Pripremio: Luka RIBIČIČ

Broj dokumenta: 400085-44-2/17

Politika Halcom CA: Javni dio internih pravila za EU kvalifikovane digitalne potvrde za pravna lica

Izdanje: 02

Politika Halcom CA

Javni dio internih pravila Halcom CA za EU kvalifikovane digitalne potvrde za pravna lica

Dokument važi od: 15.6.2026.

CPName: Halcom CA PO

Politika	CPOID	Vrsta potvrde	Generacija
Halcom CA PO e-signature 1	1.3.6.1.4.1.5939.5.1.3	QCert for ESig QRemManage for QSigCD	G1
Halcom CA PO e-signature 2	1.3.6.1.4.1.5939.5.1.4	QCert za ESig QRemManage for QSigCD	G1
Halcom CA PO e-seal 1	1.3.6.1.4.1.5939.5.3.2 1.3.6.1.4.1.5939.5.4.2	QCert for Eseal QRemManage for QSigCD Cert for ESeal	G1 G1
Halcom CA PO e-seal 2	1.3.6.1.4.1.5939.5.3.3 1.3.6.1.4.1.5939.5.4.3	QCert for Eseal QRemManage for QSigCD Cert for Eseal	G1 G1
Halcom CA web 1	1.3.6.1.4.1.5939.5.2.5	QWAC	G1

Halcom CA web 2	1.3.6.1.4.1.5939.5.2.6	QWAC	G1
Halcom CA PO e-sig 1 G2	1.3.6.1.4.1.5939.5.1.7	QCert for ESig QRemManage for QSigCD	G2
Halcom CA e-seal 1 G2	1.3.6.1.4.1.5939.5.3.7 1.3.6.1.4.1.5939.5.4.7	QCert for Eseal QRemManage for QSigCD Cert for ESeal	G2 G2
Halcom CA web 1 G2	1.3.6.1.4.1.5939.5.2.7	QWAC	G2
Halcom CA PO e-sig 1 G3	1.3.6.1.4.1.5939.5.1.8	QCert for ESig QRemManage for QSigCD	G3
Halcom CA e-seal 1 G3	1.3.6.1.4.1.5939.5.3.8 1.3.6.1.4.1.5939.5.4.8	QCert for Eseal QRemManage for QSigCD Cert for ESeal	G3 G3
Halcom CA web 1 G3	1.3.6.1.4.1.5939.5.2.8	QWAC	G3

Historija:

Izdanje	broj dokumenta i priloga	Opis promjene	Autor	Datum posljednje izmjene
1	400085-44-1/17	Početno izdanje (spajanje svih CP-ova za pravna lica)	L. Ribičič	23.5.2025.
2	400085-44-2/17	Nova CA generacija – G3, OT potvrde, e-pečat potvrde u cloudu	L. Ribičič	20.5.2026

Sadržaj

1. UVOD

(1) Halcom CA je najstariji i najveći pružatelj usluga povjerenja u Sloveniji, koji koristi najsigurnije tehnologije, uključujući korištenje sigurnih nosača podataka i sigurnog clouda, za pružanje svojih usluga u području elektroničkog potpisivanja, elektroničkog pečatiranja, elektroničkog vremenskog žigosanja, validacije i drugih usluga.

(2) Ova politika je javni dio internih pravila Halcom CA za kvalifikovane digitalne potvrde za poslovne subjekte (pravna lica, samostalne poduzetnike i druga fizička lica registrovana za obavljanje djelatnosti).

(3) Forma i sadržaj ove politike usklađeni su s Uredbom eIDAS, Uredbom eIDAS 2.0, međunarodnom preporukom IETF RFC i evropskim ETSI standardima, između ostalog.

1.1. Pregled

(1) Ova politika predstavlja nedjeljivu cjelinu općih pravila poslovanja pružatelja usluga povjerenja Halcom CA u vezi s izdavanjem kvalificiranih digitalnih potvrda, uređuje svrhu, rad i metodologiju upravljanja kvalificiranim digitalnim potvrdama, kao i sigurnosne zahtjeve koje moraju ispunjavati pružatelj usluga povjerenja Halcom CA, imaoci potvrda, treća lica koja se oslanjaju na te potvrde, te odgovornost svih navedenih osoba.

(2) Halcom CA je pružatelj usluga povjerenja koji izdaje i upravlja kvalificiranim digitalnim potvrdama za provjeru valjanosti elektroničkih potpisa, elektroničkih pečata i autentifikaciju web stranica. Pružatelj usluga povjerenja Halcom CA posluje u okviru Halcom d.d.

(3) Halcom CA izdaje kvalifikovane digitalne potvrde sa najmanje jednim parom ključeva.

(4) Sve odredbe ove politike u vezi s ponašanjem Halcom CA na odgovarajući način su prenesene i detaljnije specificirane u javno objavljenim općim pravilima poslovanja pružatelja usluga povjerenja (CPS) i definirane u odredbama povjerljivih internih pravila pružatelja usluga povjerenja, kojima se definira infrastruktura, odredbe u vezi s osobljem Halcom CA (kompetencije, zadaci, ovlaštenja i potrebni uvjeti pojedinih članova osoblja), fizička sigurnost (pristup prostorijama, rukovanje hardverom i softverom), sigurnost softvera (sigurnosne postavke servera, sigurnosne kopije itd.) i interna kontrola (kontrola fizičkog pristupa, ovlaštenja itd.).

(5) Halcom CA izdaje potvrde i obavlja druge aktivnosti pružatelja usluga povjerenja u skladu s važećim pravnim poretkom Republike Slovenije i Europske unije, te u skladu s Uredbom eIDAS, Uredbom eIDAS 2.0, tehničkim zahtjevima ETSI-ja, standardom IETF RFC i grupom standarda ISO/IEC i drugim srodnim standardima.

(6) Halcom CA objavljuje popis prijavnih službi koje omogućavaju sticanje kvalificiranih digitalnih potvrda za pravna lica na internetu.

1.2. Identifikacijski podaci politike

(1) Oznaka operativnih politika za EU digitalne potvrde za pravna lica:

Politika	CPOID	Vrsta potvrde
Halcom CA PO e-signature 1	1.3.6.1.4.1.5939.5.1.3	QCert for ESig
Halcom CA PO e-signature 2	1.3.6.1.4.1.5939.5.1.4	QCert for ESig
Halcom CA PO e-seal 1	1.3.6.1.4.1.5939.5.3.2 1.3.6.1.4.1.5939.5.4.2	QCert for ESeal Cert for ESeal
Halcom CA PO e-seal 2	1.3.6.1.4.1.5939.5.3.3 1.3.6.1.4.1.5939.5.4.3	QCert for ESeal Cert for ESeal
Halcom CA web 1	1.3.6.1.4.1.5939.5.2.5	QWAC
Halcom CA web 2	1.3.6.1.4.1.5939.5.2.6	QWAC
Halcom CA PO e-sig 1 G2	1.3.6.1.4.1.5939.5.1.7	QCert for ESig
Halcom CA e-seal 1 G2	1.3.6.1.4.1.5939.5.3.7 1.3.6.1.4.1.5939.5.4.7	QCert for ESeal Cert for ESeal
Halcom CA web 1 G2	1.3.6.1.4.1.5939.5.2.7	QWAC
Halcom CA PO e-sig 1 G3	1.3.6.1.4.1.5939.5.1.8	QCert for ESig QRemManage for QSigCD
Halcom CA e-seal 1 G3	1.3.6.1.4.1.5939.5.3.8 1.3.6.1.4.1.5939.5.4.8	QCert for Eseal QRemManage for QSigCD Cert for ESeal
Halcom CA web 1 G3	1.3.6.1.4.1.5939.5.2.8	QWAC

(2) Svaki potvrda sadrži referencu politike u obliku CPOID-a (vidjeti tačku 7.1.2).

1.3. Subjekti

1.3.1 Pružatelj usluga od povjerenja Halcom CA

(1) Halcom CA je pružatelj usluga od povjerenja koji izdaje i upravlja kvalifikovanim digitalnim potvrdama koje povezuju podatke za potvrđivanje valjanosti:

- kvalifikovanog elektronskog potpisa sa fizičkim licem, ovlaštenim predstavnikom pravnog lica,
- kvalifikovanog elektronskog pečata kod pravnog lica,
- kvalifikovane elektronske potvrde za autentifikaciju web stranice kod pravnog lica.

(2) Pružatelj usluga od povjerenja Halcom CA posluje u okviru Halcom d.d.

1.3.2 Prijavna služba Halcom CA

(1) Prijavna služba za pružatelja usluga od povjerenja obavlja sljedeće zadatke:

- provjera identiteta pravnog lica, ovlaštenog predstavnika pravnog lica i drugih važnih podataka za upravljanje kvalifikovanim digitalnim potvrdama,
- primanje zahtjeva za dobijanje potvrda,
- prihvatanje zahtjeva za opoziv potvrda,
- izdavanje potrebne dokumentacije pravnim licima, imaocima ili budućim imaocima,
- prosljeđivanje zahtjeva i ostalih podataka na siguran način pružatelju usluga od povjerenja Halcom CA.

(2) Pored svoje prijavne službe, pružatelj usluga od povjerenja Halcom CA može ovlastiti i druge organizacije u poslovnom i javnom sektoru za obavljanje poslova prijavne službe. Svaka takva organizacija će biti ugovorno obavezna od strane pružatelja usluga od povjerenja Halcom CA da se pridržava strogih sigurnosnih uvjeta u skladu s važećom europskom i slovenskom regulativom te međunarodnim, europskim i slovenskom standardima i preporukama, kao i politikama, pravilima poslovanja i internim pravilima Halcom CA.

(3) Pružatelj usluga od povjerenja Halcom CA imageografski raširenu prijavnu službu, koja potencijalnim imaocima omogućava jednostavnu registraciju u svom mjestu ili obližnjoj lokaciji. Informacije o lokacijama prijavnih službi dostupne su na web stranici pružatelja usluga od povjerenja Halcom CA.

1.3.3 Naručioci i imaoci potvrda

(1) Imaoc potvrde, koji je ovlašteno fizičko lice pravnog lica, pravno lice ili uređaj pravnog lica, koristi svoje podatke (par ključeva/parove ključeva) koje mu je dodijelio pružatelj usluga od povjerenja za kvalifikovano elektronsko potpisivanje, pečatiranje, autentifikaciju web stranice i kvalifikovane digitalne potvrde kako bi povezao ovaj elektronski potpis, pečat ili autentifikaciju web stranice s imaocem.

(2) Podimaoc zahtjeva za potvrdu je pravno lice.

(3) Imaoc potvrde je:

- ovlašteno lice pravnog lica ili
- sam poslovni subjekt ili uređaj kojim upravlja.

(4) U slučaju potvrde za autentifikaciju web stranice, imaoc može izuzetno biti i fizička osoba.

1.3.4 Treća lica

(1) Treća lica su lica koje se oslanjaju na izdane potvrde i druge usluge pružatelja usluga od povjerenja Halcom CA, a mogu biti fizička ili pravna lica.

(2) Treća lica moraju slijediti upute pružatelja usluga od povjerenja Halcom CA i uvijek moraju provjeriti validnost potvrde, svrhu korištenja potvrde, period važenja potvrde itd. Detaljnije obaveze i odgovornosti trećih lica navedene su u tačkama 4.5.2. i 9.6.4.

(3) Treća lica ne moraju nužno biti imaoci potvrda pružatelja usluga od povjerenja Halcom CA ili

digitalnih potvrda drugih pružatelja usluga od povjerenja. .

1.4. Svrha upotrebe

Halcom CA upravlja (izdaje i provjerava, opoziva, produžava, pohranjuje, objavljuje) kvalifikovanim pravnim digitalnim potvrdama za provjeru valjanosti elektronskog potpisa, elektronskog pečata ili autentifikacije web stranice (u daljnjem tekstu potvrda) namijenjenim pravnim licima.

1.4.1 Ispravna upotreba potvrda i ključeva

(1) Potvrde su namijenjene za elektronsko potpisivanje jednostrane ili međusobne komunikacije između imaoca potvrde i za upotrebu u različitim aplikacijama i za različite svrhe koje se pojavljuju na tržištu. Potvrde se mogu koristiti u svrhe kao što su, između ostalog:

1) identifikacija imaoca,
2) potvrda identifikacije imaoca ,
3) potpisivanja, pečatiranja dokumenata u elektronskom obliku,
4) šifriranja i dešifriranja dokumenata u elektronskom obliku.
5) autentifikacija web stranice, itd.

(2) Elektronski potpis, elektronski pečat i potvrda za autentifikaciju web stranice mogu se koristiti u aplikacijama kao što su:

1) elektronsko ili mobilno bankarstvo,
2) aplikacije e-uprave ili mobilne uprave,
3) aplikacije za e-zdravlje ili mobilno zdravstvo,
4) potpisivanje, pečatiranje elektronskih ili mobilnih obrazaca,
5) sigurno poslovanje s tijelima i organizacijama javnog sektora i s drugim pravnim ili fizičkim licima,
6) druge aplikacije ili usluge koje zahtijevaju upotrebu kvalifikovane digitalne potvrde,
7) kontrola pristupa .

1.4.2 Neovlaštena upotreba

(1) Zabranjeno je koristiti potvrde izdate u skladu s ovom politikom na način koji je suprotan odredbama ove politike ili važećih propisa, ili izvan opsega dozvoljene upotrebe navedene u prethodnom tački.

(2) Potvrde nisu namijenjene za preprodaju.

1.5. Upravljanje politikama

1.5.1 Upravitelj politika

(1) Ovom i drugim politikama upravlja pružatelj usluga od povjerenja Halcom CA, koji posluje u okviru Halcom d.d.

(2) Adresa kontrolora: Halcom dd
Dunajska cesta 123
1000 LJUBLJANA
Slovenija

1.5.2 Ovlaštene kontakt osobe

(1) Za pitanja u vezi s ovom politikom, možete se obratiti ovlaštenim osobama pružatelja usluga od povjerenja, koje možete kontaktirati na adresi i brojevima telefona navedenim u nastavku.

(2) Halcom CA Adresa: Halcom CA
Dunajska cesta 123
1000 LJUBLJANA
Slovenija
Telefon: (+386) 01 200 3 4 86
E-pošta: ca@halcom.si
E-mail za opoziv: ca_preklici@halcom.si

1.5.3 Osoba odgovorna za usklađenost pružatelja usluga od povjerenja Halcom CA s politikom

Ovlaštena lica pružatelja usluga od povjerenja odgovorna su za usklađenost poslovanja pružatelja usluga od povjerenja Halcom CA s ovom politikom, u skladu sa svojim odgovornostima.

1.5.4 Postupak za usvajanje nove politike

(1) Svaki novi prijedlog politike podliježe tehnološkoj i pravnoj reviziji prije nego što ga odobri generalni direktor Halcom d.d., s ciljem osiguranja zakonitosti, sigurnosti i kvalitete.

(2) Pružatelj usluga od povjerenja može izdati izmjene pojedinačnih odredbi primjenjive politike, kako je navedeno u tački 9.12.

1.6. Skraćenice i termini

1.6.1 Skraćenice

CA	Pružatelj usluga od povjerenja koji izdaje potvrde (engl.: Certificate Authority ili Certificate Agency).
CPName	Naziv politike pružatelja usluga od povjerenja (engl.: Certification Policy Name), jedinstveno povezan s međunarodnim CPOID brojem politike (engl.: Certification Policy Object Identifier).
CPOID	Međunarodni broj koji jedinstveno identificira politiku rada (engl.: Certification Policy Object IDentifier).
CRL	Certificate Revocation List – lista opozvanih digitalnih potvrda.

DN	Jedinstveno prepoznatljivo ime (uporedi definiciju prepoznatljivog imena) (engl.: Distinguished Name).
CP	Politika pružatelja usluga od povjerenja (engl. Certificate Policy). Politika uređuje svrhu, rad i metodologiju upravljanja uslugom, kao i odgovornosti i sigurnosne zahtjeve koje moraju ispuniti pružatelj usluga od povjerenja, imaoci potvrda (korisnici usluga) i treća lica koje se oslanjaju na ove potvrde/usluge.
CPS	CPS (engl. Certification Practice Statement) predstavlja opšta pravila poslovanja pružatelja usluga od povjerenja.
LDAP	Lightweight Directory Access Protocol je protokol koji definira pristup imeniku i specificiran je prema preporuci IETF-a (Internet Engineering Task Force) IETF RFC 3494:.
S/MIME	Secure Multipurpose Internet Mail Extensions
SSL	Secure Sockets Layer
TLS	Transport Layer Security
PKI	Public Key Infrastructure je infrastruktura javnih ključeva.
EŠEI	Jedinstveni elektronski identifikacijski broj
HSM	Modul hardverske sigurnosti (engl. Hardware Security Module).
G1, G2, G3	Prva, druga ili treća generacija Halcom CA root i podređenih potvrda.
QCert for ESig/ ESeal	Kvalifikovana digitalna potvrda izdana na sigurnom mediju (engl.: QSCD – Qualified signature creation device). Halcom CA može izdati potvrdu na pametnoj kartici, USB pametnom ključu ili u cloudu (HSM). Potvrda je namijenjena za kvalifikovani elektronski potpis/pečat (engl. Qualified electronic signature/seal).
Cert for Esig/ ESeal	Kvalifikovana digitalna potvrda izdana u datoteci, namijenjena za napredni elektronski potpis/pečat (engl. Advanced electronic signature/seal).
QWAC	Kvalificirana digitalna potvrda za web autentifikaciju (engl. Qualified web authentication certificate).
QTimestamp	Kvalificirani vremenski pečat (engl. Qualified Time stamp)
OT potvrda	OT potvrda (eng. One Time Certificate) je potvrda sa kratkom važnošću, namijenjena za jednokratno potpisivanje dokumenta ili grupe dokumenata.

1.6.2 Izrazi

Imenik potvrda	Imenik X.500 potvrda, gdje se pohranjuju potvrde po preporuci X.509 verzije 3 i gdje im se može pristupiti putem LDAP protokola.

Identifikacija	Identifikacija znači proces korištenja identifikacijskih podataka osobe u fizičkom ili elektronskom obliku koji jedinstveno predstavljaju fizičko ili pravno lice ili fizičko lice koje predstavlja pravno lice.
Pružatelj usluga povjerenja	Fizičko ili pravno lice koje izdaje potvrde ili obavlja druge usluge od povjerenja (engl.: Trust Service provider - TSP).
Prijavna služba	Usluga ili osoba koja prihvata zahtjeve za potvrde i vrši identifikaciju i provjeru identiteta potencijalnih imaoca u ime pružatelja usluga od povjerenja (engl.: Registration Authority - RA).
Jedinstveno ime	Jedinstveno ime u potvrdi (usp. DN definicija) koje nedvosmisleno i jedinstveno definira korisnika u strukturi imenika.

2. OBJAVLJIVANJE INFORMACIJA I JAVNI IMENIK POTVRDA

2.1. Zbirka dokumenata

(1) Pružatelj usluga od povjerenja Halcom CA objavljuje sve što se tiče njegovog poslovanja, obavještenja imaocima i trećim licima, te ostale važne dokumente na web stranici Halcom CA na adresi www.halcom.com (saželi bitnih komponenti i na engleskom jeziku).

(2) Dokumenti koji su javno dostupni su:

- cjenovnik,
- Politika korištenja usluga povjerenja (CP),
- Pravila rada pružatelja usluga povjerenja (CPS),
- narudžbenice i drugi ugovori o uslugama pružatelja usluga od povjerenja,
- upute za sigurno korištenje digitalnih potvrda,
- informacije o primjenjivim propisima i standardima koji se odnose na rad pružatelja usluga od povjerenja, i,
- ostale informacije vezane za rad Halcom CA.

(3) Dokumenti koji predstavljaju povjerljivi dio internih pravila pružatelja usluga od povjerenja Halcom CA nisu javno dostupni.

2.2. Imenik potvrda

(1) Nove politike se objavljuju kako je naznačeno u tački 9.10.

(2) Sve potvrde pružatelja usluga od povjerenja temelje se na standardu X.509 i objavljene su u centralnom imeniku na serveru ldap.halcom.si, koji je pod nadzorom HALCOM CA. Iz razloga zaštite podataka, javno je dostupan samo registar opozvanih potvrda, koji je dio imenika.

(3) Opozvane potvrde se odmah objavljuju u registru opozvanih potvrda (za detalje pogledajte tačku 4.9.8.), a po potrebi se objavljuju i druge javno dostupne informacije ili dokumenti.

(4) Pristup imeniku izdatih potvrda dozvoljen je samo ovlaštenim korisnicima koji provjeravaju veliki broj izdatih potvrda.

2.3. Učestalost objavljivanja

(1) Nova politika mora biti objavljena najkasnije sljedećeg radnog dana nakon njenog usvajanja.

(2) Halcom CA osigurava da se potvrde objavljuju u centralnom imeniku odmah (maksimalno pet (5) sekundi) nakon njihovog izdavanja.

(3) Lista opozvanih potvrda se osvježava odmah (maksimalno pet (5) sekundi) nakon što je potvrda opozvana u javnom imeniku opozvanih potvrda Halcom CA. Ovo osvježavanje se također prenosi na web stranice nakon nekoliko minuta kašnjenja.

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

2.4. Upravljanje pristupom do zbirke dokumenata

(1) Centralni imenik je dostupan na serveru ldap.halcom.si, TCP port 389 putem LDAP protokola. Javno je dostupan samo registar opozvanih potvrda, koji je dio imenika.

(2) Uz odgovarajuće mjere tehničke sigurnosti informacija, Halcom CA obezbjeđuje kontrole koje sprječavaju neovlašteno dodavanje, izmjenu ili brisanje podataka u javnom imeniku potvrda.

3. IDENTITET IMAOCA POTVRDE

3.1. Imenovanje

Različita imena sadržana u potvrdi nedvosmisleno i jedinstveno definiraju imaoca potvrde, osim ako nije drugačije propisano ovom politikom ili sadržajem kvalifikovane digitalne potvrde.

3.1.1 Prepoznatljivo ime

(1) U skladu sa IETF RFC 5280, svaka potvrda sadrži informacije o imaocu potvrde i pružatelju usluga od povjerenja u obliku prepoznatljivog imena. Prepoznatljivo ime je oblikovano u skladu sa IETF RFC 5280 i standardom X501.

(2) Pružatelj usluga od povjerenja potvrda naveden je u polju Izdavatelj engl. Issuer . Osnovne informacije o vlasniku, sadržane u prepoznatljivom imenu potvrde za fizička lica, navedene su u polju Imaoc engl. Subject.

(3) Serijski broj, koji je također sadržan u prepoznatljivom imenu, određuje pružatelj usluga od povjerenja Halcom CA (više o tome u članu 3.1.5).

(4) U skladu sa eIDAS uredbom, eIDAS uredbom 2.0 i ETSI standardima, Halcom CA može koristiti i druge semantičke identifikatore fizičkih lica i poslovnih subjekata prilikom kreiranja prepoznatljivog imena stranih fizičkih lica i/ili stranih poslovnih subjekata, kao što su "PNO", "IDC" ili "PAS" i ISO 3161-1 kod države za identifikaciju na osnovu nacionalnog registracijskog broja ili broja pasoša ili lične

karte za fizička lica, a za poslovne subjekte "NTR" i ISO 3161-1 kod države za identifikaciju na osnovu identifikatora iz nacionalnog registra poslovnih subjekata ili lokalnog koda (dva znaka u skladu sa lokalnom definicijom u određenoj zemlji, koji se smatra prikladnim za nacionalni i evropski nivo).

(5) Halcom CA može pri formiranju prepoznatljivog imena stranih fizičkih osoba i/ili stranih poslovnih subjekata koristiti i druge semantičke identifikatore fizičkih osoba i poslovnih subjekata, kao što su 'PNO', 'IDC', 'PAS' ili 'EID', te ISO 3166-1 oznaku države za identifikaciju na osnovu nacionalnog matičnog broja ili broja pasoša, lične karte ili sredstva za elektronsku identifikaciju za fizičke osobe, a za poslovne subjekte 'NTR' i ISO 3166-1 oznaku države za identifikaciju na osnovu identifikatora iz nacionalnog registra poslovnih subjekata ili lokalnu oznaku (dva znaka u skladu s lokalnom definicijom u određenoj državi, koja se smatra prikladnom za nacionalni i evropski nivo).

(6) Za kvalifikovane potvrde za svrhu identifikacije pružatelja platnih usluga, u skladu s prvim stavom člana 34. Delegirane uredbe Komisije (EU) 2018/389 od 27. novembra 2017. o dopuni Direktive (EU) 2015/2366 Evropskog parlamenta i Vijeća u vezi s regulatornim tehničkim standardima za snažnu autentikaciju klijenata te zajedničke i sigurne otvorene standarde komunikacije (RTS SCA), koristi se semantički identifikator 'PSD' s ISO 3166-1 oznakom države, ulogom pružatelja platnih usluga, nazivom nadležnog organa (NCA) gdje je pružatelj platnih usluga registriran i registracijskim brojem pružatelja platnih usluga navedenim u službenim evidencijama tog organa.

(7) Pružatelj usluga povjerenja Halcom CA može koristiti i druge semantičke identifikatore fizičkih osoba i poslovnih subjekata u skladu s lokalnom definicijom u određenoj državi članici, ako se to zahtijeva na nacionalnom ili evropskom nivou.

(8) Pružatelj usluga povjerenja Halcom CA može pri izdavanju kvalifikovane digitalne potvrde u polje Imaoc (engl. Subject) dodati i atribut 1.3.6.1.4.1.5939.2.9, koji predstavlja vrstu potvrde (npr. označava da se radi o kvalificiranoj digitalnoj potvrdi u oblaku, na pametnoj kartici ili USB ključu i sl.).

(9) Potvrde pružaoca usluga od povjerenja Halcom CA:

Vrsta potvrde	Naziv polja	Ugledno ime	Generacija
Root potvrda pružatelja usluga povjerenja Halcom CA	Izdavatelj, engl. Issuer i Imaoc, engl. Subject	C= SI O=Halcom d.d. 2.5.4.97 = VATSI-43353126 CN = Halcom Root Certificate Authority	G1
	Izdavatelj, engl. Issuer i Imaoc, engl. Subject	C= SI O=Halcom d.d. 2.5.4.97 = VATSI-43353126 CN = Halcom Root CA G2	G2
	Izdavatelj, engl. Issuer i Imaoc, engl. Subject	C= SI O=Halcom d.d. 2.5.4.97 = VATSI-43353126 CN = Halcom Root CA G3	G3
Podređena (Intermediate) potvrda	Izdavatelj engl. Issuer	C= SI O=Halcom d.d. 2.5.4.97 = VATSI-43353126	G1

pružatelja usluga povjerenja Halcom CA		CN = Halcom Root Certificate Authority	
	Imaoc, engl. Subject	C= SI O=Halcom d.d. 2.5.4.97= VATSI-43353126 CN= <identifikator podređene potvrde>	
Podređena (Intermediate) potvrda pružatelja usluga povjerenja Halcom CA	Izdavatelj engl. Issuer	C= SI O=Halcom d.d. 2.5.4.97 = VATSI-43353126 CN = Halcom Root CA G2	G2
	Imaoc, engl. Subject	C= SI O=Halcom dd 2.5.4.97= VATSI-43353126 CN= < identifikator podređene potvrde>	
Podređena (Intermediate) potvrda pružatelja usluga povjerenja Halcom CA	Izdavatelj engl. Issuer	C= SI O= Halcom d.d. 2.5.4.97 = VATSI-43353126 CN= Halcom Root CA G3	G3
	Imaoc, engl. Subject	C= SI O=Halcom dd 2.5.4.97= VATSI-43353126 CN= < identifikator podređene potvrde>	
Kvalifikovana digitalna potvrda korisnika	Izdavatelj engl. Issuer	C= SI O Halcomu dd 2.5.4.97= VATSI-43353126 CN= < identifikator podređene potvrde>	G1, G2, G3
	Imaoc, engl. Subject	C= <dvoslovni ISO kod države> CN=<ime i prezime> SN= <prezime> G= <ime> SERIALNUMBER = <semantički identifikator imaoca> i/ili 1.3.6.1.4.1.5939.2.2= <poreski broj imaoca> E= <e-pošta>	

Vrsta potvrde	Naziv polja	Ugledno ime	Generacija
Root potvrda pružatelja usluga od povjerenja Halcom CA	Izdavatelj, engl. Issuer i Imaoc, engl. Subject	C= SI O=Halcom d.d. 2.5.4.97 = VATSI-43353126	G1

		CN = Halcom Root Certificate Authority	
	Izdavatelj, engl. Issuer i Imaoc, engl. Subject	C= SI O=Halcom d.d. 2.5.4.97 = VATSI-43353126 CN = Halcom Root CA G2	G2
Podređena (Intermediate) potvrda pružatelja usluga od povjerenja Halcom CA	Izdavatelj engl. Issuer	C= SI O Halcomu dd 2.5.4.97= VATSI-43353126 CN = Halcom Root Certificate Authority	G1
	Imaoc, engl. Subject	C= SI O Halcomu dd 2.5.4.97= PDV<dvocifreni ISO kod države>-<poreski broj pravnog lica> CN= <identifikator podređene potvrde>	
Podređena (Intermediate) potvrda pružatelja usluga od povjerenja Halcom CA	Izdavatelj engl. Issuer	C= SI O= Halcom d.d. 2.5.4.97 = VATSI-43353126 CN= Halcom Root CA G2	G2
	Imaoc, engl. Subject	C= SI O Halcomu dd 2.5.4.97= PDV<dvocifreni ISO kod države>-<poreski broj pravnog lica> CN= <identifikator podređene potvrde>	
Kvalifikovana digitalna potvrda korisnika	Izdajatelj, angl. Issuer	C= SI O= Halcom d.d. 2.5.4.97= VATSI-43353126 CN= <oznaka podrejenega potrdila>	G1 i G2
Potvrda za elektronski potpis	Imetnik, angl. Subject	C= <dvoslovni ISO kod države> O= <naziv pravnog lica> 2.5.4.97= PDV<dvocifreni ISO kod države>-<poreski broj pravnog lica> i/ili 1.3.6.1.4.1.5939.2.3= <poreski broj pravnog lica> CN= <ime i prezime> SN= <prezime> G= <ime> SERIALNUMBER = TIN<dvocifreni ISO kod države>-<poreski broj imaoca> i/ili	G1 i G2

		1.3.6.1.4.1.5939.2.2= < porezni broj imaoca> E= <e-mail>	
Potvrda za elektronski pečat	Imetnik, angl. Subject	C= <dvoslovni ISO kod države> O= <naziv pravnog lica> 2.5.4.97= PDV<dvoslovni ISO kod države>-<poreski broj pravnog lica> i/ili 1.3.6.1.4.1.5939.2.3= <poreski broj pravnog lica> CN= <naziv informacionog sistema ili odjeljenja> E= <e-mail>	G1 i G2
Potvrda za autentifikaciju web stranica	Imetnik, angl. Subject	C= <dvoslovni ISO kod države> O= <naziv pravnog lica> 2.5.4.97= PDV<dvoslovni ISO kod države>-<poreski broj pravnog lica> i/ili 1.3.6.1.4.1.5939.2.3= <poreski broj pravnog lica> OU = web potvrdai CN= <naziv i domena web stranice> SN= <domena> G= <naziv web stranice> E = <e-pošta>	G1 i G2

(10) Pružatelj usluga od povjerenja Halcom CA može po potrebi koristiti dodatna polja za prepoznatljivo ime imaoca potvrde.

3.1.2 Zahtjevi za kreiranje prepoznatljivog imena

(1) Oznaka pravnog lica uključena u prepoznatljiv naziv u skladu s odredbama tačke 3.1.1 mora ispunjavati sljedeće zahtjeve:

- mora biti jedinstvena, registrovana u poslovnom ili drugom službenom registru,
- mora biti semantički povezana s imaocem ili pravnim licem,
- maksimalna dužina može biti četrdeset dva (42) znaka.

(2) Halcom CA zadržava pravo da odbije naziv preduzeća, naziv ili oznaku pravnog lica ako utvrdi:

- da je neprikladno ili uvredljivo,
- da je obmanjujući za treća lica ili već pripada drugom pravnom ili fizičkom licu,
- da je to suprotno važećim propisima.

3.1.3 Korištenje anonimnih imena ili pseudonima

Upotreba anonimnih imena ili pseudonima nije dozvoljena.

3.1.4 Pravila za tumačenje prepoznatljivih imena

(1) Informacije o imaocu potvrde u prepoznatljivom nazivu G1 potvrda sadrže slova engleske abecede, a preostali znakovi se konvertuju prema pravilu u nastavku:

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

(2) Pružatelj usluga od povjerenja dužan je osigurati upotrebu drugih nepredviđenih znakova korištenjem odgovarajuće kombinacije slova.

(3) Informacije o imaocu potvrde u prepoznatljivom nazivu G2 i G3 potvrda sadrže znakove iz UTF-8 kodne tabele.

(4) Halcom CA zadržava pravo izmjene zapisa o prepoznatljivim imenima. Pružatelj usluga od povjerenja Halcom CA dužan je objaviti promjenu na web stranici pružatelja usluga od povjerenja Halcom CA najmanje osam (8) dana prije implementacije.

3.1.5 Jedinstvenost prepoznatljivih imena

Prepoznatljiva imena su jedinstvena za svaku izdatu potvrdu i nedvosmisleno i jedinstveno identificiraju imaoca u strukturi imenika.

3.1.6 Zaštita imena ili robnih marki

(1) Pravna lica ili imaoci ne mogu zahtijevati nazive državnih organa ili organa lokalne zajednice, imena, oznake, žigove ili druge elemente intelektualnog vlasništva koji pripadaju trećim licima s tim bi povrijedili prava intelektualnog vlasništva ili druga prava trećih lica ili odredbe važećih propisa.

(2) Svi sporovi rješavaju se isključivo između pogođene strane i imaoca potvrde.

(3) Odgovornost za korištenje imena ili zaštitnih znakova isključivo je na poslovnom subjektu. Pružatelj usluga od povjerenja Halcom CA nije dužan provjeravati i/ili obavještavati imaoca ili pravno lice o tome.

3.2. Provjera identiteta imaoca prilikom prvog izdavanja potvrde

3.2.1 Metoda za posjedovanje vlasništva nad privatnim ključem

Dokazivanje posjedovanja privatnog ključa koji pripada javnom ključu u potvrdi osigurano je sigurnim procedurama prije i tokom preuzimanja potvrde i standardom PKCS#10.

3.2.2 Provjera identiteta organizacije

(1) Informacije o pravnom licu date su u prepoznatljivom nazivu, pogledajte tačke 3.1.1 i 3.1.2.

(2) Zakonski zastupnik pravnog lica garantuje tačnost podataka potpisivanjem dokumentacije za dobijanje potvrde.

(3) Pružatelj usluga od povjerenja Halcom CA provjerava ispravnost podataka pravnog lica i identitet odgovorne osobe kod relevantnih službi, službenih evidencija ili uz pomoć službeno odobrene dokumentacije.

3.2.3 Provjera identiteta imaoca

(1) Prijavna služba pružatelja usluga od povjerenja Halcom CA će nesporno utvrditi identitet imaoca potvrde u skladu s važećim propisima ili će dostaviti podatke o imaocima iz svojih baza podataka dobivene postupkom koji prijavna služba koristi u druge svrhe i osigurava ekvivalentan nivo pouzdanosti u skladu s važećim propisima.

(2) U slučaju da prijavna služba pružatelja usluga povjerenja Halcom CA djeluje u drugoj državi članici EU, identitet imaoca potvrda (državljana te države) može se provjeriti i u skladu s nacionalnom regulativom u toj državi članici, koja osigurava ekvivalentan nivo pouzdanosti i smatra se prikladnom za nacionalni i evropski nivo.

(3) Identitet imaoca potvrda može se provjeriti na osnovu sredstva visoke razine na ličnoj karti, koja je izdata u obliku digitalne potvrde pohranjene na čipu lične karte.

(4) Poslovni subjekt, kao poslodavac ili nalogodavac imaoca potvrde, obavezuje se da će osigurati da se nalogodavci pridržavaju svih odredbi Politike Halcom CA i važećih propisa .

(5) Pružatelj usluga od povjerenja Halcom CA provjerava lične podatke imaoca u odgovarajućim registrima, osim ako važećim propisima nije drugačije određeno .

3.2.4 Neprovjereni podaci u potvrdaima

Halcom CA ne provjerava ispravnost i funkcionalnost adrese e-pošte imaoca potvrde.

3.2.5 Provjera ovlaštenja zaposlenika za dobijanje potvrdaa

(1) Potpisivanjem dokumentacije za dobijanje potvrde, zakonski zastupnik privrednog subjekta garantuje da želi da dobije odgovarajuću potvrdu za poslovni subjekt i/ili određenu osobu koja je zaposlena ili obavlja poslove za taj poslovni subjekt ili uređaj kojim upravlja poslovni subjekt .

(2) Zakoniti zastupnik poslovnog subjekta može potvrditi narudžbu odgovarajuće potvrde i na drugi način, koji u skladu s nacionalnom regulativom osigurava ekvivalentan nivo pouzdanosti i smatra se prikladnim za nacionalni i evropski nivo

3.2.6 Uzajamno priznavanje

(1) Pružalac usluga od povjerenja Halcom CA nije obavezan ugovorno sarađivati s drugim pružaocima usluga od povjerenja ili garantovati za njih, čak i ako drugi pružalac ima status kvalifikovanog pružaoca usluga od povjerenja.

(2) Pružatelj usluga od povjerenja Halcom CA garantuje da će međusobno priznavanje vršiti isključivo nakon potpisivanja pisanog ugovora s drugim pružateljima usluga od povjerenja, koji moraju ispunjavati nivo sigurnosnih zahtjeva koji je usporediv ili viši od onog koji je propisao pružatelj usluga od povjerenja Halcom CA.

(3) Ako se ne obezbijedi eksterna i nezavisna procjena usklađenosti drugog pružaoca usluga od povjerenja, ovlaštena lica Halcom CA će pregledati interna pravila drugog pružaoca usluga od povjerenja i njegovu usklađenost sa sigurnosnim zahtjevima.

(4) Troškove potrebne infrastrukture koju pružatelj usluga od povjerenja Halcom CA zahtijeva za međusobno priznavanje snosi drugi pružatelj usluga od povjerenja.

3.3. Provjera imaoca za ponovno izdavanje potvrde

3.3.1 Provjera imaoca prilikom obnavljanja potvrde

Identitet imaoca prilikom ponovnog izdavanja potvrde se provjerava:

- u prijavnoj službi pružatelja usluga od povjerenja Halcom CA ili od strane prijavne službe ovlaštenih izvođača
- na osnovu već izdate važeće kvalifikovane digitalne potvrde koju je izdao kvalifikovani pružalac usluga od povjerenja, pri čemu pružalac usluga od povjerenja Halcom CA provjerava podatke pravnog lica i imaoca u odgovarajućim registrima,
- putem evropskog novčanika za digitalni identitet ili na osnovu prijavljenog sredstva elektronske identifikacije koje ispunjava zahtjeve u vezi s visokom razinom pouzdanosti.

3.3.2 Provjera imaoca za ponovnu certifikaciju nakon opoziva

Provjera imaoca se vrši u skladu sa odredbama člana 3.2.3.

3.4. Provjera identiteta prilikom zahtjeva za opoziv

(1) Zahtjev za opoziv potvrde podnosi poslovni subjekt ili imaoc:

- u prijavnoj službi, gdje ovlaštena lica provjeravaju identitet podnosioca zahtjeva,
- elektronski, ali zahtjev mora biti digitalno potpisan kvalificiranom digitalnom potvrdom, čime se ujedno dokazuje i identitet podnosioca zahtjeva,
- Ako imaoc potvrde zatraži opoziv potvrde putem telefona ili e-pošte, pružatelj usluga od povjerenja Halcom CA nalaže suspenziju potvrde. Tek na osnovu pismenog zahtjeva za opoziv potvrde, potvrda se zapravo opoziva.

(2) Detaljan postupak otkazivanja: tačka 4.9.3.

4. UPRAVLJANJE POTVRDAMA

4.1. Dobijanje potvrde

4.1.1 Ko može dobiti potvrdu?

(1) Potencijalni imaoc potvrde izdane u skladu s ovom politikom može biti:

- ovlašteno lice pravnog lica ili
- sam poslovni entitet ili uređaj kojim upravlja.

(2) Potvrda se neće izdati potencijalnom nosiocu ako je pravno lice ili ovlaštena osoba uvrštena na listu osoba protiv kojih su Ujedinjene nacije, Evropska unija, Republika Slovenija, Ujedinjeno Kraljevstvo, Kanada, Australija ili Sjedinjene Američke Države izrekle restriktivne mjere (sankcije).

4.1.2 Postupak za potencijalnog imaoca za dobivanje potvrde i odgovornosti

(1) Potvrda za elektronski potpis izdaje se na osnovu ispravno popunjenog i potpisanog obrasca narudžbenice i zahtjeva za izdavanje potvrde (u daljem tekstu: narudžbenica) od strane zakonskog zastupnika pravnog lica i budućeg imaoca potvrde.

(2) Potvrda za elektronski pečat i autentifikaciju web stranice izdaje se na osnovu propisno popunjenog i potpisanog obrasca narudžbe za izdavanje potvrde (u daljnjem tekstu: narudžbenica) od strane zakonskog zastupnika pravnog lica ili posredovanih podataka iz baza podataka prijavne službe, pribavljeni postupkom koji prijavna služba koristi za druge svrhe i koji, u skladu s važećim propisima, osigurava ekvivalentan nivo pouzdanosti..

(3) Zakonski zastupnik podnosi zahtjev prijavnoj službi Halcom CA i podmiruje finansijske obaveze vezane za izdavanje potvrde. Narudžbenice za izdavanje digitalne potvrde dostupne su u prijavnoj službi Halcom CA i na web stranici Halcom CA. Cjenovnik usluga javno je objavljen na web stranici Halcom CA.

(4) Potpisivanjem narudžbenice, zakonski zastupnik također ovlašćuje ovlašteno lice pravnog lica (imaoca ili administratora digitalne potvrde) da u ime i za račun pravnog lica valjano i sigurno elektronski potpiše zahtjev za obnovu postojeće digitalne potvrde ili izdavanje nove s istim podacima u skladu s tada važećom politikom i cjenovnikom pružatelja usluga od povjerenja Halcom CA, ali samo pod uvjetom da se siguran elektronski potpis ili elektronski pečat mogu provjeriti.

(5) Zakonski zastupnik pravnog lica podnosi zahtjev u pisanoj formi.

(6) Prije izdavanja narudžbenice, Halcom CA će upoznati pravno lice i (u slučaju elektronskog potpisa) budućeg korisnika sa ovom politikom i općim pravilima poslovanja pružatelja usluga od povjerenja Halcom CA.

(7) Halcom CA zadržava pravo da odbije zahtjev za potvrdu bez posebnog pismenog obrazloženja zbog nedovoljnih podataka, dokumentacije ili prekomjernog rizika za sigurnost ili zakonitost poslovanja.

4.2. Postupak po prijemu zahtjeva za dobijanje potvrde

4.2.1 Provjera identiteta budućeg imaoca

(1) Ovlaštena osoba prijavne službe provjerava identitet zakonskog zastupnika i (u slučaju elektronskog potpisa) imaoca na osnovu važećeg ličnog dokumenta sa slikom prilikom posjete prijavnoj službi ili putem kurirske službe ili sigurnog elektronskog portala prilikom dostave pametne kartice, PIN koda, autorizacijskog koda ili narudžbenice za cloud potvrda.

(2) Prijavna služba pružatelja usluga od povjerenja Halcom CA može također posredovati podatke iz svojih baza podataka, dobivenih postupkom koji prijavna služba koristi u druge svrhe i koji, u skladu s važećim propisima, osigurava ekvivalentan nivo pouzdanosti.

(3) U slučaju da prijavna služba pružatelja usluga povjerenja Halcom CA djeluje u drugoj državi članici EU, identitet imaoca potvrda (državljana te države) može se provjeriti i u skladu s nacionalnom regulativom u toj državi članici, koja osigurava ekvivalentan nivo pouzdanosti i smatra se prikladnom za nacionalni i evropski nivo.

(4) Identitet imaoca potvrda može se provjeriti na osnovu sredstva visoke razine na ličnoj karti, koja je izdata u obliku digitalne potvrde pohranjene na čipu lične karte.

(5) Ovlaštene osobe su dužne provjeriti identitet pravnog lica i budućeg imaoca, odnosno sve podatke koji su navedeni u zahtjevu i dostupni su u službenim evidencijama ili drugim službenim važećim dokumentima.

(6) Prijavne službe provjeravaju popunjene prijave i prihvataju originalnu dokumentaciju te je na siguran način prosljeđuju Halcom CA.

4.2.2 Odobrenje/odbijanje zahtjeva

(1) Ovlaštena lica pružatelja usluga od povjerenja Halcom CA odobravaju narudžbenicu za dobijanje potvrde ili, u slučaju netačnih ili nepotpunih podataka ili neispunjavanja obaveza, istu odbijaju, o čemu se poslovni subjekt ili budući imaoc odmah obavještava lično ili putem e-maila.

(2) U slučaju odobrenja, pružatelj usluga od povjerenja Halcom CA će obavijestiti potencijalnog imaoca u skladu s važećim propisima prije izdavanja potvrde.

4.2.3 Vrijeme za izdavanje potvrde

Na osnovu odobrene narudžbenice i izmirenih finansijskih obaveza vezanih za izdavanje potvrde, Halcom CA izdaje potvrdu najkasnije u roku od pet (5) radnih dana od prijema uplate.

4.3. Izdavanje potvrde

4.3.1 Postupak pružatelja usluga povjerenja Halcom CA

(1) Proces proizvodnje zavisi od vrste potvrde.

- Napredna kvalifikovana digitalna potvrda

  Proces proizvodnje potvrde i za par/dva para ključeva sastoji se od jasno odvojenih dijelova (ili funkcija), sa njihovim odgovarajuće odvojenim podsistemima:

  1. prethodna personalizacija sigurnog medija (generiranje ključeva na kartici/USB ključu i lozinke za zaštitu potvrde),
  2. obrada zahtjeva za izdavanje potvrde,
  3. priprema potvrde,
  4. personalizacija sigurnog medija (izdavanje i zapisivanje potvrde, štampanje podataka imaoca),

5. štampa lozinke (PIN koda – samo u slučaju slanja preporučenom poštom),
6. prosljeđivanje potvrde i lične lozinke (PIN koda) i obavještavanje imaoca.

Potvrda na sigurnom mediju i pripadajuća lična lozinka (PIN kod) šalju se imaocu preporučenom poštom, u dvije odvojene pošiljke, u razmaku od jednog radnog dana. Lična lozinka (PIN kod) može se imaocu poslati i putem drugog sigurnog kanala (putem posebne web stranice, gdje se imaoc identifikuje putem posebnog linka primljenog putem e-maila, i drugog podatka poznatog imaocu (npr. broj ličnog dokumenta, poreski broj imaoca, posljednje četiri cifre ili CVV kod platne ili kreditne kartice ili slično)). U izuzetnim slučajevima, pakete imaocu mogu dostaviti i lično ovlaštena lica prijavne službe.

- Kvalifikovana digitalna potvrda u cloudu:

Proces proizvodnje potvrde i para ključeva sastoji se od jasno odvojenih dijelova (ili funkcija), sa njihovim odgovarajuće odvojenim podsistemima:

1. obrada zahtjeva za izdavanje potvrde,
2. priprema potvrde i registracijskih i aktivacijskih kodova,
3. prosljeđivanje registracijskog i aktivacijskog koda i obavještenja imaocu,
4. generiranje ključeva na sigurnom mediju za pohranu u cloudu i izdavanje potvrde.

Registracijski i aktivacijski kodovi šalju se imaocu putem dva odvojena kanala, jednog putem e-maila, a drugog putem drugog sigurnog kanala (siguran web portal dostupan sa kvalifikovanom potvrdom, lična dostava redovnom poštom ili putem posebne web stranice gdje se imaoc identificira putem posebnog linka primljenog putem e-maila i drugog podatka poznatog imaocu (npr. broj ličnog dokumenta, porezni broj imaoca, posljednje četiri cifre ili CVV kod platne ili kreditne kartice ili slično)). Izuzetno, jedan od navedenih kodova imaocu može dostaviti i lično ovlaštena osoba iz prijavne službe Halcom CA.

- Jednokratna kvalifikovana digitalna potvrda u cloudu (engl. One Time, u daljem tekstu OT potvrda):

Proces proizvodnje potvrde i para ključeva sastoji se od jasno odvojenih dijelova (ili funkcija), sa njihovim odgovarajuće odvojenim podsistemima:

1. obrada elektronske prijave za izdavanje OT potvrde,,
2. provjera valjanosti aktivacijskih podataka za izdavanje potvrde,
3. generiranje ključa na sigurnom nosaču u oblaku i izdavanje OT potvrde,
4. potpisivanje dokumenta ili skupa dokumenata.

- Kvalifikovana digitalna potvrda za informacione sisteme i autentifikaciju web stranica

Proces proizvodnje potvrde i para ključeva sastoji se od jasno odvojenih dijelova (ili funkcija), sa njihovim odgovarajuće odvojenim podsistemima:

1. obrada zahtjeva za izdavanje potvrde,
2. dobijanje elektronskog zahtjeva (ang. »certificate request«),
3. personalizacija i izdavanje potvrde,
4. prosljeđivanje potvrde imaocu ili administratoru sistema ili web stranice.

• Kvalificirana digitalna potvrda za elektronski pečat u cloudu:

Proces proizvodnje potvrde i za par/dva para ključeva sastoji se od jasno odvojenih dijelova (ili funkcija), sa njihovim odgovarajuće odvojenim podsistemima:

1. obrada prijave za izdavanje potvrde,
2. pribavljanje elektronskog zahtjeva za pristup potvrdi (engl. »certificate request«),
3. personalizacija, izdavanje i autorizacija potvrde,
4. dostavljanje potvrde imaocu odnosno administratoru sistema,
5. priprema potvrde u oblaku i aktivacija pristupa.

Potvrda za elektronski pečat u cloudu namijenjena je elektronskom pečatanju dokumenata ili skupova dokumenata u različitim aplikacijama na tržištu. Pristup potvrdi u cloudu moguć je samo s kvalifikovanom digitalnom potvrdom za pristup, koju izdaje pružatelj usluga povjerenja Halcom CA, te preko IP adrese koju je ovlastio pružatelj usluga povjerenja.

(2) Imaoc kvalificirane potvrde može za pristup svojoj potvrdi i aktivacijskim podacima koristiti isključivo mobilne ili web aplikacije pružatelja Halcom d.d. ili trećih pružatelja koje je Halcom CA prethodno odobrio. Spisak odobrenih aplikacija objavljen je na web stranici Halcom CA. Korištenje neodobrenih aplikacija nije dozvoljeno i predstavlja kršenje uslova izdavanja potvrde te može dovesti do trenutnog opoziva potvrde. Ako aplikacija ili njena autorizacija za pristup potvrdama u oblaku ne funkcioniše u okviru Halcom d.d., pružatelj usluga povjerenja Halcom CA takvu organizaciju ugovorno obavezuje na ispunjavanje strogih sigurnosnih uslova u skladu s važećim evropskim i bosanskohercegovačkim propisima, standardima, preporukama, politikama i općim pravilima rada Halcom CA. Imaoc potvrde sklapanjem ugovora o izdavanju potvrde izričito dozvoljava tehničke provjere svoje upotrebe aplikacije u obimu potrebnom za osiguravanje usklađenosti s uslovima ove politike i važećim zakonodavstvom.

(3) Naručitelj i imaoc digitalne potvrde, u pravilu, nisu identične osobe kao Halcom CA ili prijavna služba Halcom CA. Ako Halcom CA prijavna služba naruči potvrdu za sebe ili svoje ovlaštene zaposlenike, takvu narudžbu dodatno pažljivo provjerava osoblje Halcom CA.

(4) Ako Halcom CA naruči potvrdu za sebe ili ovlaštena lica, izdavanje svih takvih potvrda dodatno pažljivo provjeravaju Službenik za internu kontrolu i Službenik za usklađenost s propisima.

(5) Svi opisani postupci su osmišljeni tako da ih pojedinac ne može samostalno izvršiti.

(6) Pružatelj usluga od povjerenja Halcom CA može, na osnovu pisanog ugovora, ovlastiti provjerene vanjske izvođače radova za određene zadatke (npr. ispis podataka o imaocu, ispis PIN kodova, dostavu itd.), koje redovno nadzire i za koje je odgovoran kao da sam obavlja zadatke.

4.3.2 Obavještenje imaoca o izdavanju

Pogledajte prethodni tačku.

4.4. Preuzimanje potvrde

4.4.1 Postupak preuzimanja potvrde

(1) Za napredne potvrde, preuzimanje potvrda nije potrebno, jer budući imaoc potvrdu prima na sigurnom mediju i pripadajuću ličnu lozinku (PIN kod) preporučenom poštom, putem drugog sigurnog kanala ili, izuzetno, može mu ga dostaviti ovlaštena osoba Halcom CA, vidjeti tačku 4.3.1.

(2) Za cloud potvrde preuzimanje potvrda nije potrebno, jer ga sigurno pohranjuje Halcom CA, pružatelj usluga od povjerenja, nakon što ga imaoc odobri. Korisniku se dodjeljuju samo pristupni kodovi za sigurni cloud, pogledajte tačku 4.3.1.

(3) Kod OT potvrda preuzimanje potvrde nije potrebno, jer je istu po ovlaštenju imaoca privremeno pohranio pružatelj usluga povjerenja Halcom CA, vidi poglavlje 4.3.1.

(4) U slučaju potvrde za informacione sisteme ili web stranice, poslovni subjekt lokalno inicira generiranje ključeva i određuje lozinku za njihovu zaštitu. Pružatelj usluga od povjerenja Halcom CA, na osnovu primljenog elektronskog zahtjeva (»certificate request«) , generira potvrdu i prosljeđuje je poslovnom subjektu, koji koristi prethodno spomenutu lozinku za kreiranje potvrde s pripadajućim parom ključeva.

(5) Kod potvrda za elektronski pečat u cloudu preuzimanje potvrde nije potrebno, jer je istu po ovlaštenju imaoca sigurno pohranio pružatelj usluga povjerenja Halcom CA. Korisniku se izdaje samo potvrda za pristup te se omogućava ovlašteni pristup sigurnom cloud-u, vidi poglavlje 4.3.1.

(6) Po prijemu potvrde, pravno lice mora odmah provjeriti podatke u potvrdi i odmah obavijestiti pružatelja usluga od povjerenja Halcom CA o eventualnim greškama ili problemima.

4.4.2 Objavljivanje potvrde

Proces je opisan u tački 2.

4.4.3 Obavještenje pružatelja usluga povjerenja o izdavanju potvrde trećim licima

Pružatelj usluga od povjerenja Halcom CA ne obavještava treća lica o izdavanju pojedinačne potvrde imaocima potvrda. Prijavna služba može dobiti informacije o izdavanju potvrda za koje je prihvatio zahtjeve za izdavanje.

4.5. Obaveze i odgovornosti korisnika u vezi s korištenjem potvrda

4.5.1 Obaveze imaoca potvrda

(1) Imaoc ili budući imaoc potvrde dužan je:

- Upoznati se s politikom i da je se pridržava prije izdavanja potvrde,
- postupati u skladu s politikom i drugim važećim propisima,
- nakon prijema ili aktivacije potvrde, provjeriti podatke u potvrdi i odmah obavijestiti Halcom

CA o eventualnim greškama ili problemima ili zatražiti opoziv potvrda,

- pratiti sva obavještenja od Halcom CA i djelovati u skladu s tim,
- u skladu s obavještenjima, na odgovarajući način ažurirati potreban hardver i softver za siguran rad s potvrdama,
- odmah obavijestiti Halcom CA o svim promjenama vezanim za potvrdu,
- zatražiti opoziv potvrde ako je privatni ključ kompromitovan na način koji utiče na pouzdanost korištenja ili ako postoji rizik od zloupotrebe,
- zatražiti opoziv cloud potvrde ako je mobilni telefon izgubljen ili ukraden ili ako postoji rizik od zloupotrebe,
- koristiti potvrdu u svrhu navedenu u potvrdi (vidjeti tačku 7.1.) i na način određen politikom Halcom CA.

(2) Imaoc ili budući imaoc potvrde je također dužan zaštititi privatni ključ:

- Pažljivo zaštititi podatke za primanje ili aktiviranje potvrde od neovlaštenih osoba,
- pohraniti privatni ključ i potvrdu na način i na sredstvima za sigurno pohranjivanje privatnih ključeva u skladu s obavijestima i preporukama Halcom CA,
- zaštititi privatni ključ i sve ostale povjerljive podatke odgovarajućom lozinkom u skladu s preporukama Halcom CA ili na drugi način tako da im pristup ima samo imaoc,
- Pažljivo zaštititi lozinke radi zaštite ili pristupa privatnom ključu,
- nakon isteka ili opoziva potvrde, postupiti u skladu s obavještenjima Halcom CA.

4.5.2 Obaveze trećih lica

(1) Treće lice koja se oslanja na potvrdu mora:

- rukovati i koristiti potvrde u skladu i u svrhu sa politikom i drugim važećim propisima,
- pažljivo razmotriti sve potencijalne rizike i odgovornosti pri korištenju potvrda i uspostaviti politiku o tome kako će se oni koristiti,
- obavijestiti Halcom CA ako se sazna da su privatni ključevi imaoca potvrda na koje se oslanja kompromitovani na način koji utiče na pouzdanost korištenja, ili ako postoji rizik od zloupotrebe, ili ako su se podaci navedeni u potvrdi promijenili,
- oslanjati se na potvrdu samo u svrhu navedenu u potvrdi (vidjeti tačku 6.1.7.) na način određen politikom,
- tokom korištenja potvrde, provjeriti da se potvrda ne nalazi u registru opozvanih potvrda,
- tokom korištenja potvrdaa, provjeriti da li je digitalni potpis kreiran u roku važenja i za odgovarajuću svrhu potvrde,
- tokom korištenja potvrde, provjeriti potpis potvrde pružatelja usluga od povjerenja Halcom CA, koji je objavljen u ovoj politici i na web stranici Halcoma,
- pridržavati se drugih odredbi, ako je zaključen ugovor s pružateljem usluga od povjerenja Halcom CA o korištenju potvrda.

(2) Da bi provjerila valjanost potpisa ili druge kriptografske operacije, treće lice mora koristiti softver

i hardver koji može pouzdano provjeriti sve gore navedene zahtjeve za sigurnu upotrebu potvrde.

4.6. Ponovno izdavanje potvrde

(1) Produženje važenja potvrde moguće je samo na zahtjev imaoca potvrde. Produženje je moguće samo za napredne kvalifikovane digitalne potvrde i kvalifikovane potvrde u cloudu.

(2) Nakon isteka napredne potvrdae, imaoc mora podnijeti zahtjev za novu potvrdu nakon jednokratnog (1x) obnavljanja.

(3) Prije isteka potvrde, imaoc potvrde može elektronskim putem zatražiti izdavanje nove digitalne potvrde, koji će potpisati još uvijek važećom potvrdom.

(4) Produženje OT potvrde nije moguće. OT potvrda se koristi samo za jednokratni potpis, zbog čega se izdavanje nove OT potvrde vrši pri svakom zahtjevu za potpis.

(5) Ponovno izdavanje potvrde za autentikaciju web stranica, informacionih sistema i vremensko žigosanje odvija se na isti način kao i prvo pribavljanje potvrde (vidi poglavlje 4.1.).

4.6.1 Okolnosti koje zahtijevaju ponovno izdavanje potvrde

Imaoci naprednih i cloud potvrda mogu osigurati kontinuitet korištenja svoje digitalne potvrde podnošenjem elektronskog zahtjeva za ponovno izdavanje prije isteka digitalne potvrde. Zahtjev za novo izdavanje može se podnijeti i nakon isteka digitalne potvrde.

4.6.2 Osobe koje mogu zatražiti ponovno izdavanje potvrde

Važenje potvrde može se produžiti samo na zahtjev imaoca napredne kvalifikovane digitalne potvrde i kvalifikovane potvrde u cloudu.

4.6.3 Postupak za obradu zahtjeva za ponovno izdavanje potvrde

Proces osigurava da ovlaštena osoba koja traži ponovno izdavanje potvrde bez promjene javnog ključa zapravo bude imaoc potvrde.

4.6.4 Obavještenje imaoca o novoizdanoj potvrdi

Pogledajte tačku 4.3.1.

4.6.5 Postupak preuzimanja novoizdane potvrde

Pogledajte tačku 4.4.1.

4.6.6 Objavljivanje novoizdane potvrde

Proces je opisan u Tački 2.

4.6.7 Obavještenje pružatelja usluga od povjerenja o izdavanju potvrde trećim licima

Pružatelj usluga od povjerenja Halcom CA ne obavještava treća lica o izdavanju pojedinačnih potvrda imaocima potvrda. Prijavna služba može dobiti informacije o izdavanju potvrda za koje je prihvatila zahtjeve za izdavanje.

4.7. Regeneracija ključa

4.7.1 Razlozi za regeneraciju

Nije podržano.

4.7.2 Kome je potrebna regeneracija?

Nije podržano.

4.7.3 Postupak za izdavanje zahtjeva za regeneraciju

Nije podržano.

4.7.4 Obavještenje imaocu potvrde o novoizdanoj potvrdi

Nije podržano.

4.7.5 Proces preuzimanja

Nije podržano.

4.7.6 Objavljivanje potvrda pružatelja usluga od povjerenja s novim parovima ključeva

Nije podržano.

4.7.7 Obavještenje pružatelja usluga od povjerenja o izdavanju potvrda trećim licima

Nije podržano.

4.8. Promjena potvrde

(1) U slučaju promjene podataka koja utiče na validnost prepoznatljivog imena ili drugih podataka u potvrdi, potvrda se mora opozvati.

(2) Za dobijanje nove potvrde potrebno je ponoviti postupak dobijanja nove potvrde, kako je navedeno u tački 4.1.

4.8.1 Okolnosti za promjenu potvrde

Nije podržano.

4.8.2 Ko traži promjenu

Nije podržano.

4.8.3 Postupak za podnošenje zahtjeva za promjenu

Nije podržano.

4.8.4 Obavještenje o izdavanju nove potvrde

Nije podržano.

4.8.5 Preuzimabnje izmijenjene potvrde

Nije podržano.

4.8.6 Objavljivanje izmijenjene potvrde

Nije podržano.

4.8.7 Obavještenje drugim subjektima o promjenama

Nije podržano.

4.9. Opoziv i suspenzija potvrde

(1) Poslovni subjekt ili imaoc potvrde može u bilo kojem trenutku zatražiti opoziv potvrde, a to mora učiniti u sljedećim slučajevima:

1. Promjene prepoznatljivog imena (DN),
2. kada pravno lice ili imaoc potvrde promijeni ključne informacije vezane za potvrdu (ime ili prezime, naziv firme ili pravnog lica, zaposlenje itd.),
3. kada se utvrdi ili posumnja da je ključ za potpisivanje otkriven ili da je potvrda zloupotrijebljena,
4. zamjena potvrde drugom potvrdom (npr. u slučaju gubitka sigurnog medija, gubitka mobilnog telefona, gubitka lozinki za pristup podacima na kartici itd.).

(2) Halcom CA može opozvati potvrdu i bez zahtjeva imaoca u slučajevima iz prvog stava ili na osnovu zahtjeva nadležnog suda, prekršajnog ili upravnog organa.

(3) Potvrda se može opozvati dvadeset četiri (24) sata dnevno. Detaljna uputstva za opoziv potvrde objavljena su na web stranici Halcom CA.

(4) Halcom CA će opozvati potvrdu na osnovu važećeg zahtjeva za opoziv potvrde najkasnije u roku od četiri (4) sata. U slučaju nepredviđenih okolnosti, Halcom CA će izuzetno opozvati potvrdu najkasnije u roku od osam (8) sati nakon prijema važećeg zahtjeva za opoziv potvrde. Tokom ovog vremena, opozvana potvrda će biti označena kao opozvana u imeniku i dodat u registar opozvanih potvrda. Ako imaoc potvrde Halcom CA podnese nevažeći zahtjev za opoziv potvrde, bit će obaviješten o nevažećem zahtjevu za opoziv i bit će obaviješten o uputama za podnošenje važećeg zahtjeva za opoziv.

4.9.1 Razlozi za opoziv

(1) Pravno lice ili imaoc mora zatražiti opoziv potvrde u sljedećim slučajevima:

- ako je privatni ključ imaoca potvrde kompromitovan na način koji utiče na pouzdanost korištenja,
- ako postoji rizik od zloupotrebe privatnog ključa ili potvrde imaoca,
- ako su se ključni podaci navedeni u potvrdi promijenili ili su netačni.

(2) Pružatelj usluga od povjerenja Halcom CA opoziva potvrdu i bez zahtjeva imaoca čim sazna za:

- da su informacije u potvrdi netačne ili da je potvrda izdata na osnovu netačnih informacija,
- da je došlo do greške prilikom provjere identiteta podataka u prijavnoj službi,
- da su se promijenile druge okolnosti koje utiču na važenje potvrde,

- zbog neispunjavanja obaveza imaoca,
- da svi troškovi upravljanja digitalnom potvrdom nisu podmireni,
- da je infrastruktura pružatelja usluga od povjerenja kompromitovana na način koji utječe na pouzdanost potvrde,
- da je privatni ključ imaoca potvrde kompromitovan na način koji utiče na pouzdanost korištenja,
- da će Halcom CA prestati izdavati potvrde ili da je pružatelju usluga od povjerenja zabranjeno upravljanje potvrdama i da njegove aktivnosti nije preuzeo drugi pružatelj usluga povjerenja,
- da je opoziv naložio nadležni sud, prekršajni ili upravni organ.

(3) Imaoc digitalne potvrde može zahtijevati ponovno generiranje lične lozinke (PIN koda) za napredne potvrde, odnosno registracijskih i aktivacijskih kodova za potvrde u cloud-u u slučaju da je e-pristupne podatke samo zaboravio, te pod civilnom i krivičnom odgovornošću jamči da ne postoji mogućnost da je privatni ključ ugrožen na način koji utiče na pouzdanost upotrebe i da ne postoji opasnost zloupotrebe privatnog ključa ili potvrde imaoca.

4.9.2 Ko traži opoziv?

Opoziv potvrde može zahtijevati:

- ovlašteno lice pružatelja usluga od povjerenja Halcom CA,
- zakonski zastupnik pravnog lica,
- imaoc,
- nadležni sud, prekršajni ili upravni organ.

4.9.3 Procedura za opoziv

(1) Zakonski zastupnik pravnog lica ili imaoc može zatražiti opoziv:

- lično tokom radnog vremena u prijavnoj službi,
- elektronski dvadeset četiri (24) sata dnevno, svakog dana u godini, ako postoji mogućnost zloupotrebe ili nepouzdanosti potvrde, a u suprotnom tokom sati koji se smatraju radnim vremenom državnih organa prema važećem zakonu.

(2) Ako se traži opoziv:

- lično, potrebno je popuniti odgovarajući zahtjev za opoziv potvrde i podnijeti ga prijavnoj službi,
- elektronski, imaoc mora poslati elektronsku poruku Halcom CA sa zahtjevom za opoziv, koji mora biti digitalno potpisan/ovjeren pouzdanom potvrdom radi njegove provjere,
- Ako imaoc potvrde zatraži opoziv potvrde putem telefona ili e-pošte, pružatelj usluga od povjerenja Halcom CA nalaže suspenziju potvrde. Tek na osnovu pismenog zahtjeva za opoziv potvrde, potvrda se zapravo opoziva.

(3) Poslovni subjekt ili imaoc mora uvijek biti obaviješten o datumu i vremenu opoziva. Pružalac usluga od povjerenja, na pisani zahtjev pravnog lica ili imaoca, dužan je dostaviti i dodatne

informacije o opozivu (podaci o osobi koja traži opoziv, razlog opoziva itd.).

(4) Sudovi, organi za prekršaje i upravni organi, koji također mogu tražiti opozic, to čine u skladu sa zakonima koji uređuju postupak pred njima (krivični postupak, građanski postupak, opći upravni postupak i drugi).

(5) Odredbe koje se odnose na opoziv se na odgovarajući način primjenjuju i na postupke koji se odnose na ponovno generisanje PIN koda za napredne potvrde, odnosno registracijske i aktivacijske kodove za potvrde u cloudu.

4.9.4 Vrijeme za izdavanje zahtjeva za opoziv

Opoziv se mora odmah zatražiti ako postoji mogućnost zloupotrebe ili nepouzdanosti itd. hitnih slučajeva. U ostalim slučajevima, opoziv se može zatražiti prvog radnog dana tokom radnog vremena koje važi za prijavne službe (pogledajte sljedeći tačku).

4.9.5 Vrijeme od prijema zahtjeva za opoziv do izvršenja opoziva

(1) Po prijemu valjanog zahtjeva za opoziv, pružatelj usluga od povjerenja Halcom CA:

- opozove potvrdu najkasnije u roku od četiri (4) sata, ako je opoziv uzrokovan rizikom od zloupotrebe ili nepouzdanosti itd.,
- u suprotnom, prvog radnog dana nakon prijema zahtjeva za opoziv.

(2) Nakon opoziva, takva potvrda se odmah (maksimalno 5 sekundi) dodaje u registar opozvanih potvrda.

4.9.6 Zahtjevi za provjeru registra opozvanih potvrda za treća lica

(1) Prije korištenja potvrde, treća lica koja se oslanjaju na nju moraju provjeriti najnoviji objavljeni registar opozvanih potvrda. Iz razloga autentičnosti i integriteta, uvijek je potrebno provjeriti autentičnost ovog registra, koji je digitalno potpisao Halcom CA.

(2) Treće lice mora provesti kompletan lanac procesa provjere povjerenja za svaku korištenu digitalnu potvrdu u skladu s evropskim i međunarodnim standardima i preporukama.

4.9.7 Učestalost objavljivanja registra opozvanih potvrda

Registar opozvanih potvrda se osvježava (za pristup registru, pogledajte tačku 7.2.3):

- nakon svakog opoziva potvrde,
- jednom dnevno, ako nema novih unosa ili promjena u registru opozvanih potvrda, otprilike dvadeset četiri (24) sata nakon posljednjeg osvježavanja.

4.9.8 Vrijeme objave registra opozvanih potvrda

(1) Objavljivanje novog registra opozvanih potvrda vrši se:

- u javnom imeniku na serveru ldap://ldap.halcom.si odmah (maksimalno 5 sekundi),
- na web stranici http://domina.halcom.si/crls sa zakašnjenjem od najviše deset (10) minuta.

(2) Pružatelj usluga od povjerenja Halcom CA osigurava najveću moguću dostupnost svojih usluga,

sve dane u godini, ne uzimajući u obzir nepredviđene okolnosti. U slučaju nepredviđenih kvarova i neplaniranih tehničkih ili servisnih intervencija na infrastrukturi, Halcom CA će objaviti registar opozvanih potvrda najkasnije u roku od osam (8) sati. U slučaju nepredviđenih okolnosti nastalih kao posljedica više sile ili vanrednih događaja, Halcom CA će izuzetno objaviti registar opozvanih potvrda najkasnije u roku od dvadeset četiri (24) sata, ali prije isteka posljednjeg važećeg registra opozvanih potvrda.

4.9.9 Provjera statusa potvrda u realnom vremenu

Protokol za online provjeru statusa potvrda (OCSP) podržan je u skladu s evropskim i međunarodnim standardima i preporukama (vidjeti tačku 7.3). Online usluga provjere statusa potvrda (OCSP) može raditi s maksimalnim kašnjenjem od jedne (1) minute od objave novog registra.

4.9.10 Zahtjevi za provjeru statusa potvrda u realnom vremenu

Prilikom korištenja potvrda, treća lica bi uvijek trebale provjeriti da li je potvrda na koji se oslanjaju opozvana.

4.9.11 Drugi načini pristupa statusu potvrda

Nisu podržani.

4.9.12 Posebni zahtjevi pri zloupotrebi privatnog ključa

Nisu specificirani.

4.9.13 Razlozi za suspenziju

(1) Ako imaoc potvrde zatraži opoziv potvrde telefonom ili elektronskim putem, potvrda će biti privremeno suspendovana dok se ne primi originalni pisani zahtjev.

(2) Ako imaoc potvrde, treća lica ili druge osobe, državni ili srodni organi, ili sam pružatelj usluga od povjerenja, izraze sumnju da se s potvrdom postupa kršeći ovu politiku ili važeće propise, potvrda će biti privremeno suspendirana do donošenja konačne odluke.

4.9.14 Ko traži suspenziju?

Pogledajte tačku 4.9.13

4.9.15 Postupak suspenzije

Pogledajte tačku 4.9.13

4.9.16 Vrijeme suspenzije

Pogledajte tačku 4.9.134

4.10. Provjera statusa potvrda

4.10.1 Pristup za verifikaciju

(1) Registar opozvanih potvrda javno je objavljen na serveru ldap://ldap.halcom.si/ korištenjem LDAP protokola i na http://domina.halcom.si/crls korištenjem HTTP protokola.

(2) Provjera statusa potvrda u realnom vremenu dostupna je na http://ocsp.halcom.si .

(3) Detalji o objavljivanju i pristupu nalaze se u tačkama 7.2 i 7.3.

4.10.2 Dostupnost

(1) Provjera statusa potvrda dostupna je dvadeset četiri (24) sata dnevno, svakog dana u godini.

(2) Pružatelj usluga od povjerenja Halcom CA osigurava najveću moguću dostupnost svojih usluga, sve dane u godini, ne uzimajući u obzir nepredviđene okolnosti. U slučaju nepredviđenih kvarova i neplaniranih tehničkih ili servisnih intervencija na infrastrukturi, Halcom CA će ponovo omogućiti status provjere potvrda najkasnije u roku od osam (8) sati. U slučaju nepredviđenih okolnosti nastalih kao posljedica više sile ili vanrednih događaja, Halcom CA će izuzetno omogućiti provjeru statusa potvrda najkasnije u roku od dvadeset četiri (24) sata, ali prije isteka posljednjeg važećeg registra opozvanih potvrda.

4.10.3 Ostale informacije za provjeru statusa

Nisu propisani.

4.11. Prekid odnosa između imaoca i pružatelja usluga od povjerenja

Odnos između imaoca ili pravnog lica i pružatelja usluga od povjerenja Halcom CA prestaje ako:

- potvrda imaoca ističe i nije obnovljena,
- potvrda je opozvana i imaoc ne traži novi.

4.12. Otkrivanje kopije ključeva za dešifriranje

4.12.1 Razlozi za otkrivanje kopije ključeva za dešifriranje

Nije podržano.

4.12.2 Ko traži otkrivanje kopije ključeva za dešifriranje

Nije podržano.

4.12.3 Postupak za podnošenje zahtjeva za otkrivanje kopije ključeva za dešifriranje

Nije podržano.

5. UPRAVLJANJE I SIGURNOSNI NADZOR INFRASTRUKTURE

(1) Halcom CA planira i implementira sve sigurnosne mjere u skladu sa grupom standarda ISO/IEC 27000 i Common Criteria EAL4+, kao i tehničkim zahtjevima ETSI.

(2) Oprema Halcom CA nalazi se u posebnim, odvojenim prostorijama i zaštićena je na više nivoa sistemom fizičkog i protivprovalnog tehničkog obezbjeđenja. Oprema je zaštićena od neovlaštenog pristupa. Također je zaštićena i osigurana sistemom zaštite od požara, sistemom za sprječavanje izlivanja vode, sistemom ventilacije i višeslojnim sistemom neprekidnog napajanja.

(3) Halcom CA pohranjuje sigurnosne kopije i medije za distribuciju na način koji u najvećoj mogućoj mjeri sprječava gubitak, upad ili neovlašteno korištenje ili izmjenu pohranjenih informacija. Kako za obnovu podataka, tako i za arhiviranje važnih informacija, obezbijeđene su rezervne kopije koje se čuvaju na lokaciji različitoj od one na kojoj je smješten softver za upravljanje potvrdama, s ciljem osiguranja ponovne funkcionalnosti u slučajevima kada bi podaci na osnovnoj lokaciji bili uništeni.

(4) Detaljan opis Halcom CA infrastrukture, operativnih operacija, procedura upravljanja infrastrukturom i nadzora nad sigurnosnom politikom njenog rada utvrđen je njenim internim pravilima.

5.1. Fizička sigurnost

(1) Oprema pružatelja usluga od povjerenja zaštićena je višeslojnim sistemom fizičke i elektronske sigurnosti.

(2) Sigurnost infrastrukture pružatelja usluga od povjerenja provodi se u skladu sa stručnim preporukama za najviši nivo sigurnosti.

(3) Potpuni opis infrastrukture pružatelja usluga od povjerenja i procedure za njeno upravljanje i sigurnost određeni su internim pravilima pružatelja usluga od povjerenja.

5.1.1 Lokacija i zgrada pružatelja usluga od povjerenja

(1) Oprema pružatelja usluga od povjerenja u Halcom CA nalazi se u posebnim, osiguranim, odvojenim prostorijama.

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

(3) Detaljne odredbe sadržane su u internim pravilima pružatelja usluga od povjerenja Halcom CA.

5.1.2 Fizički pristup infrastrukturi pružatelja usluga povjerenja

(1) Pristup infrastrukturi pružatelja usluga od povjerenja odobrava se samo ovlaštenim osobama pružatelja usluga od povjerenja u skladu s njihovim zadacima i ovlaštenjima (vidjeti tačku 5.2.1).

(2) Svi pristupi su zaštićeni u skladu sa zakonodavstvom i preporukama.

(3) Detaljne odredbe sadržane su u internim pravilima pružatelja usluga od povjerenja Halcom CA.

5.1.3 Napajanje i ventilacija

(1) Infrastruktura pružatelja usluga od povjerenja ima neprekidno napajanje i odgovarajuće sisteme klimatizacije.

(2) Detalji o ovome su navedeni u internim pravilima pružatelja usluga od povjerenja Halcom CA.

5.1.4 Zaštita od poplava

(1) Infrastruktura pružatelja usluga od povjerenja nije izložena riziku od poplave, osim u slučajevima više sile.

(2) Detalji o ovome su navedeni u internim pravilima pružatelja usluga od povjerenja Halcom CA.

5.1.5 Zaštita od požara

(1) Prostorije pružatelja usluga od povjerenja moraju biti zaštićene od svakog mogućeg izbijanja požara.

(2) Detalji o ovome su navedeni u internim pravilima pružatelja usluga od povjerenja Halcom CA.

5.1.6 Pohranjivanje nosača podataka

(1) Nosioci podataka, bilo u papirnom ili elektronskom obliku, moraju se sigurno čuvati u zaštićenim objektima.

(2) Sigurnosne kopije softvera i šifriranih baza podataka pružatelja usluga od povjerenja Halcom CA redovno se ažuriraju i pohranjuju u dvije odvojene i fizički osigurane prostorije, na različitim lokacijama.

5.1.7 Odlaganje otpada

(1) Halcom CA osigurava sigurno odlaganje i uništavanje dokumenata u fizičkom i elektronskom obliku.

(2) Zbrinjavanje otpada vrši posebna komisija u skladu s internim pravilima pružatelja usluga od povjerenja Halcom CA.

(3) Ovo je detaljno navedeno u Opštim pravilima poslovanja i internim pravilima pružaoca usluga od povjerenja Halcom CA.

5.1.8 Skladištenje na udaljenoj lokaciji

Pogledajte tačku 5.1.6.

5.2. Organizacijska struktura pružatelja usluga od povjerenja

5.2.1 Organizacijske grupe

(1) Operativno, organizacijsko i profesionalno ispravno funkcioniranje pružatelja usluga od povjerenja Halcom CA nadgleda interni kontrolor koji ne obavlja poslove vezane za upravljanje potvrdama.

(2) Ovlaštena lica pružatelja usluga od povjerenja Halcom CA uključuju:

- zaposleni u kompaniji Halcom CA, pružatelju usluga od povjerenja, i
- prijavne službe .

(3) Zaposleni kod pružatelja usluga od povjerenja u Halcom CA podijeljeni su u četiri organizacijske grupe koje pokrivaju sljedeća sadržajna područja:

- upravljanje informacionim sistemom,
- upravljanje potvrdama,
- sigurnost i kontrola,
- regulatorno.

Organizacijska grupa	Uloga	Osnovni zadaci	Broj ljudi
Upravljanje informacionim sistemom	Glavni sistem administrator	• Priprema početne konfiguracije sistema, • početno podešavanje parametara novih podređenih pružatelja usluga povjerenja, • postavljanje početne konfiguracije mreže, • priprema nosača podataka za hitno ponovno pokretanje sistema u slučaju katastrofalnog gubitka sistema, • sigurno skladištenje i distribucija kopija i nadogradnji na zasebnu lokaciju.	2
	Sistem administrator	• Upravljanje postupcima za izdavanje potvrda, • pomoć podređenim pružaocima usluga od povjerenja, • Ovlaštenje podređenih pružatelja usluga od povjerenja, • pristup protokolu za potpisivanje potvrda, • sigurno skladištenje i distribucije kopija i nadogradnji na zasebnu lokaciju.	2
Upravljanje potvrdaima	Sistemski operater 1	• Priprema sistemskih kopija, nadogradnja i vraćanje softvera, sigurno skladištenje i distribucija kopija i nadogradnji, • administrativne funkcije vezane za održavanje, • izvođenje arhiviranja potrebnih sistemskih zapisa, • štampa PIN kodova,	2

		• dnevna provjera sistema.	
	Operater za autorizaciju	• Potvrđivanje izdavanja potvrda i generiranje lozinke.	2
	Operater za potvrde	• Predpersonalizacija sigurnih pametnih kartica, • priprema potvrda (obrada potpisanih zahtjeva za potvrde), • personalizacija (izrada potvrda, snimanje na siguran medij, štampanje podataka imaoca na siguran medij), • distribucija potvrda.	2
	Operater za kodove	• Distribucija PIN kodova.	2
	Službenik za prijavu	• Identifikacija imaoca potvrda.	2
	Službenik za opoziv	• Priprema zahtjeva za opoziv, • opoziv potvrda.	2
Sigurnost i kontrola	Sigurnosni administrator	• Utvrđivanje sigurnosnih pravila i praćenje njihovog poštivanja, • pregled sistemske dokumentacije i kontrolnih zapisa radi nadzora rada, • lična saradnja i pomoć pri godišnjem popisu dokumentacije podređenih pružatelja usluga od povjerenja.	2
	Službenik za internu kontrolu	• Praćenje sigurnosnih pravila i njihovog poštivanja, • kontrola sistemske dokumentacije i kontrolnih dnevnika za kontrolu rada.	2
Regulatorni	Službenik za zaštitu privatnosti i usklađenost s propisima	• Nezavisno i samostalno vođenje, procjena privatnosti i zaštite ličnih podataka, • osiguranje usklađenosti s važećim evropskim i slovenačkim propisima, međunarodnim standardima i preporukama,	1

		• stručna pomoć menadžmentu i zaposlenima u operativnoj implementaciji mjera zaštite privatnosti i osiguravanju usklađenosti s propisima.	

5.2.2 Broj ljudi za pojedinačne zadatke

(1) Operativne radne uloge su osmišljene tako da u najvećoj mogućoj mjeri spriječe mogućnost zloupotrebe i podijeljene su između pojedinačnih organizacijskih grupa:

Organizaciona grupa: Upravljanje informacionim sistemom

Uloga: Glavni sistem administrator

Broj osoba: 2

Zadaci:

1. Priprema početne konfiguracije sistema, uključujući sigurno pokretanje i gašenje sistema.
2. Početno podešavanje parametara novih podređenih pružatelja usluga od povjerenja.
3. Postavljanje početne konfiguracije mreže.
4. Priprema nosača podataka za hitno ponovno pokretanje sistema u slučaju katastrofalnog gubitka sistema.
5. Sigurno pohranjivanje i distribucija kopija i nadogradnje na zasebnu lokaciju.

Organizaciona grupa: Upravljanje informacionim sistemom

Uloga: Administrator sistema

Broj osoba: 2

Zadaci:

1. Upravljanje postupcima za izdavanje potvrda.
2. Pomoć podređenim pružateljima usluga od povjerenja.
3. Ovlašćivanje podređenih pružatelja usluga od povjerenja.
4. Pristup protokolu za potpisivanje potvrda.
5. Sigurno pohranjivanje i distribucija kopija i nadogradnje na zasebnu lokaciju.

Organizacijska grupa: Upravljanje potvrdama

Uloga: Sistemski operater 1

Broj osoba: 2

Zadaci:

1. Priprema kopija sistema, nadogradnja i obnova softvera, sigurno pohranjivanje i distribucija kopija i nadogradnji na zasebnu lokaciju.

2. Administrativne funkcije vezane za održavanje baze podataka pružatelja usluga od povjerenja i pomoć u istrazi odstupanja od pravila.

3. Promjene naziva servera i/ili mrežne adrese.

4. Vršenje arhiviranja potrebnih sistemskih zapisa.

5. Štampa PIN kodova.

6. Dnevna provjera sistema.

Organizacijska grupa: Upravljanje potvrdama

Uloga: Operater autorizacije

Broj osoba: 2

Zadaci:

1. Potvrda izdavanja potvrda i generiranja lozinke.

Organizacijska grupa: Upravljanje potvrdama

Uloga: Operater potvrda

Broj osoba: 2

Zadaci:

1. Predpersonalizacija sigurnih nosioca.

2. Priprema potvrda (obrada potpisanih zahtjeva za potvrde).

3. Personalizacija (izrada potvrda, snimanje na siguran medij, štampanje podataka imaoca na siguran medij).

4. Distribucija potvrda .

Organizacijska grupa: Upravljanje potvrdama

Uloga: Operater za kodove

Broj osoba: 2

Zadaci:

1. Distribucija PIN kodova.

Organizacijska grupa: Upravljanje potvrdama

Uloga: Službenik za prijavu

Broj osoba: 2

Zadaci:

1. Identifikacija imaoca potvrda.

Organizacijska grupa: Upravljanje potvrdama

Uloga: Službenik za opoziv

Broj osoba: 2

Zadaci:

1. Priprema zahtjeva za opoziv.
2. Opoziv potvrda.

Organizacijska grupa: Sigurnost i kontrola

Uloga: Sigurnosni administrator

Broj osoba: 2

Zadaci:

1. Postavljanje sigurnosnih pravila i praćenje njihovog poštivanja.
2. Pregled sistemske dokumentacije i kontrolnih zapisa radi kontrole rada.
3. Lična saradnja i pomoć pri godišnjem popisu dokumentacije podređenih pružatelja usluga od povjerenja.

Organizacijska grupa: Sigurnost i kontrola

Uloga: Službenik za internu kontrolu

Broj osoba: 2

Zadaci:

1. Praćenje sigurnosnih pravila i njihovog poštivanja.
2. Nadzor sistemske dokumentacije i kontrolnih zapisa za kontrolu rada.

Organizacijska grupa: Regulatorna

Uloga: Službenik za zaštitu privatnosti i usklađenost s propisima

Broj osoba: 1

Zadaci:

1. Nezavisno i autonomno vođenje, procjena privatnosti i zaštite ličnih podataka.
2. Osiguranje usklađenosti s važećim evropskim i slovenačkim propisima, međunarodnim standardima i preporukama.

3. Stručna pomoć menadžmentu i zaposlenima u operativnoj implementaciji mjera zaštite privatnosti i osiguravanju usklađenosti s propisima.

(2) Naveden je minimalni broj zaposlenih za svaku poziciju.

5.2.3 Identifikacija za obavljanje pojedinačnih zadataka

Verifikacija identiteta i prava pristupa za obavljanje pojedinačnih zadataka u skladu s ulogom pojedine organizacijske grupe, kao i za obavljanje zadataka aplikativne usluge, osigurani su sigurnosnim mehanizmima i kontrolnim procedurama u skladu s internim pravilima pružatelja usluga od povjerenja Halcom CA.

5.2.4 Nekompatibilnost zadataka

Za svaku ulogu, interna pravila Halcom CA precizno određuju s kojim ulogama ona može, a s kojim ne može biti kompatibilna. Neke zahtijevaju prisustvo najmanje dvije ovlaštene osobe. U slučaju nepredviđenog odsustva određenih zaposlenika, njihove uloge preuzimaju drugi zaposlenici, osim ako to nije nekompatibilno prema internim pravilima.

5.3. Nadzor nad osobljem

(1) Operativno, organizacijsko i profesionalno ispravno funkcioniranje pružatelja usluga od povjerenja Halcom CA nadgleda interni kontrolor koji ne obavlja poslove vezane za upravljanje potvrdama.

(2) Službenik za unutrašnju kontrolu nadzire rad Halcom CA. U slučaju uočenih nedostataka, službenik za unutrašnju kontrolu nalaže odgovarajuće mjere za otklanjanje tih nedostataka, koje je Halcom CA dužan provesti, te nadzire provođenje naloženih mjera.

5.3.1 Potrebne kvalifikacije i iskustvo osoblja

Halcom CA zapošljava pouzdano i profesionalno kvalifikovano osoblje koje nije osuđivano ni za jedno krivično djelo. Svi zaposleni redovno prolaze obuku i stiču dodatna znanja iz svoje oblasti stručnosti.

5.3.2 Kvalifikovanost osoblja

Osoblje pružatelja usluga od povjerenja ima odgovarajuće kvalifikacije i iskustvo u skladu sa zahtjevima važećih propisa i tehničkih standarda i preporuka.

5.3.3 Dodatno obučavanje osoblja

Sve potrebne obuke obezbjeđuju se osobama koje obavljaju zadatke gore navedenih organizacijskih grupa i zadatke prijavne službe.

5.3.4 Zahtjevi za redovnu obuku

Osoblje se obučava prema potrebama ili inovacijama vezanim za rad infrastrukture pružatelja usluga od povjerenja Halcom CA.

5.3.5 Promjena zadataka

Nije propisano.

5.3.6 Sankcije

Sankcije u slučaju neovlaštenog ili nemarnog obavljanja poslova provode se za ovlaštena lica pružatelja usluga povjerenja u skladu s važećim propisima i internim pravilima pružatelja usluga od povjerenja Halcom CA.

5.3.7 Zahtjevi za vanjske izvođače

Isti zahtjevi primjenjuju se na sve vanjske izvođače kao i na ovlaštena lica pružatelja usluga od povjerenja Halcom CA.

5.3.8 Pristup osoblja dokumentaciji

Ovlaštenim osobama pružatelja usluga povjerenja dostavlja se sva potrebna dokumentacija u skladu s njihovim dužnostima i zadacima.

5.4. Sigurnosne provjere sistema

5.4.1 Vrste logova

(1) Pružatelj usluga od povjerenja Halcom CA redovno provjerava i evidentira sve što ima značajan utjecaj na:

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

(2) Detaljne informacije o ovome utvrđene su u internim pravilima pružatelja usluga od povjerenja Halcom CA, u skladu s Uredbom.

5.4.2 Učestalost pregleda logova

Pružatelj usluga od povjerenja Halcom CA svakodnevno provodi sigurnosne provjere svoje infrastrukture i evidentira probleme.

5.4.3 Period čuvanja logova

Logovi se čuvaju najmanje deset (10) godina od njihovog nastanka, osim ako posebnim zakonom nije predviđen duži period.

5.4.4 Zaštita logova

Logovi su zaštićeni u skladu sa sigurnosnim mehanizmima koji osiguravaju najviši nivo sigurnosti.

5.4.5 Sigurnosne kopije logova

Sigurnosne kopije logova se vrše svakodnevno.

5.4.6 Prikupljanje podataka za logove

Podaci se prikupljaju automatski ili ručno, ovisno o vrsti podataka.

5.4.7 Obavještavanje osobe koja je izazvala incident

Nije potrebno obavijestiti osobu koja je uzrokovala događaje.

5.4.8 Procjena ranjivosti sistema

(1) Analizu logova i nadzor nad provođenjem svih procedura redovno vrše ovlaštena lica pružatelja usluga od povjerenja ili automatski korištenjem drugih sigurnosnih mehanizama na svim informacijsko-komunikacijskim uređajima pružatelja usluga od povjerenja.

(2) Procjena ranjivosti se vrši na osnovu analize logova, sigurnosnih događaja i drugih relevantnih podataka.

5.5. Dugoročno čuvanje podataka

5.5.1 Vrste dugoročno zadržanih podataka

Pružatelj usluga od povjerenja Halcom CA pohranjuje sljedeće materijale u skladu s odredbama važećih propisa:

- logovi,
- zapisnici,
- sve dokaze o provjeri identiteta imaoca ili pravnih lica,
- sve zahtjeve,
- potvrde i registar opozvanih potvrda,
- operativne politike,
- objave i obavještenja pružatelja usluga od povjerenja Halcom CA i
- ostale dokumente u skladu sa važećim propisima.

5.5.2 Period čuvanja

(1) Dugoročno pohranjeni podaci koji se odnose na ključeve i digitalne potvrde čuvaju se najmanje deset (10) godina nakon isteka potvrda na koji se podaci odnose, osim ako posebnim zakonom nije predviđen duži period.

(2) Ostali dugoročno pohranjeni podaci čuvaju se najmanje deset (10) godina od njihovog nastanka, osim ako posebnim zakonom nije predviđen duži period.

5.5.3 Zaštita dugoročno pohranjenih podataka

(1) Dugoročno čuvani podaci se pohranjuju na siguran način.

(2) Detaljnija pravila utvrđena su Općim pravilima poslovanja i internim pravilima pružatelja usluga od povjerenja Halcom CA, u skladu s važećim propisima, standardima i preporukama.

5.5.4 Sigurnosna kopija dugoročno pohranjenih podataka

(1) Kopija dugoročno čuvanih podataka pohranjuje se na sigurnom mjestu.

(2) Detaljnija pravila utvrđena su Općim pravilima poslovanja i internim pravilima pružatelja usluga od povjerenja Halcom CA, u skladu s važećim propisima, standardima i preporukama.

5.5.5 Zahtjev za vremenskim žigom

Nije propisano.

5.5.6 Metoda prikupljanja podataka

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

(2) Detaljnija pravila utvrđena su Općim pravilima poslovanja i internim pravilima pružatelja usluga od povjerenja Halcom CA, u skladu s važećim propisima, standardima i preporukama.

5.5.7 Postupak za pristup i provjeru dugoročno pohranjenih podataka

(1) Pristup dugoročno pohranjenim podacima moguć je samo ovlaštenim osobama.

(2) Detaljnija pravila utvrđena su Općim pravilima poslovanja i internim pravilima pružatelja usluga od povjerenja Halcom CA, u skladu s važećim propisima, standardima i preporukama.

5.6. Promjena javnog ključa pružatelja usluga od povjerenja Halcom CA

U slučaju novoizdane vlastite potvrde pružatelja usluga od povjerenja Halcom CA, postupak se objavljuje na web stranici pružatelja usluga od povjerenja Halcom CA.

5.7. Plan oporavka

5.7.1 Postupak u slučaju upada i zloupotrebe

Detaljnija pravila su navedena u Opštim pravilima poslovanja i internim pravilima pružaoca usluga od povjerenja Halcom CA, u skladu sa važećim propisima, standardima i preporukama.

5.7.2 Postupak u slučaju kvara softvera ili podataka

Detaljnija pravila su navedena u Opštim pravilima poslovanja i internim pravilima pružaoca usluga od povjerenja Halcom CA, u skladu sa važećim propisima, standardima i preporukama.

5.7.3 Postupak u slučaju kompromitovanja privatnog ključa pružatelja usluga od povjerenja Halcom CA

Detaljnija pravila su navedena u Opštim pravilima poslovanja i internim pravilima pružaoca usluga od povjerenja Halcom CA, u skladu sa važećim propisima, standardima i preporukama.

5.7.4 Plan oporavka

Osigurano je dupliciranje kritičnih sistema i pohranjivanje podataka na geografski udaljenim lokacijama. Detaljniji aranžmani navedeni su u Općim operativnim pravilima i internim pravilima pružatelja usluga od povjerenja Halcom CA, u skladu s važećim propisima, standardima i preporukama.

5.8. Prekid rada Halcom CA

Detaljnija pravila su navedena u Opštim pravilima poslovanja i internim pravilima pružaoca usluga od povjerenja Halcom CA, u skladu sa važećim propisima, standardima i preporukama.

6. ZAHTJEVI TEHNIČKE SIGURNOSTI

6.1. Generisanje i instaliranje ključeva

6.1.1 Generisanje ključeva

(1) Parovi ključeva pružatelja usluga povjerenja Halcom CA za potpisivanje i provjeru validnosti potpisa kreirani su u skladu s najvišim sigurnosnim standardima u hardverskom sigurnosnom modulu, u sigurnom okruženju provajdera usluga od povjerenja Halcom CA.

(2) Par ključeva imaoca naprednih kvalificiranih potvrda generiraju se na sigurnom mediju, u sigurnom okruženju pružatelja usluga od povjerenja Halcom CA.

(3) Par ključeva imaoca kvalificiranih potvrda u cloudu i OT potvrda generira se u hardverskom sigurnosnom modulu, u sigurnom okruženju pružatelja usluga od povjerenja Halcom CA.

(4) Par ključeva kvalifikovanih potvrda za autentifikaciju informacionih sistema i web stranica generiše se na serveru imaoca.

6.1.2 Dostava privatnog ključa imaocima

(1) Privatni ključevi naprednih potvrda dostavljaju se imaocu na sigurnom mediju preporučenom poštom. U izuzetnim slučajevima, pošiljku imaocu može dostaviti i lično ovlaštena osoba iz Halcom CA.

(2) Privatni ključ potvrde u cloudu se ne dostavlja imaocu, jer ga sigurno čuva pružatelj usluga od povjerenja Halcom CA, nakon odobrenja imaoca. Privatni ključ OT potvrde briše se iz hardverskog sigurnosnog modula nakon jednokratne upotrebe.

(3) Privatni ključevi potvrda za informacione sisteme i autentifikaciju web stranica se ne prenose kod imaoca, jer se generišu na serveru.

6.1.3 Dostava javnog ključa pružatelju usluga od povjerenja

(1) Za napredne potvrde, ključevi se generiraju na sigurnom mediju, u sigurnom okruženju pružatelja usluga povjerenja Halcom CA.

(2) Za potvrde u cloudu i OT potvrde, ključevi se generiraju u hardverskom sigurnosnom modulu, u sigurnom okruženju pružatelja usluga od povjerenja Halcom CA.

(3) Za potvrde za informacione sisteme i autentifikaciju web stranica, ključeve generira imaoc, na računaru ili serveru. PKCS#10 zahtjev za izdavanje potvrda (engl. »certificate request«) se prenosi s računara korisnika na pružatelja usluga od povjerenja putem sigurne mrežne veze .

6.1.4 Dostava javnog ključa pružatelja usluga od povjerenja

Potvrda s javnim ključem pružatelja usluga od povjerenja Halcom CA dostavlja se imaocu ili je dostupan trećim licima:

- u javnom imeniku ldap://ldap.halcom.si koristeći LDAP protokol (vidi tačku 2.3),
- u PEM formatu na https://www.halcom.com/si/halcom-ca/politike-in-dokumenti/ , gdje se autentičnost potvrde mora dodatno provjeriti.

6.1.5 Dužina ključa

Potvrda	Dužina RSA ključa [bit]
Korjenska (Root) potvrda pružatelja usluga od povjerenja Halcom CA	G1 - Najmanje 2048 G2 - Najmanje 4096 G3 - Najmanje 4096
Srednja/Podređena (Intermediate) potvrda pružatelja usluga od povjerenja Halcom CA	G1 - Najmanje 2048 G2 - Najmanje 4096 G3 - Najmanje 4096
Kvalifikovana digitalna potvrda korisnika	G1 - Najmanje 2048 G2 - Najmanje 3072 G3 - Najmanje 3072

6.1.6 Generisanje i kvalitet parametara javnog ključa

Kvalitet ključnih parametara provajdera usluga od povjerenja Halcom CA osigurava proizvođač softvera korištenjem visokokvalitetnih generatora slučajnih brojeva.

6.1.7 Svrha ključeva i potvrda

(1) Svrha korištenja ključeva ili potvrdaan avedena je u potvrdi u polju upotreba ključa (engl.keyUsage) i proširena upotreba ključa (engl.extended keyUsage) u skladu sa X.509 v.3 .

(2) Privatni ključ pružatelja usluga od povjerenja Halcom CA koristi se za potpisivanje potvrda i registra opozvanih potvrda, a javni ključ u potvrdi pružatelja usluga od povjerenja koristi se za provjeru valjanosti potpisa.

(3) Profil potvrda dat je u tački 7.1.

6.2. Zaštita privatnog ključa

6.2.1 Standardi kriptografskih modula

Privatni ključ pružatelja usluga od povjerenja HALCOM CA zaštićen je u kriptografskom modulu certificiranom prema FIPS 140-2 Level 3 i/ili Common Criteria EAL4+ .

6.2.2 Kontrola privatnog ključa od strane ovlaštenih osoba

Odredbe u vezi s pristupom privatnom ključu pružatelja usluga od povjerenja Halcom CA utvrđene su u internim pravilima pružatelja usluga od povjerenja Halcom CA, u skladu s važećim propisima i Općim pravilima poslovanja.

6.2.3 Otkrivanje kopije privatnog ključa

Odredbe u vezi s otkrivanjem privatnog ključa pružatelja usluga od povjerenja Halcom CA utvrđene su internim pravilima pružatelja usluga od povjerenja Halcom CA, u skladu s važećim propisima i Općim pravilima poslovanja.

6.2.4 Sigurnosna kopija privatnog ključa

Odredbe u vezi sa sigurnosnom kopijom privatnog ključa pružaoca usluga od povjerenja Halcom CA utvrđene su u internim pravilima pružaoca usluga od povjerenja Halcom CA, u skladu sa važećim propisima i Opštim pravilima poslovanja.

6.2.5 Arhiviranje privatnog ključa

(1) Privatne ključeve Halcom CA mogu kopirati i pohranjivati samo ovlaštene osobe pružatelja usluga od povjerenja Halcom CA. Sigurnosne kopije ključeva moraju se pohranjivati s istim nivoom zaštite kao i ključevi koji se koriste.

(2) Detaljnije odredbe za kopiranje privatnog ključa pružatelja usluga od povjerenja Halcom CA utvrđene su u internim pravilima pružatelja usluga od povjerenja Halcom CA, u skladu s važećim propisima i Općim pravilima poslovanja.

6.2.6 Prijenos privatnog ključa iz/u kriptografski modul

(1) Privatni ključevi za napredne potvrde kreiraju se na sigurnom mediju kojim se potom prenose imaocu potvrde.

(2) Privatni ključevi za potvrde u cloudu i OT potvrde generiraju se i pohranjuju u kriptografskom modulu koji je certificiran prema FIPS 140-2 Level 3 i/ili Common Criteria EAL4+.

(3) Privatne ključeve korisnika potvrda za autentifikaciju informacionih sistema i web stranica kreira i pohranjuje imaoc.

6.2.7 Pohranjivanje privatnog ključa u kriptografskom modulu

(1) Privatni ključ pohranjuje HALCOM CA pružatelj usluga od povjerenja u kriptografskom modulu certificiranom u skladu s FIPS 140-2 Level 3 i/ili Common Criteria EAL4+.

(2) Privatni ključevi korisnika:

- napredne potvrde se kreiraju i pohranjuju na sigurnom mediju,
- Potvrde u cloudu i OT potvrde se kreiraju i pohranjuju u kriptografskom modulu
- Potvrde za informacione sisteme i autentifikaciju web stranica kreira i pohranjuje imaoc.

6.2.8 Postupak za aktiviranje privatnog ključa

(1) Postupak aktiviranja privatnog ključa pružatelja usluga od povjerenja Halcom CA provodi se na siguran način u skladu s odredbama internih pravila pružatelja usluga od povjerenja Halcom CA.

(2) Halcom CA preporučuje da imaoci koriste softversko okruženje koje onemogućava pristup njihovom privatnom ključu bez unosa odgovarajuće lozinke prilikom odjave ili nakon isteka određenog vremenskog perioda.

(3) Imaoc potvrde za potpisivanje u cloudu može koristiti uslugu kvalifikovanog elektronskog potpisa

u cloudu. U takvom slučaju, imaoc ili drugi pošiljatelj u njegovo ime dužan je sigurno prenijeti pružatelju usluga od povjerenja Halcom CA elektronički dokument koji će biti kvalificirano elektronički potpisan. Imaoc zatim na siguran način putem mobilnog uređaja i korištenjem sigurnosne procedure koju je propisao pružatelj usluga od povjerenja Halcom CA (upotreba PIN-a i mobilnih sigurnosnih postupaka) odobrava kvalifikovani elektronski potpis u cloudu. Na osnovu odobrenja imaoca, pružatelj usluga od povjerenja Halcom CA koristi privatni ključ imaoca u cloudu i kvalifikovano elektronski potpisuje dokument, te potpisani dokument dostavlja imaocu ili drugom pošiljaocu dokumenta.

(4) Imaoc OT potvrde odobrava kvalifikovani elektronski potpis u cloud-u putem mobilne ili web aplikacije, koju potpisnik sa visokim nivoom povjerenja može koristiti isključivo pod vlastitom kontrolom. Na osnovu odobrenja imaoca, pružalac usluga povjerenja Halcom CA generiše i koristi privatni ključ imaoca u cloud-u te kvalifikovano elektronski potpisuje dokument, a potpisani dokument dostavlja imaocu ili drugom pošiljaocu dokumenta.

(5) Pristup usluzi kvalifikovanog elektronskog pečata moguć je samo uz kvalifikovanu digitalnu potvrdu, koju izdaje pružalac usluga povjerenja Halcom CA, te preko IP adrese koju je ovlastio pružalac usluga povjerenja. Imaoc potvrde može odobriti kvalifikovani elektronski pečat u cloudu i putem mobilne ili web aplikacije, koju potpisnik sa visokim nivoom povjerenja može koristiti isključivo pod vlastitom kontrolom.

(6) Ako aplikacija ili njena autorizacija za pristup potvrdama u cloud-u ne funkcioniše u okviru Halcom d.d., pružalac usluga povjerenja Halcom CA takvu organizaciju ugovorno obavezuje na ispunjavanje strogih sigurnosnih uslova u skladu sa važećim evropskim, slovenačkim i bosanskim propisima, standardima, preporukama, kao i politikama i općim pravilima rada Halcom CA.

(7) Radi zaštite povjerljivosti elektronskih dokumenata imaoca, imaoc ili drugi pošiljalac u njegovo ime može zahtijevati da pružalac usluga od povjerenja Halcom CA, prilikom potpisivanja u cloudu, kako je opisano u prethodnom stavu, ne traži prijem cijelog dokumenta za kvalifikovani elektronski potpis u cloudu, već samo hash vrijednost takvog dokumenta. U takvom slučaju, korisnik je obaviješten prije potpisivanja. Potvrđivanjem potpisa, imaoc prihvata da Halcom CA ne pruža nikakvu provjeru izračuna hash vrijednosti ili drugih sigurnosnih mehanizama u vezi sa elektronskim dokumentom i da je za to u potpunosti odgovoran.

6.2.9 Postupak za deaktivaciju privatnog ključa

Proces deaktivacije privatnog ključa pružatelja usluga od povjerenja Halcom CA provodi se na siguran način u skladu s odredbama internih pravila pružatelja usluga od povjerenja Halcom CA.

6.2.10 Postupak uništavanja privatnog ključa

(1) Postupak uništavanja privatnog ključa pružatelja usluga od povjerenja Halcom CA provodi se na siguran način u skladu s odredbama internih pravila pružatelja usluga od povjerenja Halcom CA i uputama proizvođača hardverskog sigurnosnog modula. Privatni ključ se uništava na način da se ne može vratiti.

(2) Uništavanje privatnih ključeva na strani imaoca je odgovornost imaoca. Mora koristiti odgovarajuće aplikacije za sigurno brisanje naprednih potvrde.

(3) Privatni ključ potvrde u cloudu i OT potvrde se automatski uništava nakon isteka potvrde. Halcom

CA može uništiti privatni ključ cloud potvrde prije zahtjeva imaoca potvrde. Privatni ključ se uništava na način koji ga čini nemogućim za vraćanje.

6.2.11 Svojstva kriptografskog modula

Sigurnosni moduli hardvera u skladu su sa standardima navedenim u tački 6.2.1 .

6.3. Ostali aspekti upravljanja ključevima

6.3.1 Arhiviranje javnog ključa

Pružatelj usluga od povjerenja Halcom CA arhivira svoj javni ključ i javne ključeve imaoca kako je navedeno u tački 5.5.

6.3.2 Period važenja javnih i privatnih ključeva

(1) Važenje potvrda prikazano je u donjoj tabeli.

Vrsta potvrde	Potvrda	Ključ	Validnost
Napredna potvrda za elektronski potpis	par ključeva za digitalno potpisivanje/provjeru	Privatni ključ za potpisivanje	3 godine
		Javni ključ za provjeru	3 godine
	par ključeva za dešifriranje/šifriranje	Privatni ključ za dešifriranje	3 godine
		Javni ključ za šifriranje	3 godine
Napredna potvrda za elektronski pečat	par ključeva za digitalno žigosanje/provjeru	Privatni ključ za žigosanje	3 godine
		Javni ključ za provjeru	3 godine
	par ključeva za dešifriranje/šifriranje	Privatni ključ za dešifriranje	3 godine
		Javni ključ za šifriranje	3 godine
Potvrda u cloudu	par ključeva za digitalno potpisivanje/provjeru	Privatni ključ za potpisivanje	1 - 3 godine
		Javni ključ za provjeru	1 - 3 godine
Potvrda za informacione sisteme	par ključeva za digitalno žigosanje/provjeru	Privatni ključ za žigosanje	3 godine
		Javni ključ za provjeru	3 godine
Potvrda za autentifikaciju web stranice	par ključeva za autentifikaciju web stranice	Privatni ključ	1 - 3 godine
		Javni ključ	1 - 3 godine
OT potvrda	par ključeva za digitalno potpisivanje/provjeru	Privatni ključ	Do 10 minuta
		Javni ključ	Do 10 minuta

(2) U posebnim slučajevima, Halcom CA može odrediti i drugačiji period važenja potvrda za pojedinačnu potvrdu.

6.4. Lozinke za pristup potvrdama ili ključevima

6.4.1 Generisanje lozinke

(1) Lozinka za korištenje napredne potvrde (PIN kod) i broj za otključavanje sigurnog medija (PUK kod) generiraju se na web stranici Halcom CA. Imaoc mora promijeniti lični broj prije prve upotrebe potvrde.

(2) Registracijski i aktivacijski kod za potvrde u cloud-u kreira se na strani Halcom CA. U procesu aktivacije korisnik postavlja svoju ličnu šifru (PIN kod) za pristup potvrdi u cloudu. Aktivacija potvrde u cloudu može se obaviti i putem različitih mobilnih i web aplikacija, koje potpisnik sa visokim nivoom povjerenja može koristiti isključivo pod vlastitom kontrolom. Imaoc potvrde može za pristup svojoj potvrdi i aktivacijskim podacima koristiti isključivo mobilne ili web aplikacije pružaoca Halcom d.d. ili trećih pružalaca koje je Halcom CA prethodno odobrio. Spisak odobrenih aplikacija objavljen je na web stranici Halcom CA. Korištenje neodobrenih aplikacija nije dozvoljeno i predstavlja kršenje uslova izdavanja potvrde te može dovesti do trenutnog opoziva potvrde. Ako aplikacija ili njena autorizacija za pristup potvrdama u cloudu ne funkcioniše u okviru Halcom d.d., pružalac usluga povjerenja Halcom CA takvu organizaciju ugovorno obavezuje na ispunjavanje strogih sigurnosnih uslova u skladu sa važećim evropskim i slovenačkim propisima, standardima, preporukama, kao i politikama i općim pravilima rada Halcom CA. Imaoc potvrde zaključenjem ugovora o izdavanju potvrde izričito dozvoljava tehničke provjere svoje upotrebe aplikacije u obimu potrebnom za osiguravanje usklađenosti sa uslovima ove politike i važećom legislativom.

(3) Lozinke za generisanje ključa i aktivacija OT potvrde odvijaju se putem različitih mobilnih i web aplikacija, koje potpisnik sa visokim nivoom povjerenja može koristiti isključivo pod vlastitom kontrolom (npr. korištenje jednokratne lozinke, PIN koda i/ili drugih mobilnih postupaka).

(4) Pristup potvrdi za elektronski pečat u cloudu moguć je samo uz kvalifikovanu digitalnu potvrdu, koju izdaje pružalac usluga povjerenja Halcom CA, te preko IP adrese koju je ovlastio pružalac usluga povjerenja. Imaoci potvrda sami određuju lozinku kojom štite pristup ključevima potvrde za pristup. Potvrđivanje elektronskog žiga u cloud-u može se obaviti i putem različitih mobilnih i web aplikacija, koje potpisnik sa visokim nivoom povjerenja može koristiti isključivo pod vlastitom kontrolom (npr. korištenje jednokratne lozinke, PIN koda i/ili drugih mobilnih postupaka). Imaoc potvrde može za pristup svojoj potvrdi i aktivacijskim podacima koristiti isključivo mobilne ili web aplikacije pružaoca Halcom d.d. ili trećih pružalaca koje je Halcom CA prethodno odobrio. Spisak odobrenih aplikacija objavljen je na web stranici Halcom CA. Korištenje neodobrenih aplikacija nije dozvoljeno i predstavlja kršenje uslova izdavanja potvrde te može dovesti do trenutnog opoziva potvrde. Ako aplikacija ili njena autorizacija za pristup potvrdama u cloud-u ne funkcioniše u okviru Halcom d.d., pružalac usluga povjerenja Halcom CA takvu organizaciju ugovorno obavezuje na ispunjavanje strogih sigurnosnih uslova u skladu sa važećim evropskim i bosanskim propisima, standardima, preporukama, kao i politikama i općim pravilima rada Halcom CA. Imaoc potvrde zaključenjem ugovora o izdavanju potvrde izričito dozvoljava tehničke provjere svoje upotrebe aplikacije u obimu potrebnom za osiguravanje usklađenosti sa uslovima ove politike i važećom legislativom.

(5) Imaoci potvrda za informacione sisteme i autentikaciju web stranica sami određuju lozinku kojom štite pristup svojim privatnim ključevima. Halcom CA preporučuje korištenje sigurnih lozinki, da se lozinka za pristup privatnom ključu ne pohranjuje ili da se pohrani na sigurno mjesto, te da joj ima pristup isključivo imaoc.

6.4.2 Zaštita lozinkom

(1) Lozinku za korištenje napredne potvrde (PIN kod) i lozinku za otključavanje sigurnog medija (

PUK kod) sigurno generira pružatelj usluga od povjerenja Halcom CA. Halcom CA šalje obje lozinke imaocu potvrde preporučenom poštom ili putem drugog sigurnog kanala (lična dostava redovnom poštom, sigurni web portal ili druga slična sigurna metoda) ili, izuzetno, dostavlja ih lično. Halcom CA preporučuje da se obje lozinke čuvaju na sigurnom mjestu kojem samo imaoc ima pristup.

(2) Registracijski i aktivacijski kod za potvrde u cloudu sigurno se kreiraju kod pružaoca usluga povjerenja Halcom CA. Kodovi se imaocu dostavljaju putem dva odvojena kanala – jedan putem elektronske pošte, a drugi putem drugog sigurnog kanala (sigurni web portal dostupan s kvalifikovanom potvrdom, lična dostava klasičnom poštom ili neki drugi sličan siguran način). Izuzetno, jedan od navedenih kodova ovlaštena osoba prijavne službe Halcom CA može imaocu predati i lično. Kodovi su namijenjeni isključivo aktivaciji pristupa potvrdi u cloudu, tokom koje korisnik sam postavlja svoju ličnu šifru (PIN kod). Aktivacija potvrde u cloudu može se obaviti i putem različitih mobilnih i web aplikacija, koje potpisnik sa visokim nivoom povjerenja može koristiti isključivo pod vlastitom kontrolom. Imaoc potvrde može za pristup svojoj potvrdi i aktivacijskim podacima koristiti isključivo mobilne ili web aplikacije pružaoca Halcom d.d. ili trećih pružalaca koje je Halcom CA prethodno odobrio. Spisak odobrenih aplikacija objavljen je na web stranici Halcom CA. Korištenje neodobrenih aplikacija nije dozvoljeno i predstavlja kršenje uslova izdavanja potvrde te može dovesti do trenutnog opoziva potvrde. Ako aplikacija ili njena autorizacija za pristup potvrdama u cloudu ne funkcioniše u okviru Halcom d.d., pružalac usluga povjerenja Halcom CA takvu organizaciju ugovorno obavezuje na ispunjavanje strogih sigurnosnih uslova u skladu sa važećim evropskim i slovenačkim propisima, standardima, preporukama, kao i politikama i općim pravilima rada Halcom CA. Imaoc potvrde zaključenjem ugovora o izdavanju potvrde izričito dozvoljava tehničke provjere svoje upotrebe aplikacije u obimu potrebnom za osiguravanje usklađenosti sa uslovima ove politike i važećom legislativom.

(3) Aktivacija OT potvrde može se obaviti putem različitih mobilnih i web aplikacija, koje potpisnik sa visokim nivoom povjerenja može koristiti isključivo pod vlastitom kontrolom. Ako aplikacija ili njena autorizacija ne funkcioniše u okviru Halcom d.d., pružalac usluga povjerenja Halcom CA takvu organizaciju ugovorno obavezuje na ispunjavanje strogih sigurnosnih uslova u skladu sa važećim evropskim i slovenačkim propisima, standardima, preporukama, kao i politikama i općim pravilima rada Halcom CA.

(4) Aktivacija potvrde za elektronski pečat u cloudu moguća je samo uz kvalifikovanu digitalnu potvrdu, koju izdaje pružalac usluga povjerenja Halcom CA, te preko IP adrese koju je ovlastio pružalac usluga povjerenja. Korištenje potvrde može se obaviti i putem različitih mobilnih i web aplikacija, koje potpisnik sa visokim nivoom povjerenja može koristiti isključivo pod vlastitom kontrolom. Ako aplikacija ili njena autorizacija ne funkcioniše u okviru Halcom d.d., pružalac usluga povjerenja Halcom CA takvu organizaciju ugovorno obavezuje na ispunjavanje strogih sigurnosnih uslova u skladu sa važećim evropskim i slovenačkim propisima, standardima, preporukama, kao i politikama i općim pravilima rada Halcom CA. Imaoc potvrde može za pristup svojoj potvrdi i aktivacijskim podacima koristiti isključivo mobilne ili web aplikacije pružaoca Halcom d.d. ili trećih pružalaca koje je Halcom CA prethodno odobrio. Spisak odobrenih aplikacija objavljen je na web stranici Halcom CA. Korištenje neodobrenih aplikacija nije dozvoljeno i predstavlja kršenje uslova izdavanja potvrde te može dovesti do trenutnog opoziva potvrde. Ako aplikacija ili njena autorizacija za pristup potvrdama u cloudu ne funkcioniše u okviru Halcom d.d., pružalac usluga povjerenja Halcom CA takvu organizaciju ugovorno obavezuje na ispunjavanje strogih sigurnosnih uslova u skladu sa važećim evropskim i slovenačkim propisima, standardima, preporukama, kao i politikama i općim pravilima rada Halcom CA. Imaoc potvrde zaključenjem ugovora o izdavanju potvrde izričito dozvoljava tehničke provjere svoje upotrebe aplikacije u obimu potrebnom za osiguravanje

usklađenosti sa uslovima ove politike i važećom legislativom.

(5) Imaoci potvrda za autentifikaciju informacionih sistema i web stranica sami određuju lozinku za zaštitu pristupa svojim privatnim ključevima. Halcom CA preporučuje da se lozinka za pristup privatnom ključu ne pohranjuje ili da se pohranjuje na sigurnom mjestu i da samo imaoc ima pristup njoj.

6.4.3 Ostali aspekti lozinki

Nisu propisani.

6.5. Sigurnosni zahtjevi za informacionu i komunikacijsku opremu pružatelja usluga od povjerenja

6.5.1 Specifični tehnički sigurnosni zahtjevi

Detaljnija pravila su navedena u Opštim pravilima poslovanja i internim pravilima pružaoca usluga od povjerenja Halcom CA, u skladu sa važećim propisima, standardima i preporukama.

6.5.2 Nivo sigurnosne zaštite

Detaljnija pravila su navedena u Opštim pravilima poslovanja i internim pravilima pružaoca usluga od povjerenja Halcom CA, u skladu sa važećim propisima, standardima i preporukama.

6.6. Tehnička kontrola životnog ciklusa pružatelja usluga od povjerenja

6.6.1 Kontrola razvoja sistema

Halcom CA koristi softver i hardver koji je certificiran prema FIPS 140-2 Level 3 i/ili Common Criteria EAL4+.

6.6.2 Upravljanje sigurnošću

Detaljnija pravila su navedena u Opštim pravilima poslovanja i internim pravilima pružaoca usluga od povjerenja Halcom CA, u skladu sa važećim propisima, standardima i preporukama.

6.6.3 Kontrola životnog ciklusa

Detaljni tehnički zahtjevi navedeni su u Općim pravilima poslovanja i internim pravilima pružatelja usluga od povjerenja Halcom CA.

6.7. Kontrola sigurnosti mreže

Detaljnija pravila su navedena u Opštim pravilima poslovanja i internim pravilima pružaoca usluga od povjerenja Halcom CA, u skladu sa važećim propisima, standardima i preporukama.

6.8. Vremensko označavanje

Nije propisano.

7. PROFIL POTVRDA I REGISTRA OPOZVANIH

POTVRDA

7.1. Profil potvrda

(1) Na osnovu ove politike, Halcom CA izdaje napredne potvrde, potvrde u cloudu, potvrde za informacione sisteme, potvrde za autentifikaciju web stranica i OT potvrde namijenjene poslovnim subjektima.

(2) Sve potvrde uključuju podatke koji su određeni za kvalifikovane potvrde u skladu s uredbom eIDAS i uredbom eIDAS 2.0.

(3) Potvrde pružatelja usluga od povjerenja Halcom CA slijede standard X.509.

7.1.1 Verzija potvrda

Sve potvrde od Halcom CA pružatelja usluga od povjerenja slijede X.509 standard, verziju 3.

7.1.2 Profil potvrdaa s ekstenzijama

7.1.2.1 Profil korijenske (Root) potvrde

Nazivi polja	Vrijednost ili značenje
Osnovna polja u potvrdi	
Verzija, engl. Version	V3
Identifikacijskia oznaka potvrde, engl. Serial Number	G1: 0cdf9b
	G2: 6fb450b4a6bbeebb983055e81d53c040
	G3: 7539c53f6170763fb3c445b870ef6174
Algoritam potpisa, engl. Signature algorithm	G1: Sha256RSA
	G2: RSASSA-PSS
	G3: RSASSA-PSS
Izdavatelj, engl. Issuer	G1: C=SI, O=Halcom dd, 2.5.4.97 = VATSI-43353126 CN=Halcom Root Certificate Authority
	G2: C=SI, O=Halcom dd, 2.5.4.97 = VATSI-43353126 CN=Halcom Root CA G2
	G3: C=SI, O=Halcom d.d., 2.5.4.97 = VATSI-43353126 CN=Halcom Root CA G3
Validnost, engl. Validity	G1: Valid from: <10.6.2016 07:07:50 GMT > Valid to: <10.6.2036 07:07:50 GMT >
	G2: Valid from: < 19.3. 2025 09:00:00 GMT> Valid to: <19.3.2045 09:00:00 GMT>
	G3: Valid from: < 19.3. 2026 10:00:00 GMT> Valid to: <19.3.2046 10:00:00 GMT>
Imaoc, engl. Subject	G1: C=SI, O=Halcom dd, 2.5.4.97 = VATSI-43353126 CN=Halcom Root Certificate Authority
	G2: C=SI, O=Halcom dd, 2.5.4.97 = VATSI-43353126 CN=Halcom Root CA G2
	G3: C=SI, O=Halcom d.d., 2.5.4.97 = VATSI-43353126 CN=Halcom Root CA G3

Algoritam javnog ključa subjekta, engl. Subject Public Key Algorithm	G1: RSA
	G2: RSASSA-PSS
	G3: RSA
Javni ključ, engl. Public Key (... bits)	modul, eksponent,...
Javni ključ imaoca, koji pripada odgovarajućem paru ključeva, šifriran alogoritmom RSA ili RSASSA-PSS, engl. Public Key	G1: dužina ključa je najmanje 2048 bita
	G2: dužina ključa je najmanje 4096 bita
	G3: dužina ključa je najmanje 4096 bita
X.509v3 ekstenzije	
Upotreba ključa, OID 2.5.29.15, engl. Key Usage	Certificate Signing, Off-line CRL Signing, CRL Signing
Identifikator ključa imaoca, OID 2.5.29.14, engl. Subject Key Identifier	G1: 42aea643c79828b0
	G2: 4e14b2790896f4b6
	G3: 4ba6657603985167
Osnovna ograničenja, OID 2.5.29.19, engl. Basic Constraints	Subject Type=CA Path Length Constraint=None
Dodatna identifikacija (nije dio digitalnog potvrde)	
Identifikacijski otisak potvrde – SHA1, engl. Certificate Fingerprint – SHA1	Identifikacijski otisak potvrde prema SHA1

7.1.2.2 Profil podređenih potvrda za elektronski potpis

(1) Halcom CA PO e-signature 1

Nazivi polja	Vrijednost ili značenje
Osnovna polja u potvrdi	
Verzija, engl. Version	V3
Identifikacijski kod potvrde, engl. Serial Number	0cecab
Algoritam potpisa, engl. Signature algorithm	Sha256RSA
Izdavatelj, engl. Issuer	CN = Halcom Root Certificate Authority 2.5.4.97 = VATSI-43353126 O = Halcom dd C = SI
Validnost, engl. Validity	Valid from: <15.6.2016 10:34:13 GMT > Valid to: <15.6.2026 10:34:13 GMT >
Imaoc, engl. Subject	CN = Halcom CA PO e-signature 1 2.5.4.97 = VATSI-43353126 O = Halcom dd C = SI

Algoritam javnog ključa subjekta, engl. Subject Public Key Algorithm	RSA
Javni ključ, angl. Public Key (… bits)	modul, eksponent,…
Javni ključ imaoca, koji pripada odgovarajućem paru ključeva, šifriran RSA ili RSASSA-PSS algoritmom, engl. Public Key	dužina ključa je 2048 bita
X.509v3 ekstenzije	
Objava registra opozvanih potvrdaa, OID 2.5.29.31, angl. CRL Distribution Points	URL=ldap://ldap.halcom.si/cn=Halcom%20Root%20Certificate%20Authority,o=Halcom,c=SI?certificaterevocationlist;binary URL=http://domina.halcom.si/crls/halcom_root_certificate_authority.crl
Upotreba ključa, OID 2.5.29.15, engl. Key Usage	Certificate Signing, Off-line CRL Signing, CRL Signing
Identifikator ključa pružatelja usluga povjerenja, OID 2.5.29.35, engl. Authority Key Identifier	KeyID=42aea643c79828b0
Identifikator ključa imaoca, OID 2.5.29.14, engl. Subject Key Identifier	40f695209b79c209
Osnovna ograničenja, OID 2.5.29.19, engl. Basic Constraints	Subject Type=CA Path Length Constraint=None
Dodatna identifikacija (nije dio digitalne potvrde)	
Identifikacijski otisak potvrde – SHA1, engl. Certificate Fingerprint – SHA1	Identifikacijski otisak potvrde prema SHA1

(2) Halcom CA PO e-signature 2

Nazivi polja	Vrijednost ili značenje
Osnovna polja u potvrdi	
Verzija, engl. Version	V3
Identifikacijski kod potvrde, engl. Serial Number	136c16
Algoritam potpisa, engl. Signature algorithm	Sha256RSA

Izdavatelj, engl. Issuer	CN = Halcom Root Certificate Authority 2.5.4.97 = VATSI-43353126 O = Halcom dd C = SI
Validnost, engl. Validity	Valid from: <03.04.2023 07:00:00 GMT > Valid to: <03.04.2033 07:00:00 GMT >
Imaoc, engl. Subject	CN = Halcom CA PO e-signature 2 2.5.4.97 = VATSI-43353126 O = Halcom dd C = SI
Algoritam za javni ključ, engl. Subject Public Key Algorithm	RSA
Javni ključ, engl. Public Key (... bits)	modul, eksponent,...
Javni ključ imaoca, koji pripada odgovarajućem paru ključeva, šifriran RSA algoritmom, engl. RSA Public Key	dužina ključa je 3072 bita
X.509v3 ekstenzije	
Objava registra opozvanih potvrda, OID 2.5.29.31, engl. CRL Distribution Points	URL=ldap://ldap.halcom.si/cn=Halcom%20Root%20Certificate%20Authority,o=Halcom,c=SI?certificaterevocationlist;binary URL=http://domina.halcom.si/crls/halcom_root_certificate_authority.crl
Korištenje ključa, OID 2.5.29.15, engl. Key Usage	Certificate Signing, Off-line CRL Signing, CRL Signing
Identifikator ključa pružatelja usluga povjerenja, OID 2.5.29.35, engl. Authority Key Identifier	ID ključa=42aea643c79828b0
Identifikator ključa imaoca, OID 2.5.29.14, engl. Subject Key Identifier	434d32751603c975
Osnovna ograničenja, OID 2.5.29.19, engl. Basic Constraints	Subject Type=CA Path Length Constraint=None
Dodatna identifikacija (nije dio digitalne potvrde)	
Identifikacijski otisak potvrde – SHA1, engl. Certificate Fingerprint – SHA1	Identifikacijski otisak potvrde prema SHA1

(3) Halcom CA PO e-sign 1G2

Nazivi polja	Vrijednost ili značenje

Osnovna polja u potvrdi	
Verzija, engl. Version	V3
Identifikacijski kod potvrde, engl. Serial Number	70cacd5bdedf11534925d1c8c89d22d5
Algoritam potpisa, engl. Signature algorithm	RSASSA-PSS
Izdavatelj, engl. Issuer	CN = Halcom Root CA G2 2.5.4.97 = VATSI-43353126 O = Halcom dd C = SI
Validnost, engl. Validity	Valid from: <25.3.2025 10:00:00 GMT> Valid to: <25.3.2035 09:00:00 GMT>
Imaoc, engl. Subject	CN = Halcom CA PO e-sign 1 G2 2.5.4.97 = VATSI-43353126 O = Halcom dd C = SI
Algoritam za javni ključ, engl. Subject Public Key Algorithm	RSASSA-PSS
Javni ključ, engl. Public Key (... bits)	modul, eksponent,...
Javni ključ imaoca, koji pripada odgovarajućem paru ključeva, šifriran RSA algoritmom, engl. RSA Public Key	Dužina ključa je 4096 bit
X.509v3 ekstenzije	
Objava registra opozvanih potvrda, OID 2.5.29.31, engl. CRL Distribution Points	URL=ldap://ldap.halcom.si/cn=Halcom%20Root%20CA%20G2,o=Halcom,c=SI?certificaterevocationlist;binary URL=http://domina.halcom.si/crls/halcom_root_ca_g2.crl
Korištenje ključa, OID 2.5.29.15, engl. Key Usage	Certificate Signing, Off-line CRL Signing, CRL Signing
Identifikator ključa pružatelja usluga od povjerenja, OID 2.5.29.35, engl. Authority Key Identifier	KeyID=4e14b2790896f4b6
Identifikator ključa imaoca, OID 2.5.29.14, engl. Subject Key Identifier	41753bf986c7cb9c
Osnovna ograničenja, OID 2.5.29.19, engl. Basic Constraints	Subject Type=CA Path Length Constraint=None
Dodatna identifikacija (nije dio digitalne potvrde)	

Identifikacijski otisak potvrde – SHA1, engl. Certificate Fingerprint – SHA1	Identifikacijski otisak potvrde prema SHA1

(4) Halcom CA PO e-sign 1G3

Nazivi polja	Vrijednost ili značenje
Osnovna polja u potvrdi	
Verzija, engl. Version	V3
Identifikacijski kod potvrde, engl. Serial Number	4169334d33852535c55db054b61ea552
Algoritam potpisa, engl. Signature algorithm	RSASSA-PSS
Izdavatelj, engl. Issuer	CN = Halcom Root CA G3 2.5.4.97 = VATSI-43353126 O = Halcom dd C = SI
Validnost, engl. Validity	Valid from: <2.4.2026 09:01:00 GMT> Valid to: <2.4.2036 09:01:00 GMT>
Imaoc, engl. Subject	CN = Halcom CA PO e-sig 1 G3 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Algoritam za javni ključ, engl. Subject Public Key Algorithm	RSA
Javni ključ, engl. Public Key (... bits)	modul, eksponent,...
Javni ključ imaoca, koji pripada odgovarajućem paru ključeva, šifriran RSA algoritmom, engl. RSA Public Key	Dužina ključa je 4096 bit
X.509v3 ekstenzije	
Objava registra opozvanih potvrda, OID 2.5.29.31, engl. CRL Distribution Points	URL=ldap://ldap.halcom.si/cn=Halcom%20Root%20CA%20G3,o=Halcom,c=SI?certificaterevocationlist;binary URL=http://domina.halcom.si/crls/halcom_root_ca_g3.crl
Korištenje ključa, OID 2.5.29.15, engl. Key Usage	Certificate Signing, Off-line CRL Signing, CRL Signing
Identifikator ključa pružatelja usluga od povjerenja, OID 2.5.29.35, engl. Authority Key Identifier	KeyID=4ba6657603985167

Identifikator ključa imaoca, OID 2.5.29.14, engl. Subject Key Identifier	46b69ca3e4fa428d
Osnovna ograničenja, OID 2.5.29.19, engl. Basic Constraints	Subject Type=CA Path Length Constraint=None
Dodatna identifikacija (nije dio digitalne potvrde)	
Identifikacijski otisak potvrde – SHA1, engl. Certificate Fingerprint – SHA1	Identifikacijski otisak potvrde prema SHA1

7.1.2.3 Profil podređene potvrde za elektronski pečat

(1) Halcom CA PO e-seal 1

Nazivi polja	Vrijednost ili značenje
Osnovna polja u potvrdi	
Verzija, engl. Version	V3
Identifikacijski kod potvrde, engl. Serial Number	0e0ed0
Algoritam potpisa, engl. Signature algorithm	Sha256RSA
Izdavatelj, engl. Issuer	CN = Halcom Root Certificate Authority 2.5.4.97 = VATSI-43353126 O = Halcom dd C = SI
Validnost, engl. Validity	Valid from: <22.4.2017 08:00:00 GMT> Valid to: <22.4.2027 08:00:00 GMT>
Imaoc, engl. Subject	CN = Halcom CA PO e-seal 1 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Algoritam javnog ključa, engl. Subject Public Key Algorithm	RSA
Javni ključ, engl. Public Key (... bits)	modul, eksponent,...
Javni ključ imaoca, koji pripada odgovarajućem paru ključeva, šifriran RSA algoritmom, engl. RSA Public Key	dužina ključa je 2048 bita
X.509v3 ekstenzije	
Objava registra opozvanih potvrda, OID 2.5.29.31, engl. CRL Distribution Points	URL=ldap://ldap.halcom.si/cn=Halcom%20Root%20Certificate%20Authority,o=Halcom,c=SI?certificaterevocationlist;binary URL=http://domina.halcom.si/crls/halcom_root_certificate_authority.crl

Korištenje ključa, OID 2.5.29.15, engl. Key Usage	Certificate Signing, Off-line CRL Signing, CRL Signing
Identifikator ključa pružatelja usluga od povjerenja, OID 2.5.29.35, engl. Authority Key Identifier	KeyID=42aea643c79828b0
Identifikator ključa imaoca, OID 2.5.29.14, engl. Subject Key Identifier	49487650770ab10c
Osnovna ograničenja, OID 2.5.29.19, engl. Basic Constraints	Subject Type=CA Path Length Constraint=None
Dodatna identifikacija (nije dio digitalne potvrde)	
Identifikacijski otisak potvrde – SHA1, engl. Certificate Fingerprint – SHA1	Identifikacijski otisak potvrde prema SHA1

(2) Halcom CA PO e-seal 2

Nazivi polja	Vrijednost ili značenje
Osnovna polja u potvrdi	
Verzija, engl. Version	V3
Identifikacijski kod potvrde, engl. Serial Number	136c18
Algoritam potpisa, engl. Signature algorithm	Sha256RSA
Izdavatelj, engl. Issuer	CN = Halcom Root Certificate Authority 2.5.4.97 = VATSI-43353126 O = Halcom dd C = SI
Validnost, engl. Validity	Valid from: <04/03/2023 07:00:00 GMT> Valid to: <04/03/2033 07:00:00 GMT>
Imaoc, engl. Subject	CN = Halcom CA PO e-sealt 2 2.5.4.97 = VATSI-43353126 O = Halcom dd C = SI
Algoritam za javni ključ, engl. Subject Public Key Algorithm	RSA
Javni ključ, engl. Public Key (... bits)	modul, eksponent,...

Javni ključ imaoca, koji pripada odgovarajućem paru ključeva, šifriran RSA algoritmom, engl. RSA Public Key	dužina ključa je 3072 bit
X.509v3 ekstenzije	
Objava registra opozvanih potvrda, OID 2.5.29.31, engl. CRL Distribution Points	URL=ldap://ldap.halcom.si/cn=Halcom%20Root%20Certificate%20Authority,o=Halcom,c=SI?certificaterevocationlist;binary URL=http://domina.halcom.si/crls/halcom_root_certificate_authority.crl
Korištenje ključa, OID 2.5.29.15, engl. Key Usage	Certificate Signing, Off-line CRL Signing, CRL Signing
Identifikator ključa pružatelja usluga od povjerenja, OID 2.5.29.35, engl. Authority Key Identifier	KeyID=42aea643c79828b0
Identifikator ključa imaoca, OID 2.5.29.14, engl. Subject Key Identifier	4735c8bc61e25d9e
Osnovna ograničenja, OID 2.5.29.19, engl. Basic Constraints	Subject Type=CA Path Length Constraint=None
Dodatna identifikacija (nije dio digitalne potvrde)	
Identifikacijski otisak potvrde – SHA1, engl. Certificate Fingerprint – SHA1	Identifikacijski otisak potvrde prema SHA1

(3) Halcom CA e-seal 1 G2

Nazivi polja	Vrijednost ili značenje
Osnovna polja u potvrdi	
Verzija, engl. Version	V3
Identifikacijski kod potvrde, engl. Serial Number	65a0bbcece218f6ce1136d5d3ad65d43
Algoritam potpisa, engl. Signature algorithm	RSASSA-PSS
Izdavatelj, engl. Issuer	CN = Halcom Root CA G2 2.5.4.97 = VATSI-43353126 O = Halcom dd C = SI
Validnost, engl. Validity	Valid from: <25.03.2025 10:00:00 GMT> Valid to <25.03.2035 09:00:00 GMT>

Imaoc, engl. Subject	CN = Halcom CA e-seal 1 G2 2.5.4.97 = VATSI-43353126 O = Halcom dd C = SI
Algoritam za javni ključ, engl. Subject Public Key Algorithm	RSASSA-PSS
Javni ključ, engl. Public Key (... bits)	modul, eksponent,...
Javni ključ imaoca, koji pripada odgovarajućem paru ključeva, šifriran RSA algoritmom, engl. RSA Public Key	Dužina ključa je 4096 bit
X.509v3 ekstenzije	
Objava registra opozvanih potvrda, OID 2.5.29.31, engl. CRL Distribution Points	URL=ldap://ldap.halcom.si/cn=Halcom%20Root%CA%20G2,o=Halcom,c=SI?certificaterevocationlist;binary URL=http://domina.halcom.si/crls/halcom_root_ca_g2.crl
Korištenje ključa, OID 2.5.29.15, engl. Key Usage	Certificate Signing, Off-line CRL Signing, CRL Signing
Identifikator ključa pružatelja usluga od povjerenja, OID 2.5.29.35, engl. Authority Key Identifier	KeyID=4e14b2790896f4b6
Identifikator ključa imaoca, OID 2.5.29.14, engl. Subject Key Identifier	4125fcd8fad6662f
Osnovna ograničenja, OID 2.5.29.19, engl. Basic Constraints	Subject Type=CA Path Length Constraint=None
Dodatna identifikacija (nije dio digitalne potvrde)	
Identifikacijski otisak potvrde – SHA1, engl. Certificate Fingerprint – SHA1	Identifikacijski otisak potvrde prema SHA1

(4) Halcom CA e-seal 1 G3

Nazivi polja	Vrijednost ili značenje
Osnovna polja u potvrdi	
Verzija, engl. Version	V3
Identifikacijski kod potvrde, engl. Serial Number	40a0315ca93f043edb4b890c73246c19
Algoritam potpisa, engl. Signature algorithm	RSASSA-PSS

Izdavatelj, engl. Issuer	CN = Halcom Root CA G3 2.5.4.97 = VATSI-43353126 O = Halcom dd C = SI
Validnost, engl. Validity	Valid from: <02.04.2026 09:02:00 GMT> Valid to <02.04.2036 09:02:00 GMT>
Imaoc, engl. Subject	CN = Halcom CA e-seal 1 G3 2.5.4.97 = VATSI-43353126 O = Halcom dd C = SI
Algoritam za javni ključ, engl. Subject Public Key Algorithm	RSA
Javni ključ, engl. Public Key (... bits)	modul, eksponent,...
Javni ključ imaoca, koji pripada odgovarajućem paru ključeva, šifriran RSA algoritmom, engl. RSA Public Key	Dužina ključa je 4096 bit
X.509v3 ekstenzije	
Objava registra opozvanih potvrda, OID 2.5.29.31, engl. CRL Distribution Points	URL=ldap://ldap.halcom.si/cn=Halcom%20Root%CA%20G3,o=Halcom,c=SI?certificaterevocationlist;binary URL=http://domina.halcom.si/crls/halcom_root_ca_g3.crl
Korištenje ključa, OID 2.5.29.15, engl. Key Usage	Certificate Signing, Off-line CRL Signing, CRL Signing
Identifikator ključa pružatelja usluga od povjerenja, OID 2.5.29.35, engl. Authority Key Identifier	KeyID=4ba6657603985167
Identifikator ključa imaoca, OID 2.5.29.14, engl. Subject Key Identifier	462d8ba5e3c50364
Osnovna ograničenja, OID 2.5.29.19, engl. Basic Constraints	Subject Type=CA Path Length Constraint=None
Dodatna identifikacija (nije dio digitalne potvrde)	
Identifikacijski otisak potvrde – SHA1, engl. Certificate Fingerprint – SHA1	Identifikacijski otisak potvrde prema SHA1

7.1.2.4 Profil podređenih potvrda za autentifikaciju web stranica

(1) Halcom CA web 1

Nazivi polja	Vrijednost ili značenje

Osnovna polja u potvrdi	
Verzija, engl. Version	V3
Identifikacijski kod potvrde, engl. Serial Number	0e0ed2
Algoritam potpisa, engl. Signature algorithm	Sha256RSA
Izdavatelj, engl. Issuer	CN = Halcom Root Certificate Authority 2.5.4.97 = VATSI-43353126 O = Halcom dd C = SI
Validnost, engl. Validity	Valid from: <22.04.2017 08:00:00 GMT> Valid to: <22.04.2027 08:00:00 GMT>
Imaoc, engl. Subject	CN = Halcom CA web 1 2.5.4.97 = VATSI-43353126 O = Halcom dd C = SI
Algoritam za javni ključ, engl. Subject Public Key Algorithm	RSA
Javni ključ, engl. Public Key (... bits)	modul, eksponent,...
Javni ključ imaoca, koji pripada odgovarajućem paru ključeva, šifriran RSA algoritmom, engl. RSA Public Key	dužina ključa je 2048 bit
X.509v3 ekstenzije	
Objava registra opozvanih potvrda, OID 2.5.29.31, engl. CRL Distribution Points	URL=ldap://ldap.halcom.si/cn=Halcom%20Root%20Certificate%20Authority,o=Halcom,c=SI?certificaterevocationlist;binary URL=http://domina.halcom.si/crls/halcom_root_certificate_authority.crl
Upotreba ključa, OID 2.5.29.15, engl. Key Usage	Certificate Signing, Off-line CRL Signing, CRL Signing
Identifikator ključa pružatelja uslugaod povjerenja, OID 2.5.29.35, engl. Authority Key Identifier	KeyID=42aea643c79828b0
Identifikator ključa imaoca, OID 2.5.29.14, engl. Subject Key Identifier	48420b17edae9e70
Osnovna ograničenja, OID 2.5.29.19, engl. Basic Constraints	Subject Type=CA Path Length Constraint=None
Dodatna identifikacija (nije dio digitalne potvrde)	

Identifikacijski otisak potvrde – SHA1, engl. Certificate Fingerprint – SHA1	Identifikacijski otisak potvrde prema SHA1

(2) Halcom CA web 2

Nazivi polja	Vrijednost ili značenje
Osnovna polja u potvrdi	
Verzija, engl. Version	V3
Identifikacijska oznaka potvrde, engl. Serial Number	6be5967ab71177ca1478b28751b05cbc
Algoritam potpisa, engl. Signature algorithm	Sha256RSA
Izdavatelj, engl. Issuer	CN = Halcom Root Certificate Authority 2.5.4.97 = VATSI-43353126 O = Halcom dd C = SI
Validnost, engl. Validity	Valid from: <25.03.2025 09:00:00 GMT> Valid to: <25.02.2035 08:00:00 GMT>
Imaoc, engl. Subject	CN = Halcom CA web 2 2.5.4.97 = VATSI-43353126 O = Halcom dd C = SI
Algoritam za javni ključ, engl. Subject Public Key Algorithm	RSA
Javni ključ, engl. Public Key (... bits)	modul, eksponent,...
Javni ključ imaoca, koji pripada odgovarajućem paru ključeva, šifriran RSA algoritmom, engl. RSA Public Key	dužina ključa je 3072 bit
X.509v3 ekstenzije	
Objava registra opozvanih certifikata, OID 2.5.29.31, engl. CRL Distribution Points	URL=ldap://ldap.halcom.si/cn=Halcom%20Root%20Certificate%20Authority,o=Halcom,c=SI?certificaterevocationlist;binary URL=http://domina.halcom.si/crls/halcom_root_certificate_authority.crl
Upotreba ključa, OID 2.5.29.15, engl. Key Usage	Certificate Signing, Off-line CRL Signing, CRL Signing
Identifikator ključa pružatelja usluga od povjerenja, OID 2.5.29.35, engl. Authority Key Identifier	KeyID=42aea643c79828b0

Identifikator ključa imaoca, OID 2.5.29.14, engl. Subject Key Identifier	408cacc9cbc74c1f
Osnovna ograničenja, OID 2.5.29.19, engl. Basic Constraints	Subject Type=CA Path Length Constraint=None
Dodatna identifikacija (nije dio digitalne potvrde)	
Identifikacijski otisak potvrde – SHA1, engl. Certificate Fingerprint – SHA1	Identifikacijski otisak potvrde prema SHA1

(3) Halcom CA web 1 G2

Nazivi polja	Vrijednost ili značenje
Osnovna polja u potvrdi	
Verzija, engl. Version	V3
Identifikacijski kod potvrde, engl. Serial Number	5b8a526a57748dbaf4198edaa1a80472
Algoritam potpisa, engl. Signature algorithm	RSASSA-PSS
Izdavatelj, engl. Issuer	CN = Halcom Root CA G2 2.5.4.97 = VATSI-43353126 O = Halcom dd C = SI
Validnost, engl. Validity	Valid from: <25.03.2025 10:00:00 GMT> Valid to: <25.03.2035 09:00:00 GMT>
Imaoc, engl. Subject	CN = Halcom CA web 1 G2 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Algoritam za javni ključ, engl. Subject Public Key Algorithm	RSASSA-PSS
Javni ključ, engl. Public Key (... bits)	modul, eksponent,...
Javni ključ imaoca, koji pripada odgovarajućem paru ključeva, šifriran RSA algoritmom, engl. RSA Public Key	Dužina ključa je 4096 bit
X.509v3 ekstenzije	
Objava registra opozvanih potvrda, OID 2.5.29.31, engl. CRL Distribution Points	URL=ldap://ldap.halcom.si/cn=Halcom%20Root%20CA%20G2,o=Halcom,c=SI?certificaterevocationlist;binary URL=http://domina.halcom.si/crls/halcom_root_ca_g2.crl

Korištenje ključa, OID 2.5.29.15, engl. Key Usage	Certificate Signing, Off-line CRL Signing, CRL Signing
Identifikator ključa pružatelja usluga od povjerenja, OID 2.5.29.35, engl. Authority Key Identifier	ID ključa=4e14b2790896f4b6
Identifikator ključa imaoca, OID 2.5.29.14, engl. Subject Key Identifier	4e9125213b702aca
Osnovna ograničenja, OID 2.5.29.19, engl. Basic Constraints	Subject Type=CA Path Length Constraint=None
Dodatna identifikacija (nije dio digitalne potvrde)	
Identifikacijski otisak potvrde – SHA1, engl. Certificate Fingerprint – SHA1	Identifikacijski otisak potvrde prema SHA1

(4) Halcom CA web 1 G3

Nazivi polja	Vrijednost ili značenje
Osnovna polja u potvrdi	
Verzija, engl. Version	V3
Identifikacijski kod potvrde, engl. Serial Number	7f5cd6c8280e02dfefd0cd910db1517f
Algoritam potpisa, engl. Signature algorithm	RSASSA-PSS
Izdavatelj, engl. Issuer	CN = Halcom Root CA G3 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Validnost, engl. Validity	Valid from: <02.04.2026 09:03:00 GMT> Valid to: <02.04.2036 09:03:00 GMT>
Imaoc, engl. Subject	CN = Halcom CA web 1 G3 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Algoritam za javni ključ, engl. Subject Public Key Algorithm	RSA
Javni ključ, engl. Public Key (... bits)	modul, eksponent,...

Javni ključ imaoca, koji pripada odgovarajućem paru ključeva, šifriran RSA algoritmom, engl. RSA Public Key	Dužina ključa je 4096 bit
X.509v3 ekstenzije	
Objava registra opozvanih potvrda, OID 2.5.29.31, engl. CRL Distribution Points	URL=ldap://ldap.halcom.si/cn=Halcom%20Root%20CA%20G3,o=Halcom,c=SI?certificaterevocationlist;binary URL=http://domina.halcom.si/crls/halcom_root_ca_g3.crl
Korištenje ključa, OID 2.5.29.15, engl. Key Usage	Certificate Signing, Off-line CRL Signing, CRL Signing
Identifikator ključa pružatelja usluga od povjerenja, OID 2.5.29.35, engl. Authority Key Identifier	KeyID=4ba6657603985167
Identifikator ključa imaoca, OID 2.5.29.14, engl. Subject Key Identifier	4a4af4272960b712
Osnovna ograničenja, OID 2.5.29.19, engl. Basic Constraints	Subject Type=CA Path Length Constraint=None
Dodatna identifikacija (nije dio digitalne potvrde)	
Identifikacijski otisak potvrde – SHA1, engl. Certificate Fingerprint – SHA1	Identifikacijski otisak potvrde prema SHA1

7.1.2.5 Profil potvrda krajnjih korisnika

Nazivi polja	Vrijednost ili značenje
Osnovna polja u potvrdi	
Verzija, engl. Version	V3
Identifikacijski kod potvrde, engl. Serial Number	jedinstveni interni broj potvrde
Algoritam potpisa, engl. Signature algorithm	G1: Sha256RSA
	G2: RSASSA-PSS
	G3: RSASSA-PSS
Izdavatelj, engl. Issuer	prepoznatljivo ime izdavatelja, pogledajte tačke 3.1.1. i 7.1.2.2.
Validnost, engl. Validity	Valid from: <datum važenja po GMT> Valid to: <kraj važenja po GMT>
Imaoc, engl. Subject	Ime i prezime imaoca, pogledajte tačku 3.1.1.
Algoritam za javni ključ, engl. Subject Public Key Algorithm	RSA
Javni ključ, engl. Public Key (... bits)	modul, eksponent,...

Javni ključ imaoca, koji pripada odgovarajućem paru ključeva, šifriran RSA algoritmom, engl. RSA Public Key	dužine ključeva variraju (pogledajte tačku 6.1.5) G1: najmanje 2048 bit
	G2: najmanje 3072 bit
	G3: najmanje 3072 bit
X.509v3 ekstenzije	
Objava registra opozvanih potvrda, OID 2.5.29.31, engl. CRL Distribution Points	U zavisnosti od izdavaoca, pogledajte tačku 7.2.2
Korištenje ključa, OID 2.5.29.15, engl. Key Usage	Napredna potvrda za cloud i informacione sisteme: Digital Signature, Non Repudiation, Key Encipherment Potvrde za autentifikaciju web stranice: Digital Signature, Key Encipherment
Identifikator ključa pružatelja usluga od povjerenja, OID 2.5.29.35, engl. Authority Key Identifier	G1: Halcom CA PO e-signature 1: KeyID=40f695209b79c209 Halcom CA PO e-signature 2: KeyID=434d32751603c975 Halcom CA PO e-seal 1: KeyID=49487650770ab10c Halcom CA PO e-seal 2: KeyID=4735c8bc61e25d9e Halcom CA web 1: KeyID=48420b17edae9e70 Halcom CA web 2: KeyID=408cacc9cbc74c1f
	G2: Halcom CA PO e-sig 1 G2: KeyID=41753bf986c7cb9c Halcom CA e-seal 1 G2: KeyID=4125fcd8fad6662f Halcom CA web 1 G2: KeyID=4e9125213b702aca
	G3: Halcom CA PO e-sig 1 G3: KeyID=46b69ca3e4fa428d Halcom CA e-seal 1 G3: KeyID=462d8ba5e3c50364 Halcom CA web 1 G3: KeyID=4a4af4272960b712
EŠEI	jedinstveni elektronski identifikacijski broj (pogledajte sljedeću tačku)

(1) Polje Upotreba ključa (engl. Key Usage) je označeno kao kritično.

(2) Imaoc može posjedovati samo jednu važeću potvrdu iste vrste, osim u periodu od šezdeset (60) dana prije isteka važenja ove potvrde, kada imaoc može dobiti novu potvrdu.

7.1.2.6 Jedinstveni elektronski identifikacijski broj

U skladu sa članom 24. Zakona o elektronskoj identifikaciji i uslugama od povjerenja (Uradni list Republike Slovenije, br. 121/21 i 189/21 – ZDU-1M), članom 52. Uredbe o određivanju sredstava elektronske identifikacije i korištenju centralne usluge za online registraciju i elektronski potpis (Uradni list Republike Slovenije, br. 29/22), Jedinstveni elektronski identifikacijski broj (EŠEI) imaoca se upisuje u kvalifikovanu potvrda za elektronski potpis, elektronski pečat ili autentifikaciju web

stranice kao privatno proširenje kvalifikovane potvrde. Potonje se upisuje kao nezavisno polje za proširenje, zapisano u ASN.1 notaciji:

SEQUENCE :
OBJECT_IDENTIFIER : '1.3.6.1.4.1.58536.1.1.1.1.1' <OID ekstenzija za vrijednost EŠEI fizičke osobe>
OCTET_STRING :
IA5String : 'xxxxxxxxxxxx' <vrijednost>

SEQUENCE :
OBJECT_IDENTIFIER : '1.3.6.1.4.1.58536.1.1.1.1.2' ' <OID ekstenzije za EŠEI vrijednost pravnog lica>
OCTET_STRING :
IA5String : 'xxxxxxxxxxxx' <vrijednost>

7.1.2.7 Zahtjevi za adresu e-pošte

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

- neprikladna ili uvredljiva,
- da obmanjuje treća lica,
- je u suprotnosti s važećim propisima i standardima.

(2) Nisu propisana nikakva druga ograničenja u vezi s elektronskim adresama.

7.1.3 Identifikacijske oznake algoritama

(1) Potvrde koje izdaje Halcom CA potpisuje pružatelj usluga od povjerenja algoritmom navedenim u vrijednosti polja algoritam potpisa:

- G1: sha256RSA, identifikacijski kod: OID 1.2.840.113549.1.1.11 ili
- G2: RSASSA-PSS, identifikacijski kod: OID 1.2.840.113549.1.1.10,
- G3: RSASSA-PSS, identifikacijski kod: OID 1.2.840.113549.1.1.10.

(2) Kompletan set algoritama, formata podataka i protokola dostupan je kod ovlaštenih osoba pružatelja usluga od povjerenja Halcom CA.

7.1.4 Format prepoznatljivog imena

Pogledajte tačku 3.1.1.

7.1.5 Ograničenja koja se tiču imena

Ograničenja imena (polje u potvrdi engl. nameConstraints) nisu propisana.

7.1.6 Oznaka politike potvrde

Pogledajte tačku 7.1.2.

7.1.7 Ograničenja korištenja

Ograničenja korištenja (polje u potvrdi engl. usage policy constraints extension) nisu propisana.

7.1.8 Sintaksa i značenje oznaka politike potvrda

Potvrde koje izdaje Halcom CA, pružatelj usluga od povjerenja, koriste specifične podatke policyQualifiers, koji se obrađuju u skladu sa standardima IETF RFC i ETSI.

7.1.9 Važnost bitnih dopuna politika

Nije podržano.

7.2. Profil registra opozvanih potvrda

(1) Halcom CA registri opozvanih potvrda su liste opozvanih potvrda (CRL) i nalaze se u sljedećim granama:

- G1:
  - CN= Halcom CA PO e-signature 1
    O = Halcom
    C = SI
  - CN= Halcom CA PO e-signature 2
    O = Halcom
    C = SI
  - CN= Halcom CA PO e-seal 1
    O = Halcom
    C = SI
  - CN= Halcom CA PO e-seal 2
    O = Halcom
    C = SI
  - CN= Halcom CA web 1
    O = Halcom
    C = SI
  - CN= Halcom CA web 2
    O = Halcom
    C = SI
- G2:
  - CN= Halcom CA PO e-sig 1 G2
    O = Halcom
    C = SI
  - CN= Halcom CA e-seal 1G2
    O = Halcom
    C = SI
  - CN= Halcom CA web 1 G2
    O = Halcom
    C = SI
- G3:
  - CN= Halcom CA PO e-sig 1 G3
    O = Halcom
    C = SI
  - CN= Halcom CA e-seal 1G3
    O = Halcom

C = SI
- CN= Halcom CA web 1 G3
  O = Halcom
  C = SI

(2) Registar opozvanih potvrda osvježava se nakon svakog opoziva potvrda ili najmanje jednom dnevno ako nema novih unosa ili promjena u registru opozvanih potvrda (24 sata nakon posljednjeg osvježavanja).

(3) Registar opozvanih potvrda sadrži jedinstveni interni serijski broj opozvane potvrde te vrijeme i datum opoziva.

7.2.1 Verzija

(1) Registar opozvanih potvrda je u skladu s ITU-T preporukom za X.509 (2005) i ISO/IEC 9594-8:2014.

(2) Registar opozvanih potvrda je trajno dostupan u javnom imeniku potvrda (vidjeti tačku 2.3):

- putem LDAP protokola i
- putem HTTP protokola.

7.2.2 Sadržaj i proširenja registra

(1) Registar opozvanih potvrdaa, pored ostalih podataka u skladu s preporukom X.509, sadrži (osnovna polja i proširenja detaljnije su prikazana u tabeli ispod):

- Identifikacijske oznakei opozvanih potvrda i
- vrijeme i datum opoziva.

7.2.2.1 Registar opoziva korijenskih (Root) potvrda (CRL podređenih ili intermediate potvrda)

Naziv polja	Vrijednost ili značenje
Osnovna polja u CRL	
Verzija, engl. Version	V2
Algoritam potpisa, engl. Signature Algorithm	G1: Sha256RSA
	G2: RSASSA-PSS
	G3: RSASSA-PSS
Potpis pružatelja usluga od od povjerenja, engl. Signature	Potpis Halcom CA
Prepoznatljivo ime pružatelja usluga povjerenja, engl. Issuer	G1: CN = Halcom Root Certificate Authority 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI

	G2: CN = Halcom Root CA G2 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
	G3: CN = Halcom Root CA G3 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Vrijeme izdavanja CRL, engl. thisUpdate	Effective date: <vrijeme izdavanja po GMT>
Vrijeme izdavanja sljedeće CRL, engl. nextUpdate	Next Update:: <vrijeme sljedećeg izdanja po GMT>
identifikacijske oznake opozvanih potvrda i vrijeme opoziva, engl. revokedCertificate	Serial Number: <identifikacijska oznaka opozvane digitalne potvrde> Revocation Date: <vrijeme opoziva po GMT>
X.509v2 CRL ekstenzije	
Broj CRL liste, engl. CRL number	Redni broj CRL liste
Identifikator ključa pružatelja usluga od povjerenja, engl. Authority Key Identifier (OID 2.5.29.35)	G1: Halcom Root Certificate Authority: KeyID=42aea643c79828b0
	G2: Halcom Root CA G2: KeyID=4e14b2790896f4b6
	G3: Halcom Root CA G3: KeyID= 4ba6657603985167
engl. issuerAltName (OID 2.5.28.18)	Ne koristi se
engl. deltaCRLindicator (OID 2.5.29.27)	Ne koristi se
engl. issuingDistribuitionPoint (OID 2.5.29.28)	Ne koristi se

7.2.2.2 Podređene (intermediate) opozvane potvrde (CRL korisničkih potvrda)

Naziv polja	Vrijednost ili značenje
Osnovna polja u CRL	
Verzija, engl. Version	V2
Algoritam potpisa, engl. Signature Algorithm	G1: Sha256RSA
	G2: RSASSA-PSS
	G3: RSASSA-PSS
Potpis pružatelja usluga od od povjerenja, engl. Signature	Potpis Halcom CA
Prepoznatljivo ime pružatelja usluga od povjerenja, engl. Issuer	prepoznatljivo ime izdavatelja, pogledajte tačke 3.1.1 i 7.1.2.2.

Vrijeme izdavanja CRL, engl. thisUpdate	Effective date: <vrijeme izdavanja po GMT>
Vrijeme izdavanja sljedeće CRL, engl. nextUpdate	Next Update:: <vrijeme sljedećeg izdanja po GMT>
identifikacijske oznake opozvanih potvrda i vrijeme opoziva, engl. revokedCertificate	Serial Number: <identifikacijska oznaka opozvane digitalne potvrde> Revocation Date: <vrijeme opoziva po GMT>
X.509v2 CRL ekstenzije	
Broj CRL liste, engl. CRL number	Redni broj CRL liste
Identifikator ključa pružatelja usluga od povjerenja, engl. Authority Key Identifier (OID 2.5.29.35)	G1: Halcom CA PO e-signature 1: KeyID=40f695209b79c209 Halcom CA PO e-signature 2: KeyID=434d32751603c975 Halcom CA PO e-seal 1: KeyID=49487650770ab10c Halcom CA PO e-seal 2: KeyID=4735c8bc61e25d9e Halcom CA web 1: KeyID=48420b17edae9e70 Halcom CA web 2: KeyID=408cacc9cbc74c1f
	G2: Halcom CA PO e-sig 1 G2: KeyID=41753bf986c7cb9c Halcom CA e-seal 1 G2: KeyID=4125fcd8fad6662f Halcom CA web 1 G2: KeyID=4e9125213b702aca
	G3: Halcom CA PO e-sig 1 G3: KeyID=46b69ca3e4fa428d Halcom CA e-seal 1 G3: KeyID=462d8ba5e3c50364 Halcom CA web 1 G3: KeyID=4a4af4272960b712
engl. issuerAltName (OID 2.5.28.18)	Ne koristi se
engl. deltaCRLindicator (OID 2.5.29.27)	Ne koristi se
engl. issuingDistribuitionPoint (OID 2.5.29.28)	Ne koristi se

7.2.3 Objavljivanje registra opozvanih potvrda

Halcom CA objavljuje registar u javnom imeniku na serveru ldap://ldap.halcom.si koristeći LDAP protokol i http://domina.halcom.si/crls koristeći HTTP protokol.

7.3. Profil provjere statusa potvrda u stvarnom vremenu

(1) Provjera statusa digitalnih potvrda u realnom vremenu dostupna je na http://ocsp.halcom.si

(2) Profil OCSP poruke (zahtjev/odgovor) za uslugu provjere statusa potvrda u realnom vremenu je u skladu s IETF RFC preporukom.

7.3.1 Verzija provjere statusa u stvarnom vremenu

Pružatelj usluga od povjerenja Halcom CA koristi OCSP verziju 1 poruka u skladu s IETF RFC preporukom.

7.3.2 Profil provjere statusa u stvarnom vremenu

OCSP (Zahtjev/Odgovor) poruke za provjeru statusa potvrda u stvarnom vremenu podržavaju Nonce ekstenziju koja nije označena kao kritična.

8. NADZOR

(1) Halcom CA ima internog kontrolora sa odgovarajućim tehnološkim i pravnim znanjem koji ne obavlja zadatke vezane za upravljanje potvrdama.

(2) Službenik za internu kontrolu vrši nadzor nad radom Halcom CA. U slučaju uočenih nedostataka, nalaže odgovarajuće mjere za otklanjanje tih nedostataka, koje je Halcom CA dužan provesti, te nadzire provođenje naloženih mjera.

(3) Halcom CA podliježe eksternoj nezavisnoj reviziji jednom godišnje, koju provodi Akreditovano tijelo.

(4) Svi relevantni ETSI standardi dostupni su na web stranici Halcom CA.

8.1. Učestalost kontrole

(1) Službenik za internu kontrolu mora izvršiti kontrolu najmanje jednom godišnje.

(2) Vanjski revizor za ISO 9001 i ISO 27001 provodi reviziju jednom godišnje.

(3) Službenik za vanjski nadzor provodi reviziju poslovanja u skladu sa ETSI standardima jednom godišnje.

8.2. Vrsta i kvalifikovanost nadzora

(1) Službenik za internu kontrolu posjeduje odgovarajuće tehnološko i pravno znanje.

(2) Službenik za vanjsku kontrolu posjeduje odgovarajuće tehnološko i pravno znanje.

8.3. Nezavisnost nadzora

(1) Službenik za internu kontrolu ne obavlja zadatke vezane za upravljanje potvrdama.

(2) Službenik za vanjsku kontrolu ne obavlja zadatke vezane za upravljanje potvrdama.

8.4. Područja kontrole

Područja kontrole su navedena u internim pravilima pružatelja usluga od povjerenja Halcom CA.

8.5. Mjere pružatelja usluga povjerenja

U slučaju utvrđenih nedostataka ili grešaka, službenik interne/eksterne kontrole nalaže odgovarajuće mjere za otklanjanje tih nedostataka, koje je Halcom CA dužan provesti, te nadzire provođenje naloženih mjera. Provođenje mjera detaljno je precizirano u internim pravilima pružatelja usluga od povjerenja Halcom CA.

8.6. Objavljivanje rezultata kontrole

Rezultati kontrola se čuvaju kod pružatelja usluga od povjerenja Halcom CA.

9. FINANSIJSKA I DRUGA PRAVNA PITANJA

9.1. Cjenovnik

Halcom CA utvrđuje cjenovnik za korištenje potvrda, svojih usluga, potrebne opreme i infrastrukture i objavljuje cjenovnik na svojoj web stranici.

9.1.1 Cijena izdavanja i obnavljanja potvrda

Cijena izdavanja i obnavljanja potvrda određena je važećim cjenovnikom.

9.1.2 Cijena pristupa potvrdama

(1) Pristup javnom imeniku potvrda je besplatan, osim ako se stranke ne dogovore drugačije.

(2) Cijena korištenja i potpisivanja potvrda u cloudu određena je važećim cjenovnikom ili ugovorom.

9.1.3 Cijena pristupa statusu potvrda i registru opozvanih potvrda

Registar opozvanih potvrda dostupan je besplatno svim osobama.

9.1.4 Cijene ostalih usluga

Cijene za ostale usluge, opremu i infrastrukturu određene su važećim cjenovnikom.

9.1.5 Povrat troškova

Nije propisano.

9.2. Finansijska odgovornost

9.2.1 Osiguranje

Halcom CA ima odgovarajuće osiguranje od odgovornosti. Detaljnije informacije objavljene su na web stranici.

9.2.2 Ostalo pokriće

Nije propisano.

9.2.3 Osiguranje imaoca

Nije propisano.

9.3. Zaštita poslovnih podataka

9.3.1 Zaštićeni podaci

(1) Pružatelj usluga od povjerenja Halcom CA sljedeće podatke tretira povjerljivo:

- sve zahtjeve za dobijanje potvrda ili drugih usluga,

- sve povjerljive informacije koje se odnose na finansijske obaveze,
- bilo koje povjerljive informacije koje su predmet međusobnog ugovora s trećim licima, i
- sva ostala pitanja koja su uključena u interna pravila poslovanja pružatelja usluga od povjerenja Halcom CA u skladu s Uredbom.

(2) Pružatelj usluga povjerenja Halcom CA obrađuje sve potencijalno povjerljive informacije o poslovnim subjektima, imaocima i trećim licima koje su nužno potrebne za usluge upravljanja potvrdama u skladu s važećim zakonodavstvom.

9.3.2 Nezaštićeni podaci

Pružatelj usluga od povjerenja Halcom CA javno objavljuje samo poslovne informacije koje nisu povjerljive u skladu s važećim zakonom.

9.3.3 Odgovornost za sigurnost

(1) Halcom CA ne preuzima nikakvu odgovornost za sadržaj podataka koje imaoc potvrde elektronski šifrira ili potpisuje, čak i ako je imaoc ili treće lice postupio u skladu sa svim važećim propisima, svim odredbama ove politike i drugim pravilima Halcom CA ili je slijedio sva njegova uputstva.

(2) Halcom CA ne preuzima nikakvu odgovornost za posljedice koje proizlaze iz nepoštivanja sigurnosnih zahtjeva od strane imaoca potvrda navedenih u tački 4.5.1 ove politike.

9.4. Zaštita ličnih podataka

9.4.1 Plan zaštite ličnih podataka

Halcom CA pažljivo štiti lične podatke u skladu s važećim evropskim i slovenačkim propisima, međunarodnim standardima i preporukama, redovno provodi pisane procjene uticaja i osigurava privatnost već zadanim postavkama. U Halcom d.d. radi ovlaštenik za privatnost kao službena osoba za zaštitu podataka.

9.4.2 Zaštićeni lični podaci

Zaštićeni podaci su svi lični podaci koje pružalac usluga od povjerenja Halcom CA prikupi u zahtjevima za svoje usluge ili u relevantnim registrima radi dokazivanja identiteta imaoca ili tokom pružanja usluga povjerenja.

Zbog prirode upotrebe potvrda i odredbi važećih propisa i standarda, podaci u potvrdama i registru opozvanih potvrda dostupni su trećim licima koje se oslanjaju na potvrde ili provjeravaju njihovu validnost.

9.4.3 Nezaštićeni lični podaci

Ne postoje drugi potencijalno nezaštićeni lični podaci osim onih navedenih u potvrdi i registru opozvanih potvrda.

9.4.4 Odgovornost za zaštitu ličnih podataka

Pružatelj usluga od povjerenja Halcom CA odgovoran je za zaštitu podataka u skladu s važećim propisima o zaštiti podataka i odredbama internog Pravilnika o zaštiti podataka.

9.4.5 Ovlaštenje u vezi s korištenjem ličnih podataka

Imaoc ovlašćuje pružaoca usluga od povjerenja Halcom CA da koristi lične podatke na zahtjevu za dobijanje potvrda, posebnu pisanu saglasnost za obradu ličnih podataka ili za druge slučajeve kasnije u drugom pisanom obliku.

9.4.6 Prosljeđivanje ličnih podataka

(1) Pružatelj usluga od povjerenja Halcom CA ne daje druge podatke o imaocima potvrda koji nisu navedeni u potvrdi, osim ako su određeni podaci posebno potrebni za obavljanje specifičnih usluga ili aplikacija vezanih za potvrde i pružatelj usluga od povjerenja Halcom CA je za to ovlašten (vidjeti prethodni tačku), ili na zahtjev nadležnog suda, prekršajnog organa, organa za provođenje zakona, upravnog organa ili druge ovlaštene osobe. Halcom CA pažljivo provjerava svaki takav zahtjev i daje podatke samo u mjeri u kojoj je to potrebno, kako je određeno važećim propisima.

(2) Podaci se daju bez pismene saglasnosti samo u slučajevima kada to predviđaju važeći evropski ili slovenački propisi sa zakonskom snagom.

9.4.7 Ostale odredbe u vezi sa zaštitom ličnih podataka

Nisu propisani.

9.5. Odredbe o pravima intelektualnog vlasništva

Odredbe vezane za autorska prava, srodna i druga prava intelektualnog vlasništva:

- Sva prava na privatnom ključu pripadaju imaocu potvrde,
- Na javnim ključevima, svi podaci na potvrdi, na direktoriju potvrda i registru opozvanih potvrda, te ova politika pripadaju Halcom CA.

9.6. Obaveze i odgovornosti

9.6.1 Obaveze i odgovornosti pružatelja usluga povjerenja Halcom CA

(1) Pružalac usluga od povjerenja Halcom CA je dužan:

- postupati u skladu sa svojim internim pravilima i drugim važećim propisima i zakonima,
- postupati u skladu s međunarodnim preporukama,
- objaviti sve važne dokumente koji određuju njegovo poslovanje (operativne politike, zahtjeve, cjenovnik, upute za sigurno korištenje kvalifikovanih digitalnih potvrda itd.),
- objaviti na svojim web stranicama sve informacije o promjenama u vezi s aktivnostima pružatelja usluga od povjerenja koje na bilo koji način utječu na imaoce potvrda i treća lica,
- osigurati rad prijavnih službi u skladu s odredbama HALCOM CA i drugim važećim propisima,
- pridržavati se odredbi o sigurnom rukovanju ličnim, poslovnim i povjerljivim podacima o pružaocu usluga od povjerenja, imaocima potvrda ili trećim licima,
- opozvati potvrdu i objaviti opozvanu potvrdu u registru opozvanih potvrda kada utvrdi da

su dati razlozi u skladu s ovom politikom ili drugim važećim propisima,

- izdati kvalifikovane digitalne potvrde u skladu s ovom politikom i drugim propisima i preporukama.

(2) Pružalac usluga od povjerenja Halcom CA je dužan:

- osigurati tačnost podataka u izdatim potvrdama,
- osigurati ispravnu objavu registra opozvanih potvrda,
- osigurati jedinstvenost prepoznatljivih imena,
- osigurati odgovarajuću fizičku sigurnost prostorija i pristup prostorijama pružatelja usluga od povjerenja,
- kao odgovoran upravitelj, osigurati nesmetan rad i maksimalnu dostupnost usluge,
- kao odgovoran upravitelj, osigurati da su usluge što dostupnije,
- kao odgovoran upravitelj, brinuti se o nesmetanom radu svih ostalih pratećih službi,
- pokušati riješiti nastale probleme što je bolje moguće i u najkraćem mogućem roku,
- voditi računa o optimizaciji hardvera i softvera i
- informirati korisnike o važnim stvarima i
- ispunjavati sve ostale zahtjeve u skladu s ovom politikom.

(3) Pružatelj usluga od povjerenja Halcom CA osigurava najveću moguću dostupnost svojih usluga, sve dane u godini, osim u sljedećim slučajevima:

- planirane i 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 pružatelja usluga od povjerenja Halcom CA i
- nedostupnost kao rezultat više sile ili vanrednih događaja.

(4) Pružatelj usluga od povjerenja Halcom CA mora najaviti radove na održavanju ili nadogradnju infrastrukture najmanje tri (3) dana prije početka radova.

(5) Pružatelj uslugaod povjerenja Halcom CA odgovoran je za sve izjave u ovom dokumentu i za provedbu svih odredbi ove politike.

(6) Ostale obaveze ili odgovornosti pružatelja usluga od povjerenja Halcom CA utvrđuju se eventualnim međusobnim ugovorom s trećim licem.

9.6.2 Obaveza i odgovornost prijavne službe

(1) Prijavna služba je dužna:

- provjeriti identitet imaoca ili budućih imaoca,
- primiti zahtjeve za usluge Halcom CA,

- provjeriti zahtjeve,
- izdati potrebnu dokumentaciju poslovnim subjektima, imaocima ili budućim imaocima,
- proslijediti zahtjeve i ostale podatke na siguran način u Halcom CA.

(2) Prijavna služba je odgovorna za sprovođenje svih odredbi ove politike i drugih zahtjeva dogovorenih sa pružateljem usluga od povjerenja Halcom CA.

9.6.3 Obaveze i odgovornost imaoca potvrda

(1) Poslovni subjekt odgovara za:

- šteta nastala u slučaju zloupotrebe potvrde od obavještenja o opozivu do opoziva,
- bilo kakvu štetu uzrokovanu direktno ili indirektno dozvoljavanjem korištenja ili zloupotrebe potvrde imaoca od strane neovlaštenih osoba,
- bilo kakvu drugu štetu nastalu zbog nepoštivanja odredbi ove politike i drugih obavještenja od strane Halcom CA i važećih propisa.

(2) Obaveze imaoca u vezi s korištenjem potvrda utvrđene su u tački 4.5.1.

9.6.4 Obaveze i odgovornost trećih lica

(1) Prilikom prve upotrebe Halcom CA potvrde u skladu s ovom politikom, treće lice koje se oslanja na potvrdu mora pažljivo pročitati ovu politiku i redovno pratiti sva obavještenja od Halcom CA od tada nadalje.

(2) Treće lice mora uvijek pažljivo provjeriti, prilikom korištenja potvrde, da li se potvrda nalazi u registru opozvanih potvrda.

(3) Ako potvrda sadrži podatke o trećem licu, treće lice je dužno zatražiti opoziv potvrde ako sazna da je privatni ključ kompromitovan na način koji utiče na pouzdanost korištenja, ili ako postoji rizik od zloupotrebe, ili ako su se podaci navedeni u potvrdi promijenili.

(4) Treće lice se može pozivati na takvu potvrdu sve dok se ona ne opozove.

(5) Treće lice može u bilo kojem trenutku zatražiti sve informacije u vezi s validnošću bilo koje izdane potvrde, odredbama ove politike i obavještenjima Halcom CA.

9.6.5 Obaveze i odgovornost drugih osoba

Nije propisano .

9.7. Ograničenje odgovornosti

Pružatelj usluga od povjerenja Halcom CA ne odgovara za bilo kakvu štetu nastalu usljed:

- korištenja potvrda u svrhu i na način koji nije izričito predviđen ovom politikom,
- nepravilne ili neadekvatne zaštite lozinki ili privatnih ključeva imaoca, izdavanje povjerljivih podataka ili ključeva trećim licima i neodgovorno ponašanje imaoca,
- zloupotreba ili upad u informacioni sistem imaoca potvrde, a time i u podatke potvrde, od strane neovlaštenih osoba,

- nefunkcionalnost ili loše funkcionisanje informacione infrastrukture imaoca potvrde ili trećih lica,
- neprovjeravanje podataka i validnosti potvrda u registru opozvanih potvrda,
- neprovjeravanje roka važenja potvrda,
- radnji imaoca potvrda ili trećih lica koja krše obavještenja, politike i druge propise Halcom CA,
- omogućavanja korištenja ili zloupotrebe potvrda imaoca od strane neovlaštenih osoba,
- Izdavanja potvrde s netačnim ili nepouzdanim podacima ili drugim radnjama imaoca ili pružatelja usluga povjerenja,
- korištenja potvrda i važenja potvrda u slučaju promjena podataka potvrda, elektroničkih adresa ili promjene imena imaoca,
- ispada infrastrukture koji nije u domenu upravljanja pružatelja usluga od povjerenja Halcom CA,
- podataka koji su šifrirani ili potpisani pomoću potvrda,
- ponašanja imaoca prilikom korištenja potvrda, čak i ako je imaoc ili treće lice postupilo u skladu sa svim odredbama ove politike, obavještenjima Halcom CA ili drugim važećim propisima,
- korištenja i pouzdanosti hardvera i softvera imaoca potvrde ,
- greške u izračunu hash vrijednosti, provjeri ove vrijednosti ili drugim sigurnosnim procedurama u vezi s potpisivanjem elektronskog dokumenta, ako je imaoc zatražio potpis u cloudu isključivo na osnovu hash vrijednosti, a bez dostavljanja cijelog elektronskog dokumenta pružatelju usluga od povjerenja Halcom CA.

9.8. Ograničenje upotrebe

Nije propisano.

9.9. Naplata štete

Strana odgovorna za bilo kakvu štetu uzrokovanu nepoštivanjem odredbi ove politike i važećeg zakonodavstva snosi odgovornost.

9.10. Važenje politike

(1) Halcom CA zadržava pravo da promijeni svoju operativnu politiku i nadogradi svoju infrastrukturu bez prethodne najave imaocima potvrda. Važeće potvrde ostat će važećedo datuma isteka i nastavit će podlijegati operativnoj politici koja je bila na snazi u vrijeme njihovog izdavanja. Svepotvrde izdane nakon stupanja na snagu nove politike podliježu novoj politici.

(2) Ova politika stupa na snagu danom usvajanja od strane Halcom CA.

9.10.1 Period važenja

(1) Nova verzija ili izmjena politike pružatelja usluga od povjerenja Halcom CA objavljuje se na web stranici pružatelja usluga povjerenja Halcom CA osam (8) dana prije stupanja na snagu, pod novim identifikacijskim brojem (CP $_{OID}$) i datumom stupanja na snagu.

(2) Kraj važenja politike nije fiksan i vezan za važenje potvrda izdatih u skladu s politikom.

9.10.2 Kraj važenja politike

(1) Po objavljivanju nove politike, one odredbe koje se ne mogu razumno zamijeniti odgovarajućim odredbama nove politike (na primjer, postupak kojim se utvrđuje način na koji je ovaj potvrda izdana itd.) ostat će na snazi za sve potvrde izdane u skladu s ovom politikom.

(2) Pružatelj usluga povjerenja može izdati izmjene pojedinačnih odredbi primjenjive politike, kako je navedeno u članu 9.12.

9.10.3 Posljedice isteka politike

(1) Po izdavanju nove politike, sve kvalifikovane digitalne potvrde izdane nakon tog datuma tretirat će se prema novoj politici.

(2) Nova politika ne utiče na važenje potvrda izdatih prema prethodnim politikama. Takve potvrde će ostati važeće do kraja perioda važenja i, gdje je to moguće, bit će tretirane prema novoj politici.

9.11. Komunikacija između subjekata

(1) Kontaktni podaci pružatelja usluga od povjerenja objavljeni su na web stranici i navedeni su u tački 1.3.1.

(2) Kontaktni podaci imaoca potvrde navedeni su u zahtjevima koji se odnose na potvrde.

(3) Kontaktni podaci trećih lica navedeni su u svakom međusobnom ugovoru između trećeg lica i pružatelja usluga od povjerenja Halcom CA.

9.12. Izmjene i dopune

9.12.1 Postupak za prihvatanje izmjena i dopuna

(1) Izmjene ili dopune ove politike može objaviti pružatelj usluga povjerenja u obliku izmjena i dopuna ove politike, pod uslovom da ne uključuju značajne promjene u poslovanju pružatelja usluga od povjerenja.

(2) Izmjene se usvajaju u skladu s istim postupkom kao i politika.

(3) Ako promjene i dopune značajno utiču na rad pružatelja usluga od povjerenja, nadležno ministarstvo će biti obaviješteno u skladu s istim postupkom kao i za politiku.

(4) Način označavanja dodataka određuje pružatelj usluga od povjerenja Halcom CA.

9.12.2 Važenje i objavljivanje izmjena i dopuna

(1) Pružatelj usluga povjerenja Halcom CA određuje početak i kraj važenja izmjena i dopuna.

(2) Izmjene i dopune bit će objavljene na web stranici Halcom CA osam (8) dana prije stupanja na snagu.

9.12.3 Promjena identifikacijskog broja politike

Ako usvojene izmjene i dopune utiču na korištenje potvrda, tada pružatelj usluga od povjerenja Halcom CA može dodijeliti novi identifikacijski kod politike (CP $_{OID}$) ili izmjene i dopune.

9.13. Postupak rješavanja sporova

(1) Sve pritužbe imaoca potvrda rješavat će službenik za privatnost i usklađenost s propisima.

(2) Sve sporove između imaoca potvrda ili trećih lica i Halcom CA rješava nadležni sud u Ljubljani.

9.14. Primjenjivo zakonodavstvo

Na odluke o ovoj politici primjenjuje se pravo Evropske unije i Republike Slovenije.

9.15. Usklađenost s važećim zakonodavstvom

(1) Nadzor nad usklađenošću poslovanja pružatelja usluga od povjerenja Halcom CA s važećim propisima provode nadležni inspektorat i akreditirana tijela za ocjenjivanje usklađenosti.

(2) Akreditovano tijelo za ocjenjivanje usklađenosti dužno je da revidira pružaoca usluga od povjerenja Halcom CA najmanje svaka 24 mjeseca. Svrha revizije je da se potvrdi da li kvalifikovani pružalac usluga od povjerenja i kvalifikovane usluge od povjerenja koje on pruža ispunjavaju zakonske zahtjeve.

(3) Interne provjere usklađenosti provode ovlaštene osobe unutar pružatelja usluga od povjerenja Halcom CA.

9.16. Opće odredbe

(1) Pružatelj usluga od povjerenja Halcom CA može sklapati međusobne ugovore s drugim subjektima ako je to određeno važećim zakonodavstvom ili drugim propisima.

(2) Ako bilo koja odredba ove politike jeste ili postane nevažeća, to neće uticati na preostale odredbe. Nevažeća odredba će biti zamijenjena važećom, koja će biti što bliža svrsi koju je nevažeća odredba namjeravala postići.

9.17. Ostale odredbe

Nisu propisani.

Mjesto i datum:
Ljubljana, 20.5.2026.

Izvršni direktor:
Gregor Pelhan