

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 o podatki imetnikov 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 podatke, ki v skladu z veljavno zakonodajo niso zaupne narave (osebni podatki, poslovne skrivnosti in podobno).

9.3.3 Odgovornost glede varovanja

(1) Halcom CA ne prevzema nobene odgovornosti za vsebino podatkov, 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 te politike in drugih pravil Halcom CA oziroma upošteval vsa njegova navodila.

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

9.4. Varovanje osebnih podatkov

9.4.1 Načrt varovanja osebnih podatkov

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

9.4.2 Varovani osebni podatki

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

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

9.4.3 Nevarovani osebni podatki

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

9.4.4 Odgovornost glede varovanja osebnih podatkov

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

9.4.5 Pooblastilo glede uporabe osebnih podatkov

Ni predpisano.

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 pooblaščenice 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 prijavnne službe

Ni definirano.

9.6.3 Obveznosti in odgovornost imetnika potrdila

(1) Imetnik potrdila odgovarja za:

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

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

9.6.4 Obveznosti in odgovornost tretjih oseb

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

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

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

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

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

9.6.5 Obveznosti in odgovornost drugih oseb

Ni predpisano.

9.7. Omejitev odgovornosti

Ponudnik storitev zaupanja Halcom CA ni odgovoren za škodo, ki bi nastala zaradi:

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

9.8. Omejitev glede uporabe

Ni predpisano.

9.9. Poravnava škode

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

9.10. Veljavnost politike

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

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

9.10.1 Čas veljavnosti

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

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

9.10.2 Konec veljavnosti politike

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

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

9.10.3 Učinek poteka veljavnosti politike

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

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

9.11. Komuniciranje med subjekti

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

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

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

9.12. Spremembe in dopolnitve

9.12.1 Postopek za sprejem sprememb in dopolnitev

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

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

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

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

9.12.2 Veljavnost in objava sprememb in dopolnitev

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

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

9.12.3 Sprememba identifikacijske številke politike

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

9.13. Postopek v primeru sporov

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

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

9.14. Veljavna zakonodaja

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

9.15. Skladnost z veljavno zakonodajo

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

(2) Akreditiran organ za ugotavljanje skladnosti ponudnika storitev zaupanja Halcom CA revidira najmanj vsakih štiriindvajset (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 pooblaščenice 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, 20.5.2026

Izvršni direktor

Gregor Pelhan