Autor: LUKA RIBIČIČ

Broj dokumenta: 400085-8-9/17

Halcom CA: Opća pravila poslovanja (CPS),

Izdanje: 10

# Halcom CA

## Opća pravila poslovanja (CPS)

Dokument je na snazi od: 15.06.2024.

| Izdanje | Broj dokumenta i priloz | Opis promjene | Autor | Datum izmjene |
|---|---|---|---|---|
| 1 | 400085-38-0/17 | Prevod CPS Izdaja št. 2 (IPS 400085-8-2/17) | L. Ribičič | 27.2.2018 |
| 2 | 400085-39-1/17 | Prevod CPS Izdaja št. 3 (IPS 400085-8-3/17) | L. Ribičič | 1.6.2018 |
| 3 | 400085-39-2/17 | Prevod CPS Izdaja št. 4 (IPS 400085-8-4/17) | L. Ribičič | 24.5.2019. |
| 4 | 400085-39-3/17 | Prevod CPS Izdaja št. 5 (IPS 400085-8-5/17) | S.Lazić | 29.4.2020 |
| 5 | 40085-39-4/17 | Prevod COS Izdaja št. 6 ((IPS 40085-8-6/17) | S.Lazić | 3.2.2021 |
| 6 | 40085-39-5/17 | Prevod COS Izdaja št. 7 ((IPS 40085-8-7/17) | S.Lazić | 21.5.2021 |
| 6 | 40085-39-5/17 | Prevod COS Izdaja št.8 (IPS 40085-8-8/17) | S.Lazić | 15.6.2022 |
| 7 | 40085-39-6/17 | Prevod COS Izdaja št.9 (IPS 40085-8-9/17) | S.Lazić | 23.5.2023 |
| 8 | 40085-39-7/17 | Prevod COS Izdaja št.10 (IPS 40085-8-9/17) | L.Ribičič | 22.5.2024 |

# Sadržaj

# 1. UVOD

(1) Ovaj dokument predstavlja Opća pravila poslovanja (u daljem tekstu: CPS) pružaoca usluga povjerenja u oblasti elektronskih potpisa, elektronskih pečata, elektronskih vremenskih pečata, validacija i drugih usluga.

(2) Halcom CA je najstariji i najveći pružalac usluga povjerenja (u daljnjem tekstu: TSP) u Sloveniji koji za implementaciju svojih usluga u oblasti elektronskog potpisivanja, elektronskih pečata, elektronskih vremenskih pečata, validacije i drugih usluga koristi najsigurnije tehnologije, uključujući upotrebu sigurnih nosača podataka i sigurne oblake (cloud).

(3) Sve odredbe CPS-a koje se odnose na poslovanje Halcom CA su propisno prenesene i detaljnije definisane u odredbama internih pravila. To je povjerljivi dio internih pravila i sastoji se od povjerljivih dokumenata koji definišu infrastrukturu, odredbe koje se odnose na zaposlenike Halcom CA (nadležnosti, zadaci, ovlaštenja i potrebni uslove koje moraju ispunjavati pojedini članovi osoblja), fizička sigurnost (pristup prostorijama, rukovanje hardverom i softverom), sigurnost softvera (sigurnosne postavke servera, sigurnosne kopije...) i interne revizije (kontrola fizičkog pristupa, ovlasti...).

## 1.1. Pregled

(1) CPS su opća pravila za rad TSP-a HALCOM CA za izdavanje certifikata, njima se reguliše svrha, način rada i metodologija upravljanja certifikatima i sigurnosnim uslovima koje moraju ispunjavati TSP HALCOM CA, pretplatnici, subjekti i treća lica na koja se certifikati odnose, kao i odgovornost svih tih osoba.

(2) Halcom CA pruža sljedeće usluge:

- Kvalifikovani certifikati za elektronske potpise,
- Kvalifikovana usluga potvrđivanja validnosti elektronskih potpisa,
- Kvalifikovana usluga pohranjivanja elektronskih potpisa,
- Kvalifikovani certifikati za elektronske pečate,
- Kvalifikovana usluga potvrđivanja validnosti elektronskih pečata,
- Kvalifikovana usluga pohranjivanja elektronskih pečata,
- Kvalifikovani elektronski vremenski pečati,
- Kvalifikovani certifikati za potvrdu autentičnosti internet lokacije.

(3) TSP Halcom CA posluje unutar Halcoma d.d.

(4) Halcom CA izdaje:

- Kvalifikovane digitalne certifikate za elektronske potpise,
- Kvalifikovane digitalne certifikate za elektronske pečate,
- Kvalifikovane digitalne certifikate za potvrdu autentičnosti internet lokacije i
- Kvalifikovane digitalne certifikate za vremenske pečate.

(5) Halcom CA izdaje certifikate i vrši druge djelatnosti TSP-a u skladu sa važećim zakonskim propisima Republike Slovenije i Evropske unije, te u skladu sa eIDAS uredbom, tehničkim zahtjevima iz ETSI, IETF RFC standarda, ISO/IEC porodice standarda i ostalih povezanih standarda.

(6) Halcom CA na svojim web stranicama objavljuje spisak registrovanih tijela koja pružaju usluge pribavljanja certifikata.

### 1.1.1 Osnovni dokumenti TSP-a Halcom CA

Ispod navedeni javni dokumenti sadrže više detaljnih pravila, uslova, prava i obaveza koje TSP Halcom CA mora ispunjava u svojim aktivnostima:

- Pravila Halcoma CA za kvalifikovane digitalne certifikate pravnih lica,
- Pravila Halcoma CA za kvalifikovane digitalne potpise za fizička lica,
- Pravila Halcoma CA za kvalifikovane digitalne certifikate za potvrdu autentičnosti web stranica,
- Pravila Halcoma CA za kvalifikovane vremenske pečate,
- Izjava o korištenju certifikata.

### 1.1.2 Veze između osnovnih dokumenata TSP-a Halcom CA

(1) Ovom politikom su uređeni zahtjevi TSP-a, a CPS osigurava operativne procese kojima se ti zahtjevi ispunjavaju. Izjava o korištenju certifikata (CPS) definiše način na koji pružalac usluga daje tehničke, organizacijske i procesne uslove za poslovanje koji su definisani u Politici Halcoma CA.

(2) Pravila su uopćen dokument u poređenju sa CPS-om. U CPS-u se nalazi detaljan opis načina rada TSP-a Halcom CA, kao i poslovnih i operativnih procesa izdavanja certifikata i njihovim upravljanjem.

(3) Pravila su definisana nezavisno od određene operativne jedinice unutar TSP-a, a CPS sadrži detaljan opis organizacijske strukture i operativnih procesa unutar TSP-a Halcom CA.

### 1.1.3 Standardi

Halcom CA izdaje certifikate i provodi ostale aktivnosti TSP-a u skladu sa mjerodavnim pravom Republike Slovenije i Evropske Unije i u skladu sa tehničkim uslovima opisanim u ETSI, IETF RFC standardu i ISO/IEC porodici standarda i ostalim relevantnim standardima.

### 1.1.4 Interna pravila Halcoma CA

(1) Detaljan opis infrastrukture, poslovanja, procedura za upravljanje infrastrukturom i nadzora nad sigurnosnim pravilima poslovanja Halcoma CA je dat u internim pravilima.

(2) Interna pravila su povjerljivi dokumenti i čine poslovnu tajnu TSP-a Halcom CA.

(3) Interna pravila sadrže detaljne odredbe koje se odnose na:
- Sistem fizičke kontrole ulaska u prostorije Halcoma CA,
- Sistem logičke kontrole pristupanja računarskim mrežama Halcoma CA,
- Sistem u Halcomu CA za osiguranje privatnih ključeva,
- Sistem raspodjele odgovornosti u Halcomu CA za aktivaciju privatnog ključa,
- Procedure i osoblje uključeno u pružanje usluga povjerenja,
- Procedure za nepredviđene okolnosti (vatra, poplava, zemljotresi, upad u prostorije ili u informacijski sistem TSP-a).

(4) Halcom CA je predmet vanjske nezavisne revizije koju jednom godišnje provodi akreditovano tijelo.

## 1.2. Pružalac usluga povjerenja Halcom CA

Halcom CA je odgovaran za izdavanje sljedećih kvalifikovanih digitalnih certifikata:

- Halcom Root Certificate Authority (korijenski certifikat Halcom CA)
- Halcom CA PO e- signature 1 (posrednički/podređeni certifikat za kvalifikovane digitalne certifikate za pravna lica),
- Halcom CA PO e- signature 2 (posrednički/podređeni certifikat za kvalifikovane digitalne certifikate za pravna lica),
- Halcom CA FO e-signature 1 (posrednički/podređeni certifikat za kvalifikovane digitalne certifikate za fizička lica),
- Halcom CA FO e-signature 2 (posrednički/podređeni certifikat za kvalifikovane digitalne certifikate za fizička lica),
- Halcom CA PO e-seal 1 (posrednički/podređeni certifikat za kvalifikovane digitalne certifikate za elektronske pečate)
- Halcom CA PO e-seal 2 (posrednički/podređeni certifikat za kvalifikovane digitalne certifikate za elektronske pečate)
- Halcom CA web 1 (posrednički/podređeni certifikat za kvalifikovane digitalne certifikate za potvrdu autentičnosti web stranice)
- Halcom CA TSA 1 (posrednički/podređeni certifikat za kvalifikovane digitalne vremenske pečate)
- Korisnički certifikati:
    1. Fizička lica:
        - Certifikati za elektronsko potpisivanje,
        - Certifikati za potvrdu autentičnosti web stranice.
    2. Pravna lica:
        - Certifikati za elektronsko potpisivanje (fizička lica koja zastupaju pravna lica),
        - Certifikati za potvrdu autentičnosti web stranice,
        - Certifikati za elektronske pečate,

## 1.3. PKI učesnici

### 1.3.1 Pružalac usluga povjerenja Halcom CA

Halcom CA je TSP koji izdaje i upravlja certifikatima za elektronsko potpisivanje, elektronske pečate, elektronske vremenske pečate, validaciju i ostale usluge. TSP Halcom posluje unutar Halcom d.d.

### 1.3.2 Registracijsko tijelo Halcoma CA

(1) Registracijsko tijelo (u daljem tekstu: RA) obavlja sljedeće zadatke za TSP:

1. provjera identiteta fizičkih lica, pravnih lica, fizičkih lica koja su povezana sa pravnim licima, zakonskih predstavnika pravnih lica i ostalih relevantnih podataka za upravljanje certifikatima,
2. primanje obrazaca zahtjeva za izdavanje certifikata,
3. primanje zahtjeva za opoziv certifikata,
4. izdavanje neophodne dokumentacije za subjekat ili za buduće subjekte,
5. Prenos obrazaca zahtjeva, zahtjeva i ostalih informacija na sigurna način TSP-u Halcom CA.

(2) TSP Halcom CA može ovlastiti druge organizacije iz poslovnog i javnog sektora, pored svojih RA, da obavljaju zadatke koji pripadaju RA ili druge aktivnosti za koje im TSP Halcom CA da ovlaštenje. Halcom CA ugovorom obavezuje te organizaciju na ispunjavanje strogih sigurnosnih uslova u skladu sa mjerodavnim evropskim i slovenskim uredbama i međunarodnim, evropskim i slovenskim standardima, preporukama i pravilima, CPS-om i internim pravilima Halcoma CA.

(3) TSP Halcom CA ima geografski raširene RA čime se budućim subjektima omogućava laka registracija u njihovim matičnim ili susjednim gradovima. Informacije o lokacijama RA su dostupne na internet stranici TSP-a Halcom CA.

### 1.3.3 Pretplatnici i subjekti koji koriste certifikat

(1) Pretplatnik/subjekat certifikata može biti fizičko lice ili pravno lice (u zavisnosti od vrste certifikata)

| Usluga | Izdavalac | Pretplatnik | Subjekat |
|---|---|---|---|
| Certifikati za pravna lica (e-signature) | Halcom CA PO e-signature 1 | Pravno lice | Fizičko lice |
| Certifikati za pravna lica (e-signature) | Halcom CA PO e-signature 2 | Pravno lice | Fizičko lice |
| Certifikati za elektronske pečate | Halcom CA PO e-seal 1 | Pravno lice | Uređaj / server |
| Certifikati za elektronske pečate | Halcom CA PO e-seal 2 | Pravno lice | Uređaj / server |
| Certifikati za potvrdu autentičnosti web stranice | Halcom CA web 1 | Pravno lice / fizičko lice | Server |
| Certifikati za fizička lica | Halcom CA FO e-signature 1 | Fizičko lice | Fizičko lice |
| Certifikati za fizička lica | Halcom CA FO e-signature 2 | Fizičko lice | Fizičko lice |
| Certifikati za elektronske vremenske pečate | Halcom CA TSA 1 | TSP | Uređaj / server |

### 1.3.4 Pouzdajuće strane

(1) Treća lica su osobe koje se oslanjaju na izdate certifikate i ostale usluge TSP-a Halcom CA, a koje mogu biti fizička ili pravna lica.

(2) Treća lica moraju pratiti upute TSP-a Halcom CA i uvijek moraju provjeriti validnost certifikata (opoziv), svrhu korištenja certifikata, period validnosti certifikata (rok trajanja), itd. Obaveze i odgovornosti trećih lica su detaljnije obrađene u Odjeljcima 4.5.2 i 9.6.4

(3) Treća lica ne moraju obavezno biti subjekti certifikata TSP-a Halcom CA ili digitalnih certifikata drugih pružalaca usluga povjerenja.

## 1.4. Korištenje certifikata

Halcom CA upravlja (izdaje, provjerava, opoziva, obnavlja, pohranjuje, objavljuje) kvalifikovane certifikate za elektronske potpise, elektronske pečate, potvrdu autentičnosti web stranica i vremenske pečate. Certifikati su namijenjeni fizičkim licima i pravnim licima.

### 1.4.1 Odgovarajuća namjena certifikata

(1) Certifikati za elektronske potpise/pečate se namijenjeni za potpisivanje/pečaćenje unilateralnih ili uzajamnih komunikacija između subjekata certifikata i za korištenje u raznim aplikacijama i u različite svrhe koje se susreću na tržištu. Između ostalog, certifikati se mogu koristit za sljedeću namjenu:

1) identifikacija subjekta,

2) otkrivanje identiteta subjekta,
3) potpisivanje/stavljanje pečata na dokumente u elektronskoj formi,
4) šifrovanje i dešifrovanje dokumenata u elektronskoj formi.

Elektronski potpis/pečat se može koristiti u sljedećim aplikacijama:

1) elektronsko ili mobilno bankarstvo,
2) aplikacije koje se koriste za eVladu ili mVladu (engleski: *eGovernment ili mGovernment*),
3) aplikacije koje se koriste za eZdravlje ili mZdravlje (engleski: *eHealth ili mHealth*),
4) elektronski potpisi/pečati ili mobilni obrasci,
5) sigurna veza sa tijelima i organizacijama iz javnog sektora i sa ostalim fizičkim i pravnim licima,
6) ostale aplikacije ili usluge u kojima se traži certifikat,
7) kontrola pristupa.

(2) Certifikati za potvrdu autentičnosti web stranica su namijenjeni za:

1) Identifikaciju web stranice,
2) otkrivanje identiteta web stranice
3) kontrolu pristupa
4) uspostavljanje sigurnih veza.

(3) Sigurnosni vremenski pečati se koriste u raznim aplikacijama i za razne svrhe koje se pojavljuju na tržištu. Između ostalog, vremenski pečati se koriste u aplikacijama kao što su:

1) Elektronsko bankarstvo,
2) elektronska pohrana podataka, dokumentarnog ili arhivskog materijala
3) aplikacije eVlade,
4) druge aplikacije gdje dokaz određene akcije ili činjenice mora biti zagarantovan istovjetnim vremenskim izvorom.

### 1.4.2 Zabranjene upotrebe certifikata

(1) Zabranjena je upotreba certifikata, koji su izdati u skladu sa pravilima, koja je suprotna odredbama pravila ili uredbama koje su na snazi ili je izvan djelokruga dozvoljene upotrebe koja se navodi u prethodnom odjeljku.

(2) Certifikati nisu namijenjeni za preprodaju.

## 1.5. Upravljanje pravilima

### 1.5.1 Organizacija koja upravlja dokumentom

(1) Pravilima i CPS-om upravlja TSP Halcom CA koji djeluje u okviru Halcoma d.d.

**(2)** Adresa upravitelja:

**Halcom d.d.**
**Tržaška 118**
**1000 LJUBLJANA**
**Slovenija**

### 1.5.2 Kontakt osoba

(1) Za pitanja koja su vezana za CPS i pravila, možete se obratiti ovlaštenim licima TSP-a koja možete dobiti na dolje navedenoj adresi i brojevima telefona.

**(2)** Halcom CA adresa:

**Halcom CA**
**Tržaška 118**
**1000 LJUBLJANA**
**Slovenija**
**Tel.: (+386) 01 200 34 86**

**E-mail: ca@halcom.si**
**E-mail za opozive: ca_opozivi@halcom.si**

### 1.5.3 Odgovorna osoba za utvrđivanje usklađenosti CPS-a sa pravilima

U skladu sa datim odgovornostima, ovlašteno osoblje TSP-a Halcom CA je odgovorno za usklađenost Halcoma CA sa CPS-om i pravilima.

### 1.5.4 Procedure za odobravanje CPS-a

(1) U cilju osiguranja zakonitosti, sigurnosti i kvalitete, svaki prijedlog za novi CPS je predmet tehnološkog i pravnog pregleda prije nego odobrenje izda Generalni direktor Halcoma d.d.

(2) TSP može izdati izmjene za pojedinačne odredbe kao što se navodi u odjeljku 9.12.

## 1.6. Definicije i akronimi

### 1.6.1 Definicije

| | |
|---|---|
| **CA** | Pružalac usluga povjerenja koji izdaje certifikate (Ovlašteno tijelo za certifikate ili Agencija za certifikate). |
| **CPName** | Naziv pravila o certifikaciji koja su isključivo vezana za identifikator međunarodne politike o certifikaciji (CPOID). |
| **CP** | Ova pravila upravljaju svrhom, izvođenjem i metodologijom upravljanja uslugom, kao i odgovornostima i sigurnosnim uslovima koje mora ostvariti TSP, pretplatnik na certifikat ili subjekat i treća lica koja se oslanjaju na te certifikate/usluge. |
| **CPS** | Izjava o korištenju certifikata predstavlja opća pravila TSP-a. |
| **CPOID** | Međunarodni broj kojim je definiše identifikator pravila o certifikaciji. |
| **CRL** | Spisak opozvanih certifikata |
| **DN** | Jedinstveni prepoznatljivi naziv |
| **LDAP** | Aplikacijski protokol za čitanje i pisanje imenika je protokol koji daje pristup imeniku i određuje ga IETF (Radno tijelo za razvoj interneta) u svojoj preporuci IETF REC 3494. |
| **S/MIME** | Sigurne višenamjenske ekstenzije e-pošte na internetu |
| **SSL** | Sloj sigurnih utičnica |
| **TLS** | Sigurnost sloja transporta |
| **PKI** | Infrastruktura javnog ključa |
| **QSCD** | Sredstvo za izradu kvalifikovanih potpisa (sigurni nosač za privatne ključeve) |

### 1.6.2 Akronimi

| | |
|---|---|
| **Pružalac usluga povjerenja (TSP)** | Fizičko ili pravno lice koje izdaje certifikat ili pruža druge usluge povjerenja. |
| **Spremište certifikata (centralni direktorij)** | Spremište certifikata u skladu sa X.500 smjernicama gdje se certifikati pohranjuju prema preporuci iz smjernica X.509, verzija 3, kojem se može pristupiti putem LDAP protokola. |
| **Identifikacija** | Identifikacijom se označava procedura za korištenje ličnih podataka u fizičkoj ili elektronskoj formi koje zajedno predstavljaju fizičko ili pravno lice, ili fizičko lice koje predstavlja pravno lice. |
| **Registracijsko tijelo (RA)** | Usluga ili lice koje prima Obrasce za zahtjeve za izdavanje certifikata, zahtjeve za opoziv, identifikaciju i verifikaciju identiteta budućih pretplatnika i subjekata u ime TSP-a. |
| **Prepoznatljivo ime** | Jedinstveno ime u certifikatu (DB), koje bez dileme i na jedinstven način identifikuje korisnika u strukturi direktorija. |

# 2. ODGOVORNOSTI OBJAVLJIVANJA I ODRŽAVANJA SPREMIŠTA

## 2.1. Spremišta

(1) TSP Halcom CA će na web stranici Halcoma CA (http://www.halcom.si) javnosti učiniti dostupno sve što ima veze sa njegovim poslovanjem, obavještenja subjektima i trećim licima kao i ostale relevantne dokumente.

(2) Dokumenti dostupni za javnost su:

1. cjenovnik,
2. pravila o certifikatima (CP),
3. Izjave o korištenju certifikata TSP-a (CPS)
4. Obrasci izjave za zahtjev za certifikat, zahtjevi za opoziv, i ostale usluge koje su predmet ugovora sa TSP-om,
5. upute za sigurno korištenje digitalnih certifikata,
6. informacije o važećim uredbama i standardima u vezi sa poslovanjem TSP-a, i
7. ostale informacije vezane za poslovanje Halcoma CA.

(3) Dokumenti koji čine povjerljivi dio interih pravila TSP-a Halcom CA nisu dostupni javnosti.

## 2.2. Objava informacija o certifikaciji

(1) CPS i nova pravila se objavljuju u skladu sa navodima iz odjeljka 9.10.

(2) Svi TSP certifikati se temelje na X.509 standardu i objavljuju se u centralnom direktoriju na serveru ldap.halcom.si, koji je u vlasništvu Halcoma CA. U svrhu zaštite podataka, javnosti je dostupan samo registar opozvanih certifikata koji je dio direktorija.

(3) Status opozvanih certifikata se objavljuje odmah u registru opozvanih certifikata (detaljnije objašnjeno u odjeljku 4.9.8), a ostale javno dostupne informacije ili dokumenti se objavljuju prema potrebi.

(4) Pristup direktoriju izdatih certifikata je dozvoljen samo ovlaštenim korisnicima koji potvrđuju veći broj izdatih certifikata.

## 2.3. Vrijeme ili učestalost objavljivanja

(1) CPS ili nova pravila se objavljuju najkasnije sljedećeg radnog dana nakon što budu prihvaćena.

(2) Halcom CA će se pobrinuti da certifikati budu odmah objavljeni u centralnom direktoriju (nakon najviše 5 sekundi) nakon objavljivanja.

(3) Spisak opozvanih certifikata će se odmah osvježiti (najviše 5 sekundi) nakon opozivanja certifikata iz javnog registra opozvanih certifikata Halcoma CA. Uz odgodu od nekoliko minuta, spisak poučenih certifikata se također objavljuje na web stranici.

(4) Javno dostupne informacije ili dokumenti (osim gore navedenih) se objavljuju po potrebi.

## 2.4. Kontrola pristupa spremištima

(1) Centralni direktorij je dostupan na serveru ldap.halcom.si, TCP port 389 prema LDAP protokolu. Javno je dostupan samo registar opozvanih certifikata, koji je dio direktorija.

(2) Uz odgovarajuće tehničke mjere sigurnosti informacija, Halcom CA osigurava kontrole koje sprječavaju neovlašteno dodavanje, mijenjanje ili brisanje podataka u javnom direktoriju certifikata.

# 3. IDENTIFIKACIJA I POTVRDA AUTENTIČNOSTI

## 3.1. Imenovanje

Prepoznatljivi nazivi, sadržani u certifikatu, nedvosmisleno i jedinstveno identifikuju subjekat certifikata, osim ako to nije drugačije propisano ovim CPS-om ili sadržajem kvalifikovanog digitalnog certifikata.

### 3.1.1 Vrste naziva

(1) U skladu sa IETF RFC 5280, svaki certifikat sadrži informacije o subjektu i TSP-u u obliku prepoznatljivog naziva. Prepoznatljivo ime je dizajnirano u skladu sa IETF RFC 5280 i X.501 standardom.

(2) TSP je naveden u izdatom certifikatu u polju Izdavalac. Osnovne informacije o subjektu sadržane u prepoznatljivom nazivu certifikata za fizička ili pravna lica navedene su u polju Subjekat izdatog certifikata.

(3) Serijski broj, koji je također uvršten u prepoznatljivi naziv, određuje TSP Halcom CA (više pojedinosti u odjeljku 3.1.5).

(4) Prema eIDAS Uredbi i ETSI standardima, Halcom CA može, u formiranju prepoznatljivog imena stranih fizičkih osoba i / ili stranih poslovnih subjekata, koristiti i druge semantičke identifikatore fizičkih osoba i poslovnih subjekata, poput "PNO", "IDC "ili" PAS "i ISO 3161-1 kod države za identifikaciju na temelju nacionalnog identifikacijskog broja ili broja pasoša ili lične karte za fizičke osobe i poslovne subjekte" NTR "i ISO 3161-1 kod države za identifikaciju na temelju identifikatora iz nacionalnog registra poslovnih subjekata ili lokalni identifikator (dva znaka prema lokalnoj definiciji u određenoj zemlji, koja se smatra prikladnom na nacionalnoj i europskoj razini).

(1) Ponuđač usluge od povjerenja Halcom CA može prilikom izdavanja kvalifikovane digitalne potvrde u polje Imaoc (eng. Subject) dodati atribut 1.3.6.1.4.1.5939.2.9 koji predstavlja vrstu ponude (npr. označava da se radi o cloud certifikatu, certifikatu na pemtnoj kartici ili USB ključu).

**Certifikati pružaoca usluga povjerenja Halcom CA**:

| Tip certifikata | Naziv polja | Prepoznatljivo ime |
|---|---|---|
| Korijenski certifikat | Izdavalac i subjekat | C= SI<br>O= Halcom d.d.<br>2.5.4.97 = VATSI-43353126<br>CN= Halcom korijensko certifikacijsko tijelo |
| Posrednički/podređeni certifikat za pravna lica | Izdavalac | C= SI<br>O= Halcom d.d. |

| | | |
|---|---|---|
| | | 2.5.4.97 = VATSI-43353126<br>CN= Halcom korijensko certifikacijsko tijelo |
| | Subjekat | C= SI<br>O= Halcom d.d.<br>2.5.4.97= VATSI-43353126<br>CN= Halcom CA PO e-signature 1 ili<br>CN= Halcom CA PO e-signature 2 |
| Posrednički/podređeni certifikat za fizička lica | Izdavalac | C= SI<br>O= Halcom d.d.<br>2.5.4.97 = VATSI-43353126<br>CN= Halcom korijensko certifikacijsko tijelo |
| | Subjekat | C= SI<br>O= Halcom d.d.<br>2.5.4.97= VATSI-43353126<br>CN= Halcom CA FO e-signature 1 ili<br>CN= Halcom CA FO e-signature 2 |
| Posrednički/podređeni certifikat za elektronske pečate | Izdavalac | C= SI<br>O= Halcom d.d.<br>2.5.4.97 = VATSI-43353126<br>CN= Halcom korijensko certifikacijsko tijelo |
| | Subjekat | C= SI<br>O= Halcom d.d.<br>2.5.4.97= VATSI-43353126<br>CN= Halcom CA PO e-seal 1 ili<br>CN= Halcom CA PO e-seal 2 |
| Posrednički/podređeni certifikat za potvrdu autentičnosti web stranice | Izdavalac | C= SI<br>O= Halcom d.d.<br>2.5.4.97 = VATSI-43353126<br>CN= Halcom korijensko certifikacijsko tijelo |
| | Subjekat | C= SI<br>O= Halcom d.d.<br>2.5.4.97= VATSI-43353126<br>CN= Halcom CA web 1 |
| Posrednički/podređeni certifikat za vremenske pečate | Izdavalac | C= SI<br>O= Halcom d.d.<br>2.5.4.97 = VATSI-43353126<br>CN= Halcom korijensko certifikacijsko tijelo |
| | Subjekat | C= SI<br>O= Halcom d.d.<br>2.5.4.97= VATSI-43353126<br>CN= Halcom CA TSA 1 |

- Certifikati krajnjih korisnika

| Tip certifikata | Naziv polja | Prepoznatljivo ime |
|---|---|---|
| Certifikat za pravna lica (e-signature) | Izdavalac | C= SI<br>O= Halcom d.d.<br>2.5.4.97= VATSI-43353126<br>CN= Halcom CA PO e-signature 1 ili<br>CN= Halcom CA PO e-signature 2 |
| | Subjekat | C= SI<br>O= <name of legal person><br>2.5.4.97=<VAT+2 character ISO country code-identifier><br>and/or<br>1.3.6.1.4.1.5939.2.3=<VAT number of legal person><br>CN=<name and surname><br>SN= <surname><br>G= <name><br>SERIALNUMBER=<TIN+2 character ISO country code-identifier><br>and/or |

| | | |
|---|---|---|
| | | 1.3.6.1.4.1.5939.2.2= <TIN number of natural person><br>E= <e-mail> |

| | | |
|---|---|---|
| Certifikat za fizička lica (e-signature) | Izdavalac | C= SI<br>O= Halcom d.d.<br>2.5.4.97= VATSI-43353126<br>CN= Halcom CA FO e-signature 1 ili<br>CN= Halcom CA FO e-signature 2 |
| | Subjekat | C= SI<br>CN=<name and surname> SN= <surname><br>G= <name><br>SERIALNUMBER=<TIN+2 character ISO country code-identifier> and/or<br>1.3.6.1.4.1.5939.2.2=<TIN number of natural person> E= <email> |
| Certifikat za elektronske pečate | Izdavalac | C= SI<br>O= Halcom d.d.<br>2.5.4.9= VATSI-43353126<br>CN= Halcom CA PO e-seal 1 ili<br>CN= Halcom CA PO e-seal 2 |
| | Subjekat | C= SI<br>O= <name of legal person> 2.5.4.97=<VAT+2 character ISO country code-identifier><br>and/or<br>1.3.6.1.4.1.5939.2.3= <VAT number of legal person><br>CN=<name of the information system or department><br>E= <email> |
| Certifikat za potvrdu autentičnosti web stranice | Izdavalac | C= SI<br><br>O= Halcom d.d.<br>2.5.4.97= VATSI-43353126<br>CN= Halcom CA web 1 |
| | Subjekat | C= SI<br>O= <name of legal person><br>2.5.4.97=<VAT+2 character ISO country code-identifier><br>and/or<br>1.3.6.1.4.1.5939.2.3= <VAT number of legal person><br>OU= server or web certificates<br>CN=<website name and domain><br>SN= <domain><br>G= <website name><br>E = <e-mail> |
| Certifikat za vremenske pečate | Izdavalac | C= SI<br>O= Halcom d.d.<br>2.5.4.97= VATSI-43353126<br>CN= Halcom CA TSA 1 |
| | Subjekat | C= SI<br>O= <name of legal person or trust service provider><br>2.5.4.97=<VAT+2 character ISO country code-identifier><br>and/or<br>1.3.6.1.4.1.5939.2.3= <VAT number of legal person><br>CN=<name of the certificate or time-stamping service><br>E= <e-mail> |

### 3.1.2 Potreba za kreiranjem imena sa značenjem

(1) Oznaka fizičkog ili pravnog lica koja je dio prepoznatljivog imena u skladu sa odredbama Odjeljka 3.1.1 mora ispunjavati sljedeće zahtjeve:

- mora biti jedinstveno registrovana u poslovnom ili drugom zvaničnom registru,
- mora biti smisleno povezana sa fizičkim ili pravnim licem,
- maksimalna dužina može biti četrdeset i dva (42) znaka.

(2) U slučaju certifikata za potvrdu autentičnosti web stranice, ime web stranice mora biti potpuno kvalifikovano ime domene.

(3) Halcom CA zadržava pravo da odbije firmu, ime ili brend pravnog lica ako utvrdi:

- da je neprikladna ili uvredljiva,
- zavarava treće strane ili već pripada drugom pravnom ili fizičkom licu,
- da je u suprotnosti sa važećim propisima.

### 3.1.3 Anonimnost ili pseudonimi pretplatnika

Upotreba anonimnih imena ili pseudonima nije dozvoljena.

### 3.1.4 Pravila za tumačenje raznih oblika naziva

(1) Informacija o subjektu certifikata u prepoznatljivom nazivu sadrži slova engleske abecede, a preostali znakovi se pretvaraju kako slijedi:

| Znak | Konverzija |
|---|---|
| Č | C |
| Ć | C |
| Đ | DJ |
| Š | S |
| Ž | Z |
| Ü | UE |
| Ö | OE |
| Ø | OE |
| ß | SS |
| Ń | N |
| Ŕ | RZ |

(2) Uz odgovarajuću kombinaciju slova, TSP će se pobrinuti za korištenje drugih nepredviđenih znakova.

### 3.1.5 Jedinstvenost naziva

Prepoznatljivi nazivi su jedinstveni za svaki izdati certifikat, te na nedvosmislen i jedinstven način identifikuju subjekat u strukturi direktorija.

### 3.1.6 Prepoznavanje, potvrda autentičnosti i uloga zaštitnih znakova

(1) Pravna ili fizička lica ne smiju zatražiti da koriste imena državnih organa ili organa lokalne zajednice, vlastita imena, oznake, zaštitne znakove ili druge elemente intelektualnog vlasništva koji pripadaju trećim licima i čime bi se prekršila prava intelektualnog vlasništva ili druga prava trećih lica ili odredbe važećih propisa.

(2) Potencijalni sporovi se rješavaju isključivo između povrijeđene strane i subjekta certifikata.

(3) Odgovornost u vezi korištenja imena ili zaštićenih zaštitnih znakova je isključivo na strani pravnog lica. TSP Halcom CA nije obavezan da provjeri i/ili upozori subjekat ili pravno lice.

## 3.2. Prva validacija identiteta

Identitet budućeg subjekta prilikom prvog izdavanja certifikata provjerava se u TSP-u RA ili direktno u TSP-u Halcom CA. Halcom CA prije izdavanja certifikata provjerava podatke budućeg subjekta i pravnog lica u odgovarajućim registrima.

### 3.2.1 Metod za dokazivanje posjedovanja privatnog ključa

Demonstracija postojanja privatnog ključa koji pripada javnom ključu u certifikatu osigurava se sigurnim procedurama prije i prilikom prihvatanja certifikata i standardom PKCS # 10.

### 3.2.2 Potvrda autentičnosti identiteta organizacije

(1) Podaci o pravnom licu daju se prepoznatljivim imenom, vidi odjeljak 3.1.1 i 3.1.2.

2) Zakonski predstavnik pravnog lica svojim potpisom garantuje tačnost podataka u dokumentaciji za dobijanje certifikata.

(3) TSP Halcom CA će provjeriti ispravnost podataka o pravnom licu i identitet odgovornog lica sa odgovarajućim službama, službenim evidencijama ili u službenoj dokumentaciji.

(4) Halcom CA će, na osnovu zahtjeva za certifikat za provjeru autentičnosti web stranice, provjeriti vlasništvo nad domenom (naznačeno na zahtjevu) kod ovlaštenog registra domena.

### 3.2.3 Potvrda autentičnosti individualnog identiteta

(1) RA TSP Halcom CA će provjeriti identitet subjekata certifikata u skladu sa važećim propisima (službeni dokument sa slikom) ili obezbjeđuje podatke o imaocima iz svojih baza podatak, dobivenih upotrebom postupka od strane prijavne službe koja se koristi u drugu svrhu, što pruža ekvivalentno uvjerenje.

(2) TSP Halcom CA će provjeriti lične podatke subjekta u odgovarajućim registrima, osim ako je drugačije određeno važećim propisima.

### 3.2.4 Nepotvrđene informacije o pretplatnicima

Halcom CA ne provjerava tačnost i rad e-maila subjekta.

### 3.2.5 Validacija ovlasti

Zakonski predstavnik pravnog lica, potpisivanjem obrasca zahtjeva za izdavanje certifikata, garantuje da želi pribaviti certifikat za pravno lice i / ili određeno fizičko lice koje je zaposleno kod ili obavlja poslove za ovo pravno lice.

### 3.2.6 Kriteriji za međusobnu saradnju

(1) TSP Halcom CA nije obavezan da ugovara ili garantuje za druge pružaoce usluga povjerenja čak i ako drugi TSP ima status kvalifikovanog TSP-a ili TSP-a kvalifikovanih digitalnih certifikata.

(2) TSP Halcom CA će osigurati da uzajamno priznavanje bude dozvoljeno tek nakon potpisivanja pisanog ugovora sa drugim TSP-ovima, ali samo ako ispunjavaju nivo sigurnosnih zahtjeva koji su približni ili veći od onih koje propisuje TSP Halcom CA.

(3) Ako nije garantovana vanjska i nezavisna procjena usklađenosti drugog TSP-a, ovlaštena lica Halcom CA-a pregledavaju interna pravila drugog TSP-a i njegovu usklađenost sa sigurnosnim zahtjevima

(4) Trošak potrebne infrastrukture koju zahtijeva TSP Halcom CA za uzajamno priznavanje snosi drugi TSP.

## 3.3. Identifikacija i potvrda autentičnosti za zahtjeve za ponovno izdavanje ključa

### 3.3.1 Identifikacija i potvrda autentičnosti za rutinsko ponovno izdavanje ključa

Identitet subjekata u ponovnom izdavanju certifikata se provjerava:

- u RA TSP-a Halcom CA
- na osnovu već izdatog validnog digitalnog certifikata koji je izdao TSP, gdje TSP Halcom CA provjerava podatke o pravnom licu i / ili fizičkom licu u relevantnim registrima.

### 3.3.2 Identifikacija i potvrda autentičnosti za ponovno izdavanje ključa nakon opoziva

Verifikacija subjekata se provodi u skladu sa odredbama odjeljka 3.2.3.

## 3.4. Identifikacija i potvrda autentičnosti za zahtjeve za opoziv

(1) Zahtjev za opoziv certifikata podnosi pravno lice ili subjekat:
• lično u RA, gdje ovlaštena lica verifikuju identitet podnosioca zahtjeva,
• elektronskim putem, ali zahtjev za opoziv mora biti digitalno potpisan sa kvalifikovanim certifikatom, čime se pokazuje identitet podnosioca zahtjeva,
• Ako vlasnik potvrde preko telefona ili elektronske pošte zahtjeva poništenje potvrde, ponuđač usluge povjerenja Halcom CA odredi suspenziju potvrde. Tek na osnovu pismenog zahtjeva za poništenje potvrde se stvarno izvede prekid potvrde.

(2) Detaljna procedura za opoziv: odjeljak 4.9.3.4.9.3.

# 4. OPERATIVNI ZAHTJEVI ŽIVOTNOG CIKLUSA CERTIFIKATA

## 4.1. Zahtjev za izdavanje certifikata

### 4.1.1 Ko može podnijeti zahtjev za certifikat

Budući predmet certifikata su fizička lica, fizička lica identifikovana u saradnji sa pravnim licem ili pravnim licima za svoje uređaje.

Za dobijanje certifikata, moraju biti ispunjeni sljedeći uslovi:

- popunjen i lično dostavljen obrazac prijave za certifikat ili ugovor u RA,
- identifikacijski uslovi,
- finansijski uslovi.

Budućem imaocu neće se izdati potvrda ako je poslovni subjekt ili opunomoćenik uključen u popis osoba protiv kojih se primjenjuju restriktivne mjere (sankcije) Ujedinjenih naroda, Europske unije, Republike Slovenije, Ujedinjenog Kraljevstva, Kanade, Australije ili Sjedinjenih Država.

### 4.1.2 Proces upisa i odgovornosti

(1) Kvalifikovani certifikati za fizička lica koja su povezana sa pravnim licima:

1) Certifikat se izdaje na osnovu uredno popunjenog i potpisanog obrasca zahtjeva za izdavanje certifikata od strane zakonskog predstavnika pravnog lica i budućeg subjekta certifikata. Zakonski predstavnik podnosi zahtjev za izdavanje certifikata RA-u Halcom CA-a i izmiruje finansijske obaveze vezane za izdavanje certifikata. Obrasci za podnošenje

certifikata mogu se dobiti od Halcom CA RA-a i sa Halcom CA web stranice. Cjenovnik usluga je javno dostupan na web stranici Halcom-a CA.

2) Potpisivanjem obrasca prijave za certifikat, zakonski predstavnik ovlašćuje fizičko lice koje sarađuje sa pravnim licem (subjekat digitalnog certifikata) da u ime i za račun pravnog lica valjano potpiše obrazac zahtjeva elektronskog certifikata za obnovu postojećeg digitalnog certifikata ili za izdavanje novog sa istim podacima u skladu sa važećom politikom i cjenovnikom TSP-a Halcom CA, ali samo pod uslovom da se može izvršiti validacija sigurnog elektronskog potpisa.

3) Zakonski predstavnik pravnog lica podnosi zahtjev prijave za certifikat u pisanom obliku.

4) Prije izdavanja obrasca prijave za certifikat, Halcom CA obavještava pravno lice i budućeg subjekta o pravilima i o CPS-u TSP-a Halcom CA.

5) Prije izdavanja obrasca prijave za certifikat, Halcom CA obavještava buduće subjekte o pravilima, CPS-u i o poslovanju TSP-a Halcom CA.

(2) Kvalifikovani certifikati za fizička lica:

1) Certifikat se izdaje na temelju valjano ispunjenog i potpisanog obrasca prijave za certifikat od strane budućeg subjekta certifikata (fizičko lice). Fizičko lice podnosi obrazac prijave za certifikat RA-u Halcoma CA i podmiruje finansijske obaveze u vezi sa izdavanjem certifikata. Obrazac prijave za certifikat se može dobiti u RA-u Halcoma CA i na web stranici Halcoma CA. Cjenovnik usluga je javno dostupan na web stranici Halcoma CA.

2) Budući subjekat certifikata podnosi obrazac prijave za certifikat u pisanom obliku.

3) Prije izdavanja obrasca prijave za certifikat, Halcom CA obavještava buduće subjekte o pravilima, CPS-u i o poslovanju TSP-a Halcom CA.

(3) Kvalifikovani certifikati za elektronske pečate:

1) Certifikat se izdaje na temelju valjano ispunjenog i potpisanog obrasca prijave za certifikat od strane zakonskog predstavnika pravnog lica. Zakonski predstavnik podnosi obrazac prijave za certifikat RA-u Halcoma CA i podmiruje finansijske obaveze u vezi sa izdavanjem certifikata. Obrazac prijave za certifikat se može dobiti u RA-u Halcoma CA i na web stranici Halcoma CA. Cjenovnik usluga je javno dostupan na web stranici Halcoma CA.

2) Potpisivanjem obrasca prijave za certifikat, zakonski predstavnik dozvoljava elektronsku obnovu postojećeg digitalnog certifikata ili izdavanje novog sa istim podacima u skladu sa važećom politikom i cjenovnikom TSP-a Halcom CA, ali samo pod uslovom da se može izvršiti validacija kvalifikovanog elektronskog potpisa.

3) Zakonski predstavnik pravnog lica podnosi zahtjev prijave za certifikat u pisanom obliku.

4) Prije izdavanja obrasca prijave za certifikat, Halcom CA obavještava buduće subjekte o pravilima, CPS-u i o poslovanju TSP-a Halcom CA.

(4) Kvalifikovani certifikati za potvrdu autentičnosti web stranice:

1) Certifikat se izdaje na temelju valjano ispunjenog i potpisanog obrasca prijave za certifikat od strane vlasnika web stranice (fizičko lice ili zakonski predstavnik pravnog lica). Vlasnik web stranice podnosi obrazac prijave za certifikat RA-u Halcoma CA i podmiruje finansijske obaveze u vezi sa izdavanjem certifikata. Obrazac prijave za certifikat se može dobiti u RA-u Halcoma CA i na web stranici Halcoma CA. Cjenovnik usluga je javno dostupan na web stranici Halcoma CA.

2) Vlasnik web stranice podnosi obrazac prijave za certifikat u pisanom obliku.

3) Prije izdavanja obrasca prijave za certifikat, Halcom CA obavještava buduće subjekte o

pravilima, CPS-u i o poslovanju TSP-a Halcom CA.

(5) Kvalifikovani certifikati za vremenske pečate:

1) Certifikati za vremenske pečate su namijenjeni samo za TSP.

2) TSP Halcom CA nije obavezan da zaključuje ugovore sa drugim TSP-ovima čak i ako drugi TSP ima status kvalifikovanog TSP-a.

3) TSP Halcom CA osigurava izdavanje certifikata nakon potpisivanja pisanog ugovora sa drugim TSP-om koji mora ispunjavati nivo sigurnosnih zahtjeva koji su približni ili veći od onih koje propisuje TSP Halcom CA.

4) Ako se ne garantuje eksterno i nezavisno ocjenjivanje usklađenosti sa drugim TSP-om, ovlaštena lica iz Halcoma CA pregledaju interna pravila drugog TSP-a i njihovu usklađenost sa sigurnosnim zahtjevima.

5) Prije izdavanja obrasca prijave za certifikat, Halcom CA obavještava buduće subjekte o pravilima, CPS-u i o poslovanju TSP-a Halcom CA.

6) Halcom CA zadržava pravo da odbije obrazac prijave za certifikat bez posebnog pismenog objašnjenja zbog neodgovarajućih podataka, dokumentacije ili sigurnosnih ili pravnih razloga.

## 4.2. Obrada zahtjeva za izdavanje certifikata

### 4.2.1 Obavljanje funkcija identifikacije i potvrde autentičnosti

(1) Ovlašteno lice iz RA potvrđuje identitet zakonskog predstavnika i/ili subjekta koji ima važeći identifikacijski dokument sa slikom prilikom posjete RA-u ili putem kurirske službe po isporuci certifikata.

(2) U slučaju elektronskog slanja obrasca prijave za certifikat, ovlašteno lice ili server TSP-a Halcom CA provode validaciju elektronskog potpisa/pečata. Identitet budućeg subjekta i/ili pretplatnika se dokazuje uz dokazivanje validnosti njegovog elektronskog potpisa ili pečata.

(3) Ovlaštena lica moraju obavezno provjeriti identitet pravnog lica i/ili budućih subjekata ili svih podataka koji se navode na obrascu prijave za certifikat i koji su dostupni u zvaničnoj evidenciji ili drugim službenih važećim dokumentima.

(4) RA provjerava popunjene obrasce prijave za certifikate i preuzimaju originalnu dokumentaciju koju na siguran način prenosu Halcomu CA.

### 4.2.2 Odobravanje ili odbijanje zahtjeva za izdavanje certifikata

(1) Ovlaštena lica u TSP-u Halcom CA odobravaju obrazac prijave za certifikat ili ga odbijaju u slučaju netačnih ili nepotpunih podataka, ili neispunjavanja obaveza, o čemu se pravno lice ili budući subjekat odmah obavještavaju lično ili putem emaila.

(2) U slučaju odobravanja, Halcom CA obavještava budućeg subjekta, prije izdavanja certifikata, u skladu sa važećim odredbama.

### 4.2.3 Vrijeme za obradu zahtjeva za izdavanje certifikata

Na temelju prethodno odobrenih zahtjeva za izdavanje certifikata i podmirenih finansijskih obaveza u vezi sa izdavanjem certifikata, Halcom CA izdaje certifikat najkasnije u roku od pet (5) radnih dana od primitka uplate.

## 4.3. Izdavanje certifikata

### 4.3.1 TSP Halcom CA aktivnosti tokom izdavanja certifikata

(1) Proizvodni proces za izdavanje certifikata zavisi od vrste certifikata:

- Napredni kvalifikovani certifikati

  Proizvodni proces za certifikate i za dva para ključeva sastoji se od jasno razdvojenih dijelova (ili funkcija), sa svojim zasebnim podsistemima:

  1. pred-predstavljanje QSCD-a (generisanje ključeva na kartici, postavljanje lozinke za osiguranje certifikata)
  2. dobijanje obrasca zahtjeva za izdavanje certifikata,
  3. pregled obrasca zahtjeva za izdavanje certifikata,
  4. priprema certifikata,
  5. kreiranje QSCD-a (izdavanje i pohranjivanje certifikata, ispis podataka o subjektu)
  6. štampanje privatne šifre (PIN koda),
  7. distribucija certifikata i privatne lozinke (PIN koda) i obavještenja subjektu.

  Napredni certifikat za QSCD i pripadajuća privatna šifra (PIN kod) subjektu se šalju preporučenom poštom, u dvije odvojene pošiljke, u dva odvojena radna dana. Iznimno, isporuku može subjektu predati i ovlaštena osoba Halcom CA RA lično.

- Kvalifikovani cloud certifikati

  Proizvodni proces za certifikate i za jedan par ključeva se sastoji od jasno razdvojenih dijelova (ili funkcija), sa svojim zasebni podsistemima:

  1. pregled obrasca zahtjeva za izdavanje certifikata,
  2. priprema certifikata, registracije i aktivacijskog koda,
  3. slanje registracije i aktivacijskog koda i obavještenja subjektu,
  4. generisanje ključeva na sigurnoj cloud pohrani i izdavanje certifikata.

  Registracijski kod se subjektu šalje putem dva odvojena kanala, jedan putem e-pošte, a drugi putem drugog sigurnog kanala (siguran web portal kojem se može pristupiti kvalifikovanim certifikatom, preporučenom poštom ili putem posebne web stranice na kojoj se imaoc identificira posebnim kodom primljenim putem SMS-a i drugim podacima koji su mu poznati (npr. porezni broj nositelja, posljednje četiri znamenke ili CVV kod uplate ili kreditne kartice ili slično)). Iznimno, jedan od gore navedenih kodova može subjektu predati i ovlaštena osoba Halcom CA RA lično.

- Standardni kvalifikovani digitalni certifikat

  Proizvodni proces za certifikate i za jedan par ključeva se sastoji od jasno razdvojenih dijelova (ili funkcija), sa svojim zasebni podsistemima:

  1. pregled obrasca zahtjeva za izdavanje certifikata,
  2. priprema certifikata, referentnog broja i autorizacijskog koda,
  3. slanje referentnog broja, autorizacijskog koda i obavještenja subjektu,
  4. unos certifikata.

  Referentni broj se subjektu šalje e-poštom, a autorizacijski kod putem preporučene pošte. Iznimno, autorizacijski kod može subjektu predati i ovlaštena osoba Halcom CA RA lično.

- Kvalifikovani certifikat za potvrdu autentičnosti web stranice i informacijskih sistema

  Proizvodni proces za certifikate i za jedan par ključeva se sastoji od jasno razdvojenih dijelova (ili funkcija), sa svojim zasebni podsistemima:

  1. pregled obrasca zahtjeva za izdavanje certifikata,
  2. dobijanje elektronskog zahtjeva za izdavanje certifikata,

3. personalizacija i izdavanje certifikata,
4. slanje certifikata subjektu.

- Kvalifikovani certifikati za vremenske pečate

  Proizvodni proces za certifikate i za jedan par ključeva se sastoji od jasno razdvojenih dijelova (ili funkcija), sa svojim zasebni podsistemima:
  1. pregled sigurnosnih zahtjeva i internih pravila drugog TSP-a,
  2. pregled i potpisivanje ugovora za izdavanje certifikata,
  3. dobijanje elektronskog zahtjeva za izdavanje certifikata,
  4. pripremanje certifikata,
  5. personalizacija certifikata,
  6. prenos certifikata TSP-u.

(2) Pretplatnik i subjekat u pravilu nisu isto lice kao Halcom CA ili Halcom CA RA. Ako Halcom CA RA naruči certifikat za sebe ili sa svog ovlaštenog uposlenika, takav obrazac prijave za izdavanje certifikata dodatno s pažnjom provjerava osoblje Halcoma CA.

(3) Ako Halcom CA naruči certifikat za sebe ili za svoje ovlašteno lice, izdavanje svih takvih certifikata pažljivo provjeravaju interni službenici za reviziju ili službenik za regulatornu usklađenost.

(4) Procedure su osmišljene na način da ih ne može provoditi samostalno jedna osoba.

(5) Pružatelj usluga povjerenja Halcom CA može ovlastiti provjerene vanjske izvođače za određene poslove (npr. ispis podataka o vlasniku, printanje PIN-a, isporuku itd.) na temelju pisanog ugovora, što redovito prati i za koje je odgovoran kao da obavlja same zadatke.

### 4.3.2 Obavještenje o izdavanju certifikata koje pretplatniku dostavlja CA

Vidi prethodni odjeljak.

## 4.4. Prihvatanje certifikata

### 4.4.1 Postupak za prihvatanje certifikata

(1) Postupak prihvatanja certifikata zavisi od vrste certifikata:

- Napredni certifikati

  U slučaju naprednih certifikata, prihvatanje certifikata se ne primjenjuje jer budući subjekat prima certifikat putem QSCD-a, a pripadajuću ličnu šifru (PIN kod) putem preporučene pošte. U iznimnim slučajevima ovlašteno lice Halcoma CA može uručenje izvršiti lično, vidi odjeljak 4.3.1.

- Cloud certifikati

  U slučaju cloud certifikata, nije obavezno da certifikat bude prihvaćen budući da ga povjerenik Halcoma CA sigurno pohranjuje prema ovlaštenju subjekta. Subjektu se dostavljaju samo kodovi za pristup sigurnom cloud certifikatu, vidi odjeljak 4.3.1.

- Standardni certifikati

  U slučaju standardnih certifikata, budući subjekat u skladu sa uputama unosi certifikat koristeći softver Halcoma CA za unos certifikata. Autorizacijski kod se šalje preporučenom poštom budućem subjektu, vidi odjeljak 4.3.1.

- Certifikati za potvrdu autentičnosti web stranice, informacijskih sistema i vremenskih pečata

  Za certifikate za potvrdu autentičnosti web stranica, informacijskih sistema i vremenskih pečata, pravno lice pokreće generisanje ključeva i seta šifri za njihovu zaštitu. TSP Halcom CA kreira certifikat na temelju primljenog zahtjeva za izdavanje certifikata i šalje ga pravnom licu koje certifikat kreira koristeći pripadajući par ključeva uz unos gore navedene šifre.

(2) Subjekat certifikata ili pravno lice moraju odmah po primitku certifikata provjeriti podatke u certifikatu i odmah obavijestiti Halcom CA u slučaju potencijalnih grešaka ili problema.

### 4.4.2 Objavljivanje certifikata koje provodi CA

Postupak je opisan u odjeljku 2.

### 4.4.3 Obavještenje drugim licima o izdavanju certifikata od strane CA

TSP Halcom CA ne obavještava treće strane o izdavanju pojedinačnih certifikata. RA može doći u posjed informacija u vezi izdatih certifikata za koje je prihvaćen obrazac prijave za izdavanje certifikata.

## 4.5. Korištenje para ključeva i certifikata

### 4.5.1 Korištenje certifikata i privatnog ključa pretplatnika

(1) Subjekat ili budući subjekat certifikata imaju obavezu:

- upoznavanja i djelovanja u skladu sa pravilima prije izdavanja certifikata,
- poštovanja pravila i ostalih važećih odredbi,
- da provjere informacije na certifikatu nakon primanja certifikata ili aktivacije certifikata i u slučaju postojanja potencijalnih grešaka ili problem o tome odmah obavijeste Halcom CA ili zatraže opoziv certifikata

- praćenja i poštovanja svih obavještenja koja izda Halcom CA,
- da u skladu sa obavještenjima ažuriraju relevantni hardver i softver radi osiguranja sigurnog rada sa certifikatima,
- odmah obavijestiti Halcom CA o svim promjenama koje su vezane za certifikate,
- zatražiti opoziv certifikata u slučaju kompromitovanog privatnog ključa što može utjecati na pouzdanost korištenja, ili u slučaju rizika od zloupotrebe,
- zatražiti opoziv certifikata na cloudu u slučaju gubitka ili krađe mobilnog uređaja, ili u slučaju rizika od zloupotrebe,
- Koristiti certifikat u svrhu koja se navodi u certifikatu (vidi odjeljak 7.1) i na način određen pravilima Halcoma CA.

(2) Subjekat ili budući subjekat certifikata također ima sljedeće obaveze, u smislu zaštite privatnog ključa:
- pažljivo štititi podatke za upis ili aktivaciju certifikata od neovlaštenih lica,
- čuvati privatni ključ i certifikat na način i na uređajima za sigurnu pohranu privatnih ključeva u skladu sa obavještenjima i preporukama Halcoma CA,
- čuvati privatni ključ i sve ostale povjerljive informacije pod prikladnim šiframa u skladu sa preporukama Halcoma CA ili osigurati zaštitu pod kojom je pristup dat samo subjektu,
- pažljivo čuvati šifre za zaštitu ili pristup privatnom ključu,
- poduzeti korake u skladu sa obavještenjima Halcoma CA nakon isteka ili opoziva certifikata.

### 4.5.2 Obaveze treće strane koja koristi javni ključ i certifikat

(1) Treća strana koja se oslanja na certifikat mora:
- rukovati sa i koristiti certifikate u skladu sa pravilima i ostalim važećim odredbama,
- pažljivo ispitati sve rizike i odgovornosti koji se odnose na korištenje certifikata i utvrditi pravila za korištenje,
- informisati Halcom CA u slučaju da otkriju da su privatni ključevi subjekta certifikata kompromitovani na način koji može utjecati na pouzdanost korištenja ili u slučaju postojanja rizika od zloupotrebe, ili ako su podaci koji se navode u certifikatu promijenjeni,
- koristiti certifikat samo za svrhe koje se navode u certifikatu (vidi odjeljak 6.1.1) i na način koji je utvrđen pravilima,
- tokom certifikata osigurati da se certifikat ne nalazi u registru opozvanih certifikata,
- tokom korištenja certifikata potvrditi da je digitalni potpis/pečat kreiran tokom perioda validnosti i u skladu sa prikladnom svrhom certifikata,
- tokom korištenja certifikata potvrditi potpis TSP-a Halcom CA, koji je objavljen u ovom dokumentu CPS kao i na web stranici Halcoma CA.
- poštovati ostale propise u slučaju potpisivanja dodatnih ugovora o korištenju certifikata sa TSP-om Halcom CA.

(2) Za provjeru validnosti potpisa/pečata ili drugih kriptografskih operacija, treća strana mora koristiti softver i hardver kojima se mogu na siguran način provjeriti gore navedeni zahtjevi za sigurno korištenje certifikata.

## 4.6. Obnavljanje certifikata

(1) Samo subjekat certifikata može zatražiti obnavljanje certifikata.
(2) Nakon isteka naprednog certifikata, subjekat može, nakon jednog (1x) obnavljanja, podnijeti zahtjev za ponovno izdavanje certifikata.
(3) Prije isteka certifikata, subjekat certifikata može podnijeti elektronski zahtjev za izdavanje novog digitalnog certifikata koji on elektronski potpisuje validnim certifikatom.
(4) Proces obnavljanja certifikata za vremenske pečate i potvrde autentičnosti je isti kao i prvo izdavanje certifikata (vidi odjeljak 4.1)

### 4.6.1 Okolnosti za obnavljanje certifikata

Prije isteka validnosti digitalnog certifikata, subjekat certifikata osigurava kontinuitet za korištenje digitalnog certifikata podnošenjem elektronskog obrasca zahtjeva za obnavljanje. Međutim, moguće je podnijeti i obrazac zahtjeva za izdavanje novog certifikata nakon isteka validnosti digitalnog certifikata.

### 4.6.2 Ko može tražiti obnavljanje

Samo subjekat certifikata može tražiti obnavljanje certifikata.

### 4.6.3 Obrada zahtjeva za obnavljanje certifikata

Ovim postupkom se osigurava da je pravno lice i/ili fizičko lice koje podnosi zahtjev za obnavljanje certifikata uistinu subjekat certifikata i da je javni ključ nije promijenio.

### 4.6.4 Obavještenje pretplatniku o izdavanju novog certifikata

Vidi odjeljak 4.3.2.

### 4.6.5 Postupak za prihvatanje obnovljenog certifikata

Vidi odjeljak 4.4.1.

### 4.6.6 Objavljivanje obnovljenog certifikata od strane CA

Postupak je opisan u odjeljku 2.

### 4.6.7 Obavještenje ostalima o izdavanju certifikata od strane CA

Halcom CA ne obavještava pravna lica i druge organizacije o izdavanju pojedinačnih certifikata.

## 4.7. Regenerisanje ključa za certifikat

### 4.7.1 Okolnosti za regenerisanje ključa za certifikat

Nije podržano.

### 4.7.2 Ko može tražiti novi javni ključ

Nije podržano.

### 4.7.3 Obrada zahtjeva za regenerisanje ključa za certifikat

Nije podržano.

### 4.7.4 Obavještenje pretplatniku o izdavanju novog certifikata

Nije podržano.

### 4.7.5 Postupak prihvatanja regenerisanog ključa za certifikat

Nije podržano.

### 4.7.6 Objavljivanje regenerisanog ključa za certifikat od strane CA

Nije podržano.

### 4.7.7 Obavještenje drugim licima o izdavanju certifikata od strane CA

Nije podržano.

## 4.8. Izmjene certifikata

(1) U slučaju promjene informacija u certifikatu ili prepoznatljivom imenu, certifikat se mora opozvati.

(2) U svrhu dobijanja novog certifikata neophodno je ponoviti koraka procedure za dobijanje novog certifikata kao što se navodi u odjeljku 4.1.

### 4.8.1 Okolnosti za izmjenu certifikata

Nije podržano.

### 4.8.2 Ko može tražiti izmjenu certifikata

Nije podržano.

### 4.8.3 Obrada zahtjeva za izmjenu certifikata

Nije podržano.

### 4.8.4 Obavještenje pretplatniku o izdavanju novog certifikata

Nije podržano.

### 4.8.5 Postupak prihvatanja izmijenjenog certifikata

Nije podržano.

### 4.8.6 Objavljivanje izmijenjenog certifikata od strane CA

Nije podržano.

### 4.8.7 Obavještenje drugim licima o izdavanju certifikata od strane CA

Nije podržano.

## 4.9. Opozivanje i suspenzija certifikata

(1) Opozivanje certifikata može zatražiti pravno lice ili subjekat certifikata u bilo kojem trenutku, ali je ono obavezno u sljedećim slučajevima:

1. promjene u prepoznatljivom imenu (DN),
2. kad pravno lice ili subjekat certifikata izmijene ključne podatke koji se odnose na certifikat (ime ili

prezime, ime pravnog lica, e-mail adresa, zaposlenje, itd.)
3. kada se ustanovi ili kada se sumnja da je došlo do otkrivanja ključa za potpisivanje ili do zloupotrebe certifikata,
4. certifikat je zamijenjen drugim certifikatom (npr. kada dođe do gubitka certifikata, QSCD-a ili PIN-a za pristupanje QSCD-u).

(2) Halcom CA može opozvati certifikat i bez zahtjeva subjekta u slučajevima iz prvog stava ili na zahtjev nadležnog suda, organa za prekršaje ili upravnih jedinica.

(3) Opoziv certifikata je moguć 24 sata dnevno, svaki dan u godini. Detaljna uputstva za opozivanje certifikata objavljena su na Halcom CA web stranici.

(4) Na osnovu ispravnog zahtjeva za opoziv Halcom CA će opozvati certifikat najkasnije u roku od četiri (4) sata. U slučaju nastanka nepredviđenih okolnosti, Halcom CA će iznimno opozvati certifikat najkasnije osam (8) sati od prijema ispravnog zahtjeva za opoziv certifikata. Za to vrijeme opozvani certifikat će biti označen kao opozvan i dodan u registar opozvanih certifikata (CRL). Ako je subjekat certifikata podnio netačan zahtjev za opoziv certifikata, Halcom CA će obavijestiti subjekta o netačnom zahtjevu i uputiti ga da dostavi ispravan zahtjev za opoziv.

### 4.9.1 Okolnosti za opozivanje

(1) Opoziv certifikata mora zahtijevati pravno lice ili subjekat u slučaju:
- ako je privatni ključ subjekta certifikata ugrožen na način koji utiče na pouzdanost korištenja,
- ako postoji rizik od zloupotrebe privatnog ključa ili certifikata subjekta,
- ako su informacije u certifikatu promijenjene ili netačne.

(2) TSP Halcom CA ukida certifikat čak i bez zahtjeva subjekta po nastanku neke od sljedećih okolnosti:
- informacije iz certifikata se netačne ili je certifikat izdat na osnovu netačnih informacija,
- došlo je do greške u provjeri identiteta podataka u RA,
- promijenile su se druge okolnosti koje utiču na validnost certifikata,
- propust subjekta da ispuni obaveze,
- ne izmiruju se finansijske obaveze za digitalne certifikate,
- infrastruktura TSP je ugrožena na način koji utiče na pouzdanost certifikata,
- privatni ključ subjekta certifikata je ugrožen na način koji utiče na pouzdanost korištenja,
- Halcom CA će prestati sa izdavanjem certifikata ili je TSP-u zabranjeno da upravlja certifikatima, a njegove aktivnosti nisu preuzete od strane drugog TSP-a,

- Opoziv je zatražio nadležni sud, organ za prekršaje ili upravna jedinica.

(3) Subjekat digitalnog certifikata može zatražiti regenerisanje PIN-a za napredne certifikate trideset (30) dana nakon izdavanja ili referentni broj i autorizacijske kodove za standardne certifikate ili registracijske i aktivacijske kodove za cloud certifikate u slučaju da je zaboravio podatke za e-pristup i pod punom građanskom i krivičnom odgovornošću garantuje da ne postoji mogućnost da je ili da će privatni ključ biti kompromitovan na način koji može biti štetan za pouzdanost korištenja i da ne postoji rizik od zloupotrebe privatnog ključa ili certifikata subjekta.

### 4.9.2 Ko može zahtijevati opoziv

Zahtjev za opoziv certifikata može podnijeti:

- ovlašteno lice TSP-a Halcom CA,
- zakonski predstavnik pravnog lica,
- subjekat,
- nadležni sud, organ za prekršaje ili upravna jedinica.

### 4.9.3 Procedura slanja zahtjeva za opoziv

(1) Opoziv može zatražiti zakonski predstavnik pravnog lica ili subjekt:

• lično tokom radnog vremena u RA,

• elektronskim putem dvadeset i četiri (24) sata dnevno, u svim danima u godini, u slučaju mogućnosti zloupotrebe ili nepouzdanosti certifikata, a inače u službenom radnom vremenu državnih organa.

(2) Ako se zahtjev za opoziv podnosi:

- Lično, potrebno je popuniti odgovarajući zahtjev za opoziv certifikata i dostaviti ga RA;
- elektronski, subjekat mora poslati elektronsku poruku kompaniji Halcom CA sa zahtjevom za opoziv, koji mora biti digitalno potpisan / opečaćen sa pouzdanim certifikatom u svrhu njegove validacije.
- putem faksa, subjekat mora popuniti odgovarajući zahtjev za opoziv certifikata i poslati ga faksom na odgovarajući broj faksa (vidi odjeljak 1.3.1.), a naknadno i preporučenom poštom ili ga dostaviti u RA,
- • ako je subjekat zatražio opoziv certifikata putem telefona, e-maila ili faksa, TSP Halcom CA će obustaviti certifikat. Na osnovu pisanog zahtjeva za opoziv certifikata, izvršit će se stvarni opoziv certifikata.

(3) Pravno lice ili subjekat uvijek mora biti obaviješten o datumu, vremenu i razlozima opoziva.

(4) Sudovi, organi za prekršaje i upravne jedinice, koji mogu tražiti opoziv, to čine u skladu sa zakonima i službenim postupcima (krivični postupak, parnični postupak, opšti upravni postupak i drugi).

(5) Odredbe koje se odnose na opoziv se razumno primjenjuju na postupke koji se odnose na regenerisanje PIN kodova za napredne certifikate ili referentne brojeve i kodove autorizacije za standardne certifikate i kodove za registraciju i aktivaciju certifikata u oblaku.

### 4.9.4 Grace period za zahtjev za opoziv

Opoziv se mora zatražiti odmah ako postoji mogućnost zloupotrebe, nepouzdanosti ili sličnih hitnih slučajeva. U drugim slučajevima, opoziv se može zatražiti prvog radnog dana u zvaničnom radnom vremenu RA.

### 4.9.5 Vrijeme u kojem CA mora obraditi zahtjev za opoziv

(1) TSP Halcom CA nakon prihvatanja valjanog zahtjeva za opoziv:

- najkasnije u roku od četiri (4) sata, opoziva certifikat ako je opoziv podnesen zbog rizika od zloupotrebe ili nepouzdanosti itd.,
- u suprotnom, opoziva ga prvog radnog dana nakon prijema zahtjeva za opoziv

(2) Nakon opoziva, takav certifikat se odmah (u roku od najviše 5 sekundi) dodaje u registar opozvanih certifikata.

### 4.9.6 Zahtjev za provjeru opoziva za treće strane

Prije upotrebe treće strane koje se oslanjaju na certifikat moraju provjeriti najnoviji objavljeni registar opozvanih certifikata. Radi kredibiliteta i integriteta, uvijek je potrebno provjeriti vjerodostojnost ovog registra, koji je digitalno potpisan od strane Halcom CA

### 4.9.7 Učestalost izdavanja CRL-a

Registar opozvanih certifikata se osvježava (za pristup registru, vidi odjeljak 7.2.3):

- nakon svakog oduzimanja certifikata,
- najmanje jednom dnevno, ako ne postoje nove evidencije ili promjene u registru opozvanih certifikata, dvadeset četiri (24) sata nakon posljednjeg osvježavanja.

### 4.9.8 Maksimalna latencija za CRL

(1) Objavljivanje novog registra opozvanih certifikata se vrši:

- odmah u javnom direktoriju na serveru ldap://ldap.halcom.si (u roku od najviše 5 sekundi),
- na web stranici http://domina.halcom.si/crls uz maksimalnu odgodu od deset (10) minuta.

(2) TSP Halcom CA osigurava maksimalnu dostupnost svojih usluga, svakog dana u godini, bez uzimanja nepredviđenih okolnosti u obzir. U slučaju nepredviđenih kvarova i neplaniranih tehničkih ili servisnih intervencija na infrastrukturi, Halcom CA će objaviti registar opozvanih potvrda najkasnije u roku od 8 (osam) sati. U slučaju nepredviđenih okolnosti nastalih kao posljedica više sile ili vanrednih događaja, Halcom CA će iznimno objaviti registar opozvanih potvrda u roku od 24 sata, ali prije isteka posljednjeg važećeg registra opozvanih certifikata.

### 4.9.9 On-line opoziv / provjera dostupnosti statusa

On-line statusni protokol certifikata (OCSP) podržan je u skladu s evropskim i međunarodnim standardima i preporukama (vidi odjeljak 7.3). Provjera statusa certifikata u stvarnom vremenu može raditi s odgodom do jedne minute od objave novog registra.

### 4.9.10 Zahtjevi za provjeru online opoziva

Treće strane moraju uvijek provjeriti da li je certifikat na koji se oslanjanju zapravo opozvan.

### 4.9.11 Dostupni drugi oblici oglašavanja za opoziv

Nije podržano.

### 4.9.12 Posebni zahtjevi za kompromis ponovljenog izdavana ključa

Nije navedeno.

### 4.9.13 Okolnosti za suspenziju

(1) Ako subjekat certifikata traži opoziv putem telefona ili elektronskim putem, potvrda se privremeno obustavlja do prijema originalnog pisanog zahtjeva.

(2) Ako subjekat certifikata, treće lice ili drugo lice, sud, organ za prekršaje, upravna jedinica, srodne vlasti ili sam TSP izraze sumnju da je certifikat u suprotnosti sa politikom ili važećim propisima, certifikat će biti privremeno suspendovan do konačne odluke.

### 4.9.14 Ko može tražiti suspenziju

Vidi odjeljak 4.9.13.

### 4.9.15 Postupak podnošenja zahtjeva za suspenziju

Vidi odjeljak 4.9.13.

### 4.9.16 Trajanje perioda suspenzije

Vidi odjeljak 4.9.13.

## 4.10. Usluge statusa certifikata

### 4.10.1 Operativne karakteristike

(1) Registar opozvanih certifikata je javno dostupan na ldap://ldap.halcom.si/ serveru u okviru LDAP protokola i na http://domina.halcom.si/crls u okviru HTTP protokola.

(2) Protokol za online status certifikata je dostupan na http://ocsp.halcom.si.

(3) Pojedinosti o izdavanju i pristupu se mogu naći u odjeljcima 7.2 i 7.3.

### 4.10.2 Dostupnost usluge

(1) Validacija statusa certifikata je dostupna bez prekida, 24 sata u danu, svaki dan u godini.

(2) TSP Halcom CA osigurava maksimalnu dostupnost svojih usluga, svaki dan u godini, bez uzimanja u obzir nepredviđenih okolnosti. U slučaju nepredviđenih kvarova i neplaniranih tehničkih ili servisnih intervencija na infrastrukturi, Halcom CA će ponovo omogućiti validaciju statusa certifikata najkasnije u roku od 8 (osam) sati. U slučaju nepredviđenih okolnosti kao rezultat više sile ili vanrednih događaja, Halcom CA će iznimno omogućiti validaciju statusa certifikata u roku od 24 sata, ali prije isteka posljednjeg važećeg registra opozvanih certifikata.

### 4.10.3 Opcionalne karakteristike

Nije propisano.

## 4.11. Kraj pretplate

Veza između subjekta ili pravnog lica i TSP-a se prekida ako:

- certifikat subjekta istekne i on ga ne obnovi,
- certifikat se opozove a subjekat ne podnese zahtjev za izdavanje novog.

## 4.12. Otkrivanje kopija ključeva za dešifrovanje

### 4.12.1 Pravila i prakse za traženje kopija ključeva za dešifrovanje

Nije podržano.

### 4.12.2 Pravila i prakse enkapsulacije i traženja ključa za sesiju

Nije podržano.

### 4.12.3 Postupak kojim se zahtijeva otkrivanje kopije ključeva za dešifrovanje

Nije podržano.

# 5. KONTROLE UPRAVLJANJA, OPERATIVNE I FIZIČKE KONTROLE

(1) Halcom CA projektuje i implementira sve sigurnosne mjere u skladu sa porodicom standarda ISO / IEC 27000 i sa FIPS 140-2 Level 3 i ETSI tehničkim zahtjevima.

(2) Oprema Halcom CA je instalirana u zasebnim prostorijama i zaštićena je višeslojnim sistemom fizičke i protuprovalne tehničke zaštite. Oprema je zaštićena od neovlaštenog pristupa. Također je zaštićena sistemom zaštite od požara, sistemom protiv prolijevanja, ventilacijskim sistemom i višefaznim neprekidnim napajanjem električnom energijom.

(3) Halcom CA pohranjuje sigurnosne i distribucijske medije na takav način da se gubitak, upad ili neovlaštena upotreba ili izmjena pohranjenih podataka spriječi u najvećoj mogućoj mjeri. I za obnavljanje podataka i za arhiviranje važnih informacija, sigurnosne kopije se obezbjeđuju i pohranjuju na drugačijoj lokaciji od primarnog softvera za upravljanje certifikatima, kako bi se osigurala ponovna operacija u slučajevima gubitka podataka na primarnoj lokaciji.

(4) Detaljan opis infrastrukture Halcom CA, operacija, procedura upravljanja infrastrukturom i kontrola sigurnosne politike njegovog rada određuje se internim pravilima.

## 5.1. Kontrola fizičke sigurnosti

(1) Oprema TSP-a je zaštićena višeslojnim sistemom fizičke i elektronske sigurnosti.

(2) Zaštita infrastrukture TSP-a vrši se u skladu sa preporukama najvišeg nivoa zaštite.

(3) Kompletan opis TSP infrastrukture, njenih procedura upravljanja i zaštite određuje se internim pravilima TSP-a.

### 5.1.1 Lokacija i izgradnja stranice

(1) Oprema TSP Halcom CA nalazi se u posebnim, zaštićenim, zasebnim prostorijama.

(2) Osigurana je višeslojnim sistemom fizičke i elektronske sigurnosti.

(3) Detaljne odredbe sadržane su u internim pravilima TSP Halcom CA.

### 5.1.2 Fizički pristup

(1) Pristup infrastrukturi TSP-a dostupan je samo ovlaštenim osobama TSP-a u skladu sa njihovim zadacima i ovlaštenjima, vidi odjeljak 5.2.1.
(2) Svi pristupi su zaštićeni u skladu sa zakonodavstvom i preporukama.

(3) Detaljne odredbe sadržane su u internim pravilima TSP Halcom CA.

### 5.1.3 Napajanje i klima

(1) Infrastruktura TSP-a mora imati neprekidno napajanje i odgovarajuće sisteme klimatizacije.

(2) Detalji su navedeni u internim pravilima TSP Halcom CA.

### 5.1.4 Izloženost vodi

(1) Infrastruktura TSP-a nije izložena riziku od poplava, osim u slučaju više sile.

(2) Detalji su navedeni u internim pravilima TSP Halcom CA.

### 5.1.5 Sprječavanje i zaštita od požara

(1) Prostor pružaoca usluga povjerenja mora biti zaštićen od mogućeg izbijanja požara.

(2) Detalji su navedeni u internim pravilima TSP Halcom CA.

### 5.1.6 Pohranjivanje medija

(1) Nosači podataka, bilo u štampanom ili elektronskom obliku se sigurno pohranjuju u zaštićenim instalacijama.

(2) Sigurnosne kopije softvera i šifrovanih baza podataka Halcoma CA se redovno ažuriraju i pohranjuju na dva odvojena i fizički zaštićena područja na različitim lokacijama.

### 5.1.7 Odlaganje otpada

(1) Halcom CA garantuje sigurno odlaganje i uništavanje dokumenata u štampanom i elektronskom obliku.

(2) Odlaganje otpada provodi posebna komisija u skladu sa internim pravilima TSP-a Halcom CA.

(3) Detalji su navedeni u internim pravilima pružaoca usluga povjerenja Halcom CA.

### 5.1.8 Rezervne kopije izvan lokacije

Vidi odjeljak 5.1.6.

## 5.2. Proceduralne kontrole

### 5.2.1 Uloge povjerenja

(1) Operativnim, organizacionim i profesionalnim funkcionisanjem TSP-a Halcom CA-a upravlja službenik za internu reviziju odgovoran za upravljanje certifikatima.

(2) Ovlaštena lica TSP-a Halcom CA uključuju:
- uposlenike Halcoma CA
- RA.

(3) Zaposleni u TSP-u Halcom CA su raspoređeni u četiri organizacione grupe koje pokrivaju sljedeće značajne oblasti:
- upravljanje informacijskim sistemom,
- upravljanje certifikatima,
- sigurnost i kontrola,

- regulatorne oblasti.

| Organizaciona grupa | Uloga | Osnovni zadaci | Broj osoba |
|---|---|---|---|
| Upravljanje informacijskim sistemom | Administrator glavnog sistema | • Priprema početne konfiguracije sistema<br>• Početno podešavanje parametara za nove podređene TSP<br>• Postavljanje početne konfiguracije mreže<br>• Priprema nosača podataka za hitno ponovno pokretanje sistema u slučaju katastrofalnog gubitka sistema<br>• Sigurno čuvanje i distribucija kopija i nadogradnji na zasebnu lokaciju | 2 |
| | Administrator sistema | • Procedure za izdavanje certifikata za upravljanje<br>• Pomoć za podređene TSP<br>• Autorizovanje podređenih TSP-ova<br>• Pristup protokolu za potpisivanje certifikata<br>• Sigurno čuvanje i distribucija kopija i nadogradnji na zasebnu lokaciju | 2 |
| Upravljanje certifikatima | Sistemski operater 1 | • Priprema kopija sistema, nadogradnja i vraćanje softvera, sigurno pohranjivanje i distribuiranje kopija i nadogradnja udaljene lokacije<br>• Administrativne funkcije vezane za održavanje baze podataka TSP i pomoć u istraživanju odstupanja od pravila<br>• Mijenja ime servera i / ili mrežne adrese<br>• Izvođenje arhiviranja potrebnih sistemskih zapisa<br>• Štampanje PIN kodova<br>• Dnevni pregled sistema | 2 |
| | Operater za autorizaciju | • Potvrda certifikata i aktiviranje generisanja lozinki | 2 |
| | Operater za certifikaciju | • Pred-personalizacija QSCD-a<br>• Priprema certifikata (obrada potpisanih obrazaca za certifikate)<br>• Personalizacija (kreiranje certifikata o QSCD-u, podaci subjekta o QSCD-u)<br>• Distribucija certifikata | 2 |
| | Operater za kodove | • Podjela PIN kodova | 2 |
| | Službenik za registraciju | • Identifikacija pretplatnika / subjekata certifikata | 2 |
| Sigurnost i kontrola | Službenik za opoziv | • • Priprema zahtjeva za opoziv<br>• • Opoziv certifikata | 2 |
| | Administrator za sigurnost | • Određivanje sigurnosnih pravila i praćenje njihove usklađenosti<br>• Pregledanje dokumentacije sistema i kontrolnih dnevnika za | 2 |
| | | • praćenje rada<br>• Lična saradnja i pomoć u godišnjem popisu podređenih TSP | |
| | | • Kontrola sigurnosnih pravila i | 2 |

| | | | |
|---|---|---|---|
| | Službenik za internu reviziju | njihova usklađenost<br>• Praćenje dokumentacije sistema i kontrolnih dnevnika za kontrolu rada | |
| Regulatorne oblasti | Službenik za regulatornu usklađenost | • Nezavisno usmjeravanje, zaštita privatnosti i zaštita ličnih podataka<br>• Osiguranje poštovanja važećih evropskih i slovenskih propisa, međunarodnih standarda i preporuka<br>• Stručna pomoć menadžmentu i zaposlenima u operativnoj implementaciji mjera privatnosti i usklađenosti s propisima | 1 |

### 5.2.2 Neophodni broj osoba po zadatku

(1) Operativne radne uloge osmišljene su kako bi se spriječila mogućnost zloupotrebe u najvećoj mogućoj mjeri te su podijeljene između pojedinih, organizacijskih grupa:

**Organizacijska grupa:** Upravljanje informacijskim sistemom
**Uloga:** Administrator glavnog sistema
**Broj osoba:** 2
**Zadaci:**
1. Priprema početne konfiguracije sistema
2. Početno podešavanje parametara za nove podređene TSP
3. Postavljanje početne konfiguracije mreže
4. Priprema nosača podataka za hitno ponovno pokretanje sistema u slučaju katastrofalnog gubitka sistema
5. Sigurno čuvanje i distribucija kopija i nadogradnji na zasebnu lokaciju

**Organizacijska grupa:** Upravljanje informacijskim sistemom
**Uloga:** Administrator sistema **Broj osoba:** 2
**Zadaci:**
1. Procedure za izdavanje certifikata za upravljanje
2. Pomoć za podređene TSP
3. Autorizovanje podređenih TSP-ova
4. Pristup protokolu za potpisivanje certifikata
5. Sigurno čuvanje i distribucija kopija i nadogradnji na zasebnu lokaciju

**Organizacijska grupa:** Upravljanje certifikatima
**Uloga:** Sistemski operater 1 **Broj osoba:** 2
**Zadaci:**
1. Priprema kopija sistema, nadogradnja i vraćanje softvera, sigurno pohranjivanje i distribuiranje kopija i nadogradnja udaljene lokacije
2. Administrativne funkcije vezane za održavanje baze podataka TSP i pomoć u istraživanju odstupanja od pravila
3. Mijenja ime servera i / ili mrežne adrese
4. Izvođenje arhiviranja potrebnih sistemskih zapisa
5. Štampanje PIN kodova
6. Dnevni pregled sistema

**Organizacijska grupa:** Upravljanje certifikatima
**Uloga:** Operater za autorizaciju **Broj osoba:** 2
**Zadaci:**
1. Potvrda certifikata i aktiviranje generisanja lozinki

**Organizacijska grupa:** Upravljanje certifikatima
**Uloga:** Operater za certifikaciju **Broj**

**osoba:** 2
**Zadaci:**
1. Pred-personalizacija QSCD-a
2. Priprema certifikata (obrada potpisanih obrazaca za certifikate)
3. Personalizacija (kreiranje certifikata o QSCD-u, štampanje podataka o subjektu na QSCD)
4. Distribucija certifikata

**Organizacijska grupa:** Upravljanje certifikatima
**Uloga:** Operater za kodove
**Broj osoba:** 2
**Zadaci:**
1. Distribucija PIN kodova

**Organizacijska grupa:** Upravljanje certifikatima
**Uloga:** Službenik za registraciju **Broj**
**osoba:** 2
**Zadaci:**
1. Identifikacija pretplatnika / subjekata certifikata

**Organizacijska grupa:** Upravljanje certifikatima
**Uloga:** Službenik za opoziv
**Broj osoba:** 2
**Zadaci:**
1. Priprema zahtjeva za opoziv
2. Opozivanje certifikata

**Organizacijska grupa:** Sigurnost i kontrola
**Uloga:** Administrator za sigurnost **Broj**
**osoba:** 2
**Zadaci:**
1. Određivanje sigurnosnih pravila i praćenje njihove usklađenosti
2. Pregledanje dokumentacije sistema i kontrolnih dnevnika za praćenje rada
3. Lična saradnja i pomoć u godišnjem popisu podređenih TSP

**Organizacijska grupa:** Sigurnost i kontrola
**Uloga:** Službenik za internu reviziju **Broj**
**osoba:** 2
**Zadaci:**
1. Kontrola sigurnosnih pravila i njihova usklađenost
2. Praćenje dokumentacije sistema i kontrolnih dnevnika za kontrolu rada

**Organizacijska grupa:** Regulatorne oblasti **Uloga:**
Službenik za regulatornu usklađenost
**Broj osoba:** 1
**Zadaci:**
1. Nezavisno usmjeravanje, zaštita privatnosti i zaštita ličnih podataka
2. Osiguranje poštovanja važećih evropskih i slovenskih propisa, međunarodnih standarda i preporuka
3. Stručna pomoć menadžmentu i zaposlenima u operativnoj implementaciji mjera privatnosti i usklađenosti s propisima

(2) Minimalni broj zaposlenika je naveden za svaku ulogu.

### 5.2.3 Identifikacija i potvrda autentičnosti za svaku ulogu

Identifikacija identiteta i prava pristupa za obavljanje pojedinih zadataka u skladu sa ulogom svake organizacijske grupe, kao i za obavljanje zadataka RA osigurava se sigurnosnim mehanizmima i kontrolnim postupcima u skladu sa internim pravilima TSP-a Halcom CA.

### 5.2.4 Uloge kojima se zahtijeva odvajanje dužnosti

Interna pravila Halcoma CA precizno navode koja uloga može biti / nije kompatibilna s drugom. Za neke zadatke potrebno je prisustvo najmanje dva ovlaštena lica. U slučaju nepredviđenog odsustva određenih zaposlenih, njihovu ulogu preuzima drugi zaposleni, ako je to u skladu sa internim pravilima.

## 5.3. Kontrole sigurnosti osoblja

(1) Operativno, organizacijsko i profesionalno funkcionisanje Halcom CA-a predvodi rukovodilac interne revizije koji ne obavlja poslove vezane za upravljanje certifikatima.

(2) Službenik interne revizije nadgleda rad Halcoma CA. U slučaju otkrivenih nedostataka, službenik unutrašnje revizije će preduzeti odgovarajuće mjere kako bi otklonio te nedostatke. Halcom CA je obavezan da provede navedene mjere pod nadzorom službenika za unutrašnju reviziju.

### 5.3.1 Kvalifikacije, iskustvo i zahtjevi za odobrenje

Halcom CA zapošljava pouzdano i stručno osposobljeno kvalifikovano osoblje koje nije procesuirano za krivična djela. Svo osoblje redovno se obučava i stiče dodatna znanja iz svoje struke.

### 5.3.2 Procedure za provjeru prošlosti

Osoblje pružaoca usluga povjerenja treba da poštuje zahtjeve važećih propisa i tehničkih standarda, kao i preporuke odgovarajućih kvalifikacija i iskustva.

### 5.3.3 Zahtjevi za obuku

Osobama koje obavljaju poslove navedene u organizacijskim grupama i zadacima RA obezbjeđuje se sva potrebna obuka.

### 5.3.4 Učestalost i zahtjevi za prekvalifikaciju

Osoblje se obučava u skladu sa potrebama i/ili novostima po pitanju funkcionisanja infrastrukture TSP-a Halcom CA.

### 5.3.5 Učestalost i redoslijed rotacije poslova

Nije propisano.

### 5.3.6 Sankcije za neovlaštene aktivnosti

Sankcije u slučaju neovlaštenog ili nemarnog izvršavanja zadataka se provode za lica ovlaštena od TSP-a u skladu sa važećim pravilima i internim pravilima TSP-a Halcom CA.

### 5.3.7 Zahtjevi nezavisnog izvođača radova

Svi potencijalni nezavisni izvođači radova su predmet istih zahtjeva kao i ovlaštena lica TSP-a Halcom CA.

### 5.3.8 Dokumentacija koja se dostavlja osoblju

Ovlaštena lica TSP-a imaju pristup svoj neophodnoj dokumentaciji u skladu sa njihovim dužnostima i zadacima.

## 5.4. Procedure unošenja revizije u dnevnike

### 5.4.1 Vrsta događaja koja se unosi

(1) TSP Halcom CA redovno provjerava i evidentira sve što značajno utječe na:

- sigurnost infrastrukture,
- rad svih sigurnosnih sistema i
- da li je došlo do upada ili pokušaja upada neovlaštenih lica u opremu ili podatke.

(2) Detaljne informacije u vezi navedenog se utvrđuju u skladu sa Uredbom za interna pravila TSP-a

Halcom CA.

### 5.4.2 Učestalost obrade dnevnika

TSP Halcom CA na dnevnoj osnovi provodi sigurnosne provjere svoje infrastrukture i evidencije.

### 5.4.3 Period čuvanja dnevnika o reviziji

Dnevnici o reviziji se čuvaju najmanje sedam (7) godina nakon njihove izrade osim ako ne postoji zakon koji predviđa duži period čuvanja.

### 5.4.4 Zaštita dnevnika o reviziji

(1) Dnevnici revizije su zaštićeni u skladu sa sigurnosnim mehanizmima koji garantuju najviši nivo sigurnosti.

(2) Detalji se utvrđuju u internim pravilima TSP-a u skladu sa Uredbom.

### 5.4.5 Procedura izrade sigurnosne kopije dnevnika

(1) Sigurnosne kopije dnevnika revizije se svakodnevno izrađuju.

(2) Detalji se utvrđuju u internim pravilima TSP-a u skladu sa Uredbom.

### 5.4.6 Sistem prikupljanja revizija

(1) Podaci se prikupljaju ili automatski ili ručno u zavisnosti od vrste podataka.

(2) Detalj se utvrđuju internim pravilima TSP-a u skladu sa Uredbom.

### 5.4.7 Obavijest subjektu koji je uzročnik događaja

Nije neophodno obavijestiti subjekat koji je uzročnik događaja.

### 5.4.8 Ocjena ranjivosti sistema

(1) Detalji su utvrđeni internim pravilima TSP-a u skladu sa Uredbom.

(2) Analizu dnevnika i nadzor nad izvršenjem svih procedura redovno obavljaju ovlaštena lica TSP-a ili se provodi automatski sa drugim sigurnosnim mehanizmima na svim informacijskim i komunikacijskim uređajima koji su pod kontrolom TSP-a.

(3) Procjena ranjivosti provodi se na temelju analize dnevnika, sigurnosnih događaja i drugih relevantnih podataka.

(4) Detalji se utvrđuju u internim pravilima TSP-a u skladu sa Uredbom.

## 5.5. Arhiviranje evidencije

### 5.5.1 Vrsta evidencije za arhiviranje

Halcom CA arhivira sljedeće materijale u skladu s odredbama važećih propisa:

- dnevnici,
- evidencija,
- svi dokazi o provedenoj identifikaciji subjekta i pravnih lica,
- svi obrasci zahtjeva,
- certifikati i lista opozvanih certifikata,
- pravila,

- CPS,
- Objave i obavještenja iz TSP-a Halcom CA i
- Ostali dokumenti u sklad sa važećim uredbama.

### 5.5.2 Period čuvanja za arhivu

(1) Dugoročno pohranjeni podaci koji se odnose na ključeve i digitalne certifikate se čuvaju najmanje sedam (7) godina nakon isteka certifikata na koji se podaci odnose, ako posebnim zakonom nije predviđeno duže razdoblje.

(2) Ostali dugoročno pohranjeni podaci čuvaju se najmanje sedam (7) godina nakon nastanka, ako posebnim zakonom nije potrebno duže razdoblje.

### 5.5.3 Zaštita arhive

(1) Dugoročno pohranjeni podaci se sigurno pohranjuju.

(2) Detalji su u skladu s važećim propisima, standardima i preporukama navedenim u internim pravilima TSP-a Halcom CA.

### 5.5.4 Procedure sigurne kopije arhive

(1) Kopija podataka dugoročne arhive pohranjena je na siguran način.

(2) Detalji su u skladu s važećim propisima, standardima i preporukama navedenim u internim pravilima TSP-a Halcom CA.

### 5.5.5 Zahtjevi za vremenske pečate evidencije

Nije propisano.

### 5.5.6 Sistem prikupljanja arhive.

(1) Podaci se prikupljaju na način koji je u skladu sa vrstom dokumenta.

(2) Detalji su u skladu s važećim propisima, standardima i preporukama navedenim u internim pravilima TSP-a Halcom CA.

### 5.5.7 Procedure dobijanje i verifikaciju arhivskih informacija

(1) Pristup dugoročnim podacima je dostupan samo za ovlaštena lica.

(2) Detalji su u skladu s važećim propisima, standardima i preporukama navedenim u internim pravilima TSP-a Halcom CA.

## 5.6. Zamjena ključeva u TSP-u Halcom CA

U slučaju izdavanja novih certifikata TSP-a Halcom CA, proces se objavljuje na web stranici TSP-a Halcom CA.

## 5.7. Kompromis i oporavak od katastrofa

### 5.7.1 Procedure za upravljanje incidentima i kompromisima

(1) Detalji su u skladu s važećim propisima, standardima i preporukama navedenim u internim pravilima TSP-a Halcom CA.

### 5.7.2 Kompjuterski resursi, softver i / ili podaci su oštećeni

(1) Detalji su u skladu s važećim propisima, standardima i preporukama navedenim u internim pravilima TSP-a Halcom CA.

### 5.7.3 Postupak kompromisa u slučaju privatnog ključa lica

(1) Detalji su u skladu s važećim propisima, standardima i preporukama navedenim u internim pravilima TSP-a Halcom CA.

### 5.7.4 Mogućnost nastavka poslovanja nakon katastrofe

(1) Detalji su u skladu s važećim propisima, standardima i preporukama navedenim u internim pravilima TSP-a Halcom CA.

## 5.8. Prekid poslovanja Halcoma CA ili RA

(2) Detalji su u skladu s važećim propisima, standardima i preporukama navedenim u internim pravilima TSP-a Halcom CA.

# 6. KONTROLE TEHNIČKE SIGURNOSTI

## 6.1. Generisanje i instalacija para ključeva

### 6.1.1 Generisanje para ključeva

(1) Par ključeva CA TSP Halcom za potpisivanje i potvrđivanje potpisa kreiran je prema najvišim sigurnosnim standardima u sigurnom okruženju TSP Halcom CA.

(2) Ključevi subjekata se generišu u zavisnosti od vrste certifikata u skladu sa tabelom nastavku.

| Vrsta certifikata | Ključ | Generisanje ključeva |
|---|---|---|
| Korijenski i posrednički certifikati Halcoma CA | Par ključeva | u hardverskom sigurnosnom modulu TSP-a |
| Napredni certifikat | Dva para ključeva | na QSCD u sigurnom okruženju TSP-a Halcom CA |
| Standardni certifikat | Par ključeva | na kompjuteru subjekta |
| Cloud certifikat | Par ključeva | u hardverskom sigurnosnom modulu TSP-a |
| Certifikat za informacijske sisteme | Par ključeva | u sigurnom okruženju subjekta certifikata |
| Certifikat za potvrdu autentičnosti web stranice | Par ključeva | u sigurnom okruženju subjekta certifikata |
| Certifikat za vremenski pečat | Par ključeva | u hardverskom sigurnosnom modulu TSP-a |

### 6.1.2 Isporuka privatnog ključa pretplatniku

Način isporuke privatnog ključa je dat u tabeli ispod.

| Vrsta certifikata | Ključ | Generisanje ključeva |
|---|---|---|
| Korijenski i posrednički certifikati Halcoma CA | Privatni ključ | Bez transfera |
| Napredni certifikat | Privatni ključ | isporuka QSCD-a preporučenom poštom |

| | | |
|---|---|---|
| Standardni certifikat | Privatni ključ | Bez transfera |
| Cloud certifikat | Privatni ključ | Bez transfera |
| Certifikat za informacijske sisteme | Privatni ključ | Bez transfera |
| Certifikat za potvrdu autentičnosti web stranice | Privatni ključ | Bez transfera |
| Certifikat za vremenski pečat | Privatni ključ | Bez transfera |

### 6.1.3 Isporuka javnog ključa izdavaocu certifikata

(1) Za napredne certifikate, ključevi se generiraju na QSCD-u u sigurnom okruženju TSP-a Halcom CA.

(2) Za certifikate u oblaku, ključevi se generiraju u hardverskom sigurnosnom modulu u sigurnom okruženju TSP-a Halcom CA.

(3) Za certifikate za informacione sisteme i provjeru autentičnosti web stranice, subjekt generira ključeve. PKCS #10 zahtjev za izdavanje certifikata se zatim prenosi sa računara subjekta na TSP putem sigurne mrežne veze.

(4) Za standardne certifikate, subjekat generira ključeve. Zahtjev za izdavanje certifikata PKCS #10 i certifikat izdaje se putem Halcom CA softvera za nabavku digitalnog certifikata.

(5) Za certifikate vremenskog pečata, TSP generira ključeve u sigurnosnom modulu hardvera. PKCS #10 zahtjev za izdavanje certifikata se prenosi na TSP putem sigurne mrežne veze.

### 6.1.4 Isporuka CA javnog ključa trećim stranama

TSP Halcom CA javni ključ se isporučuju subjektu ili je dostupan trećim stranama:

- u javnom direktoriju ldap://ldap.halcom.si u okviru LDAP protokola (vidi odjeljak 2.3),
- u PEM formi na http://domina.halcom.si/crls, gdje se pouzdanost certifikata mora dodatno provjeriti.

### 6.1.5 Veličina ključeva

| Certifikat | Dužina ključa prema RSA [bit] |
|---|---|
| Korijenski certifikat Halcom CA | Najmanje 2048 |
| Posrednički certifikat Halcom CA | Najmanje 2048 |
| Korisnički certifikati | Najmanje 2048 |

### 6.1.6 Generisanje parametara javnog ključa i provjera kvalitete

Kvalitet parametara ključa TSP-a Halcom CA obezbjeđuje proizvođač softvera, koristeći kvalitetan generator slučajnih brojeva.

### 6.1.7 Svrha korištenja ključa (prema X.509 v3 polju korištenja ključa)

(1) Svrha upotrebe ključa certifikata je u skladu sa X.509 v.3 i specificirana je u polju certifikata keyUsage i prošireni keyUsage.

(2) Privatni ključ TSP Halcom CA je namijenjen za potpisivanje certifikata i CRL-ova, a javni ključ u certifikatu TSP-a se koristi za provjeru valjanosti potpisa.

(3) Profil certifikacije je opisan u odjeljku 7.1.

## 6.2. Zaštita privatnih ključeva i kontrola kriptografskog modula

### 6.2.1 Standardi i kontrole kriptografskog modula

Privatni ključ TSP-a Halcom CA je zaštićen u hardverskom sigurnosnom modulu koji je certificiran prema FIPS 140-2 nivo 3 i / ili prema Zajedničkim kriterijima EAL4 +.

### 6.2.2 Višestruka kontrola (n od m) privatnog ključa

U skladu sa važećim propisima i CPS-om, pristup privatnom ključu TSP-a Halcom CA naveden je u internim pravilima TSP-a Halcom CA.

### 6.2.3 Deponovanje privatnog ključa

U skladu sa važećim propisima i CPS-om, deponovanje privatnog ključa TSP-a Halcom CA navedeno je u internim pravilima TSP-a Halcom CA.

### 6.2.4 Sigurnosna kopija privatnog ključa

U skladu sa važećim propisima i CPS-om, sigurnosna kopija privatnog ključa TSP-a Halcom CA navedena je u internim pravilima TSP-a Halcom CA

### 6.2.5 Arhiviranje privatnog ključa

(1) Privatni ključevi Halcom CA mogu se kopirati i pohraniti samo od strane ovlaštenih osoba TSP Halcom CA. Rezervni ključevi se čuvaju sa istim nivoom zaštite kao ključevi koji se koriste.

(2) U skladu sa važećim propisima i CPS-om, arhiviranje privatnog ključa TSP Halcom CA je specificirano u internim pravilima TSP Halcom CA.

### 6.2.6 Prenos privatnog ključa u ili iz kriptografskog modula

(1) Privatni ključevi za napredne certifikate generišu se u QSCD-u koji se naknadno prenosi subjektu certifikata.

(2) Privatni ključevi za cloud certifikate generiraju se i pohranjuju u hardverskom sigurnosnom modulu koji je certificiran prema FIPS 140-2 nivo 3 i / ili prema Zajedničkim kriterijima EAL4 +.

(3) Privatne ključevi drugih certifikata kreira i pohranjuje subjekat.

### 6.2.7 Pohranjivanje privatnog ključa na kriptografskom modulu

(1) Privatni ključevi za Halcom CA TSP se pohranjuju u hardverskom sigurnosnom modulu koji je certificiran prema FIPS 140-2 nivo 3 i / ili prema Zajedničkim kriterijima EAL4 +.

(2) Privatni ključevi subjekta za:

- napredne certifikate se kreiraju i pohranjuju u QSCD,
- cloud certifikate se kreiraju i pohranjuju u hardverskom sigurnosnom modulu,
- subjekat kreira i čuva standardne certifikate,
- certifikate za informacione sisteme su kreirani i čuvaju se od strane subjekta,
- certifikate za provjeru autentičnosti web lokacije se kreiraju i pohranjuju od strane subjekt,
- certifikati vremenskog pečata se kreiraju i čuvaju u TSP sigurnosnom modulu shardware.

### 6.2.8 Način aktiviranja privatnih ključeva

(1) Postupak aktivacije privatnog ključa Halcom CA-a provodi se na siguran način u skladu s internim pravilima Halcom CA TSP-a.

(2) Halcom CA preporučuje subjektima da koriste okruženje koje, kada se odjave ili nakon nekog vremena, onemogućuje pristup svom privatnom ključu bez unošenja odgovarajuće lozinke.

(3) Subjekat cloud certifikata može koristiti kvalifikovani servis potpisivanja u cloud-u. U tom slučaju, subjekat ili drugi pošiljalac u njegovo ime, na siguran način, dostavljaju elektronski dokument Halcomu CA TSP-a koji će biti potpisan elektronski. Subjekat certifikata potom na siguran način i u skladu s postupcima TSP-a (korištenjem PIN-a i mobilnih sigurnosnih postupaka) odobrava kvalifikovani elektronski potpis u cloud-u. Na osnovu odobrenja subjekta, Halcom CA TSP-a koristi privatni ključ subjekta i elektronski potpisuje dokument i dostavlja ga subjektu ili drugom pošiljaocu dokumenta.

(4) U cilju zaštite povjerljivosti elektronskih dokumenata, subjekat može izričito pisanim putem zahtijevati da Halcomu CA TSP-a ne bude potreban cijeli elektronski dokument, kako je opisano u prethodnom stavu, već samo vrijednost raspršivanja takvog dokumenta. U tom slučaju, Halcom CA subjektu ili drugom pošiljaocu dostavlja samo elektronski potpis. Halcom CA TSP-a ne obezbjeđuje verifikaciju obračunate vrijednosti raspršivanja ili drugih sigurnosnih mehanizama za elektronski dokument, te prema tome svu odgovornost u cijelosti snosi subjekat.

### 6.2.9 Način deaktivacije privatnih ključeva

Postupak deaktivacije privatnog ključa Halcom CA-a provodi se na siguran način u skladu s internim pravilima Halcom CA TSP-a

### 6.2.10 Način uništavanja privatnih ključeva

(1) Postupak uništavanja privatnog ključa Halcom CA TSP odvija se na siguran način u skladu sa internim pravilima Halcom CA TSP i uputama proizvođača sigurnosnog modula hardvera. Privatni ključ se uništava na način da se ne može vratiti.

(2) Uništavanje privatnih ključeva od strane subjekata je u nadležnosti subjekata. Oni moraju koristiti odgovarajuće aplikacije za sigurno brisanje certifikata.

(3) Privatni ključ cloud certifikata automatski se uništava nakon isteka certifikata. Na osnovu pismenog zahtjeva subjekta, privatni ključ cloud certifikata može se uništiti prije isteka roka od strane ovlaštene osobe Halcom CA. Privatni ključ se uništava na način da se ne može vratiti.

### 6.2.11 Ocjena kriptografskog modula

Hardverski sigurnosni moduli su u skladu sa standardima datim u odjeljku 6.2.1.

## 6.3. Ostali aspekti upravljanja parom ključeva

### 6.3.1 Arhiviranje javnih ključeva

Halcom CA TSP arhivira svoj javni ključ i javne ključeve subjekata, kao što je navedeno u odjeljku 5.5.

### 6.3.2 Operativni periodi certifikata i periodi korištenja para ključeva

(1) Validnost zavisi od vrste certifikata.

| Vrsta certifikata | Ključ | Validnost |
|---|---|---|
| Korjenski certifikat | Privatni ključ | 20 godina |
| | Javni ključ | 20 godina |
| Posrednički (podređeni) certifikat | Privatni ključ | 10 godina |
| | Javni ključ | 10 godina |
| Napredni certifikat | Privatni ključ | 3 godine |

| | | |
|---|---|---|
| | Javni ključ | 3 godine |
| Standardni certifikat | Privatni ključ | 3 godine |
| | Javni ključ | 3 godine |
| Cloud certifikat | Privatni ključ | 1-3 godine |
| | Javni ključ | 1-3 godine |
| Certifikat za informacijske sisteme | Privatni ključ | 3 godine |
| | Javni ključ | 3 godine |
| Certifikat za potvrdu autentičnosti web stranice | Privatni ključ | 1-3 godine |
| | Javni ključ | 1-3 godine |
| Certifikati za vremenske pečate | Privatni ključ | 5 godina |
| | Javni ključ | 5 godina |

(3) U posebnim slučajevima, Halcom CA može odrediti i različiti period validnosti za svaki certifikat.

## 6.4. Aktivacijski podaci

### 6.4.1 Generisanje i instalacija aktivacijskih podataka

(1) Napredni certifikat

Lični identifikacioni broj (PIN kod) za korištenje naprednih certifikata i ključ za otključavanje PIN-a (PUK kod) generišu se u bezbjednom okruženju TSP-a Halcom CA. Subjekat mora promijeniti PIN kod prije prvog korištenja certifikata.

(2) Cloud certifikat

Kod za registraciju i aktivaciju za Cloud certifikate generiše se u sigurnom okruženju TSP Halcom CA. U procesu aktivacije subjekat postavlja svoj lični kod (PIN kod) za pristup cloud certifikatu.

(3) Standardni certifikat, certifikat za informacijske sisteme i za potvrdu autentičnosti web stranice

Vlasnici standardnih certifikata, certifikati informacijskog sistema i potvrde autentičnosti web stranice sami određuju lozinku za zaštitu pristupa svojim privatnim ključevima. Halcom CA preporučuje upotrebu sigurnih lozinki:

- mješovita upotreba velikih i malih slova, brojeva i posebnih znakova,
- dužine od najmanje 8 znakova,
- nije preporučljivo koristiti riječi koje su napisane u rječnicima.

### 6.4.2 Zaštita aktivacijskih podataka

(1) Napredni certifikat

PIN kod za korištenje naprednog certifikata i PUK kod za otključavanje QSCD-a sigurno su kreirani od strane Halcom CA TSP-a. Halcom CA dostavlja i šifre subjektu certifikata poštom ili lično. Halcom CA preporučuje da se obje šifre čuvaju na sigurnom mjestu kojem samo subjekat može pristupiti.

(2) Cloud certifikat

Registracijski i aktivacijski kod za cloud certifikat se kreira sigurno od strane Halcom CA TSP-a. Registracijski i aktivacijski kod se subjektu prenosi putem dva odvojena kanala, jedan putem e-pošte, a drugi putem drugog sigurnog kanala (sigurni web portal kojem se može pristupiti kvalifikovanim

certifikatom, putem preporučene pošte ili drugog sličnog sigurnog kanala). Izuzetno, ovlaštena osoba Halcoma CA RA može lično subjektu predati neki od gore navedenih kodova. Kodovi su namijenjeni samo za aktiviranje pristupa cloud certifikatu, tokom kojeg subjekat postavlja svoj lični kod (PIN kod).

(3) Standardni certifikat

Referentni broj i autorizacijski kod za unos standardnog certifikata sigurno kreira Halcom CA TSP. U procesu primanja certifikata, subjekat lično postavlja šifru da bi zaštitio pristup svojim privatnim ključevima. Halcom CA preporučuje da se šifra ne pohranjuje, ili da se pohranjuje samo na način da joj jedino subjekat može pristupiti.

(4) Certifikat za informacijske sisteme i potvrdu autentičnosti web stranice

Subjekti certifikata za informacijske sisteme i potvrdu autentičnosti web stranice sami postavljaju lozinku kako bi zaštitili svoje privatne ključeve. Halcom CA preporučuje da šifra za pristup privatnom ključu ne bude pohranjena ili da se pohrani na takav način da joj samo subjekat ima pristup.

### 6.4.3 Ostali aspekti aktivacijskih podataka

Nije propisano.

## 6.5. Kontrole sigurnosti računara

### 6.5.1 Specifični tehnički zahtjevi za sigurnost računara

Detalji su u skladu s važećim propisima, standardima i preporukama navedenim CPS-u i internim pravilima Halcom CA TSP-a.

### 6.5.2 Ocjena sigurnosti računara

Detalji su u skladu s važećim propisima, standardima i preporukama navedenim CPS-u i internim pravilima Halcom CA TSP-a.

## 6.6. Tehničke kontrole životnog ciklusa

### 6.6.1 Kontrole razvoja sistema

Halcom CA koristi softver i hardver koji su certifikovani u skladu sa FIPS 140-2 nivo 3 i/ili Zajedničkim kriterijima EAL4 +.

### 6.6.2 Kontrole upravljanja sigurnošću

Detalji su u skladu s važećim propisima, standardima i preporukama navedenim CPS-u i internim pravilima Halcom CA TSP-a.

### 6.6.3 Kontrole sigurnosti životnog ciklusa

Detaljni tehnički zahtjevi su navedeni u internim pravilima Halcom CA TSP-a.

## 6.7. Kontrole mrežne sigurnosti

Detalji su u skladu s važećim propisima, standardima i preporukama navedenim CPS-u i internim pravilima Halcom CA TSP-a..

## 6.8. Vremenski pečati

Nije propisano.

# 7. CERTIFIKAT, CRL, OCSP PROFILI

## 7.1. Profil certifikata

(1) U skladu sa CPS-om i pravilima, Halcom CA izdaje:

- Napredne certifikate,
- Cloud certifikate,
- Standardne certifikate,
- Certifikate za informacijske sisteme,
- Certifikate za potvrdu autentičnosti web stranice,
- Certifikate za vremenske pečate.

(2) Svi certifikati sadrže informacije u skladu sa Uredbom eIDAS za kvalifikovane certifikate.

*(3)* Halcom CA TSP certifikat prate standard X.509.

### 7.1.1 Brojevi verzija

Svi Halcom CA TSP certifikati prate standard X.509 v. 3.

### 7.1.2 Ekstenzije certifikata

Podaci u certifikatima su navedeni u tabeli ispod.

(1) Profil korijenskog certifikata - Halcom korijensko certifikacijsko tijelo

| Imena polja | Vrijednost ili značenje |
|---|---|
| Osnovna polja u certifikatu | |
| Verzija | V3 |
| Serijski broj | jedinstveni interni broj certifikata |
| Algoritam potpisa | Sha256RSA (OID 1.2.840.113549.1.1.11) |
| Izdaje | CN = Halcom korijensko certifikacijsko tijelo<br>2.5.4.97 = VATSI-43353126 O =<br>Halcom d.d.<br>C = SI |
| Validnost | Važi od: <10.6.2016 07:07:50 GMT ><br>Važi do: <10.6.2036 07:07:50 GMT > |
| Subjekat | CN = Halcom korijensko certifikacijsko tijelo<br>2.5.4.97 = VATSI-43353126 O =<br>Halcom d.d.<br>C = SI |
| Algoritam javnog ključa subjekta | rsaEncryption (OID 1.2.840.113549.1.1.1) |
| Javni ključ (... bita) | modul, eksponent, ... |
| Javni ključ subjekta koji pripada odgovarajućem paru ključeva, šifriran s RSA algoritmom (RSA javni ključ) | dužina ključa 2048 bits |
| Ekstenzije X.509v3 | |
| Upotreba ključa, OID 2.5.29.15 | Potpisivanje certifikata, CRL potpisivanje van mreže, CRL potpisivanje |
| Identifikator subjekta ključa, OID 2.5.29.14 | 42 ae a6 43 c7 98 28 b0 |
| Osnovna ograničenja, OID 2.5.29.19 | Tip subjekta=CA<br>Ograničenje dužine staze=None |
| Dodatna identifikacija (nije dio digitalnog certifikata) | |
| Identifikacija certifikata – SHA1 | Identifikacija certifikata SHA1 |
| | |

(2) Profil posrednih certifikata

- Halcom CA PO e-signature 1

| Imena polja | Vrijednost ili značenje |
|---|---|
| **Osnovna polja u certifikatu** | |
| Verzija | V3 |
| Serijski broj | jedinstveni interni broj certifikata |
| Algoritam potpisa | Sha256RSA (1.2.840.113549.1.1.11) |
| Izdaje | CN = Halcom korijensko certifikacijsko tijelo<br>2.5.4.97 = VATSI-43353126<br>O = Halcom d.d.<br>C = SI |
| Validnost | Važi od: <15.6.2016 10:34:13 GMT ><br>Važi do: <15.6.2026 10:34:13 GMT > |
| Subjekat | CN = Halcom CA PO e-signature 1<br>2.5.4.97 = VATSI-43353126<br>O = Halcom d.d.<br>C = SI |
| Algoritam javnog ključa subjekta | rsaEncryption (OID 1.2.840.113549.1.1.1) |
| Javni ključ (... bita) | modul, eksponent, ... |
| Javni ključ subjekta koji pripada odgovarajućem paru ključeva, šifrovan RSA algoritmom (RSA javni ključ) | dužina ključa 2048 bits |
| **Ekstenzije X.509v3** | |
| Tačke distribucije CRL-a, OID 2.5.29.31 | URL=ldap://ldap.halcom.si/cn=Halcom%20Root%20Certificate%20Authority,o=Halcom,c=SI?certificaterevocationlist;binary<br>URL=http://domina.halcom.si/crls/halcom_root_certificate_authority.crl |
| Upotreba ključa, OID 2.5.29.15 | Potpisivanje certifikata,<br>Potpisivanje CRL-a van mreže,<br>Potpisivanje CRL-a |
| Identifikator ključa tijela, OID 2.5.29.35 | KeyID=42 ae a6 43 c7 98 28 b0 |
| Identifikator subjekta ključa, OID 2.5.29.14 | 40 f6 95 20 9b 79 c2 09 |
| Osnovna ograničenja, OID 2.5.29.19 | Tip subjekta=CA<br>Ograničenje dužine staze=None |
| **Dodatna identifikacija (nije dio digitalnog certifikata)** | |
| Identifikacija certifikata – SHA1 | Identifikacija certifikata SHA1 |

- Halcom CA PO e-signature 2

| Imena polja | Vrijednost ili značenje |
|---|---|
| **Osnovna polja u certifikatu** | |
| Verzija | V3 |
| Serijski broj | jedinstveni interni broj certifikata |
| Algoritam potpisa | Sha256RSA (1.2.840.113549.1.1.11) |
| Izdaje | CN = Halcom korijensko certifikacijsko tijelo<br>2.5.4.97 = VATSI-43353126<br>O = Halcom d.d.<br>C = SI |
| Validnost | Važi od: <03.04.2023 07:00:00 GMT ><br>Važi do: <03.04.2033 07:00:00 GMT > |
| Subjekat | CN = Halcom CA PO e-signature 2<br>2.5.4.97 = VATSI-43353126<br>O = Halcom d.d.<br>C = SI |
| Algoritam javnog ključa subjekta | rsaEncryption (OID 1.2.840.113549.1.1.1) |
| Javni ključ (... bita) | modul, eksponent, ... |

| | |
|---|---|
| Javni ključ subjekta koji pripada odgovarajućem paru ključeva, šifrovan RSA algoritmom (RSA javni ključ) | dužina ključa 3072 bit |
| **Ekstenzije X.509v3** | |
| Tačke distribucije CRL-a, OID 2.5.29.31 | URL=ldap://ldap.halcom.si/cn=Halcom%20Root%20Certificate %20Authority,o=Halcom,c=SI?certificaterevocationlist;binary URL=http://domina.halcom.si/crls/halcom_root_certificate_auth ority.crl |
| Upotreba ključa, OID 2.5.29.15 | Potpisivanje certifikata, Potpisivanje CRL-a van mreže, Potpisivanje CRL-a |
| Identifikator ključa tijela, OID 2.5.29.35 | KeyID=42 ae a6 43 c7 98 28 b0 |
| Identifikator subjekta ključa, OID 2.5.29.14 | 43 4d 32 75 16 03 c9 75 |
| Osnovna ograničenja, OID 2.5.29.19 | Tip subjekta=CA Ograničenje dužine staze=None |
| **Dodatna identifikacija (nije dio digitalnog certifikata)** | |
| Identifikacija certifikata – SHA1 | Identifikacija certifikata SHA1 |

- Halcom CA FO e-signature 1

| Imena polja | Vrijednost ili značenje |
|---|---|
| **Osnovna polja u certifikatu** | |
| Verzija | V3 |
| Serijski broj | jedinstveni interni broj certifikata |
| Algoritam potpisa | Sha256RSA (1.2.840.113549.1.1.11) |
| Izdaje | CN = Halcom korijensko certifikacijsko tijelo 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI |
| Validnost | Važi od: <15.6.2016 10:34:15 GMT > Važi do: <15.6.2026 10:34:15 GMT > |
| Subjekat | CN = Halcom CA FO e-signature 1 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI |
| Algoritam javnog ključa subjekta | rsaEncryption (OID 1.2.840.113549.1.1.1) |
| Javni ključ (... bita) | modul, eksponent,... |
| Javni ključ subjekta koji pripada odgovarajućem paru ključeva, šifrovan RSA algoritmom (RSA javni ključ) | dužina ključa 2048 bit |
| **Ekstenzije X.509v3** | |
| Tačke distribucije CRL-a, OID 2.5.29.31 | URI:ldap://ldap.halcom.si/cn=Halcom%20Root%20Certificate%2 0Authority,o=Halcom,c=SI?certificaterevocationlist;binary URL=http://domina.halcom.si/crls/halcom_root_certificate_autho rity.crl |
| Upotreba ključa, OID 2.5.29.15 | Potpisivanje certifikata, Potpisivanje CRL-a van mreže, Potpisivanje CRL-a |
| Identifikator ključa tijela, OID 2.5.29.35 | KeyID=42 ae a6 43 c7 98 28 b0 |
| Identifikator ključa subjekta, OID 2.5.29.14 | 48 fb 3b 13 99 c3 4e ce |
| Osnovna ograničenja, OID 2.5.29.19 | Tip subjekta=CA Ograničenje dužine staze=None |

| Dodatna identifikacija (nije dio digitalnog certifikata) | |
|---|---|
| Identifikacija certifikata – SHA1 | Identifikacija certifikata SHA1 |

- Halcom CA FO e-signature 2

| Imena polja | Vrijednost ili značenje |
|---|---|
| Osnovna polja u certifikatu | |
| Verzija | V3 |
| Serijski broj | jedinstveni interni broj certifikata |
| Algoritam potpisa | Sha256RSA (1.2.840.113549.1.1.11) |
| Izdaje | CN = Halcom korijensko certifikacijsko tijelo<br>2.5.4.97 = VATSI-43353126<br>O = Halcom d.d.<br>C = SI |
| Validnost | Važi od: <03.04.2023 07:00:00 GMT ><br>Važi do: <03.04.2033 07:00:00 GMT > |
| Subjekat | CN = Halcom CA FO e-signature 2<br>2.5.4.97 = VATSI-43353126<br>O = Halcom d.d.<br>C = SI |
| Algoritam javnog ključa subjekta | rsaEncryption (OID 1.2.840.113549.1.1.1) |
| Javni ključ (... bita) | modul, eksponent,... |
| Javni ključ subjekta koji pripada odgovarajućem paru ključeva, šifrovan RSA algoritmom (RSA javni ključ) | dužina ključa 2048 bit |
| Ekstenzije X.509v3 | |
| Tačke distribucije CRL-a, OID 2.5.29.31 | URI:ldap://ldap.halcom.si/cn=Halcom%20Root%20Certificate%20Authority,o=Halcom,c=SI?certificaterevocationlist;binary<br>URL=http://domina.halcom.si/crls/halcom_root_certificate_autho rity.crl |
| Upotreba ključa, OID 2.5.29.15 | Potpisivanje certifikata,<br>Potpisivanje CRL-a van mreže,<br>Potpisivanje CRL-a |
| Identifikator ključa tijela, OID 2.5.29.35 | KeyID=42 ae a6 43 c7 98 28 b0 |
| Identifikator ključa subjekta, OID 2.5.29.14 | 48 c4 27 a6 6f 6e f0 2e |
| Osnovna ograničenja, OID 2.5.29.19 | Tip subjekta=CA<br>Ograničenje dužine staze=None |
| Dodatna identifikacija (nije dio digitalnog certifikata) | |
| Identifikacija certifikata – SHA1 | Identifikacija certifikata SHA1 |

- Halcom CA PO e-seal 1

| Imena polja | Vrijednost ili značenje |
|---|---|
| Osnovna polja u certifikatu | |
| Verzija | V3 |
| Serijski broj | jedinstveni interni broj certifikata |
| Algoritam potpisa | Sha256RSA (1.2.840.113549.1.1.11) |
| Izdaje | CN = Halcom korijensko certifikacijsko tijelo<br>2.5.4.97 = VATSI-43353126 O = Halcom d.d.<br>C = SI |
| Validnost | Važi od: <22.4.2017 08:00:00 GMT ><br>Važi do: <22.4.2027 08:00:00 GMT > |

| | |
|---|---|
| Subjekat | CN = Halcom CA PO e-seal 1<br>2.5.4.97 = VATSI-43353126 O = Halcom d.d.<br>C = SI |
| Algoritam javnog ključa subjekta | rsaEncryption (OID 1.2.840.113549.1.1.1) |
| Javni ključ (... bita) | modul, eksponent,... |
| Javni ključ subjekta koji pripada odgovarajućem paru ključeva, šifriran s RSA algoritmom (RSA javni ključ) | dužina ključa 2048 bits |
| Ekstenzije X.509v3 | |

| | |
|---|---|
| Tačke distribucije CRL-a, OID 2.5.29.31 | URL=ldap://ldap.halcom.si/cn=Halcom%20Root%20Certificate%20Authority,o=Halcom,c=SI?certificaterevocationlist;binary<br>URL=http://domina.halcom.si/crls/halcom_root_certificate_auth ority.crl |
| Upotreba ključa, OID 2.5.29.15 | Potpisivanje certifikata, CRL potpisivanje van mreže, CRL potpisivanje |
| Identifikator ključa tijela, OID 2.5.29.35 | KeyID=42 ae a6 43 c7 98 28 b0 |
| Identifikator subjekta ključa, OID 2.5.29.14 | 49 48 76 50 77 0a b1 0c |
| Osnovna ograničenja, OID 2.5.29.19 | Tip subjekta=CA<br>Ograničenje dužine staze=None |
| Dodatna identifikacija (nije dio digitalnog certifikata) | |
| Identifikacija certifikata – SHA1 | Identifikacija certifikata SHA1 |

- Halcom CA PO e-seal 2

| Imena polja | Vrijednost ili značenje |
|---|---|
| Osnovna polja u certifikatu | |
| Verzija | V3 |
| Serijski broj | jedinstveni interni broj certifikata |
| Algoritam potpisa | Sha256RSA (1.2.840.113549.1.1.11) |
| Izdaje | CN = Halcom korijensko certifikacijsko tijelo<br>2.5.4.97 = VATSI-43353126<br>O = Halcom d.d.<br>C = SI |
| Validnost | Važi od: <03.04.2023 07:00:00 GMT ><br>Važi do: <03.04.2033 07:00:00 GMT > |
| Subjekat | CN = Halcom CA PO e-seal 2<br>2.5.4.97 = VATSI-43353126<br>O = Halcom d.d.<br>C = SI |
| Algoritam javnog ključa subjekta | rsaEncryption (OID 1.2.840.113549.1.1.1) |
| Javni ključ (... bita) | modul, eksponent,... |
| Javni ključ subjekta koji pripada odgovarajućem paru ključeva, šifriran s RSA algoritmom (RSA javni ključ) | dužina ključa 3072 bit |
| Ekstenzije X.509v3 | |

| | |
|---|---|
| Tačke distribucije CRL-a, OID 2.5.29.31 | URL=ldap://ldap.halcom.si/cn=Halcom%20Root%20Certificate %20Authority,o=Halcom,c=SI?certificaterevocationlist;binary<br>URL=http://domina.halcom.si/crls/halcom_root_certificate_authority.crl |
| Upotreba ključa, OID 2.5.29.15 | Potpisivanje certifikata, CRL potpisivanje van mreže, CRL potpisivanje |
| Identifikator ključa tijela, OID 2.5.29.35 | KeyID=42 ae a6 43 c7 98 28 b0 |
| Identifikator subjekta ključa, OID 2.5.29.14 | 47 35 c8 bc 61 e2 5d 9e |
| Osnovna ograničenja, OID 2.5.29.19 | Tip subjekta=CA<br>Ograničenje dužine staze=None |
| Dodatna identifikacija (nije dio digitalnog certifikata) | |
| Identifikacija certifikata – SHA1 | Identifikacija certifikata SHA1 |

- Halcom CA web 1

| Imena polja | Vrijednost ili značenje |
|---|---|
| Osnovna polja u certifikatu | |
| Verzija | V3 |
| Serijski broj | jedinstveni interni broj certifikata |
| Algoritam potpisa | Sha256RSA (1.2.840.113549.1.1.11) |
| Izdaje | CN = Halcom korijensko certifikacijsko tijelo<br>2.5.4.97 = VATSI-43353126 O = Halcom d.d.<br>C = SI |
| Validnost | Važi od: <22.4.2017 08:00:00 GMT ><br>Važi do: <22.4.2027 08:00:00 GMT > |
| Subjekat | CN = Halcom CA web 1<br>2.5.4.97 = VATSI-43353126 O = Halcom d.d.<br>C = SI |
| Algoritam javnog ključa subjekta | rsaEncryption (OID 1.2.840.113549.1.1.1) |
| Javni ključ (... bita) | modul, eksponent,... |
| Javni ključ subjekta koji pripada odgovarajućem paru ključeva, šifriran s RSA algoritmom (RSA javni ključ) | dužina ključa 2048 bits |
| Ekstenzije X.509v3 | |
| Tačke distribucije CRL-a, OID 2.5.29.31 | URL=ldap://ldap.halcom.si/cn=Halcom%20Root%20Certificate %20Authority,o=Halcom,c=SI?certificaterevocationlist;binary<br>URL=http://domina.halcom.si/crls/halcom_root_certificate_auth ority.crl |
| Upotreba ključa, OID 2.5.29.15 | Potpisivanje certifikata, Potpisivanje CRL-a van mreže, Potpisivanje CRL-a |
| Identifikator ključa tijela, OID 2.5.29.35 | KeyID= 42 ae a6 43 c7 98 28 b0 |
| Identifikator subjekta ključa, OID 2.5.29.14 | 48 42 0b 17 ed ae 9e 70 |
| Osnovna ograničenja, OID 2.5.29.19 | Tip subjekta=CA<br>Ograničenje dužine staze=None |
| Dodatna identifikacija (nije dio digitalnog certifikata) | |
| Identifikacija certifikata – SHA1 | Identifikacija certifikata SHA1 |

- Halcom CA TSA 1

| Imena polja | Vrijednost ili značenje |
|---|---|
| **Osnovna polja u certifikatu** | |
| Verzija | V3 |
| Serijski broj | jedinstveni interni broj certifikata |
| Algoritam potpisa | Sha256RSA (1.2.840.113549.1.1.11) |
| Izdaje | CN = Halcom korijensko certifikacijsko tijelo<br>2.5.4.97 = VATSI-43353126 O = Halcom d.d.<br>C = SI |
| Validnost | Važi od: <22.4.2017 08:00:00 GMT ><br>Važi do: <22.4.2027 00:00:00 GMT > |
| Subjekat | CN = Halcom CA TSA 1<br>2.5.4.97 = VATSI-43353126 O = Halcom d.d.<br>C = SI |
| Algoritam javnog ključa subjekta | rsaEncryption (OID 1.2.840.113549.1.1.1) |
| Javni ključ (... bita) | modul, eksponent,... |
| Javni ključ subjekta koji pripada odgovarajućem paru ključeva, šifriran s RSA algoritmom (RSA javni ključ) | dužina ključa 2048 bits |
| **Ekstenzije X.509v3** | |
| Tačke distribucije CRL-a, OID 2.5.29.31 | URL=ldap://ldap.halcom.si/cn=Halcom%20Root%20Certificate %20Authority,o=Halcom,c=SI?certificaterevocationlist;binary<br>URL=http://domina.halcom.si/crls/halcom_root_certificate_auth ority.crl |
| Upotreba ključa, OID 2.5.29.15 | Potpisivanje certifikata, CRL potpisivanje van mreže, CRL potpisivanje |
| Identifikator ključa tijela, OID 2.5.29.35 | KeyID=42 ae a6 43 c7 98 28 b0 |
| Identifikator subjekta ključa, OID 2.5.29.14 | 43 8f 8b 56 9f 44 1e d7 |
| Osnovna ograničenja, OID 2.5.29.19 | Tip subjekta=CA<br>Ograničenje dužine staze=None |
| **Dodatna identifikacija (nije dio digitalnog certifikata)** | |
| Identifikacija certifikata – SHA1 | Identifikacija certifikata SHA1 |

(3) Profil certifikata krajnjeg korisnika

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

| Imena polja | Vrijednost ili značenje |
|---|---|
| **Osnovna polja u certifikatu** | |
| Verzija | V3 |
| Serijski broj | jedinstveni interni broj certifikata |
| Algoritam potpisa | Sha256RSA (OID 1.2.840.113549.1.1.11) |
| Izdaje | CN = Halcom CA PO e-signature 1 ili<br>CN = Halcom CA PO e-signature 2<br>2.5.4.97 = VATSI-43353126<br>O = Halcom d.d.<br>C = SI |
| Validnost | Važi od: <početak validnosti do, prema GMT-u><br>Važi do: <kraj validnosti do, prema GMT-u> |
| Subjekat | prepoznatljivo ime subjekta, Vidi odjeljak 3.1.1. |
| Algoritam javnog ključa subjekta | rsaEncryption (OID 1.2.840.113549.1.1.1) |
| Javni ključ (... bita) | modul, eksponent,... |
| Javni ključ subjekta koji pripada odgovarajućem paru ključeva, šifriran s RSA algoritmom (RSA javni ključ) | dužina ključa je min. 2048 bits, Vidi odjeljak 6.1.5. |
| **Ekstenzije X.509v3** | |
| Tačke distribucije CRL-a, OID 2.5.29.31 | URI:ldap://ldap.halcom.si/cn=Halcom%20CA%20PO%20e-signature%201,o=Halcom,c=SI?certificaterevocationlist;binary<br>URL=http://domina.halcom.si/crls/halcom_ca_po_ e- signature_1.crl |
| Upotreba ključa , OID 2.5.29.15 | Napredni certifikati: digitalni potpis, nerepudijacija, šifrovanje ključa<br>Cloud certificates: Digital Signature, Non Repudiation |
| Identifikator ključa tijela, OID 2.5.29.35 | KeyID=40 f6 95 20 9b 79 c2 09<br>Ili<br>KeyID=43 4d 32 75 16 03 c9 75 |

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

| Imena polja | Vrijednost ili značenje |
|---|---|
| **Osnovna polja u certifikatu** | |
| Verzija | V3 |
| Serijski broj | jedinstveni interni broj certifikata |
| Algoritam potpisa | Sha256RSA (OID 1.2.840.113549.1.1.11) |
| Izdaje | CN = Halcom CA FO e-signature 1 ili<br>CN = Halcom CA FO e-signature 2<br>2.5.4.97 = VATSI-43353126<br>O = Halcom d.d.<br>C = SI |
| Validnost | Važi od: <početak validnosti do, prema GMT-u><br>Važi do: <kraj validnosti do, prema GMT-u> |
| Subjekat | prepoznatljivo ime subjekta, Vidi odjeljak 3.1.1. |
| Algoritam javnog ključa subjekta | rsaEncryption (OID 1.2.840.113549.1.1.1) |
| Javni ključ (... bita) | modul, eksponent,... |
| Javni ključ subjekta koji pripada odgovarajućem paru ključeva, šifriran s RSA algoritmom (RSA javni ključ) | dužina ključa is min. 2048 bits, Vidi odjeljak 6.1.5. |
| **Ekstenzije X.509v3** | |

| | |
|---|---|
| Tačke distribucije CRL-a, OID 2.5.29.31 | URI:ldap://ldap.halcom.si/cn=Halcom%20CA%20FO%20e-signature%201,o=Halcom,c=SI?certificaterevocationlist;binary<br>URL=http://domina.halcom.si/crls/halcom_ca_fo_e- signature_1.crl |
| Upotreba ključa, OID 2.5.29.15 | Napredni certifikati: digitalni potpis, nerepudijacija, šifrovanje ključa<br>Standardni certifikati: digitalni potpis, šifrovanje ključa<br>Cloud certifikati: digital signature, non repudiation |
| Identifikator ključa tijela, OID 2.5.29.35 | KeyID=48 fb 3b 13 99 c3 4e ce<br>Ili<br>KeyID=48 c4 27 a6 6f 6e f0 2e |

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

| Imena polja | Vrijednost ili značenje |
|---|---|
| Osnovna polja u certifikatu | |
| Verzija | V3 |
| Serijski broj | jedinstveni interni broj certifikata |
| Algoritam potpisa | Sha256RSA (OID 1.2.840.113549.1.1.11) |
| Izdaje | CN = Halcom CA FO e-seal 1 ili<br>CN = Halcom CA FO e-seal 2<br>2.5.4.97 = VATSI-43353126<br>O = Halcom d.d.<br>C = SI |
| Validnost | Važi od: <početak validnosti do, prema GMT-u><br>Važi do: <kraj validnosti do, prema GMT-u> |
| Subjekat | prepoznatljivo ime subjekta, Vidi odjeljak 3.1.1. |
| Algoritam javnog ključa subjekta | rsaEncryption (OID 1.2.840.113549.1.1.1) |
| Javni ključ (... bita) | modul, eksponent,... |
| Javni ključ subjekta koji pripada odgovarajućem paru ključeva, šifriran s RSA algoritmom (RSA javni ključ) | dužina ključa is min. 2048 bit, Vidi odjeljak 6.1.5. |
| Ekstenzije X.509v3 | |
| Tačke distribucije CRL-a, OID 2.5.29.31 | URI:ldap://ldap.halcom.si/cn=Halcom%20CA%20PO%20e-seal%201,o=Halcom,c=SI?certificaterevocationlist;binary<br>URL=http://domina.halcom.si/crls/halcom_ca_po_e- seal_1.crl<br>Ili<br>URL:ldap://ldap.halcom.si/cn=Halcom%20CA%20PO%20e-seal%202,o=Halcom,c=SI?certificaterevocationlist;binary<br>URL=http://domina.halcom.si/crls/halcom_ca_po_e- seal_2.crl |
| Upotreba ključa, OID 2.5.29.15 | Digital Signature, Non Repudiation, Key Encipherment |
| Identifikator ključa tijela, OID 2.5.29.35 | KeyID=49 48 76 50 77 0a b1 0c<br>Ili<br>KeyID=47 35 c8 bc 61 e2 5d 9e |

- Halcom CA web 1

| Imena polja | Vrijednost ili značenje |
|---|---|
| Osnovna polja u certifikatu | |
| Verzija | V3 |
| Serijski broj | jedinstveni interni broj certifikata |
| Algoritam potpisa | Sha256RSA (OID 1.2.840.113549.1.1.11) |
| Izdaje | CN = Halcom CA web 1<br>2.5.4.97 = VATSI-43353126 O = Halcom d.d.<br>C = SI |

| | |
|---|---|
| Validnost | Važi od: <početak validnosti do, prema GMT-u><br>Važi do: <kraj validnosti do, prema GMT-u> |
| Subjekat | prepoznatljivo ime subjekta, Vidi odjeljak 3.1.1. |
| Algoritam javnog ključa subjekta | rsaEncryption (OID 1.2.840.113549.1.1.1) |
| Javni ključ (... bita) | modul, eksponent,... |
| Javni ključ subjekta koji pripada odgovarajućem paru ključeva, šifriran s RSA algoritmom (RSA javni ključ) | dužina ključa is min. 2048 bits, Vidi odjeljak 6.1.5. |

| Ekstenzije X.509v3 | |
|---|---|
| Tačke distribucije CRL-a, OID 2.5.29.31 | URI:ldap://ldap.halcom.si/cn=Halcom%20CA%20web%201,o=Halcom,c=SI?certificaterevocationlist;binary<br>URL=http://domina.halcom.si/crls/halcom_ca_web_1.crl |
| Upotreba ključa, OID 2.5.29.15 | Digitalni potpis, šifrovanje ključa |
| Identifikator ključa tijela, OID 2.5.29.35 | KeyID= 48 42 0b 17 ed ae 9e 70 |

- Halcom CA TSA 1

| Imena polja | Vrijednost ili značenje |
|---|---|
| Osnovna polja u certifikatu | |
| Verzija | V3 |
| Serijski broj | jedinstveni interni broj certifikata |
| Algoritam potpisa | Sha256RSA (OID 1.2.840.113549.1.1.11) |
| Izdaje | CN = Halcom CA TSA 1<br>2.5.4.97 = VATSI-43353126 O = Halcom d.d.<br>C = SI |
| Validnost | Važi od: <početak validnosti do, prema GMT-u><br>Važi do: <kraj validnosti do, prema GMT-u> |
| Subjekat | prepoznatljivo ime subjekta, Vidi odjeljak 3.1.1. |
| Algoritam javnog ključa subjekta | rsaEncryption (OID 1.2.840.113549.1.1.1) |
| Javni ključ (... bita) | modul, eksponent,... |
| Javni ključ subjekta koji pripada odgovarajućem paru ključeva, šifriran s RSA algoritmom (RSA javni ključ) | dužina ključa is min. 2048 bits, Vidi odjeljak 6.1.5. |
| Ekstenzije X.509v3 | |
| Tačke distribucije CRL-a, OID 2.5.29.31 | URI:ldap://ldap.halcom.si/cn=Halcom%20CA%20TSA%201,o=Halcom,c=SI?certificaterevocationlist;binary<br>URL=http://domina.halcom.si/crls/halcom_ca_tsa_1.crl |
| Korištenje ključa, OID 2.5.29.15., engl. Key Usage | Standardne potvrde:Digital Signature, Non Repudiation, Key Encipherment<br>Napredne potvrde: Digital Signature, Non Repudiation, Key Encipherment<br>Potvrde oblaku: Digital Signature, Non Repudiation |
| Identifikator ključa tijela, OID 2.5.29.35 | KeyID=43 8f 8b 56 9f 44 1e d7 |
| EŠEI | Jedinstveni broj elektronske identifikacije (vidi odjeljak 7.1.2.1) |

(4) Polje upotreba ključa je označeno kao ključno.

(5) Subjekat certifikata za elektronske potpise može imati jedan validan certifikat istog tipa, osim šezdeset (60) dana prije isteka tog certifikata kada subjekat može dobiti novi certifikat.

(6) Subjekat certifikata za elektronsko pečaćenje, informacione sisteme, potvrdu autentičnosti web stranice i vremensku oznaku može imati više važećih certifikata.

#### 7.1.2.1 Jedinstveni broj elektronske identifikacije

U skladu s člankom 24. Zakona o elektronskoj identifikaciji i uslugama povjerenja (Službeni list Republike Slovenije, br.121/21 i 189/21 – ZDU-1M), člankom 52. Uredbe o određivanju načina elektronske identifikacije i korištenju centralnog servisa za online registraciju i elektronski potpis (Službeni list RS, br. 29/22) Jedinstveni broj elektronske identifikacije (EŠEI) imaoca kvalificirane digitalne potvrde za elektronski potpis, elektronski pečat ili autentifikaciju web stranica se zapiše kao zasebno proširenje kvalificirane potvrde.
Ovo posljednje se zapiše kao nezavisno prošireno polje zapisano u ASN.1 notaciji:
SEQUENCE :
OBJECT_IDENTIFIER : '1.3.6.1.4.1.58536.1.1.1.1.1' <OID proširenje za vrijednost EŠEI fizičke osobe>
OCTET_STRING :
IA5String : 'xxxxxxxxxxx' <vrijednost>
SEQUENCE :
OBJECT_IDENTIFIER : '1.3.6.1.4.1.58536.1.1.1.1.2' <OID proširenje za vrijednost EŠEI poslovnog subjekta>
OCTET_STRING :
IA5String : 'xxxxxxxxxxx' <vrijednost>

#### 7.1.2.2 Zahtjevi za email adrese

(1) Halcom CA zadržava pravo da odbije zahtjev za certifikat ako utvrdi da je adresa e-pošte:

- Neprikladna ili uvredljiva,
- Daje lažne informacije trećim stranama,
- Suprotna važećim odredbama i standardima.

(2) Na elektronske adrese se ne primjenjuju nikakva druga ograničenja.

### 7.1.3 Identifikatori objekta algoritma

(1) Certifikate izdate od strane Halcom CA potpisuje TSP koristeći algoritam naveden u polju Algoritam potpisa: vrijednost "sha256RSA, identifikacioni kod: OID 1.2.840.113549.1.1.11

(2) Kompletan skup algoritama, podatkovnim formata i protokola dostupan je kod ovlaštenih osoba TSP Halcom CA.

### 7.1.4 Oblici imena

Vidi odjeljak 3.1.1.

### 7.1.5 Ograničenja za imena

Ograničenja za imena nisu propisana.

### 7.1.6 Pravila certifikata za identifikator objekta

Vidi odjeljak 7.1.2.

### 7.1.7 Korištenje ekstenzije Ograničenja pravila

Korištenje ekstenzije za ograničenje pravila nije propisano.

### 7.1.8 Kvalifikator pravila (eng. PolicyQualifier) za sintaksu i semantiku

Certifikati koje je izdao Halcom CA TSP koriste specifične informacije u vezi sa PolicyQualifiers koje su u skladu sa IETF RFC i ETSI standardima.

### 7.1.9 Obrada semantike za ključne ekstenzije za Pravila za certifikate (eng.

### Certificate Policies)

Nije podržano.

## 7.2. CRL profil

(1) Registri opozvanih certifikata Halcoma CA (CRL) se nalaze u podružnicama:

- CRL za posredničke / podređene certifikate:
  CN= Halcom Root Certificate Authority
  O = Halcom
  C = SI

- CRL za certifikate za e-potpise za pravna lica:
  CN= Halcom CA PO e-signature 1 ili CN=Halcom CA PO e-signature 2
  O = Halcom
  C = SI

- CRL za certifikate za e-potpise za fizička lica:
  CN= Halcom CA FO e-signature 1 ili CN=Halcom CA FO e-signature 2
  O = Halcom
  C = SI

- CRL za certifikate za e-pečate za pravna lica:
  CN= Halcom CA PO e-seal 1 ili CN= Halcom CA PO e-seal 2
  O = Halcom
  C = SI

- CRL za certifikate za potvrdu autentičnosti web stranice:
  CN= Halcom CA web 1
  O = Halcom
  C = SI

- CRL za certifikate za vremenske pečate:
  CN= Halcom CA TSA 1
  O = Halcom
  C = SI

(2) Registar opozvanih posredničkih / podređenih certifikata ažurira se najmanje jednom godišnje, dok se ostali CRL-ovi ažuriraju nakon svakog opoziva certifikata ili najmanje jednom dnevno, u nedostatku novih zapisa ili promjena u CRL-u (24 sata nakon posljednjeg osvježavanja).

(3) CRL-ovi sadrže jedinstveni serijski broj opozvane opozvanog certifikata i vrijeme i datum opoziva.

### 7.2.1 Brojevi verzija

(1) CRL-ovi su u skladu sa ITU-Z Preporukom za X.509 (2005) i ISO / IEC 9594-8: 2014.

(2) CRL-ovi su trajno dostupni u javnim direktorijima certifikata (vidi odjeljak 2.3):

- putem LDAP protokola i
- putem HTTP protokola.

### 7.2.2 CRL i ekstenzije za unos u CRL

(1) CRL, pored drugih podataka u skladu sa preporukom X.509, sadrži i sljedeće (osnovna polja i ekstenzije su detaljno opisane u tabeli ispod):

- Serijske brojeve opozvanih certifikata
- Vrijeme i datum opoziva.

(2) Korijenski CRL (CRL posredničkih certifikata)

| Naziv polja | Vrijednost ili značenje |
|---|---|
| Osnovna polja u CRL-u | |
| Verzija | V2 |
| Algoritam potpisa | Sha256RSA |
| Signature | Halcom CA signature |
| Prepoznatljivo ime TSP-a (Izdavalac) | CN = Halcom korijensko certifikacijsko tijelo<br>2.5.4.97 = VATSI-43353126<br>O = Halcom d.d.<br>C = SI |
| Vrijeme izdavanja CRL-a (thisUpdate) | Datum stupanja na snagu: <datum izdavanja do GMT> |
| Vrijeme izdavanja idućeg CRL-a (nextUpdate) | Sljedeće ažuriranje: < vrijeme sljedećeg izdavanja do GMT> |
| Identifikacija opozvanih certifikata i vrijeme opoziva (revokedCertificate) | Serijski broj: <identifikacijski broj opozvanog digitalnog certifikata ><br>Datum opoziva: <vrijeme opozivanja prema GMT> |
| Ekstenzije X.509v2 CRL | |
| Broj CRL liste | Serijski broj CRL liste |
| Identifikator ključa tijela (OID 2.5.29.35) | KeyID=42 ae a6 43 c7 98 28 b0 |
| issuerAltName (OID 2.5.28.18) | nije primjenjivo |
| deltaCRLindicator (OID 2.5.29.27) | nije primjenjivo |
| issuingDistribuitionPoint (OID 2.5.29.28) | nije primjenjivo |

(3) Posrednički CRL-ovi

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

| Naziv polja | Vrijednost ili značenje |
|---|---|
| Osnovna polja u CRL-u | |
| Verzija | V2 |
| Algoritam potpisa | Sha256RSA |
| Signature | Halcom CA signature |
| Prepoznatljivo ime TSP-a (Izdavalac) | CN = Halcom CA PO e-signature 1 ili<br>CN = Halcom CA PO e-signature 2<br>2.5.4.97 = VATSI-43353126<br>O = Halcom d.d.<br>C = SI |
| Vrijeme izdavanja CRL-a (thisUpdate) | Datum stupanja na snagu: < datum izdavanja do GMT> |
| Vrijeme izdavanja idućeg CRL-a (nextUpdate) | Sljedeće ažuriranje: < vrijeme sljedećeg izdavanja do GMT> |
| Identifikacija opozvanih certifikata i vrijeme opoziva (revokedCertificate) | Serijski broj: <identifikacijski broj opozvanog digitalnog certifikata><br>Datum opoziva: <vrijeme opozivanja prema GMT> |
| Ekstenzije X.509v2 CRL | |
| Broj CRL liste | Serijski broj CRL liste |
| Identifikator ključa tijela (OID 2.5.29.35) | KeyID= 40 f6 95 20 9b 79 c2 09<br>Ili<br>KeyID= 43 4d 32 75 16 03 c9 75 |
| issuerAltName (OID 2.5.28.18) | nije primjenjivo |
| deltaCRLindicator (OID 2.5.29.27) | nije primjenjivo |
| issuingDistribuitionPoint (OID 2.5.29.28) | nije primjenjivo |

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

| Naziv polja | Vrijednost ili značenje |
|---|---|
| Osnovna polja u CRL-u | |
| Verzija | V2 |
| Algoritam potpisa | Sha256RSA |
| Signature | Halcom CA signature |
| Prepoznatljivo ime TSP-a (Izdavalac) | CN = Halcom CA FO e-signature 1 ili<br>CN = Halcom CA FO e-signature 2<br>2.5.4.97 = VATSI-43353126<br>O = Halcom d.d.<br>C = SI |
| Vrijeme izdavanja CRL-a (thisUpdate) | Datum stupanja na snagu: < datum izdavanja do GMT> |
| Vrijeme izdavanja idućeg CRL-a (nextUpdate) | Sljedeće ažuriranje: < vrijeme sljedećeg izdavanja do GMT> |
| Identifikacija opozvanih certifikata i vrijeme opoziva (revokedCertificate) | Serijski broj: <identifikacijski broj opozvanog digitalnog certifikata><br>Datum opoziva: <vrijeme opozivanja prema GMT> |
| Ekstenzije X.509v2 CRL | |
| Broj CRL liste | Serijski broj CRL liste |
| Identifikator ključa tijela (OID 2.5.29.35) | KeyID= 48 fb 3b 13 99 c3 4e ce<br>Ili<br>KeyID= 48 c4 27 a6 6f 6e f0 2e |
| issuerAltName (OID 2.5.28.18) | nije primjenjivo |
| deltaCRLindicator (OID 2.5.29.27) | nije primjenjivo |
| issuingDistribuitionPoint (OID 2.5.29.28) | nije primjenjivo |

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

| Naziv polja | Vrijednost ili značenje |
|---|---|
| Osnovna polja u CRL-u | |
| Verzija | V2 |
| Algoritam potpisa | Sha256RSA |
| Signature | Halcom CA signature |
| Prepoznatljivo ime TSP-a (Izdavalac) | CN = Halcom CA PO e-seal 1 ili<br>CN = Halcom CA PO e-seal 2<br>2.5.4.97 = VATSI-43353126<br>O = Halcom d.d.<br>C = SI |
| Vrijeme izdavanja CRL-a (thisUpdate) | Datum stupanja na snagu: < datum izdavanja do GMT> |
| Vrijeme izdavanja idućeg CRL-a (nextUpdate) | Sljedeće ažuriranje: < vrijeme sljedećeg izdavanja do GMT> |
| Identifikacija opozvanih certifikata i vrijeme opoziva (revokedCertificate) | Serijski broj: <identifikacijski broj opozvanog digitalnog certifikata><br>Datum opoziva: <vrijeme opozivanja prema GMT> |
| Ekstenzije X.509v2 CRL | |
| Broj CRL liste | Serijski broj CRL liste |
| Identifikator ključa tijela (OID 2.5.29.35) | KeyID=49 48 76 50 77 0a b1 0c<br>ili<br>KeyID=47 35 c8 bc 61 e2 5d 9e |
| issuerAltName (OID 2.5.28.18) | nije primjenjivo |
| deltaCRLindicator (OID 2.5.29.27) | nije primjenjivo |
| issuingDistribuitionPoint (OID 2.5.29.28) | nije primjenjivo |

- Halcom CA web 1

| Naziv polja | Vrijednost ili značenje |
|---|---|
| Osnovna polja u CRL-u | |
| Verzija | V2 |
| Algoritam potpisa | Sha256RSA |

| | |
|---|---|
| Signature | Halcom CA signature |
| Prepoznatljivo ime TSP-a (Izdavalac) | CN = Halcom CA web 1<br>2.5.4.97 = VATSI-43353126<br>O = Halcom d.d.<br>C = SI |
| Vrijeme izdavanja CRL-a (thisUpdate) | Datum stupanja na snagu: < datum izdavanja do GMT> |
| Vrijeme izdavanja idućeg CRL-a (nextUpdate) | Sljedeće ažuriranje: < vrijeme sljedećeg izdavanja do GMT> |
| Identifikacija opozvanih certifikata i vrijeme opoziva (revokedCertificate) | Serijski broj: <identifikacijski broj opozvanog digitalnog certifikata><br>Datum opoziva: <vrijeme opozivanja prema GMT> |
| Ekstenzije X.509v2 CRL | |
| Broj CRL liste | Serijski broj CRL liste |
| Identifikator ključa tijela (OID 2.5.29.35) | KeyID=48 42 0b 17 ed ae 9e 70 |
| issuerAltName (OID 2.5.28.18) | nije primjenjivo |
| deltaCRLindicator (OID 2.5.29.27) | nije primjenjivo |
| issuingDistribuitionPoint (OID 2.5.29.28) | nije primjenjivo |

- Halcom CA TSA 1

| Naziv polja | Vrijednost ili značenje |
|---|---|
| Osnovna polja u CRL-u | |
| Verzija | V2 |
| Algoritam potpisa | Sha256RSA |
| Signature | Halcom CA signature |
| Prepoznatljivo ime TSP-a (Izdavalac) | CN = Halcom CA TSA 1<br>2.5.4.97 = VATSI-43353126 O = Halcom d.d.<br>C = SI |
| Vrijeme izdavanja CRL-a (thisUpdate) | Datum stupanja na snagu: < datum izdavanja do GMT> |
| Vrijeme izdavanja idućeg CRL-a (nextUpdate) | Sljedeće ažuriranje: < vrijeme sljedećeg izdavanja do GMT> |
| Identifikacija opozvanih certifikata i vrijeme opoziva (revokedCertificate) | Serijski broj: <identifikacijski broj opozvanog digitalnog certifikata><br>Datum opoziva: <vrijeme opozivanja prema GMT> |
| Ekstenzije X.509v2 CRL | |
| Broj CRL liste | Serijski broj CRL liste |
| Identifikator ključa tijela (OID 2.5.29.35) | KeyID= 43 8f 8b 56 9f 44 1e d7 |
| issuerAltName (OID 2.5.28.18) | nije primjenjivo |
| deltaCRLindicator (OID 2.5.29.27) | nije primjenjivo |
| issuingDistribuitionPoint (OID 2.5.29.28) | nije primjenjivo |

### 7.2.3 Objavljivanje CRL-ova

Halcom CA objavljuje CRL-ove u javnom direktoriju na ldap://ldap.halcom.si servere prema LDAP protokolu i na http://domina.halcom.si/crls prema HTTP protokolu.

## 7.3. OCSP profil

(1) Protokol za online status certifikata je dostupan na http://ocsp.halcom.si.

(2) OCSP profil za poruke (zahtjeve/odgovori) je u skladu sa IETF RFC preporukom.

### 7.3.1 Broj verzija

TSP Halcom CA koristi OCSP verziju 1 za poruke u skladu sa IETF RFC preporukom.

### 7.3.2 OCSP Ekstenzije

OCSP (zahtjev/odgovor) servisne poruke podržavaju Nonce ekstenziju koja nije označena kao ključna.

# 8. PROVJERA USKLAĐENOSTI I OSTALA OCJENJIVANJA

(1) Halcom zapošljava internog revizora sa odgovarajućim tehnološkim i pravnim znanjem. Interni službenik za kontrolu i reviziju ne obavlja poslove vezane za upravljanje certifikatima.

(2) Službenik za internu reviziju nadgleda rad Halcoma CA. U slučaju otkrivenih nedostataka, službenik za internu reviziju će preduzeti odgovarajuće mjere kako bi otklonio te nedostatke. Halcom CA je obavezan da provede navedene odgovarajuće mjere u okviru nadzora službenika za internu reviziju.

(3) Halcom CA se godišnje podvrgava vanjskoj nezavisnoj reviziji koju provodi akreditirano tijelo.

## 8.1. Učestalost ili okolnosti ocjenjivanja

(1) Interni revizor provodi aktivnosti ocjenjivanja najmanje jednom godišnje.

(2) Vanjska revizija za ISO 9001 i ISO 27001 provodi se jednom godišnje. Revizija eksterne kontrole za ETSI standarde provodi se svake dvije godine.

## 8.2. Identitet / kvalifikacije ocjenjivača

(1) Službenik za internu reviziju ima odgovarajuće tehnološko i pravno znanje.

(2) Revizor vanjske revizije mora imati odgovarajuća tehnološka i pravna znanja.

## 8.3. Odnos ocjenjivača sa subjektom koji se ocjenjuje

(1) Službenik za internu reviziju ne obavlja poslove koji se odnose na upravljanje certifikatima.

(2) Revizor vanjske revizije ne obavlja poslove vezane za upravljanje certifikatima.

## 8.4. Teme koje se obrađuju tokom ocjenjivanja

Područja za ocjenjivanje su navedena u internim pravilima TSP-a Halcom CA.

## 8.5. Aktivnosti koje se poduzimaju u slučaju nedostataka

U slučaju nedostataka, službenik za internu/vanjsku reviziju će poduzeti odgovarajuće mjere kako bi otklonio nedostatke koje je Halcom CA dužan provoditi pod njegovim nadzorom. Implementacija mjera detaljno je opisana u internim pravilima TSP-a Halcom CA.

## 8.6. Saopštavanje rezultata

TSP Halcom CA arhivira rezultate ocjenjivanja.

# 9. Ostala poslovna i pravna pitanja

## 9.1 Naknade

Halcom CA određuje cjenovnik za certifikate, usluge, potrebnu opremu i infrastrukturu i objavljuje takav cjenovnik na svojoj web stranici.

### 9.1.1 Cijena izdavanja ili obnavljanja certifikata

Cijene certifikata i njihova obnova utvrđuju se važećim cjenikom.

### 9.1.2 Cijene za pristup certifikatima

Pristup javnim certifikatima je besplatan, osim ako se ugovorne strane ne dogovore drugačije.

### 9.1.3 Opoziv ili status

CRL je dostupan svim licima besplatno.

### 9.1.4 Naknade za druge usluge

Cijene ostalih usluga, opreme i infrastrukture su određene važećim cjenovnikom.

### 9.1.5 Pravilo povrata novca

Nije propisano.

## 9.2 Finansijska odgovornost

### 9.2.1 Osiguranje

Halcom CA ima adekvatno osiguranu odgovornost. Detaljne informacije o osiguranju dostupne su na web stranici.

### 9.2.2 Ostala sredstva

Nije propisano.

### 9.2.3 Osiguranje ili garancija za krajnje korisnike

Nije propisano.

## 9.3 Povjerljivost poslovnih informacija

### 9.3.1 Opseg povjerljivih informacija

(1) TSP Halcom CA štiti povjerljivost sljedećih podataka:
- svi certifikati ili drugi obrasci za prijavu,
- sve povjerljive informacije u vezi sa finansijskim obavezama,
- sve povjerljive informacije koje podliježu međusobnim sporazumima s trećim stranama, i
- sva ostala pitanja pokrivena internim pravilima TSP-a Halcom CA u skladu sa Uredbom.

(2) Pružalac usluga povjerenja Halcom CA obrađuje sve moguće povjerljive informacije o subjektima i trećim stranama koje su strogo neophodne za usluge upravljanja certifikatima u skladu sa važećim zakonom.

### 9.3.2 Informacije koje nisu u opsegu povjerljivih informacija

TSP Halcom CA javno objavljuje samo one poslovne informacije koje nisu povjerljive u skladu sa važećim zakonom.

### 9.3.3 Odgovornost za zaštitu povjerljivih informacija

(1) Halcom CA ne preuzima nikakvu odgovornost za sadržaj podataka koji su šifrirani ili koje je subjekat

certifikata potpisao/opečatio, čak i ako su subjekat ili treća strana postupili u skladu sa svim važećim propisima, svim odredbama politike i drugim Halcom CA pravilima, ili su sve date instrukcije uzete u obzir.

(2) Halcom CA ne preuzima nikakvu odgovornost za posljedice koje proizlaze iz razloga što subjekat certifikata nije ispunio sigurnosne zahtjeve navedene u odjeljku 4.5.1 ovog dokumenta.

## 9.4 Privatnost ličnih informacija

### 9.4.1 Plan privatnosti

Halcom CA pažljivo štiti lične podatke u skladu sa evropskim i slovenačkim propisima, međunarodnim standardima i preporukama, vrši redovnu procjenu rizika i osigurava privatnost po unaprijed određenim očekivanjima. Halcomov službenik za usklađenost s propisima djeluje kao službenik za zaštitu podataka.

### 9.4.2 Informacije koje se tretiraju kao privatne

Zaštićeni podaci su svi lični podaci koje TSP Halcom CA dobiva iz obrazaca zahtjev za izdavanje certifikata za svoje usluge ili u odgovarajućim registrima u svrhu dokazivanja identiteta subjekta ili tokom obavljanja usluga povjerenja.

Zbog prirode korištenja certifikata i odredbi važećih propisa i standarda, informacije u certifikatima i CRL-u dostupne su trećim stranama koje se oslanjaju na certifikate ili potvrđuju njihovu validnost.

### 9.4.3 Informacije koje se ne smatraju privatnim

Svi podaci su zaštićeni podaci osim onih koji su naznačeni na certifikatu i u CRL-u.

### 9.4.4 Odgovornost za zaštitu privatnih informacija

Pružalac usluga povjerenja Halcom CA odgovoran je za zaštitu podataka u skladu s važećim pravilima zaštite podataka i odredbama interne politike za zaštitu podataka.

### 9.4.5 Obavještenje i saglasnost za korištenje privatnih informacija

Subjekat će ovlastiti TSP Halcom CA da obrađuje lične podatke navedene u obrascu zahtjeva za izdavanje certifikata, posebnom pisanom saglasnošću za obradu ličnih podataka, ili za druge slučajeve kasnije u drugoj izjavi u pisanom obliku.

### 9.4.6 Otkrivanje informacija shodno pravim i administrativnim procesima

(1) TSP Halcom CA neće davati nikakve podatke koji se odnose na subjekte certifikata osim onih koji su navedeni u certifikatu, osim ako su određeni podaci posebno potrebni za pružanje određenih usluga ili za obrasce prijave u vezi sa certifikatima, a korisnik je prethodno dao saglasnost TSP-u Halcom CA (vidi prethodni odjeljak), ili na zahtjev nadležnog suda, organa za provođenje zakona, upravne jedinice ili drugog ovlaštenog lica. Svaki takav zahtjev će biti pažljivo pregledan od strane Halcoma CA i podaci će se dijeliti samo u mjeri u kojoj to zahtijevaju važeći propisi.

(2) Podaci se šalju bez pismene saglasnosti samo u slučajevima kada je to predviđeno važećim evropskim ili slovenačkim zakonodavstvom.

### 9.4.7 Druge okolnosti za otkrivanje informacija

Nije propisano.

## 9.5 Prava intelektualnog vlasništva

Autorska i ostala prava intelektualnog vlasništva:

- sva prava vezana za javni ključ koji pripada subjektu certifikata,
- Sva prava vezana za javne ključeve, svi podaci o certifikatima, direktorij certifikata i CRL podaci, podaci iz CP-ova i CPS koji pripadaju Halcomu CA.

## 9.6 Izjave i garancije

### 9.6.1 CA izjave i garancije

(1) TSP Halcom CA je dužan:
- postupati u skladu sa svojim internim pravilima i drugim važećim propisima,
- postupati u skladu sa međunarodnim preporukama,
- objaviti sve relevantne dokumente koji određuju njegovo poslovanje (politike, obrasce zahtjeva za izdavanje certifikata, zahtjevi za opoziv, cjenovnici, upute za sigurno korištenje kvalifikovanih digitalnih certifikata, itd.)
- objaviti na svojoj internet stranici sve informacije o promjenama u aktivnosti TSP-a, koje na bilo koji način utječu na subjekte certifikata i treća lica,
- osigurati rad usluga obavještavanja u skladu sa odredbama HALCOM CA i drugim važećim propisima,
- pridržavati se odredbi koje se odnose na sigurnu obradu ličnih i povjerljivih informacija o TSP-u, subjektima certifikata ili trećim stranama,
- opozvati certifikat i objaviti ga na CRL-u nakon otkrivanja razloga prema ovom CPS-u ili drugim važećim propisima,
- izdati kvalifikovane digitalne certifikate u skladu s ovim CPS-om i drugim propisima i preporukama.

(2) TSP Halcom CA je dužan:
- osigurati ispravnost podataka o izdatim certifikatima,
- osigurati ispravno objavljivanje CRL-a,
- osigurati jedinstvenost prepoznatljivih imena,
- osigurati odgovarajuću fizičku sigurnost prostorija i pristup prostorijama TSP-a,
- profesionalno osigurati neprekidan rad i maksimalnu dostupnost usluge,
- profesionalno osigurati maksimalnu dostupnost usluga,
- profesionalno upravljati kontinuiranim radom svih ostalih pratećih usluga,
- na najbolji način otkloniti bilo kakve probleme u najkraćem mogućem roku,
- upravljati optimizacijom korištenog hardvera i softvera,
- informisati korisnike o važnim pitanjima i
- ispuniti sve ostale zahtjeve u skladu sa ovom politikom.

(3) TSP Halcom CA osigurava maksimalnu dostupnost svojih usluga, svaki dan u godini, osim u sljedećim slučajevima:
- planirane i unaprijed najavljene tehničke ili servisne intervencije na infrastrukturi,
- neplanirane tehničke ili servisne intervencije na infrastrukturi kao rezultat nepredviđenih kvarova,
- tehničke ili servisne intervencije zbog kvara infrastrukture izvan nadležnosti Halcom CA i
- nedostupnost kao rezultat više sile ili vanrednih događaja.

(4) TSP Halcom CA će najaviti održavanje ili modernizaciju infrastrukture najmanje tri (3) dana prije početka aktivnosti.

(5) TSP Halcom CA je isključivo odgovoran za sve informacije u ovom dokumentu i za implementaciju svih odredbi u ovom CPS-u.

(6) Ostale obaveze TSP-a Halcom CA koje se mogu odrediti mogućim uzajamnim sporazumom sa trećom stranom.

### 9.6.2 RA izjave i garancije

(1) RA je dužan:
- provjeriti identitet subjekata ili budućih subjekata,
- primiti obrazac zahtjeva za izdavanje certifikata za usluge Halcom CA,
- provjeriti obrazac zahtjeva za izdavanje certifikata,
- izdati neophodnu dokumentaciju pravnim licima, subjektima ili budućim subjektima,
- poslati obrasce i druge informacije na siguran način Halcomu CA.

(2) RA snosi odgovornost za implementaciju svih odredbi, pravila i drugih uslova CPS-a dogovorenih sa TSP-om Halcom CA.

### 9.6.3 Izjave i garancije pretplatnika

(1) Pravno lice je odgovorno za:
- štete nastale u slučaju zloupotrebe certifikata od podnošenja opoziva do opoziva,
- bilo koju štetu koja je direktno ili indirektno uzrokovana upotrebom ili zloupotrebom certifikata subjekta od strane neovlaštenih osoba,
- bilo koju drugu šteta nastala uslijed nepoštovanja CPS-a, pravila i drugih obavještenja Halcoma CA i važećih propisa

(2) Obaveze subjekta u vezi korištenja certifikata su navedene u Odjeljku 4.5.1.

### 9.6.4 Izjave i garancije treće strane

(1) Prilikom prve upotrebe Halcom CA certifikata, treća strana koja se oslanja na certifikat je dužna da pažljivo politiku i redovno prati sve obavijesti Halcom CA.

(2) U trenutku korištenja certifikata, treća strana je obavezna da uvijek temeljno provede validaciju ako certifikat nije naveden u CRL.

(3) Ako certifikat sadrži informacije o trećem licu, ta stranka zahtijeva opoziv certifikata ako utvrdi da je privatni ključ ugrožen na način koji utiče na pouzdanost upotrebe ili ako postoji rizik od zloupotrebe, ili ako su podaci navedeni u certifikatu promijenjeni.

(4) Treća strana se može osloniti na certifikat do opoziva certifikata.

(5) Treća strana može u bilo koje vrijeme zatražiti bilo koju informaciju o validnosti bilo kojeg izdatog certifikata, o odredbama politike i obavijestima Halcoma CA.

### 9.6.5 Izjave i garancije drugih učesnika

Nije propisano.

## 9.7 Odricanje od garancija

TSP Halcom CA nije odgovoran za bilo kakvu štetu koja je rezultat:
- korištenja certifikata za bilo koju svrhu ili na način koji nije izričito predviđen u ovom CPS-u,
- netačne ili neadekvatne zaštite lozinki ili privatnih ključeva subjekata, otkrivanja povjerljivih podataka ili ključeva trećim licima i neodgovornog ponašanja subjekta,
- zloupotrebe ili upada u informacioni sistem subjekta certifikata, a time i informacija o certifikatima od strane neovlaštenih lica,
- nedjelovanja ili neispravnosti informacijske infrastrukture subjekta certifikata ili trećih strana,
- nevalidacije podataka i validnosti certifikata u CRL-u,
- neprovjeravanja perioda važenja certifikata,
- ponašanje subjekta certifikata ili treće strane suprotno Halcom CA obavijestima, pravilima i drugim propisima,
- omogućavanja neovlaštenim osobama da koriste ili zloupotrijebe certifikat subjekta,
- izdate potvrda sa lažnim informacijama ili nepouzdanim podacima ili drugim sličnim aktima subjekta ili TSP-a,
- korištenja certifikata i validnosti certifikata nakon promjene podataka certifikata, email adrese ili promjene imena subjekta,
- kvara na infrastrukturi izvan domene Halcom CA TSP,
- šifrovanja ili potpisivanja podataka pomoću certifikata,
- ponašanja subjekata prilikom korištenja certifikata, čak i ako je subjekat ili treća strana ispunila sve odredbe ovog CPS-a, obavijesti Halcoma CA ili druge važeće propise,
- korištenja i pouzdanosti rada hardvera i softvera subjekata certifikata.
- greške u obračunavanju vrijednosti raspršivanja, provjera vrijednosti raspršivanja ili drugi sigurnosni postupci koji se odnose na elektronski dokument koji će se potpisati ukoliko je subjekat zahtijevao elektronski potpis u cloud-u isključivo na osnovu vrijednosti raspršivanja i bez slanja cijelog elektronskog dokumenta Halcomu CA TSP-a.

## 9.8 Ograničenja odgovornosti

Nije propisano.

## 9.9 Odštete

Strana koja ne poštuje odredbe pravila i važeće zakone je odgovorna za štetu koja može biti rezultat tog nepoštovanja.

## 9.10 Period važenja i prekid

(1) Halcom CA zadržava pravo izmjene CPS-a i nadogradnje svoje infrastrukture bez prethodnog obavještenja za subjekte certifikata.

(2) CPS stupa na snagu na dan kada ga usvoji Halcom CA.

### 9.10.1 Period važenja

Promjene nove verzije CPS-a se objavljuju na web stranici TSP-a Halcom CA osam (8) dana prije validacije, a datum stupanja na snagu mora biti jasno naznačen.

### 9.10.2 Prekid

(1) Nakon što se objavi novi CPS i pravila, za sve certifikate koji su izdati na temelju tih pravila na snazi ostaju sve (stare) odredbe koje ne mogu biti prikladno zamijenjene relevantnim odredbama iz novih politika (na primjer, postupak za utvrđivanje načina izdavanja certifikata itd.)

(2) TSP može uvesti izmjene na odredbe CPS-a kao što se navodi u Odjeljku 9.12.

### 9.10.3 Učinak prekida i nastavak važenja

(1) Validnost certifikata je regulisana pravilima.

(2) Novi CPS, a time i nova politika, ne utiče na validnost certifikata izdatih u okviru prethodnih politika. Takve potvrde ostaju na snazi do isteka roka važenja, gdje je to moguće, s njima se postupa u skladu s novom politikom.

## 9.11 Pojedinačna obavještenja i komunikacija sa učesnicima

(1) Kontakt podaci TSP-a su objavljeni na web stranici i dati su u odjeljku 1.3.1.

(2) Kontakti podaci subjekata navedeni su u obrascima zahtjeva za izdavanje certifikata.

(3) Kontakt podaci trećih strana daju se u dogovoru između treće strane i pružaoca usluga povjerenja Halcom CA.

## 9.12 Izmjene

### 9.12.1 Postupak uvođenja izmjena

(1) TSP može objaviti izmjene ili dopune CPS-a u obliku izmjena i dopuna CPS-a gdje nema značajnih promjena u učinku TSP-a.

(2) Izmjene i dopune usvajaju se u skladu s istom procedurom kao i CPS.

(3) Način označavanja izmjena i dopuna određuje TSP Halcom CA.

### 9.12.2 Mehanizam i period obavještavanja

(1) TSP Halcom CA će odrediti početak i kraj važenja izmjena i dopuna.

(2) Izmjene i dopune će biti objavljene na web stranici Halcoma CA osam (8) dana prije njihovog

stupanja na snagu.

## 9.13 Odredbe za rješavanje sporova

(1) Sve prigovore subjekata certifikata rješava službenik za usklađenost s propisima.

(2) Bilo koji spor između subjekta certifikata ili treće strane i Halcoma CA rješava nadležni sud u Ljubljani, u Sloveniji.

## 9.14 Mjerodavno pravo

Sva pitanja će biti regulisana u skladu sa zakonima Evropske unije i Republike Slovenije.

## 9.15 Usklađenost sa važećim zakonima

(1) Nadgledanje usaglašenosti TSP Halcoma CA sa važećim zakonima i propisima vrše nadležna inspekcija i akreditovana tijela za ocjenu usklađenosti.

(2) TSP Halcom CA će biti pregledan od strane akreditiranog tijela za ocjenjivanje usklađenosti najmanje svakih 24 mjeseca. Svrha revizije je provjeriti da TSP i kvalifikovane usluge povjerenja koje pruža zadovoljavaju zakonske zahtjeve.

(3) (3) Internu verifikaciju usaglašenosti vrše ovlaštena lica u okviru TSP Halcoma CA.

## 9.16 Razne odredbe

(1) TSP Halcom CA može sklopiti međusobne sporazume s drugim TSP-ovima ako je to predviđeno važećim zakonom ili drugim propisima.

(2) Ako je neka od odredbi ove politike nevažeća, to neće uticati na druge odredbe. Nevažeća odredba se zamjenjuje važećom, koja mora biti što je moguće bliža svrsi na koju se odnosila nevažeća odredba.

## 9.17 Ostale odredbe

Nije propisano.

Mjesto i datum: Ljubljana, 26.05.2023.

Glavni izvršni direktor:

Tomi Šefman