Politika Halcom CA

Javni del notranjih pravil Halcom CA

za strežniška digitalna potrdila

CPName: Halcom Secure Server CA 1

Politika za Strežniška digitalna potrdila

CPOID:1.3.6.1.4.1.5939.5.2.3

Dokument je veljaven od: 17.06.2016

Kazalo vsebine

1. UVOD 8

1.1. Pregled 8

1.2. Identifikacijski podatki politike 8

1.3. Subjekti 8
1.3.1 Overitelj Halcom CA 9
1.3.2 Prijavna služba Halcom CA 9
1.3.3 Imetniki potrdil 9
1.3.4 Tretje osebe 9

1.4. Namen uporabe 9
1.4.1 Pravilna uporaba potrdil in ključev 10
1.4.2 Nedovoljena uporaba 10

1.5. Upravljanje politike 10
1.5.1 Upravljavec politik 10
1.5.2 Pooblaščene kontaktne osebe 10
1.5.3 Odgovorna oseba glede skladnosti delovanja overitelja Halcom CA s politiko 10
1.5.4 Postopek za sprejem nove politike 11

1.6. Okrajšave in izrazi 11
1.6.1 Okrajšave 11
1.6.2 Izrazi 11

2. OBJAVE INFORMACIJ IN JAVNI IMENIK POTRDIL 11

2.1. Zbirka dokumentov 12

2.2. Javni imenik potrdil 12

2.3. Pogostnost objav 12

2.4. Upravljanje dostopa do zbirke dokumentov 12

3. ISTOVETNOST IMETNIKOV POTRDIL 13

3.1. Dodelitev imen 13
3.1.1 Razločevalna imena 13
3.1.2 Zahteve pri tvorbi razločevalnega imena 13
3.1.3 Uporaba anonimnih imen ali psevdonimov 14
3.1.4 Pravila za interpretacijo razločevalnih imen 14
3.1.5 Enoličnost razločevalnih imen 14
3.1.6 Zaščite imen oz. znamk 14

3.2. Preverjanje istovetnosti imetnikov ob prvi izdaji potrdila 14
3.2.1 Metoda za posedovanje pripadnosti zasebnega ključa 14
3.2.2 Preverjanje istovetnosti organizacije 14
3.2.3 Preverjanje istovetnosti imetnika 15
3.2.4 Nepreverjeni podatki v potrdilih 15
3.2.5 Preverjanje pooblastil zaposlenih za pridobitev potrdil 15
3.2.6 Medsebojno priznavanje 15

3.3. Preverjanje imetnikov za ponovno izdajo potrdila 15
3.3.1 Preverjanje imetnikov pri podaljšanju potrdil 15
3.3.2 Preverjanje imetnikov za ponovno pridobitev potrdila po preklicu 15

3.4. Preverjanje istovetnosti ob zahtevi za preklic 16

4. UPRAVLJANJE S POTRDILI 16

4.1. Pridobitev potrdila 16
4.1.1 Kdo lahko pridobi potrdilo 16
4.1.2 Postopek bodočega imetnika za pridobitev potrdila in odgovornosti 16

4.2. Postopek ob sprejemu zahtevka za pridobitev potrdila 16
4.2.1 Preverjanje istovetnosti bodočega imetnika 16
4.2.2 Odobritev/zavrnitev zahtevka 17
4.2.3 Čas za izdajo potrdila 17

4.3. Izdaja potrdila 17
4.3.1 Postopek overitelja Halcom CA 17
4.3.2 Obvestilo imetnika o izdaji 17

4.4. Prevzem potrdila 17
4.4.1 Postopek prevzema potrdila 17
4.4.2 Objava potrdila 18
4.4.3 Obvestilo overitelja o izdaji potrdila tretjim osebam 18

4.5. Obveznosti in odgovornosti uporabnikov glede uporabe potrdil 18
4.5.1 Obveznosti imetnika potrdila 18
4.5.2 Obveznosti za tretje osebe 18

4.6. Ponovna izdaja potrdila 19
4.6.1 Okoliščine, ki terjajo ponovno izdajo potrdila 19
4.6.2 Osebe, ki lahko zahtevajo podaljšanje potrdila 19
4.6.3 Postopek obravnave prošenj za ponovno izdajo potrdila 19
4.6.4 Obvestilo imetniku o novo izdanem potrdilu 19
4.6.5 Postopek prevzema novo izdanega potrdila 19
4.6.6 Objava novo izdanega potrdila 19
4.6.7 Obvestilo overitelja o izdaji potrdila tretjim osebam 19

4.7. Regeneriranje ključev 20
4.7.1 Razlogi za regeneracijo 20
4.7.2 Kdo zahteva regeneracijo 20
4.7.3 Postopek za izdajo zahtevka za regeneracijo 20
4.7.4 Obvestilo imetniku potrdila o novo izdanem potrdilu 20
4.7.5 Postopek prevzema 20
4.7.6 Objava potrdila overitelja z novima paroma ključev 20
4.7.7 Obvestilo overitelja o izdaji potrdila tretjim osebam 20

4.8. Sprememba potrdila 20
4.8.1 Okoliščina za spremembo potrdila 21
4.8.2 Kdo zahteva spremembo 21
4.8.3 Postopek ob zahtevku za spremembo 21
4.8.4 Obvestilo o izdaji novega potrdila 21
4.8.5 Prevzem spremenjenega potrdila 21
4.8.6 Objava spremenjenega potrdila 21
4.8.7 Obvestilo drugih subjektov o spremembi 21

4.9. Preklic in suspenz potrdila 21
4.9.1 Razlogi za preklic 22

4.9.2 Kdo zahteva preklic ... 22
4.9.3 Postopki za preklic ... 22
4.9.4 Čas za izdajo zahtevka za preklic ... 23
4.9.5 Čas od prejetega zahtevka za preklic do izvedbe preklica ... 23
4.9.6 Zahteve po preverjanju registra preklicanih potrdil za tretje osebe ... 23
4.9.7 Pogostnost objave registra preklicanih potrdil ... 23
4.9.8 Čas objave registra preklicanih potrdil ... 23
4.9.9 Sprotno preverjanje statusa potrdil ... 23
4.9.10 Zahteve za sprotno preverjanje statusa potrdil ... 23
4.9.11 Drugi načini za dostop do statusa potrdil ... 23
4.9.12 Posebne zahteve pri zlorabi zasebnega ključa ... 24
4.9.13 Razlogi za suspenz ... 24
4.9.14 Kdo zahteva suspenz ... 24
4.9.15 Postopek za suspenz ... 24
4.9.16 Čas suspenza ... 24

4.10. Preverjanje statusa potrdil ... 24
4.10.1 Dostop za preverjanje ... 24
4.10.2 Razpoložljivost ... 24
4.10.3 Druge informacije za preverjanje statusa ... 24

4.11. Prekinitev razmerja med imetnikom in overiteljem ... 24

4.12. Odkrivanje kopije ključev za dešifriranje ... 24
4.12.1 Razlogi za odkrivanje kopije ključev za dešifriranje ... 24
4.12.2 Kdo zahteva odkrivanje kopije ključev za dešifriranje ... 25
4.12.3 Postopek ob zahtevku za odkrivanje kopije ključev za dešifriranje ... 25

5. UPRAVLJANJE IN VARNOSTNI NADZOR INFRASTRUKTURE ... 25

5.1. Fizično varovanje ... 25
5.1.1 Lokacija in zgradba overitelja ... 25
5.1.2 Fizični dostop do infrastrukture overitelja ... 25
5.1.3 Napajanje in prezračevanje ... 26
5.1.4 Zaščita pred poplavo ... 26
5.1.5 Zaščita pred požari ... 26
5.1.6 Hramba nosilcev podatkov ... 26
5.1.7 Odstranjevanje odpadkov ... 26
5.1.8 Hramba na oddaljeni lokaciji ... 26

5.2. Organizacijska struktura overitelja ... 26
5.2.1 Organizacijske skupine ... 26
5.2.2 Število oseb za posamezne naloge ... 27
5.2.3 Izkazovanje istovetnosti za opravljanje posameznih nalog ... 28
5.2.4 Nezdružljivost nalog ... 29

5.3. Nadzor nad osebjem ... 29
5.3.1 Potrebne kvalifikacije in izkušnje osebja ... 29
5.3.2 Primernost osebja ... 29
5.3.3 Dodatno usposabljanje osebja ... 29
5.3.4 Zahteve za redna usposabljanja ... 29
5.3.5 Menjava nalog ... 29
5.3.6 Sankcije ... 29
5.3.7 Zahteve za zunanje izvajalce ... 29
5.3.8 Dostop osebja do dokumentacije ... 30

5.4. Varnostni pregledi sistema ... 30
5.4.1 Vrste dnevnikov ... 30
5.4.2 Pogostnost pregledov dnevnikov ... 30

5.4.3 Čas hrambe dnevnikov ... 30
5.4.4 Zaščita dnevnikov ... 30
5.4.5 Varnostne kopije dnevnikov ... 30
5.4.6 Zbiranje podatkov za dnevnike ... 30
5.4.7 Obveščanje povzročitelja dogodka ... 30
5.4.8 Ocena ranljivosti sistema ... 30

5.5. Dolgoročna hramba podatkov ... 31
5.5.1 Vrste dolgoročno hranjenih podatkov ... 31
5.5.2 Rok hrambe ... 31
5.5.3 Zaščita dolgoročno hranjenih podatkov ... 31
5.5.4 Varnostna kopija dolgoročno hranjenih podatkov ... 31
5.5.5 Zahteva po časovnem žigosanju ... 31
5.5.6 Način zbiranja podatkov ... 31
5.5.7 Postopek za dostop do dolgoročno hranjenih podatkov in njihova verifikacija ... 31

5.6. Sprememba javnega ključa overitelja Halcom CA ... 31

5.7. Okrevalni načrt ... 32
5.7.1 Postopek v primeru vdorov in zlorabe ... 32
5.7.2 Postopek v primeru okvare programske opreme, podatkov ... 32
5.7.3 Postopek v primeru ogroženega zasebnega ključa overitelja Halcom CA ... 32
5.7.4 Okrevalni načrt ... 32

5.8. Prenehanje delovanja Halcom CA ... 32

6. TEHNIČNE VARNOSTNE ZAHTEVE ... 32

6.1. Generiranje in namestitev ključev ... 32
6.1.1 Generiranje ključev ... 32
6.1.2 Dostava zasebnega ključa imetnikom ... 32
6.1.3 Dostava javnega ključa overitelju potrdil ... 33
6.1.4 Dostava overiteljevih javnih ključev ... 33
6.1.5 Dolžina ključev ... 33
6.1.6 Generiranje in kakovost parametrov javnih ključev ... 33
6.1.7 Namen ključev in potrdil ... 33

6.2. Zaščita zasebnega ključa ... 33
6.2.1 Standardi za kriptografski modul ... 33
6.2.2 Nadzor zasebnega ključa s strani pooblaščenih oseb ... 33
6.2.3 Odkrivanje kopije zasebnega ključa ... 33
6.2.4 Varnostna kopija zasebnega ključa ... 34
6.2.5 Arhiviranje zasebnega ključa ... 34
6.2.6 Prenos zasebnega ključa iz/v kriptografski modul ... 34
6.2.7 Hramba zasebnega ključa v kriptografskem modulu ... 34
6.2.8 Postopek za aktiviranje zasebnega ključa ... 34
6.2.9 Postopek za deaktiviranje zasebnega ključa ... 34
6.2.10 Postopek za uničenje zasebnega ključa ... 34
6.2.11 Lastnosti kriptografskega modula ... 34

6.3. Ostali aspekti upravljanja ključev ... 34
6.3.1 Arhiviranje javnega ključa ... 35
6.3.2 Obdobje veljavnosti za javne in zasebne ključe ... 35

6.4. Gesla za dostop do potrdil oz. ključev ... 35
6.4.1 Generiranje gesel ... 35
6.4.2 Zaščita gesel ... 35
6.4.3 Drugi aspekti gesel ... 35

6.5. Varnostne zahteve za informacijsko-komunikacijsko opremo overitelja 35
6.5.1 Specifične tehnične varnostne zahteve 35
6.5.2 Nivo varnostne zaščite 35

6.6. Tehnični nadzor življenjskega cikla overitelja 36
6.6.1 Nadzor razvoja sistema 36
6.6.2 Upravljanje varnosti 36
6.6.3 Nadzor življenjskega cikla 36

6.7. Varnostna kontrola omrežja 36

6.8. Časovno žigosanje 36

7. PROFIL POTRDIL IN REGISTRA PREKLICANIH POTRDIL 36

7.1. Profil potrdil 36
7.1.1 Različica potrdil 36
7.1.2 Profil potrdil z razširitvami 36
7.1.2.1 Zahteve za elektronski naslov 38
7.1.3 Identifikacijske oznake algoritmov 39
7.1.4 Oblika razločevalnih imen 39
7.1.5 Omejitve glede imen 39
7.1.6 Označba politike potrdila 39
7.1.7 Omejitve uporabe 39
7.1.8 Sintaksa in pomen označb politike potrdil 39
7.1.9 Pomen bistvenih dodatkov politike 39

7.2. Profil registra preklicanih potrdil 39
7.2.1 Različica 40
7.2.2 Vsebina registra in razširitve 40
7.2.3 Objava registra preklicanih potrdil 41

7.3. Profil sprotnega preverjanja statusa potrdil 41
7.3.1 Verzija sprotnega preverjanje statusa 41
7.3.2 Profil sprotnega preverjanje statusa 41

8. NADZOR 41

8.1. Pogostnost nadzora 41

8.2. Vrsta in usposobljenost nadzora 41

8.3. Neodvisnost nadzora 42

8.4. Področja nadzora 42

8.5. Ukrepi overitelja 42

8.6. Objava rezultatov nadzora 42

9. FINANČNE IN OSTALE PRAVNE ZADEVE 42

9.1. Cenik 42
9.1.1 Cena izdaje potrdil in podaljšanja 42
9.1.2 Cena dostopa do potrdil 42
9.1.3 Cena dostopa do statusa potrdila in registra preklicanih potrdil 42
9.1.4 Cene drugih storitev 42
9.1.5 Povrnitev stroškov 42

9.2. Finančna odgovornost 42
9.2.1 Zavarovalniško kritje 43
9.2.2 Drugo kritje 43
9.2.3 Zavarovanje imetnikov 43

9.3. Varovanje poslovnih podatkov 43
9.3.1 Varovani podatki 43
9.3.2 Nevarovani podatki 43
9.3.3 Odgovornost glede varovanja 43

9.4. Varovanje osebnih podatkov 43
9.4.1 Načrt varovanja osebnih podatkov 43
9.4.2 Varovani osebni podatki 43
9.4.3 Nevarovani osebni podatki 44
9.4.4 Odgovornost glede varovanja osebnih podatkov 44
9.4.5 Pooblastilo glede uporabe osebnih podatkov 44
9.4.6 Posredovanje osebnih podatkov 44
9.4.7 Druga določila glede varovanja osebnih podatkov 44

9.5. Določbe glede pravic intelektualne lastnine 44

9.6. Obveznosti in odgovornosti 44
9.6.1 Obveznosti in odgovornosti overitelja Halcom CA 44
9.6.2 Obveznost in odgovornost prijavne službe 45
9.6.3 Obveznosti in odgovornost imetnika potrdila 45
9.6.4 Obveznosti in odgovornost tretjih oseb 46
9.6.5 Obveznosti in odgovornost drugih oseb 46

9.7. Omejitev odgovornosti 46

9.8. Omejitev glede uporabe 47

9.9. Poravnava škode 47

9.10. Veljavnost politike 47
9.10.1 Čas veljavnosti 47
9.10.2 Konec veljavnosti politike 47
9.10.3 Učinek poteka veljavnosti politike 47

9.11. Komuniciranje med subjekti 47

9.12. Spremembe in dopolnitve 48
9.12.1 Postopek za sprejem sprememb in dopolnitev 48
9.12.2 Veljavnost in objava sprememb in dopolnitev 48
9.12.3 Sprememba identifikacijske številke politike 48

9.13. Postopek v primeru sporov 48

9.14. Veljavna zakonodaja 48

9.15. Skladnost z veljavno zakonodajo 48

9.16. Splošne določbe 48

9.17. Druge določbe 48

1. UVOD

(1) Ta politika je javni del notranjih pravil Halcom CA za strežniška digitalna potrdila za poslovne subjekte (pravne osebe, samostojne podjetnike in druge fizične osebe registrirane za opravljanje dejavnosti).

(2) Oblika in vsebina te politike je usklajena z mednarodnim priporočilom RFC in evropskimi standardi ETSI in drugimi.

1.1. Pregled

(1) Ta politika predstavlja nedeljivo celoto javnega dela notranjih pravil overitelja Halcom CA glede izdaje digitalnih potrdil, ureja namen, delovanje in metodologijo upravljanja digitalnih potrdil ter varnostne zahteve, ki jih morajo izpolnjevati overitelj Halcom CA, imetniki potrdil, tretje osebe, ki se zanašajo na ta potrdila, ter odgovornost vseh naštetih oseb.

(2) Halcom CA je overitelj, ki izdaja in upravlja s digitalnimi potrdili za overjanje elektronskega podpisa. Halcom CA deluje tudi kot glavni overitelj, ki skupaj s svojimi podrejenimi overitelji sestavlja hierarhično mrežo overiteljev, ki je namenjena izdajanju poslovnih potrdil in opravljanju tehnoloških storitev v zvezi z varnimi elektronskimi podpisi. Overitelj Halcom CA deluje v okviru Halcom d.d.

(3) Halcom CA izdaja strežniška digitalna potrdila z enim parom ključev.

(4) Vse določbe te politike glede ravnanja Halcom CA so ustrezno prenesene in podrobneje opredeljene v določbah notranjega dela politike, ki predstavlja zaupni del notranjih pravil in ga sestavljajo dokumenti zaupne narave, 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 overitelja v skladu z veljavnim pravnim redom Republike Slovenije in Evropske unije, ter v skladu s tehničnimi zahtevami ETSI, standardom RFC in družino standardov ISO/IEC ter drugih sorodnih standardov.

(6) Seznam prijavnih služb in operaterjev, ki omogočajo pridobitev digitalnih potrdil za poslovne subjekte, Halcom CA objavi na svojih spletnih straneh.

1.2. Identifikacijski podatki politike

(1) Oznaka te politike delovanja Halcom Secure Server CA 1 je:

CPOID:1.3.6.1.4.1.5939.5.2.3

V vsakem potrdilu je navedba politike v obliki oznake CPOID, (glej razd. 7.1.2).

1.3. Subjekti

1.3.1 Overitelj Halcom CA

Halcom CA je overitelj, ki izdaja in upravlja s digitalnimi potrdili za overjanje elektronskega podpisa. Halcom CA deluje tudi kot glavni overitelj, ki skupaj s svojimi podrejenimi overitelji sestavlja hierarhično mrežo overiteljev, ki je namenjena izdajanju osebnih potrdil in opravljanju tehnoloških storitev v zvezi z varnimi elektronskimi podpisi. Overitelj Halcom CA deluje v okviru Halcom d.d.

1.3.2 Prijavna služba Halcom CA

(1) Prijavna služba za overitelja izvaja naslednje naloge:

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

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

(3) Overitelj Halcom CA ima vzpostavljeno geografsko razpršeno prijavno službo, kar bodočim imetnikom omogoča enostavno prijavo v domačem ali bližnjem kraju. Informacije o lokacijah prijavnih služb so dostopne na spletnih straneh overitelja Halcom CA.

1.3.3 Imetniki potrdil

Imetniki potrdil uporabljajo svoje, od overitelja dodeljene, podatke (par ključev) za varno elektronsko podpisovanje in digitalna potrdila za overitev tega elektronskega podpisa.

1.3.4 Tretje osebe

(1) Tretje osebe so osebe, ki se zanašajo na izdana potrdila overitelja Halcom CA, in so lahko fizične ali pravne osebe.

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

(3) Tretje osebe niso nujno tudi imetniki potrdil overitelja Halcom CA ali digitalnih potrdil drugih overiteljev.

1.4. Namen uporabe

Halcom CA upravlja (izdaja in overja, preklicuje, podaljšuje, hrani, objavlja) s strežniškimi digitalnimi potrdili za overjanje elektronskega podpisa (v nadaljevanju potrdila), ki so namenjena poslovnim subjektom.

1.4.1 Pravilna uporaba potrdil in ključev

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

1) identifikacija strežnika,
2) izkazovanje istovetnosti strežnika,
3) kontrola dostopa,
4) vzpostavitev varnih povezav,
5) podpisovanje dokumentov v elektronski obliki,
6) šifriranje in dešifriranje dokumentov ali podatkov v elektronski obliki.

1.4.2 Nedovoljena uporaba

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

(2) Potrdila niso namenjena nadaljnji prodaji.

1.5. Upravljanje politike

1.5.1 Upravljavec politik

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

(2) Naslov upravljavca:

Halcom d.d.
Tržaška 118
1000 LJUBLJANA
Slovenija

1.5.2 Pooblaščene kontaktne osebe

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

(2) Naslov Halcom CA:

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

1.5.3 Odgovorna oseba glede skladnosti delovanja overitelja Halcom CA s politiko

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

1.5.4 Postopek za sprejem nove politike

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

(2) Overitelj 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	Overitelj potrdil (angl.: Certificate Authority ali Certificate Agency).
CPName	Ime politike delovanja overitelja (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).
LDAP	Leightweight Directory Access Protocol je protokol, ki določa dostop do imenika in je specificiran po IETF (Internet Engineering Task Force) priporočilu RFC 1777.
S/MIME	Secure Multipurpose Internet Mail Extensions
SSL	Secure Sockets Layer
TLS	Transport Layer Security
PKI	Public Key Infrastructure je infrastruktura javnih ključev.
WPKI	Wireless Public Key Infrastructure je infrastruktura javnih ključev, ki deluje preko brezžičnih povezav (npr. mobilnih telefonov in naprav).

1.6.2 Izrazi

Imenik potrdil	Imenik potrdil po priporočilu X.500, kjer so shranjena potrdila po priporočilu X.509 ver. 3, do katerih je možen dostop po protokolu LDAP.
Identifikacija	Identifikacija je ugotavljanje identitete osebe, ki se izvaja osebno s pomočjo veljavnega osebnega dokumenta ali v elektronski obliki s pomočjo veljavnega digitalnega potrdila.
Overitelj potrdila	Fizična ali pravna oseba, ki izdaja potrdila ali opravlja druge storitve v zvezi z overjanjem ali elektronskimi podpisi (angl.: Certification Authority - CA).
Prijavna služba	Služba ali oseba, ki sprejema vloge za potrdila in prevzema identificiranje in preverjanje istovetnosti bodočih imetnikov v imenu overitelja potrdil (angl.: Registration Authority - RA).
Razločevalno ime	Enolično ime v potrdilu (prim. opredelitev DN), ki nedvoumno in enolično definira uporabnika v strukturi imenika.

2. OBJAVE INFORMACIJ IN JAVNI IMENIK

POTRDIL

2.1. Zbirka dokumentov

(1) Overitelj 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.

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

- cenik,
- politike overitelja (CP/CPS),
- naročilnice in druge pogodbe za storitve overitelja,
- navodila za varno uporabo digitalnih potrdil,
- informacije o veljavnih predpisih in standardih v zvezi z delovanjem overitelja ter
- ostale informacije v zvezi z delovanjem Halcom CA.

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

2.2. Javni imenik potrdil

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

(2) Vsa potrdila overitelja temeljijo na standardu X.509 in so objavljena v centralnem imeniku na strežniku ldap.halcom.si, ki je v skrbništvu HALCOM CA. Javno dostopen je le register preklicanih potrdil, ki je del imenika ter korensko (Root) in vmesno/podrejeno (Intermediate) potrdilo overitelja.

(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 uporabniški 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 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 ter korensko (Root) in vmesno/podrejeno (Intermediate) potrdilo overitelja.

(2) Z ustreznimi tehničnimi ukrepi informacijske varnosti Halcom CA zagotavlja kontrole,

ki preprečujejo nepooblaščeno pregledovanje, dodajanje, spreminjanje ali brisanje podatkov v centralnem 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 digitalnega potrdila.

3.1.1 Razločevalna imena

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

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

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

Vrsta potrdila	Naziv polja	Razločevalno ime
Korensko (Root) potrdilo overitelja Halcom CA	Izdajatelj, angl. Issuer	C= SI O= Halcom CN= Halcom Root CA
Vmesno/podrejeno (Intermediate) potrdilo overitelja Halcom CA	Izdajatelj, angl. Issuer	C= SI O= Halcom CN= Halcom Secure Server CA 1
Strežniško potrdilo uporabnika	Nosilec, angl. Subject	2.5.4.45 =<enolična interna številka potrdila> C= SI O=<naziv poslovnega subjekta> OU= server certificates CN=<ime strežnika in domena> SN= <domena> G= <ime strežnika> E = <e-pošta>

3.1.2 Zahteve pri tvorbi razločevalnega imena

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

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

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

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

- da je v nasprotju z veljavnimi predpisi.

3.1.3 Uporaba anonimnih imen ali psevdonimov

Po tej politiki Halcom CA potrdil ne izdaja na anonimna imena ali psevdonime.

3.1.4 Pravila za interpretacijo razločevalnih imen

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

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

Z ustrezno kombinacijo črk overitelj zagotovi uporabo drugih nepredvidenih znakov.

3.1.5 Enoličnost razločevalnih imen

Razločevalna imena so enolična za vsako izdano potrdilo in nedvoumno in enolično identificirajo imetnika v strukturi imenika.

3.1.6 Zaščite imen oz. znamk

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

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

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

3.2. Preverjanje istovetnosti imetnikov ob prvi izdaji potrdila

3.2.1 Metoda za posedovanje pripadnosti zasebnega ključa

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

3.2.2 Preverjanje istovetnosti organizacije

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

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

(3) Overitelj Halcom CA pri ustreznih službah, uradnih evidencah ali s pomočjo veljavnega izpisa iz ustreznih registrov preveri pravilnost podatkov poslovnega subjekta in istovetnost odgovorne osebe.

3.2.3 Preverjanje istovetnosti imetnika

(1) Poslovni subjekt zagotavlja, da bo nesporno ugotovil istovetnost imetnikov potrdil (skrbnik strežnika) v skladu z veljavnimi predpisi (uradni dokument s sliko).

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

3.2.4 Nepreverjeni podatki v potrdilih

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

3.2.5 Preverjanje pooblastil zaposlenih za pridobitev potrdil

Zakoniti zastopnik poslovnega subjekta s podpisom na dokumentaciji za pridobitev potrdila jamči, da želi za določeno osebo (skrbnik strežnika), ki je zaposlena ali opravlja naloge za ta poslovni subjekt, pridobiti ustrezno potrdilo.

3.2.6 Medsebojno priznavanje

(1) Overitelj Halcom CA ni dolžan pogodbeno sodelovati ali jamčiti za druge overitelje tudi, če ima drugi overitelj status akreditiranega overitelja ali overitelja digitalnih potrdil.

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

(3) Pooblaščene osebe overitelja Halcom CA pregledujejo notranja pravila drugega overitelja ter njegovo izpolnjevanje varnostnih zahtev.

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

3.3. Preverjanje imetnikov za ponovno izdajo potrdila

3.3.1 Preverjanje imetnikov pri podaljšanju potrdil

Istovetnost imetnikov pri ponovni izdaji potrdila se preverja:

- na prijavni službi overitelja Halcom CA
- na podlagi že izdanega veljavnega digitalnega potrdila, ki ga je izdal overitelj Halcom CA, pri čemer overitelj Halcom CA preveri podatke poslovnega subjekta in imetnika v ustreznih registrih.

3.3.2 Preverjanje imetnikov za ponovno pridobitev potrdila po preklicu

Preverjanje imetnikov poteka skladno z določili iz razd. 3.2.3.

3.4. Preverjanje istovetnosti ob zahtevi za preklic

(1) Zahtevek za preklic potrdila poslovni subjekt odda:

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

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

4. UPRAVLJANJE S POTRDILI

4.1. Pridobitev potrdila

4.1.1 Kdo lahko pridobi potrdilo

Bodoči imetniki potrdil izdanih po tej politiki so poslovni subjekti ali fizične osebe.

4.1.2 Postopek bodočega imetnika za pridobitev potrdila in odgovornosti

(1) Potrdilo se izda na osnovi pravilno izpolnjene in podpisane naročilnice za izdajo strežniških potrdil (v nadaljevanju naročilnica) s strani zakonitega zastopnika poslovnega subjekta in skrbnika strežnika. Vlogo zakoniti zastopnik odda prijavni službi Halcom CA, ter poravna finančne obveznosti v zvezi z izdajo potrdila. Naročilnice za izdajo digitalnega potrdila so na voljo pri prijavnih službah Halcom CA in na spletni strani Halcom CA. Cenik storitev je javno objavljen na spletnih straneh Halcom CA.

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

(3) Pred izdajo potrdila Halcom CA poslovni subjekt in bodočega imetnika seznani s to politiko, splošnimi pogoji delovanja in delovanju overitelja Halcom CA.

(4) Halcom CA si pridružuje pravico do zavrnitve vloge za izdajo potrdila brez obrazložitve.

4.2. Postopek ob sprejemu zahtevka za pridobitev potrdila

4.2.1 Preverjanje istovetnosti bodočega imetnika

(1) Pooblaščena oseba na prijavni službi preveri istovetnost zakonitega zastopnika, če gre za primer osebne oddaje naročilnice na prijavni službi overitelja. Zakoniti zastopnik mora izkazati svojo istovetnost z veljavnim osebnim dokumentom s sliko.

(2) V primeru oddaje naročilnice na elektronski način pooblaščena oseba overitelja Halcom CA opravi overjanje elektronskega podpisa. Istovetnost bodočega imetnika se izkaže z veljavnostjo njegovega elektronskega podpisa.

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

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

4.2.2 Odobritev/zavrnitev zahtevka

(1) Halcom CA na podlagi prejete dokumentacije pri pooblaščenem registrarju domen preveri lastništvo domene, katero je pooblaščena oseba poslovnega subjekta navedla na zahtevku in za katero poslovnemu subjektu izdaja potrdilo.

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

(3) V primeru odobritve overitelj Halcom CA pred izdajo potrdila obvesti bodočega imetnika z vso potrebno dokumentacijo.

4.2.3 Čas za izdajo potrdila

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

4.3. Izdaja potrdila

4.3.1 Postopek overitelja Halcom CA

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

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

4.3.2 Obvestilo imetnika o izdaji

Glej prejšnji razdelek.

4.4. Prevzem potrdila

4.4.1 Postopek prevzema potrdila

(1) Poslovni subjekt na strežniku sproži generacijo ključev in določi geslo za zaščito le-teh.

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

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

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

4.4.2 Objava potrdila

Postopek je opisan v 2. razdelku

4.4.3 Obvestilo overitelja o izdaji potrdila tretjim osebam

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

4.5. Obveznosti in odgovornosti uporabnikov glede uporabe potrdil

4.5.1 Obveznosti imetnika potrdila

(1) Imetnik oziroma bodoči imetnik potrdila je dolžan:

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

(2) Imetnik oziroma bodoči imetnik potrdila je glede varovanja zasebnega ključa dolžan tudi:

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

4.5.2 Obveznosti za tretje osebe

(1) Tretja oseba, ki se zanaša na potrdilo, mora:

- ravnati in uporabljati potrdila v skladu in namenom s politiko in ostalimi veljavnimi predpisi,
- skrbno proučiti vse možnosti tveganja in odgovornosti pri uporabi potrdil in določiti politiko za način uporabe,
- obvestiti Halcom CA, če izve, da je bil zasebni ključ imetnika potrdila, na katerega

se zanaša, ogrožen na način, ki vpliva na zanesljivost uporabe, ali če obstaja nevarnost zlorabe, ali če so se spremenili podatki, navedeni v potrdilu,
- skrbeti za arhiv dokumentov,
- 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 overitelja potrdila Halcom CA, ki je objavljen v tej politiki in tudi na spletnih straneh Halcom CA oz. drugih overiteljev potrdil.
- upoštevati druge določbe, v kolikor je z overiteljem Halcom CA sklenila dogovor o uporabi potrdil.

(2) Tretja oseba mora za overjanje 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

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

4.6.1 Okoliščine, ki terjajo ponovno izdajo potrdila

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

4.6.2 Osebe, ki lahko zahtevajo podaljšanje potrdila

Podaljševanje veljavnosti potrdila ni mogoče.

4.6.3 Postopek obravnave prošenj za ponovno izdajo potrdila

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

4.6.4 Obvestilo imetniku o novo izdanem potrdilu

Glej razd. 4.3.2.

4.6.5 Postopek prevzema novo izdanega potrdila

Glej razd. 4.4.1.

4.6.6 Objava novo izdanega potrdila

Postopek je opisan v 2. razdelku.

4.6.7 Obvestilo overitelja o izdaji potrdila tretjim osebam

Overitelj Halcom CA o izdaji posameznega potrdila imetnikom potrdila ne obvešča tretjih

oseb. Prijavna služba lahko pridobi podatek o izdaji potrdil, za katere je sprejela vloge za izdajo.

4.7. Regeneriranje ključev

4.7.1 Razlogi za regeneracijo

Pred potekom veljavnosti digitalnega potrdila si z zahtevkom za novo izdajo imetniki potrdil lahko zagotovijo kontinuiteto uporabe digitalnega potrdila. Zahtevek za novo izdajo je mogoče vložiti tudi po poteku veljavnosti digitalnega potrdila.

4.7.2 Kdo zahteva regeneracijo

Regeneracija ključev je mogoča samo na prošnjo imetnika potrdila.

4.7.3 Postopek za izdajo zahtevka za regeneracijo

(1) Imetnik potrdila lahko pred iztekom veljavnosti potrdila zaprosi za izdajo novega digitalnega potrdila.

(2) Poslovni subjekt na strežniku sproži generacijo ključev in določi geslo za zaščito le-teh.

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

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

4.7.4 Obvestilo imetniku potrdila o novo izdanem potrdilu

Halcom CA o izdaji novega potrdila imetnika obvesti po elektronski pošti.

4.7.5 Postopek prevzema

Potrdilo imetniku posreduje z elektronsko pošto.

4.7.6 Objava potrdila overitelja z novima paroma ključev

Halcom CA poskrbi, da se potrdila objavijo v centralnem imeniku takoj po njihovi izdaji.

4.7.7 Obvestilo overitelja o izdaji potrdila tretjim osebam

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

4.8. Sprememba potrdila

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

(2) Za pridobitev novega potrdila je potrebno ponoviti postopek za pridobitev novega

potrdila, kot je naveden v razdelku 4.1.

4.8.1 Okoliščina za spremembo potrdila

Ni podprta.

4.8.2 Kdo zahteva spremembo

Ni podprto.

4.8.3 Postopek ob zahtevku za spremembo

Ni podprt.

4.8.4 Obvestilo o izdaji novega potrdila

Ni podprto.

4.8.5 Prevzem spremenjenega potrdila

Ni podprt.

4.8.6 Objava spremenjenega potrdila

Ni podprta.

4.8.7 Obvestilo drugih subjektov o spremembi

Ni podprto.

4.9. Preklic in suspenz potrdila

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

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

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

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

(4) Halcom CA bo na podlagi pravilne zahteve za preklic potrdila potrdilo preklical najkasneje v štirih (4) urah. V primeru nastanka nepredvidljivih okoliščin bo Halcom CA izjemoma preklical potrdilo najkasneje v 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, bo obveščen o nepravilni zahtevi za preklic potrdila in bo seznanjen z navodili za vložitev pravilne zahteve za preklic.

4.9.1 Razlogi za preklic

(1) Preklic potrdila mora poslovni subjekt ali imetnik zahtevati v primeru:

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

(2) Overitelj Halcom CA prekliče potrdilo tudi brez zahteve imetnika takoj, ko izve:

- da je podatek v potrdilu napačen ali je bilo potrdilo izdano na podlagi napačnih podatkov,
- da je prišlo do napake pri preverjanju istovetnosti podatkov na prijavni službi,
- da so se spremenile druge okoliščine, ki vplivajo na veljavnost potrdila,
- za neizpolnjevanje obveznosti imetnika,
- da niso poravnani morebitni stroški za upravljanje digitalnih potrdil,
- da je bila infrastruktura overitelja ogrožena na način, ki vpliva na zanesljivost potrdila,
- da je bil zasebni ključ imetnika potrdila ogrožen na način, ki vpliva na zanesljivost uporabe,
- da bo Halcom CA prenehal z izdajanjem potrdil ali da je bilo overitelju prepovedano upravljanje s potrdili in njegove dejavnosti ni prevzel drug overitelj,
- da je preklic odredilo pristojno sodišče, prekrškovni ali upravni organ.

4.9.2 Kdo zahteva preklic

Preklic potrdila lahko zahteva:

- pooblaščena oseba overitelja Halcom CA,
- zakoniti zastopnik poslovnega subjekta,
- imetnik (skrbnik strežniškega potrdila),
- pristojno sodišče, prekrškovni ali upravni organ.

4.9.3 Postopki za preklic

(1) Preklic lahko zakoniti zastopnik poslovnega subjekta ali imetnik zahteva:

- osebno v času uradnih ur na prijavni službi,
- elektronsko štiriindvajset (24) ur na dan vse dni v letu, če gre za možnost zlorabe ali nezanesljivosti potrdila, sicer v času, ki po veljavni zakonodaji velja za poslovni čas državnih organov,
- po faksu štiriindvajset (24) ur na dan vse dni v letu, če gre za možnost zlorabe ali nezanesljivosti potrdila, sicer v času, ki po veljavni zakonodaji velja za poslovni čas državnih organov,

(2) Če se preklic zahteva:

- osebno, je potrebno izpolniti ustrezen zahtevek za preklic potrdila ter ga oddati na prijavno službo;
- elektronsko, mora imetnik poslati na Halcom CA elektronsko sporočilo z zahtevkom za preklic, ki mora biti digitalno podpisan z zaupanja vrednim potrdilom za njegovo overjanje.
- po faksu, mora imetnik izpolniti ustrezen zahtevek za preklic potrdila ter ga poslati po FAX-u na ustrezno dežurno FAX št. (glej razd. 1.5.2.) in naknadno priporočeno poslati po pošti ali oddati na prijavno službo,
- če imetnik potrdila prek telefona, elektronske pošte ali FAX-a zahteva preklic potrdila, overitelj Halcom CA odredi suspenz potrdila. Šele na podlagi pisne zahteve za preklic potrdila, pa se dejansko izvede preklic potrdila.

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

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

4.9.4 Čas za izdajo zahtevka za preklic

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

4.9.5 Čas od prejetega zahtevka za preklic do izvedbe preklica

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

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

4.9.6 Zahteve po preverjanju registra preklicanih potrdil za tretje osebe

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

4.9.7 Pogostnost objave registra preklicanih potrdil

Register preklicanih potrdil se osvežuje (za dostop do registra glej razd. 7.2.3):
- po vsakem preklicu potrdila,
- enkrat dnevno, če ni novih zapisov oz. sprememb v registru preklicanih potrdil, in sicer približno štiriindvajset (24) ur po zadnjem osveževanju.

4.9.8 Čas objave registra preklicanih potrdil

Objava novega registra preklicanih potrdil se izvede:
- v javnem imeniku na strežniku ldap://ldap.halcom.si takoj,
- na spletni strani http://domina.halcom.si/crls pa z zakasnitvijo največ desetih (10) minut.

4.9.9 Sprotno preverjanje statusa potrdil

Protokol za sprotno preverjanje statusa OCSP (angl. Online Certificate Status Protocol) ni podprt.

4.9.10 Zahteve za sprotno preverjanje statusa potrdil

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

4.9.11 Drugi načini za dostop do statusa potrdil

Niso podprti.

4.9.12 Posebne zahteve pri zlorabi zasebnega ključa

Niso določene.

4.9.13 Razlogi za suspenz

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

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

4.9.14 Kdo zahteva suspenz

Glej razd. 4.9.13.

4.9.15 Postopek za suspenz

Glej razd. 4.9.13.

4.9.16 Čas suspenza

Glej razd. 4.9.13.

4.10. Preverjanje statusa potrdil

4.10.1 Dostop za preverjanje

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, podrobnosti o objavi in dostopu pa so v razd. 7.2 in 7.3.

4.10.2 Razpoložljivost

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

4.10.3 Druge informacije za preverjanje statusa

Niso predpisane.

4.11. Prekinitev razmerja med imetnikom in overiteljem

Razmerje med imetnikom oz. poslovnim subjektom in overiteljem se prekine, če

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

4.12. Odkrivanje kopije ključev za dešifriranje

4.12.1 Razlogi za odkrivanje kopije ključev za dešifriranje

Ni podprto.

4.12.2 Kdo zahteva odkrivanje kopije ključev za dešifriranje

Ni podprto.

4.12.3 Postopek ob zahtevku za odkrivanje kopije ključev za dešifriranje

Ni podprto.

5. UPRAVLJANJE IN VARNOSTNI NADZOR INFRASTRUKTURE

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

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

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

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

5.1. Fizično varovanje

(1) Oprema overitelja je varovana z večnivojskim sistemom fizičnega in elektronskega varovanja.

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

(3) Celoten opis infrastrukture overitelja in postopki upravljanja ter varovanje le-te so določeni z Interno politiko overitelja.

5.1.1 Lokacija in zgradba overitelja

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

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

(3) Podrobna določila so v Interni politiki overitelja Halcom CA.

5.1.2 Fizični dostop do infrastrukture overitelja

(1) Dostop do infrastrukture overitelja je omogočen samo pooblaščenim osebam overitelja 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 Interni politiki overitelja Halcom CA.

5.1.3 Napajanje in prezračevanje

(1) Infrastruktura overitelja ima zagotovljeno neprekinjeno napajanje in ustrezne klimatske sisteme.

(2) Podrobno o tem je določeno v Interni politiki overitelja Halcom CA.

5.1.4 Zaščita pred poplavo

(1) Infrastruktura overitelja ni izpostavljena nevarnosti poplav, razen v primeru višje sile.

(2) Podrobno o tem je določeno v Interni politiki overitelja Halcom CA.

5.1.5 Zaščita pred požari

(1) Prostori overitelja so varovani pred morebitnim izbruhom požara.

(2) Podrobno o tem je določeno v Interni politiki overitelja 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 overitelja 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 Interno politiko overitelja Halcom CA.

(3) Podrobno o tem je določeno v Splošnih pogojih delovanja in Interni politiki overitelja Halcom CA.

5.1.8 Hramba na oddaljeni lokaciji

Glej razd. 5.1.6.

5.2. Organizacijska struktura overitelja

5.2.1 Organizacijske skupine

(1) Operativno, organizacijsko in strokovno pravilno delovanje overitelja Halcom CA vodi vodja notranje organizacijske enote, ki je odgovorna za upravljanje digitalnih potrdil.

(2) Med pooblaščene osebe overitelja Halcom CA spadajo:

- zaposleni pri overitelju Halcom CA in

- prijavne službe.

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

Organizacijska skupina	Vloga	Osnovne naloge	Število oseb
Upravljanje z informacijskim sistemom	Upravljavec sistema	• Strategija delovanja overitelja Halcom CA • Določevanje prvega varnostnega inženirja • Operativno vodenje overitelja Halcom CA	2
Upravljanje s potrdili	Prvi varnostni inženir	• Določevanje in izvajanje pravil varnega delovanja sistema za podeljevanje potrdil • Določevanje drugih varnostnih inženirjev	2
	Drugi varnostni inženirji	• Določevanje in izvajanje pravil varnega delovanja sistema za podeljevanje potrdil	2
	Administratorji potrdil	• Upravljanje s potrdili	2
	Administratorji PIN kod	• Distribucija PIN kod	2
Varovanje in kontrola	Varnostni administrator	• Upravljanje s telekomunikacijami (sistem za preprečevanje in odkrivanje vdorov, požarna pregrada, ...) • Vzdrževanje varnostnih kopij	2
Pravno-administrativno	Pravnik		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, med seboj nezdružljive organizacijske skupine:

Organizacijska skupina: Upravljanje z informacijskim sistemom
Vloga: Upravljavec informacijskega sistema
Število oseb: 2
Naloge:
1. Priprava začetne konfiguracije sistema, vključno z varnim zagonom in ustavitvijo delovanja sistema
2. Začetna nastavitev parametrov novih podrejenih overiteljev
3. Postavitev začetne konfiguracije omrežja
4. Priprava nosilcev podatkov za zasilni ponovni start sistema v primeru katastrofalne izgube sistema
5. Priprava sistemskih kopij, nadgradnja in obnovitev programske opreme, varno shranjevanje in distribucija kopij in nadgradenj na ločeno lokacijo
6. Administrativne funkcije, ki so povezane z vzdrževanjem baze podatkov overitelja in ki pomagajo pri raziskavah odstopanj od pravil
7. Spremembe imena strežnika in/ali omrežnega naslova

8. Izvajanje arhiviranja zahtevanih sistemskih zapisov

Organizacijska skupina: Varovanje in kontrola
Vloga: Prvi varnostni inženir
Število oseb: 2
Naloge:
1. Upravljanje postopkov za izdajo potrdil
2. Pomoč podrejenim overiteljem
3. Pooblaščanje podrejenih overiteljev
4. Izpis PIN kod
5. Dostop do protokola podpisovanja potrdil

Organizacijska skupina: Upravljanje s potrdili
Vloga: Drugi varnostni inženir
Število oseb: 2
Naloge:
1. Priprava potrdil (obdelava podpisanih zahtev za potrdila)
2. Poosebljanje (izdelava potrdil, zapis na varni nosilec, tiskanje imetnikovih podatkov na varni nosilec)
3. Preklic potrdil

Organizacijska skupina: Upravljanje s potrdili
Vloga: Administrator potrdil
Število oseb: 2
Naloge:
1. Identifikacija imetnikov potrdil
2. Varna distribucija potrdil imetnikom
3. Priprava zahtev za preklic potrdil

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

Organizacijska skupina: Varovanje in kontrola
Vloga: Uslužbenec za varnost informacijskega sistema
Število oseb: 2
Naloge:
1. Določanje varnostnih pravil in nadzor njihovega upoštevanja
2. Pregledovanje sistemske dokumentacije in kontrolnih dnevnikov za nadzor dela
3. Osebno sodelovanje in pomoč pri letni inventuri dokumentacije podrejenih overiteljev

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

5.2.3 Izkazovanje istovetnosti za opravljanje posameznih nalog

Izkazovanje istovetnosti in pravice dostopov za opravljanje posameznih nalog skladno z vlogo posamezne organizacijske skupine kot tudi za opravljanje nalog prijavne službe je zagotovljena z varnostnimi mehanizmi in kontrolnimi postopki v skladu z interno politiko overitelja Halcom CA.

5.2.4 Nezdružljivost nalog

Za vsako vlogo je v interni politiki 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 interni politiki ni nezdružljivo.

5.3. Nadzor nad osebjem

(1) Pri HALCOM CA deluje organizacijska skupina za nadzor in usklajenost, ki jo sestavljajo strokovnjaki z ustreznimi tehnološkimi in pravnimi znanji, ki ne opravljajo nalog v zvezi z upravljanjem potrdil.

(2) Organizacijska skupina nadzoruje delo HALCOM CA. Organizacijska skupina 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 overitelja ima skladno z zahtevami veljavnih predpisov ter tehničnih standardov in priporočil ustrezne kvalifikacije in izkušnje.

5.3.3 Dodatno usposabljanje osebja

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

5.3.4 Zahteve za redna usposabljanja

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

5.3.5 Menjava nalog

Ni predpisana.

5.3.6 Sankcije

Sankcije v primeru nepooblaščenega ali malomarnega izvajanja nalog se za pooblaščene osebe overitelja izvajajo skladno z veljavnimi predpisi in internim pravilnikom o disciplinski in odškodninski odgovornosti delavcev.

5.3.7 Zahteve za zunanje izvajalce

Za morebitne zunanje izvajalce veljajo enake zahteve kot za pooblaščene osebe overitelja Halcom CA.

5.3.8 Dostop osebja do dokumentacije

Pooblaščenim osebam overitelja je na voljo vsa potrebna dokumentacija skladno z njihovimi zadolžitvami in nalogami.

5.4. Varnostni pregledi sistema

5.4.1 Vrste dnevnikov

(1) Overitelj 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 Interni politiki overitelja Halcom CA.

5.4.2 Pogostnost pregledov dnevnikov

Overitelj Halcom CA opravlja varnostne preglede svoje infrastrukture oz. dnevnikov dnevno.

5.4.3 Čas hrambe dnevnikov

Najpomembnejši dnevniki se hranijo trajno, vsi ostali pa šest (6) let od nastanka zapisa.

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 overitelja ali pa samodejno z drugimi varnostnimi mehanizmi na vseh informacijsko-komunikacijskih napravah overitelja.

(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

Overitelj Halcom CA v skladu z določili veljavnih predpisov hrani naslednje gradivo:

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

5.5.2 Rok hrambe

Najpomembnejši podatki se hranijo trajno, vsi ostali pa šest (6) let od nastanka zapisa.

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 pogojih delovanja in Interni politiki overitelja 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 pogojih delovanja in Interni politiki overitelja Halcom CA.

5.5.5 Zahteva po časovnem žigosanju

Podatki se časovno žigosajo enkrat letno.

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 pogojih delovanja in Interni politiki overitelja 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 pogojih delovanja in Interni politiki overitelja Halcom CA.

5.6. Sprememba javnega ključa overitelja Halcom CA

V primeru novega izdanega lastnega potrdila overitelja Halcom CA se postopek objavi na spletnih straneh overitelja 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 pogojih delovanja in Interni politiki overitelja 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 pogojih delovanja in Interni politiki overitelja Halcom CA.

5.7.3 Postopek v primeru ogroženega zasebnega ključa overitelja Halcom CA

Podrobnejša ureditev je v skladu z veljavnimi predpisi, standardi in priporočili določena v Splošnih pogojih delovanja in Interni politiki overitelja 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 pogojih delovanja in Interni politiki overitelja Halcom CA.

5.8. Prenehanje delovanja Halcom CA

Podrobnejša ureditev je v skladu z veljavnimi predpisi, standardi in priporočili določena v Splošnih pogojih delovanja in Interni politiki overitelja Halcom CA.

6. TEHNIČNE VARNOSTNE ZAHTEVE

6.1. Generiranje in namestitev ključev

6.1.1 Generiranje ključev

(1) Para ključev overitelja Halcom CA (korensko-root in vmesno/podrejeno-intermediate potrdilo) za podpisovanje in overjanje sta bila ustvarjena po najvišjih varnostnih standardih, v varnem okolju overitelja Halcom CA.

(2) Pari ključev imetnikov strežniških kvalificiranih potrdil se generirajo na strežniku, pri imetniku.

6.1.2 Dostava zasebnega ključa imetnikom

Zasebni ključ strežniških potrdil se ne prenašajo, saj se generirajo na strežniku, pri imetniku.

6.1.3 Dostava javnega ključa overitelju potrdil

Pri strežniških potrdilih se ključi generirajo pri imetniku, na računalniku ali strežniku. PKCS#10 zahtevek za izdajo potrdila (angl. »certificate request«) pa se prenese iz uporabnikovega računalnika do overitelja preko zaščitene omrežne povezave.

6.1.4 Dostava overiteljevih javnih ključev

Potrdila z javnima ključema overitelja Halcom CA sta imetniku dostavljena oz. tretjim osebam dostopna:

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

6.1.5 Dolžina ključev

Potrdilo	Dolžina ključa po RSA [bit]
Korensko (Root) potrdilo overitelja Halcom CA	2048
Vmesno/podrejeno (Intermediate) potrdilo overitelja Halcom CA	2048
Strežniško potrdilo za imetnike	2048

6.1.6 Generiranje in kakovost parametrov javnih ključev

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

6.1.7 Namen ključev in potrdil

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

(2) Za podpis potrdil in registra preklicanih potrdil je namenjen zasebni ključ overitelja Halcom CA, za overjanje pa javni ključ v overiteljevem potrdilu.

(3) Profil potrdil je podan v razdelku 7.1.

6.2. Zaščita zasebnega ključa

6.2.1 Standardi za kriptografski modul

Zasebni ključi overitelja HALCOM CA so zaščiteni v kriptografskem modulu, ki je certificiran v skladu s FIPS 140-2 nivo 3 in/ali Common Criteria EAL4+.

6.2.2 Nadzor zasebnega ključa s strani pooblaščenih oseb

Določila glede dostopa do zasebnega ključa overitelja Halcom CA so v skladu z veljavnimi predpisi in Splošnimi pogoji delovanja določena v Interni politiki overitelja Halcom CA.

6.2.3 Odkrivanje kopije zasebnega ključa

Določila glede odkrivanja zasebnega ključa overitelja Halcom CA so v skladu z veljavnimi predpisi in Splošnimi pogoji delovanja določena v Interni politiki overitelja Halcom CA.

6.2.4 Varnostna kopija zasebnega ključa

Določila glede varnostnega kopiranja zasebnega ključa overitelja Halcom CA so v skladu z veljavnimi predpisi in Splošnimi pogoji delovanja določena v Interni politiki overitelja Halcom CA.

6.2.5 Arhiviranje zasebnega ključa

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

(2) Podrobnejša določila kopiranja zasebnega ključa overitelja Halcom CA so v skladu z veljavnimi predpisi in Splošnimi pogoji delovanja določena v Interni politiki overitelja Halcom CA.

6.2.6 Prenos zasebnega ključa iz/v kriptografski modul

Zasebni ključi pri strežniških potrdilih se ne prenašajo, saj se ustvarijo pri imetniku, na računalniku ali strežniku.

6.2.7 Hramba zasebnega ključa v kriptografskem modulu

(1) Zasebne ključe overitelja HALCOM CA hrani v kriptografskem modulu, ki je certificiran v skladu s FIPS 140-2 nivo 3 in/ali Common Criteria EAL4+.

(2) Zasebni ključi uporabnikov se generirajo pri imetniku, na računalniku ali strežniku.

6.2.8 Postopek za aktiviranje zasebnega ključa

(1) Ob zaustavitvi delovanja overitelja Halcom CA programska oprema Halcom CA deaktivira zasebni ključ Halcom CA.

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

6.2.9 Postopek za deaktiviranje zasebnega ključa

Postopek za deaktiviranje zasebnega ključa overitelja Halcom CA poteka na varen način skladno z določili Interne politike overitelja Halcom CA.

6.2.10 Postopek za uničenje zasebnega ključa

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

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

6.2.11 Lastnosti kriptografskega modula

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

6.3. Ostali aspekti upravljanja ključev

6.3.1 Arhiviranje javnega ključa

Overitelj 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) Običajna veljavnost strežniškega potrdila je pet (5) let od izdaje potrdila.

Tip potrdila	Potrdilo	Ključ	Veljavnost
Strežniško potrdilo	par ključev za digitalno podpisovanje/overjanje in dešifriranje/šifriranje	Zasebni ključ	5 let
		Javni ključ	5 let

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

6.4. Gesla za dostop do potrdil oz. ključev

6.4.1 Generiranje gesel

Imetniki sami določijo geslo, s katerim zaščitijo dostop do svojih zasebnih ključev. Halcom CA priporoča uporabo varnih gesel:

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

6.4.2 Zaščita gesel

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

6.4.3 Drugi aspekti gesel

Niso predpisani.

6.5. Varnostne zahteve za informacijsko-komunikacijsko opremo overitelja

6.5.1 Specifične tehnične varnostne zahteve

Podrobnejša ureditev je v skladu z veljavnimi predpisi, standardi in priporočili določena v Splošnih pogojih delovanja in Interni politiki overitelja Halcom CA.

6.5.2 Nivo varnostne zaščite

Podrobnejša ureditev je v skladu z veljavnimi predpisi, standardi in priporočili določena v Splošnih pogojih delovanja in Interni politiki overitelja Halcom CA.

6.6. Tehnični nadzor življenjskega cikla overitelja

6.6.1 Nadzor razvoja sistema

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

6.6.2 Upravljanje varnosti

Podrobnejša ureditev je v skladu z veljavnimi predpisi, standardi in priporočili določena v Splošnih pogojih delovanja in Interni politiki overitelja Halcom CA.

6.6.3 Nadzor življenjskega cikla

Podrobne tehnične zahteve so določene v Splošnih pogojih delovanja in Interni politiki overitelja Halcom CA.

6.7. Varnostna kontrola omrežja

Podrobnejša ureditev je v skladu z veljavnimi predpisi, standardi in priporočili določena v Splošnih pogojih delovanja in Interni politiki overitelja 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 strežniška potrdila za poslovne subjekte.

(2) Vsa potrdila vključujejo podatke, ki so skladno z zakonodajo določena za normalizirana digitalna potrdila.

(3) Potrdila overitelja Halcom CA sledijo standardu X.509.

7.1.1 Različica potrdil

Vsa potrdila overitelja Halcom CA sledijo standardu X.509, in sicer različici 3.

7.1.2 Profil potrdil z razširitvami

(1) Profil Korenskega (Root) potrdila - Halcom Root CA.

Nazivi polja	Vrednost oz. pomen
Osnovna polja v potrdilu	
Različica, angl. Version	V3
Identifikacijska oznaka potrdila, angl. Serial Number	enolična interna številka potrdila
Algoritem za podpis, angl. Signature algorithm	Sha512RSA (OID 2.16.840.1.101.3.4.2.3)
Izdajatelj, angl. Issuer	C=SI, O=Halcom, CN= Halcom Root CA

Veljavnost, angl. Validity	Valid from: <8.2.2012 09:55:41 GMT > Valid to: <8.2.2032 09:55:41 GMT >
Imetnik, angl. Subject	C=SI, O=Halcom, CN= Halcom Root CA
Algoritem za javni ključ, angl. Subject Public Key Algorithm	rsaEncryption (OID 1.2.840.113549.1.1.1)
Javni ključ, angl. Public Key (... bits)	modul, eksponent,...
Imetnikov javni ključ, ki pripada ustreznemu paru ključev, šifriran z alg. RSA, angl. RSA Public Key	dolžina ključa je 2048 bitov,glej razd. 6.1.5.
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	4e 94 d8 8a 63 c2 cf 79
Osnovne omejitve, OID 2.5.29.19, angl. Basic Constraints	Subject Type=CA Path Length Constraint=None
Dodatna identifikacija (ni del digitalnega potrdila)	
razpoznavni odtis potrdila-SHA1 angl. Certificate Fingerprint – SHA1	Razpoznavni odtis potrdila po SHA1

(2) Profil Vmesnega/podrejenega (Intermediate) potrdila – Halcom Secure Server CA 1

Nazivi polja	Vrednost oz. pomen
Osnovna polja v potrdilu	
Različica, angl. Version	V3
Identifikacijska oznaka potrdila, angl. Serial Number	enolična interna številka potrdila
Algoritem za podpis, angl. Signature algorithm	Sha512RSA (OID 2.16.840.1.101.3.4.2.3)
Izdajatelj, angl. Issuer	C=SI, O=Halcom, CN= Halcom Root CA
Veljavnost, angl. Validity	Valid from: <8.2.2012 10:01:40 GMT > Valid to: <8.2.2022 10:01:40 GMT >
Imetnik, angl. Subject	C=SI, O=Halcom, CN= Halcom Secure Server CA 1
Algoritem za javni ključ, angl. Subject Public Key Algorithm	rsaEncryption (OID 1.2.840.113549.1.1.1)
Javni ključ, angl. Public Key (... bits)	modul, eksponent,...
Imetnikov javni ključ, ki pripada ustreznemu paru ključev, šifriran z alg. RSA, angl. RSA Public Key	dolžina ključa je 2048 bitov,glej razd. 6.1.5.
Razširitve X.509v3	
Objava registra preklicanih potrdil, OID 2.5.29.31, angl. CRL Distribution Points	URL=ldap://ldap.halcom.si/cn=Halcom%20Root%20CA,o=Halcom,c=SI?certificaterevocationlist;binary
Uporaba ključa, OID 2.5.29.15, angl. Key Usage	Certificate Signing, Off-line CRL Signing, CRL Signing
Identifikator overiteljevega ključa, OID 2.5.29.35, angl. Authority Key Identifier	KeyID=4e 94 d8 8a 63 c2 cf 79
Identifikator imetnikovega ključa, OID 2.5.29.14, angl. Subject Key Identifier	4c 7a 75 86 d5 49 8d 84

Osnovne omejitve, OID 2.5.29.19, angl. Basic Constraints	Subject Type=CA Path Length Constraint=None
Dodatna identifikacija (ni del digitalnega potrdila)	
razpoznavni odtis potrdila-SHA1 angl. Certificate Fingerprint – SHA1	Razpoznavni odtis potrdila po SHA1

(3) Profil strežniških potrdil končnih uporabnikov

Nazivi polja	Vrednost oz. pomen
Osnovna polja v potrdilu	
Različica, angl. Version	V3
Identifikacijska oznaka potrdila, angl. Serial Number	enolična interna številka potrdila
Algoritem za podpis, angl. Signature algorithm	Sha512RSA (OID 2.16.840.1.101.3.4.2.3)
Izdajatelj, angl. Issuer	C=SI, O=Halcom, CN= Halcom Secure Server CA 1
Veljavnost, angl. Validity	Valid from: <pričetek veljavnosti po GMT> Valid to: <konec veljavnosti po GMT>
Imetnik, angl. Subject	razločevalno ime imetnika, glej razd. 3.1.1.
Algoritem za javni ključ, angl. Subject Public Key Algorithm	rsaEncryption (OID 1.2.840.113549.1.1.1)
Javni ključ, angl. Public Key (... bits)	modul, eksponent,...
Imetnikov javni ključ, ki pripada ustreznemu paru ključev, šifriran z alg. RSA, angl. RSA Public Key	dolžina ključa je 2048 bitov,glej razd. 6.1.5.
Razširitve X.509v3	
Objava registra preklicanih potrdil, OID 2.5.29.31, angl. CRL Distribution Points	URI:ldap://ldap.halcom.si/cn=Halcom%20Secure%20Server%20CA%201,o=Halcom,c=SI?certificaterevocationlist;binary
Uporaba ključa, OID 2.5.29.15, angl. Key Usage	Digital Signature Key Encipherment
Identifikator overiteljevega ključa, OID 2.5.29.35, angl. Authority Key Identifier	KeyID=4c 7a 75 86 d5 49 8d 84
Identifikator imetnikovega ključa, OID 2.5.29.14, angl. Subject Key Identifier	identifikator imetnikovega ključa
Dodatni nazivi, angl. Subject Alternative Name	DNS Name=naziv strežnika RFC822 Name=elektronski naslov DNS Name=dodatni nazivi strežnikov (ni obvezno)
Razširjena uporaba ključa, angl. Extended Key Usage	Server Authentication Client Authentication
Politika, pod katero je bilo izdano potrdilo, OID 2.5.29.32, angl. certificatePolicies	Certificate Policy: Policy Identifier=1.3.6.1.4.1.5939.5.2.3
Dodatna 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) je označeno kot kritično (angl. critical).

(5) Imetnik ima lahko več veljavnih istovrstnih strežniških potrdil.

7.1.2.1 Zahteve za elektronski naslov

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

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

(2) Druge omejitve glede elektronskih naslovov niso predpisane.

7.1.3 Identifikacijske oznake algoritmov

(1) Potrdila, ki jih izdaja Halcom CA, so s strani overitelja podpisana z algoritmom, določenim v polju signature algorithm: vrednost »sha512RSA«, identifikacijska oznaka: OID 1.2.840.113549.1.1.13.

(2) Celoten nabor algoritmov, formatov podatkov in protokolov je na razpolago pri pooblaščenih osebah overitelja 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:

CN= Halcom Root CA	CN= Halcom Secure Server CA 1
O = Halcom	O = Halcom
C = SI	C = SI

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

(3) Register preklicanih potrdil vsebuje enolično interno serijsko številko preklicanega

potrdila ter čas in datum preklica.

7.2.1 Različica

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

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

- po protokolu LDAP in
- po protokolu HTTP.

7.2.2 Vsebina registra in razširitve

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

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

(2) Korenski 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	Sha512RSA
Overiteljev podpis, angl. Signature	podpis Halcom CA
Razločevalno ime overitelja, angl. Issuer	C=SI, O=Halcom, CN=Halcom Root CA
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 overiteljevega ključa, angl. Authority Key Identifier (OID 2.5.29.35)	KeyID= 4e 94 d8 8a 63 c2 cf 79
angl. issuerAltName (OID 2.5.28.18)	se ne uporablja
angl. deltaCRLindicator (OID 2.5.29.27)	se ne uporablja
angl. issuingDistribuitionPoint (OID 2.5.29.28)	se ne uporablja

(2) Vmesni/podrejen register preklicanih potrdil (CRL uporabniških potrdil)

Naziv polja	Vrednost oz. pomen
Osnovna polja v CRL	
Različica, angl. Version	V2
Algoritem za podpis, angl. Signature Algorithm	Sha512RSA
Overiteljev podpis, angl. Signature	podpis Halcom CA
Razločevalno ime overitelja, angl. Issuer	C=SI, O=Halcom, CN=Halcom Secure Server CA 1
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 overiteljevega ključa, angl. Authority Key Identifier (OID 2.5.29.35)	KeyID= 4c 7a 75 86 d5 49 8d 84
angl. issuerAltName (OID 2.5.28.18)	se ne uporablja
angl. deltaCRLindicator (OID 2.5.29.27)	se ne uporablja
angl. issuingDistribuitionPoint (OID 2.5.29.28)	se ne uporablja

(3) Preklicana digitalna potrdila, katerih veljavnost je potekla, ostanejo objavljena v registru.

7.2.3 Objava registra preklicanih potrdil

Halcom CA objavlja register v centralnem 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

Protokol za sprotno preverjanje statusa OCSP (angl. Online Certificate Status Protocol) ni podprt.

7.3.1 Verzija sprotnega preverjanje statusa

Protokol OCSP ni podprt.

7.3.2 Profil sprotnega preverjanje statusa

Protokol OCSP ni podprt.

8. NADZOR

(1) Pri Halcom CA deluje organizacijska skupina za nadzor in usklajenost, ki jo sestavljajo strokovnjaki z ustreznimi tehnološkimi in pravnimi znanji, ki ne opravljajo nalog v zvezi z upravljanjem potrdil.

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

8.1. Pogostnost nadzora

Organizacijska skupina za nadzor in usklajenost opravi nadzor najmanj enkrat letno.

8.2. Vrsta in usposobljenost nadzora

Organizacijsko skupino za nadzor in usklajenost sestavljajo strokovnjaki z ustreznimi tehnološkimi in pravnimi znanji.

8.3. Neodvisnost nadzora

Organizacijsko skupino za nadzor in usklajenost sestavljajo člani, ki ne opravljajo nalog v zvezi z upravljanjem potrdil.

8.4. Področja nadzora

Področja nadzora so določena v Interni politiki overitelja Halcom CA.

8.5. Ukrepi overitelja

V primeru ugotovljenih pomanjkljivosti ali napak organizacijska skupina 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 Interni politiki overitelja Halcom CA.

8.6. Objava rezultatov nadzora

Rezultati izvedbe nadzorov se hranijo pri overitelju Halcom CA.

9. FINANČNE IN OSTALE PRAVNE ZADEVE

9.1. Cenik

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

9.1.1 Cena izdaje potrdil in podaljšanja

Cena izdaje potrdil in podaljšanja je določena z veljavnim cenikom.

9.1.2 Cena dostopa do potrdil

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

9.1.3 Cena dostopa do statusa potrdila in registra preklicanih potrdil

Register preklicanih potrdil je brezplačno dostopen vsem osebam.

9.1.4 Cene drugih storitev

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

9.1.5 Povrnitev stroškov

Ni predpisana.

9.2. Finančna odgovornost

9.2.1 Zavarovalniško kritje

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

9.2.2 Drugo kritje

Ni predpisano.

9.2.3 Zavarovanje imetnikov

Ni predpisano.

9.3. Varovanje poslovnih podatkov

9.3.1 Varovani podatki

(1) Overitelj 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 Interni politiki delovanja overitelja Halcom CA.

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

9.3.2 Nevarovani podatki

Overitelj Halcom CA javno objavlja samo take poslovne podatke, ki v skladu z veljavno zakonodajo niso zaupne narave.

9.3.3 Odgovornost glede varovanja

(1) Halcom CA ne prevzema nobene odgovornosti za vsebino podatkov, ki jih imetnik potrdila elektronsko šifrira ali podpisuje, in sicer tudi v primeru, da je imetnik ali tretja oseba spoštoval vse veljavne predpise, vsa določila 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 5.1 te politike.

9.4. Varovanje osebnih podatkov

9.4.1 Načrt varovanja osebnih podatkov

Z vsemi osebnimi in zaupnimi podatki o imetnikih potrdil, ki so nujno potrebni za storitve upravljanja s potrdili, overitelj Halcom CA ravna v skladu z veljavno zakonodajo.

9.4.2 Varovani osebni podatki

Varovani podatki so vsi osebni podatki, ki jih overitelj Halcom CA pridobi na zahtevkih za

svoje storitve ali v ustreznih registrih za dokazovanje istovetnosti imetnika.

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

Overitelj Halcom CA je odgovoren v skladu z veljavnimi predpisi o varstvu podatkov.

9.4.5 Pooblastilo glede uporabe osebnih podatkov

Imetnik pooblasti overitelja Halcom CA za uporabo osebnih podatkov na zahtevku za pridobitev potrdila ali kasneje v pisni obliki.

9.4.6 Posredovanje osebnih podatkov

(1) Overitelj 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 overitelja Halcom CA imetnik pooblastil za to (glej prejšnji razdelek), ali na zahtevo pristojnega sodišča, prekrškovnega ali upravnega organa.

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

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 poslovnemu subjektu oz. imetniku potrdila,
- na javnih ključih, vseh podatkih na potrdilu, na centralnem 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 overitelja Halcom CA

(1) Overitelj 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 digitalnih potrdil ipd.),
- objavljati na svojih spletnih straneh vse informacije o tistih spremembah glede dejavnosti overitelja, ki kakorkoli vplivajo na imetnike potrdil in tretje osebe,
- zagotoviti delovanje prijavnih služb v skladu z določili HALCOM CA in ostalimi veljavnimi predpisi,
- spoštovati določila glede varnega ravnanja z osebnimi, poslovnimi in zaupnimi

podatki o overitelju, 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 digitalna potrdila v skladu s to politiko in ostalimi predpisi ter priporočili.

(2) Overitelj 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 overitelja,
- 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,
- obveščati uporabnike o pomembnih zadevah ter
- izpolnjevati vse druge zahteve v skladu s to politiko.

(3) Overitelj 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 overitelja Halcom CA in
- nedostopnost kot posledica višje sile ali izrednih dogodkov.

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

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

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

9.6.2 Obveznost in odgovornost prijavne službe

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

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

9.6.3 Obveznosti in odgovornost imetnika potrdila

(1) Poslovni subjekt odgovarja za:
- nastalo škodo v primeru zlorabe potrdila od prijave preklica do preklica,
- vsako škodo, ki je bodisi posredno ali neposredno povzročena zato, ker je bila

omogočena uporaba oz. zloraba imetnikovega potrdila s strani nepooblaščenih oseb,
- vsako drugo škodo, ki izvira iz neupoštevanja določil te politike in drugih obvestil Halcom CA ter veljavnih predpisov.

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

9.6.4 Obveznosti in odgovornost tretjih oseb

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

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

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

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

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

9.6.5 Obveznosti in odgovornost drugih oseb

Ni predpisano.

9.7. Omejitev odgovornosti

Overitelj 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 dostopa 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 overitelja,
- uporabe potrdil ter veljavnosti potrdil ob spremembah podatkov iz potrdila, elektronskih naslovov ali spremembah imen imetnikov,
- izpada infrastrukture, ki ni v domeni upravljanja overitelja 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 overitelja Halcom CA se osem (8) dni pred veljavo predhodno objavi na spletnih straneh overitelja 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) Overitelj lahko za posamezna določila veljavne politike izda dopolnitve, kot je to določeno v razd. 9.12.

9.10.3 Učinek poteka veljavnosti politike

(1) Ob izdaji nove politike se vsa 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 overitelja so objavljeni na spletnih straneh in podani v razd. 1.5.2.

(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 overiteljem Halcom CA.

9.12. Spremembe in dopolnitve

9.12.1 Postopek za sprejem sprememb in dopolnitev

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

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

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

(4) Način za označevanje dopolnitev določi overitelj Halcom CA.

9.12.2 Veljavnost in objava sprememb in dopolnitev

(1) Overitelj 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 overitelj 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 organizacijska skupina za nadzor in usklajenost (razdelek 5.3).

(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 Republike Slovenije.

9.15. Skladnost z veljavno zakonodajo

(1) Nadzor nad skladnostjo delovanja overitelja Halcom CA z veljavno zakonodajo in predpisi izvaja pristojni inšpektorat.

(2) Notranje preverjanje skladnosti delovanja izvajajo pooblaščene osebe v okviru overitelja Halcom CA.

9.16. Splošne določbe

Z ostalimi subjekti overitelj Halcom CA lahko sklene medsebojne dogovore, če to določa veljavna zakonodaja oz. drugi predpisi.

9.17. Druge določbe

Niso predpisane.

Kraj in datum:
Ljubljana, 17.06.2016

Glavni izvršni direktor
Marko Valjavec