Pripremio: Luka RIBIČIČ

Broj dokumenta: 400085-8-12/17

Politika Halcom CA: Opšta pravila rada - CPS

Izdanje: 12

Politika Halcom CA

Opšta pravila rada - CPS
(Certificate Practise Statement)

Dokument važi od: 15.6.2026.

Izdanje	broj dokumenta i priloga	Opis promjene	Autor	Datum posljednje izmjene
1	400085-8-1/17	Početno izdanje	L. Ribičič	3.1.2011.
2	4000851-8-2/17	Dodaci EIDAS-u	L. Ribičič	24.4.2017.
3	400085-8-3/17	Godišnji pregled dokumenata – bez promjena	S. Lazić	1.6.2018.
4	400085-8-4/17	Godišnji pregled dokumenata, novi korporativni identitet, dodatak za cloud potvrde	L. Ribičič	24.5.2019.
5	400085-8-5/17	Dodavanje identifikatora, osnovni kapital, identifikacija, raspodjela koda	S. Lazić	29.4.2020.
6	400085-8-6/17	Dopunjavanje profila potvrda krajnjeg korisnika (Neporicanje)	S. Lazić	3.2.2021.
7	400085-8-7/17	Godišnji pregled dokumenata, kojim se dopunjuje postupak izdavanja potvrda i istaknutih imena	S. Lazić	21.5.2021.
8	400085-8-8/17	Godišnji pregled dokumenata, uklanjanje faksa, produženje važenja potvrda u cloudau	S. Lazić	13.4.2022.
9	400085-8-9/17	Godišnji pregled dokumenata, novi privremeni potvrdai, vrijeme i period čuvanja	S. Lazić	23.5.2023.
10	400085-8-10/17	Godišnji pregled dokumenata, EŠEI	L. Ribičič	22.5.2024.
11	400085-8-11/17	Promjena u strukturi CPS-a, dodane Halcom CA potvrde druge generacije, ujedinjenje politika	L. Ribičič	22.5.2025.
12	400085-8-12/17	Nova CA generacija – G3, OT potvrde, e-pečat potvrde u cloudu	L.Ribičič	20.5.2026.

Sadržaj

1. UVOD

(1) Ovaj dokument predstavlja Opšta pravila poslovanja (u daljem tekstu: CPS (engl. Certificate Practise Statement)) pružaoca usluga od povjerenja u oblasti elektronskog potpisa, elektronskog pečata, elektronskog vremenskog žigosanja, validacije i drugih usluga.

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

(3) Sve odredbe CPS-a u vezi s ponašanjem Halcom CA su na odgovarajući način transponirane i dalje definirane u odredbama internih pravila. To su povjerljivi dokumenti koji definiraju infrastrukturu, odredbe u vezi s osobljem Halcom CA (kompetencije, zadaci, ovlaštenja i potrebni uvjeti koje pojedinačni članovi osoblja moraju ispunjavati), fizička sigurnost (pristup prostorijama, rukovanje hardverom i softverom), sigurnost softvera (postavke sigurnosti servera, sigurnosne kopije itd.) i interna kontrola (kontrola fizičkog pristupa, ovlaštenja itd.).

1.1. Pregled

(1) CPS predstavlja opšta pravila rada pružaoca usluga od povjerenja HALCOM CA za izdavanje potvrda, reguliše svrhu, rad i metodologiju upravljanja potvrdama i sigurnosne zahtjeve koje moraju ispunjavati pružalac usluga od povjerenja HALCOM CA, imaoci i treća lica koje se oslanjaju na ove potvrde, te odgovornosti svih navedenih osoba.

(2) Halcom CA je pružatelj sljedećih usluga:

- Izdavanje i potvrđivanje validnosti potvrda za elektronske potpise, potvrda za elektronske pečate, potvrda za autentifikaciju web stranica ili potvrda za pružanje drugih usluga od povjerenja,
- kreiranje i potvrđivanje validnsti elektronskih potpisa ili elektronskih pečata,
- pohranjivanje potvrda za elektronske potpise ili potvrda za elektronske pečate,
- upravljanje uređajima za daljinsko generisanje elektronskih potpisa ili uređajima za daljinsko generisanje elektronskih pečata;
- izdavanje i potvrđivanje elektronskih potvrda o atributima,
- kreiranje i potvrđivanje validnosti elektronskih vremenskih žigova.

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

(4) Halcom CA izdaje:

- kvalifikovane digitalne potvrde za elektronske potpise,
- kvalifikovane digitalne potvrde za elektronsko pečatiranje,
- kvalifikovane digitalne potvrde za autentifikaciju web stranica,
- kvalifikovane digitalne potvrde o atributima,
- kvalifikovane digitalne potvrdeza vremensko žigosanje.

(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 porodicom standarda ISO/IEC i drugim srodnim standardima.

(6) Halcom CA objavljuje popis prijavnih službi koje omogućavaju nabavku potvrda na internetu.

1.1.1 Osnovni dokumenti pružatelja usluga od povjerenja Halcom CA

Detaljnija pravila, uslovi, te prava i obaveze u vezi sa radom pružatelja usluga povjerenja Halcom CA opisani su u sljedećim javnim dokumentima:

- Politika Halcom CA za EU kvalifikovane digitalne potvrde za pravna lica,
- Politika Halcom CA za EU kvalifikovane digitalne potvrde za fizička lica,
- Politika Halcom CA za EU kvalifikovano vremensko žigosanje,
- Opšta pravila rada - CPS.

1.1.2 Veze između osnovnih dokumenata pružatelja usluga od povjerenja Halcom CA

(1) Politika definiše poslovne zahtjeve pružaoca usluga od povjerenja, a Opšta pravila poslovanja (u daljem tekstu: CPS) definišu operativne procese za ispunjavanje tih zahtjeva. CPS definiše način na koji pružalac usluga od povjerenja osigurava tehničke, organizacijske i procesne poslovne zahtjeve definirane u Politici Halcom CA.

(2) U poređenju sa CPS-om, politika je uopšteniji dokument. CPS predstavlja detaljniji opis načina na koji pružalac usluga od povjerenja Halcom CA posluje, poslovnih i operativnih procesa za izdavanje i upravljanje potvrdama.

(3) Politika se definiše nezavisno od specifične operativne jedinice pružaoca usluga od povjerenja, dok opšta pravila poslovanja predstavljaju detaljan opis organizacione strukture i operativnih procesa pružaoca usluga od povjerenja Halcom CA.

1.1.3 Standardi

Halcom CA izdaje potvrde i obavlja druge aktivnosti kao pružatelj usluga od povjerenja u skladu s važećim pravnim poretkom Republike Slovenije i Europske unije, te u skladu s tehničkim zahtjevima ETSI-ja, IETF RFC standarda i porodice standarda ISO/IEC i drugih srodnih standarda.

1.1.4 Interna pravila Halcom CA

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

(2) Interna pravila su povjerljivi dokumenti i predstavljaju poslovnu tajnu pružatelja usluga od povjerenja Halcom CA.

(3) Interna pravila moraju sadržavati detaljne odredbe o:

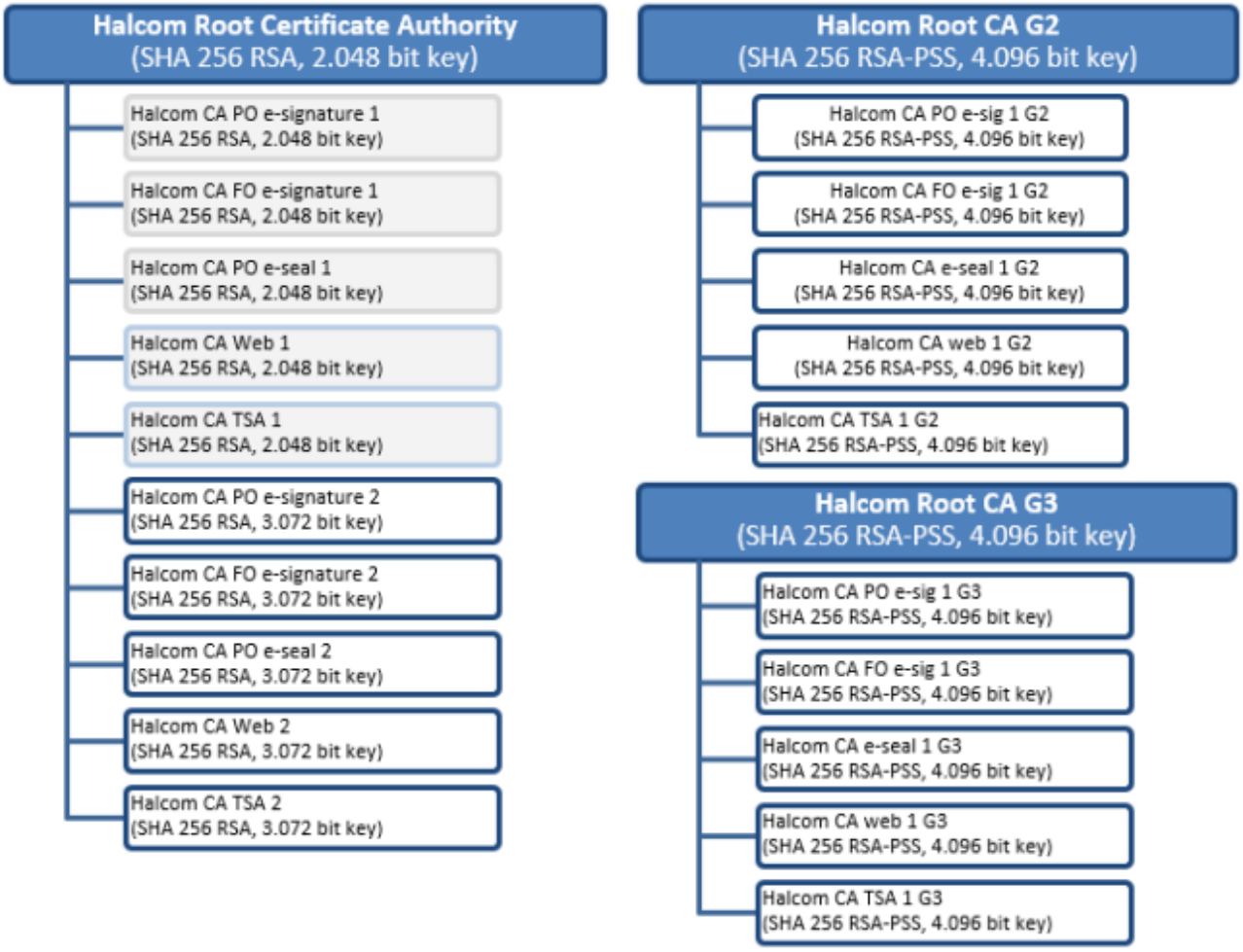
- sistemu za kontrolu fizičkog pristupa u prostorije Halcom CA

- sistemu logičke kontrole pristupa računarskoj mreži Halcom CA,
- sistemu zaštite privatnih ključeva Halcom CA,
- sistemu distribuirane odgovornosti za aktiviranje privatnih ključeva Halcom CA,
- procedurama i osoblju uključenom u pružanje usluga od povjerenja,
- postupcima u nepredviđenim okolnostima (požar, poplava, zemljotres, upad u prostorije ili informacioni sistem pružaoca usluga od povjerenja).

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

1.2. Pružatelj usluga od povjerenja Halcom CA

(1) Struktura Halcom CA (prva i druga generacija):



(2) Halcom CA je odgovoran za izdavanje sljedećih korijenskih (root) digitalnih potvrda.

Naziv potvrda	Svrha upotrebe	Generacija
Halcom Root Certificate Authority	Izdavanje među/podređenih potvrda	G1
Halcom Root CA G2	Izdavanje među/podređenih potvrda	G2

Halcom Root CA G3	Izdavanje među/podređenih potvrda	G3

G3(3) Halcom CA je odgovoran za izdavanje sljedećih među/podređenih (intermediate) potvrda.

Naziv potvrda	Svrha upotrebe	Generacija
Halcom CA FO e-signature 1	Izdavanje potvrda za e-potpis za fizička lica	G1
Halcom CA FO e-signature 2	Izdavanje potvrda za e-potpis za fizička lica	G1
Halcom CA PO e-signature 1	Izdavanje potvrda za e-potpis za pravna lica	G1
Halcom CA PO e-signature 2	Izdavanje potvrda za e-potpis za pravna lica	G1
Halcom CA PO e-seal 1	Izdavanje potvrda za e-pečat za pravna lica	G1
Halcom CA PO e-seal 2	Izdavanje potvrda za e-pečat za pravna lica	G1
Halcom CA web 1	Izdavanje potvrda za autentifikaciju web stranice	G1
Halcom CA web 2	Izdavanje potvrda za autentifikaciju web stranice	G1
Halcom CA TSA 1	Izdavanje potvrda za vremenski pečat	G1
Halcom CA TSA 2	Izdavanje potvrda za vremenski pečat	G1
Halcom CA FO e-sig 1 G2	Izdavanje potvrda za e-potpis za fizička lica	G2
Halcom CA PO e-sig 1 G2	Izdavanje potvrda za e-potpis za pravna lica	G2
Halcom CA e-seal 1 G2	Izdavanje potvrda za e-pečat za pravna lica	G2
Halcom CA web 1 G2	Izdavanje potvrda za autentifikaciju web stranice	G2
Halcom CA TSA 1 G2	Izdavanje potvrda za vremenski pečat	G2
Halcom CA FO e-sig 1 G3	Izdavanje potvrda za e-potpis za fizička lica	G3
Halcom CA PO e-sig 1 G3	Izdavanje potvrda za e-potpis za fizička lica	G3
Halcom CA e-seal 1 G3	Izdavanje potvrda za e-pečat za pravna lica	G3
Halcom CA web 1 G2	Izdavanje potvrda za autentifikaciju web stranice	G3
Halcom CA TSA 1 G3	Izdavanje potvrda za vremenski pečat	G3

1.3. Subjekti

1.3.1 Pružatelj usluga od povjerenja Halcom CA

Halcom CA je pružatelj usluga od povjerenja koji izdaje i upravlja potvrdama za elektronske potpise, elektronski pečat, elektronski vremenski pečat, validaciju i druge usluge. 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 povjerenja obavlja sljedeće zadatke:

- Provjera identiteta fizičkih lica, pravnih lica, ovlaštenih predstavnika pravnih lica i drugih, za upravljanje potvrdama, važnim podacima,
- zaprimanje zahtjeva za dobijanje potvrda,
- zaprimanje zahtjeva za opoziv potvrda,
- izdavanje potrebne dokumentacije 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 uslova u skladu s važećim europskom i slovenskom regulativom te međunarodnim, europskim i slovenskim standardima i preporukama, kao i politikama, općim pravilima poslovanja i internim pravilima Halcom CA.

(3) Pružatelj usluga od povjerenja Halcom CA uspostavio je geografski raspršenu uslugu prijavnih službi, koja potencijalnim imaocima omogućava jednostavnu registraciju u 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) Naručioc/imaoc potvrda može biti fizičko lice ili poslovni subjekt (u zavisnosti od vrste potvrda).

Usluga	Izdavač	Naručioc	Imaoc
Potvrde za elektronski potpis	Halcom CA FO e-signature 1	Fizička osoba	Fizička osoba
	Halcom CA FO e-signature 2		
	Halcom CA FO e-sig 1 G2		
	Halcom CA FO e-sig 1 G3		
	Halcom CA PO e-signature 1	Pravno lice	Fizička osoba
	Halcom CA PO e-signature 2		
	Halcom CA PO e-sig 1 G2		
	Halcom CA PO e-sig 1 G3		
Potvrde za elektronski pečat	Halcom CA PO e-seal 1	Pravno lice	Uređaj ili server
	Halcom CA PO e-seal 2		
	Halcom CA e-seal 1 G2		

	Halcom CA e-seal 1 G3		
Potvrde za autentifikaciju web stranice	Halcom CA web 1	Pravno lice ili izuzetno fizičko lice	Uređaj ili server
	Halcom CA web 2		
	Halcom CA web 1 G2		
	Halcom CA web 1 G3		
Elektronske potvrde za vremenski pečat	Halcom CA TSA 1	Pružatelj usluga od povjerenja	Uređaj ili server
	Halcom CA TSA 2		
	Halcom CA TSA 1 G2		
	Halcom CA TSA 1 G3		

1.3.4 Treća lica

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

(2) Treća lica moraju slijediti upute pružatelja usluga od povjerenja Halcom CA i uvijek moraju provjeriti validnost potvrda, svrhu korištenja potvrda, period važenja potvrda 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 potvrdama za elektronske potpise, elektronsko pečatenje, autentifikaciju web stranica i vremenski pečat. Potvrde su namijenjene fizičkim i pravnim licima.

1.4.1 Ispravna upotreba potvrda i ključeva

(1) Potvrde za elektronski potpis/pečat namijenjene su za potpisivanje/pečatiranje jednostrane ili međusobne komunikacije između nositelja potvrda i za upotrebu u različitim primjenama i za različite svrhe koje se pojavljuju na tržištu. Između ostalog, potvrde se mogu koristiti u svrhe kao što su:

1) identifikacija imaoca,
2) dokaz identiteta imaoca,
3) potpisivanje/pečatiranje dokumenata u elektronskom obliku,
4) šifriranje i dešifriranje dokumenata u elektronskom obliku.

(2) Elektronski potpis/pečat može se koristiti u aplikacijama kao što su:

1) elektronsko ili mobilno bankarstvo,
2) aplikacije e-uprave ili m-uprave,
3) aplikacije za e-zdravlje ili m-zdravlje,
4) potpisivanje/pečatiranje elektronskih ili mobilnih obrazaca,
5) osigurano poslovanje s tijelima i organizacijama javnog sektora i s drugim pravnim ili fizičkim

licima,

6) druge aplikacije ili usluge koje zahtijevaju upotrebu potvrda,
7) kontrola pristupa .

(3) Potvrde za autentifikaciju web stranice namijenjene su za:

1) identifikacija web stranice,
2) dokazivanje identiteta web stranice,
3) kontrola pristupa,
4) uspostavljanje sigurnih veza.

(4) Sigurnosni vremenski pečati se koriste u raznim primjenama i za različite svrhe koje se pojavljuju na tržištu. Između ostalog, vremenski pečati se koriste u primjenama i svrhama kao što su:

1) elektronsko bankarstvo,
2) elektronsko skladištenje podataka, dokumentarnog ili arhivskog materijala,
3) aplikacije e-uprave,
4) druge primjene gdje je potrebno osigurati povezanost određene radnje ili činjenice s tačnim izvorom vremena.

1.4.2 Neovlaštena upotreba

(1) Zabranjeno je koristiti potvrde izdate u skladu s politikama na način suprotan odredbama politika ili važećih propisa, ili izvan opsega dozvoljene upotrebe navedene u prethodnom odjeljku.

(2) Potvrde nisu namijenjene za preprodaju.

1.5. Upravljanje dokumentima

1.5.1 Upravitelj dokumenata

(1) CPS-om i njegovim 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 općim pravilima i politikama poslovanja, 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 34 86

E-mail: ca@halcom.com

E-mail za opoziv : ca_preklici@halcom.si

1.5.3 Odgovorna osoba za usklađenost poslovanja pružatelja usluga od povjerenja Halcom CA s dokumentima

Ovlaštena lica pružatelja usluga povjerenja odgovorna su za usklađenost poslovanja pružatelja usluga od povjerenja Halcom CA sa CPS-om i politikama, u skladu sa svojim odgovornostima.

1.5.4 Postupak za prihvatanje dokumenata

(1) Svaki prijedlog za novi CPS podliježe tehnološkoj i pravnoj reviziji prije nego što ga odobri generalni direktor Halcom d.d., kako bi se osigurala zakonitost, sigurnost i kvalitet.

(2) Pružatelj usluga od povjerenja može izdati izmjene pojedinačnih odredbi 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).
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 (Izjava o praksi certificiranja) predstavlja opšta pravila poslovanja pružatelja usluga od povjerenja.
CPOID	Međunarodni broj koji jedinstveno identificira politiku certifikacije (Certification Policy Object IDentifier).
CRL	Lista opozvanih potvrda – lista opozvanih digitalnih potvrda.
DN	Jedinstveno prepoznatljivo ime (uporedi definiciju prepoznatljivog imena).
LDAP	Lightweight Directory Access Protocol je protokol koji definira pristup direktorijima i specificiran je prema preporuci IETF-a (Internet Engineering Task Force) IETF RFC 3494 .

S/MIME	Sigurna višenamjenska proširenja internet pošte
SSL	Sloj sigurnih utičnica
TLS	Sigurnost transportnog sloja
PKI	Infrastruktura javnog ključa je infrastruktura javnog ključa.
EŠEI	Jedinstveni elektronski identifikacijski broj
HSM	Modul hardverske sigurnosti.
G1, G2 ili G3	Prva, druga ili treća generacija Halcom CA root i podređenih potvrda.
QCert za ESig/ESeal	Kvalifikovana digitalne potvrda izdan na sigurnom mediju (QSCD – Qualified signature creation device). Halcom CA može izdati potvrda na pametnoj kartici, USB pametnom ključu ili u cloudau (HSM). Potvrda je namijenjena za kvalifikovani elektronski potpis/pečat.
Potvrda za Esig/ESeal	Kvalifikovana digitalna potvrda izdana u datoteci namijenjenoj za napredni elektronski potpis/pečat.

1.6.2 Izrazi

Pružatelj usluga povjerenja	Fizičko ili pravno lice koje izdaje potvrde ili obavlja druge usluge od povjerenja (engl.: Trust Service provider - TSP).
Imenik potvrda	Imenik X.500 certifikata, gdje se pohranjuju X.509 certifikati 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.
Prijavna služba	SLužba ili osoba koja prihvata zahtjeve za potvrde i vrši identifikaciju i provjeru identiteta potencijalnih vlasnika u ime pružatelja usluga od povjerenja potvrda (engl.: Registration Authority - RA).
Prepoznatljivo ime	Jedinstveno ime u potvrdi (usp. DN definicija) koje nedvosmisleno i jedinstveno definira korisnika u strukturi direktorija.

2. OBJAVLJIVANJE INFORMACIJA I JAVNI IMENIK POTVRDA

2.1. Prikupljanje dokumenata

(1) Pružatelj usluga od povjerenja Halcom CA objavljuje sve u vezi njegovog poslovanja, obavještenja vlasnicima i trećim stranama, 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 od povjerenja (CP),
- opšta pravila za rad pružatelja usluga od 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) CPS i nove politike objavljuju se kako je navedeno u tački 9.10.

(2) Sve potvrde pružatelja usluga od povjerenja temelje se na standardu X.509 i objavljeni 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) CPS ili nove politike objavljuju se najkasnije sljedećeg radnog dana nakon 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 imenikui opozvanih potvrda Halcom CA. Ovo osvježavanje se također prenosi na web stranice sa 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 direktorij je dostupan na serveru ldap.halcom.si, TCP port 389 putem LDAP protokola. Javno je dostupan samo registar opozvanih potvrda, koji je dio direktorija.

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

3. IDENTITET IMAOCA POTVRDE

3.1. Imenovanje

Različita imena sadržana u potvrdau 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 tački 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) Za kvalifikovane potvrde u svrhu identifikacije pružatelja platnih usluga, u skladu s prvim stavkom člana 34. Delegirane uredbe Komisije (EU) 2018/389 od 27. novembra 2017. godine kojom se dopunjuje Direktiva (EU) 2015/2366 Evropskog parlamenta i Vijeća u vezi s regulatornim tehničkim standardima za snažnu autentifikaciju korisnika i zajedničkim i sigurnim standardima otvorene komunikacije (RTS SCA), koristi se semantički identifikator "PSD" s kodom zemlje ISO 3161-1, uloga pružatelja platnih usluga, naziv nadležnog tijela (NCA) kod kojeg je pružatelj platnih usluga registriran i registracijski broj pružatelja platnih usluga kako je naveden u službenim evidencijama tog tijela.

(6) Prilikom izdavanja kvalifikovane digitalne potvrde, pružatelj usluga od povjerenja Halcom CA može u polje Imaoc (engl. Subject) dodati i atribut 1.3.6.1.4.1.5939.2.9, koji predstavlja vrstu potvrda (npr. označava da se radi o kvalifikovanoj digitalnoj potvrdi u cloudu, na pametnoj kartici ili USB ključu itd.).

(7) Potvrde pružatelja usluga povjerenja Halcom CA:

Vrsta potvrda	Naziv polja	Ugledno ime	Generacija
Root potvrda pružatelja uslugaod 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
	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 pružatelja usluga od povjerenja Halcom CA	Izdavatelj engl. Issuer	C= SI O=Halcom d.d. 2.5.4.97 = VATSI-43353126 CN = Halcom Root Certificate Authority	G1
	Imaoc, engl. Subject	C= SI O=Halcom d.d. 2.5.4.97= VATSI-43353126 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= VATSI-43353126 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 G3	G3
	Imaoc, engl. Subject	C= SI O=Halcomu 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

Potvrda za elektronski potpis za pravna lica	Imaoc, engl. 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> SERIJSKI BROJ= TIN<dvocifreni ISO kod države>-<poreski broj imaoca> i/ili 1.3.6.1.4.1.5939.2.2= < porezni broj imaoca> E= <e-mail>	G1, G2, G3
Potvrda za elektronski potpis za fizička lica	Imaoc, engl. Subject	C= <dvoslovni ISO kod države> CN= <ime i prezime> SN= <prezime> G= <ime> SERIJSKI BROJ= TIN<dvocifreni ISO kod države>-<poreski broj imaoca> i/ili 1.3.6.1.4.1.5939.2.2= <poreski broj imaoca> E= <e-mail>	G1, G2, G3
Potvrda za elektronski pečat	Imaoc, engl. Subject	C= <dvoslovni ISO kod države> O= <naziv poslovnog subjekta> 2.5.4.97=PDV<dvoslovni ISO kod države>-<poreski broj poslovnog subjekta> i/ili 1.3.6.1.4.1.5939.2.3= <poreski broj poslovnog subjekta> CN=<naziv informacionog sistema ili odjeljenja> E= <e-mail>	G1, G2, G3
Potvrda za autentifikaciju web stranice	Imaoc, engl. Subject	C= <dvoslovni ISO kod države> O= <naziv poslovnog subjekta> 2.5.4.97=PDV<dvoslovni ISO kod države>-<poreski broj poslovnog subjekta> i/ili 1.3.6.1.4.1.5939.2.3= <poreski broj poslovnog subjekta> OU = web certificates CN= <naziv i domena web stranice> SN= <domena>	G1, G2, G3

		G= <naziv web stranice> E = <e-mail>	
Potvrda za vremenski pečat	Imaoc, engl. Subject	C= <dvoslovni ISO kod države> O= <naziv poslovnog subjekta ili pružatelja usluga od povjerenja> 2.5.4.97= PDV<dvocifreni ISO kod države>-<poreski broj poslovnog subjekta> i/ili 1.3.6.1.4.1.5939.2.3= <poreski broj poslovnog subjekta> CN= <ime potvrde ili servisa za vremenski pečat> E= <e-mail>	G1, G2, G3

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

3.1.2 Zahtjevi pri formiranju prepoznatljivog imena

(1) Oznaka fizičke ili pravne osobe uključena u prepoznatljivo ime 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) U slučaju potvrde za server, naziv servera mora biti potpuno domensko ime (engl. fully qualified domain name).

(3) Halcom CA zadržava pravo da odbije firmu, naziv ili oznaku poslovnog subjekta 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) Podaci o imaocu potvrde u prepoznatljivom imenu potvrda G1 sadrže slova engleske abecede, a preostali znakovi se pretvaraju prema sljedećem pravilu:

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 povjerenja dužan je osigurati upotrebu drugih nepredviđenih znakova korištenjem odgovarajuće kombinacije slova.

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

(4) Halcom CA zadržava pravo izmjene zapisa o prepoznatljivim. 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) Poslovni subjekti ili imaoci ne mogu zahtijevati nazive državnih organa ili organa lokalne zajednice, imena, oznake, pečate ili druge elemente intelektualnog vlasništva koji pripadaju trećim licima i time 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 poslovni subjekt o tome.

3.2. Provjera identiteta budućih imaoca prilikom prvog izdavanja potvrda

Identitet potencijalnih imaoca prilikom prvog izdavanja potvrda provjerava se u prijavnoj službi pružatelja usluga od povjerenja ili direktno kod pružatelja usluga od povjerenja Halcom CA. Prije izdavanja potvrda, Halcom CA provjerava podatke potencijalnog imaoca i pravnog lica u relevantnim registrima.

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 potvrda i standardom PKCS#10.

3.2.2 Provjera identiteta organizacije

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

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

(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.

(4) Na osnovu zahtjeva za potvrda za autentifikaciju web stranice kod ovlaštenog registrara domena, pružatelj usluga od povjerenja Halcom CA provjerava vlasništvo nad domenom koju je ovlašteno lice pravnog lica naznačilo u zahtjevu.

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 potvrdama

Halcom CA ne provjerava ispravnost i funkcionalnost e-mail adrese imaoca potvrda.

3.2.5 Provjera ovlaštenja zaposlenika za dobijanje potvrda

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

(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,
- na osnovu već izdane važeće kvalifikovane digitalne potvrde koju je izdao pružalac usluga od povjerenja, pri čemu pružalac usluga od povjerenja Halcom CA provjerava podatke pravnog lica i imaoca u odgovarajućim registrima.

3.3.2 Provjera imaoca za ponovno dobivanje potvrde nakon opoziva

Provjera imaoca se vrši u skladu sa odredbama tačke 3.2.3.

3.4. Provjera identiteta prilikom zahtjeva za opoziv

(1) Zahtjev za opoziv potvrde podnosi pravno lice ili imaoc:

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

(2) Detaljan postupak opoziva: tačka 4.9.3.

4. UPRAVLJANJE POTVRDAMA

4.1. Dobijanje potvrda

4.1.1 Ko može dobiti potvrdu?

(1) Budući imaoci potvrda su fizička lica, ovlašteni predstavnici pravnih lica ili pravna lica za vlastite uređaje.

(2) Za dobijanje potvrde moraju biti ispunjeni sljedeći uslovi:

- popunjen i lično predat obrazac za narudžbu ili ugovor u prijavnoj službi,
- obaveza identifikacije,
- finansijske obaveze.

(3) Potvrda se neće izdati potencijalnom imaocu 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 dobijanje potvrda i odgovornosti potencijalnog imaoca

(1) Kvalifikovana potvrda za ovlaštene predstavnike pravnih lica:

1) Potvrda za elektronski potpis izdaje se na osnovu pravilno popunjene i potpisane generalne narudžbenice i zahtjeva za izdavanje potvrde (u daljem tekstu narudžbenica) od strane zakonitog zastupnika poslovnog subjekta i budućeg imaoca potvrde, ili na osnovu dostavljenih podataka iz baza podataka prijavne službe, pribavljenih postupkom koji prijavna služba koristi za druge svrhe i koji u skladu sa važećim propisima osigurava jednak nivo pouzdanosti.

2) Zakoniti zastupnik podnosi ili potvrđuje zahtjev kod prijavne službe Halcom CA te izmiruje finansijske obaveze u vezi sa izdavanjem potvrde. Narudžbenice za izdavanje digitalne potvrde dostupne su kod prijavnih službi Halcom CA i na web stranici Halcom CA. Cjenovnik usluga javno je objavljen na web stranicama Halcom CA.

3) Potpisom narudžbenice zakoniti zastupnik također ovlašćuje ovlaštenu osobu poslovnog subjekta (imaoca digitalne potvrde) da u ime i za račun poslovnog subjekta može valjano i sigurno elektronski potpisati zahtjev za produženje postojećeg digitalnog potvrđenja ili izdavanje novog sa istim podacima, u skladu sa tada važećom politikom i cjenovnikom pružaoca usluga povjerenja Halcom CA, ali samo pod uslovom da je sigurni elektronski potpis moguće provjeriti.

4) Zakoniti zastupnik poslovnog subjekta podnosi zahtjev u pisanom obliku.

5) Prije izdavanja narudžbenice, Halcom CA obavještava pravno lice i budućeg imaoca o politici i općim pravilima poslovanja pružatelja usluga od povjerenja Halcom CA.

(2) Kvalifikovana potvrda za fizička lica:

1) Potvrda se izdaje na osnovu pravilno popunjenog i potpisanog zahtjeva za izdavanje potvrde (u daljem tekstu narudžbenica) od strane budućeg imaoca potvrde ili na osnovu dostavljenih podataka iz baza podataka prijavne službe, pribavljenih postupkom koji prijavna služba koristi za druge svrhe i koji u skladu sa važećim propisima osigurava jednak nivo pouzdanosti.

2) Imaoc potvrde podnosi ili potvrđuje zahtjev kod prijavne službe Halcom CA te izmiruje finansijske obaveze u vezi sa izdavanjem potvrde. Narudžbenice za izdavanje digitalne potvrde dostupne su kod prijavnih službi Halcom CA i na web stranici Halcom CA. Cjenovnik usluga javno je objavljen na web stranicama Halcom CA.

3) Budući imaoc potvrde podnosi zahtjev u pisanom obliku.

4) Prije izdavanja narudžbenice, Halcom CA obavještava budućeg imaoca o CPS-u, politici i poslovanju pružatelja usluga povjerenja Halcom CA.

(3) Kvalifikovana potvrda za elektronski pečat:

1) Potvrda za elektronski pečat izdaje se na osnovu pravilno popunjene i potpisane narudžbenice za izdavanje potvrde (u daljem tekstu narudžbenica) od strane zakonitog zastupnika poslovnog subjekta ili na osnovu dostavljenih podataka iz baza podataka prijavne službe, pribavljenih postupkom koji prijavna služba koristi za druge svrhe i koji u skladu sa važećim propisima osigurava jednak nivo pouzdanosti.

2) Zakoniti zastupnik podnosi zahtjev prijavnoj službi Halcom CA te izmiruje finansijske obaveze u vezi sa izdavanjem potvrde. Narudžbenice za izdavanje digitalne potvrde dostupne su kod prijavnih službi Halcom CA i na web stranici Halcom CA. Cjenovnik usluga javno je objavljen na web stranicama Halcom CA.

3) Zakoniti zastupnik poslovnog subjekta podnosi zahtjev u pisanom obliku.

4) Prije izdavanja narudžbenice, Halcom CA obavještava budućeg imaoca o CPS-u, politici i poslovanju pružatelja usluga od povjerenja Halcom CA.

(4) Kvalifikovana potvrda za autentifikaciju web stranice:

1) Potvrda za autentikaciju web stranice izdaje se na osnovu pravilno popunjene i potpisane narudžbenice za izdavanje potvrde (u daljem tekstu narudžbenica) od strane zakonitog zastupnika poslovnog subjekta ili na osnovu dostavljenih podataka iz baza podataka prijavne službe, pribavljenih postupkom koji prijavna služba koristi za druge svrhe i koji u skladu sa važećim propisima osigurava jednak nivo pouzdanosti.

2) Zakoniti zastupnik podnosi zahtjev prijavnoj službi Halcom CA te izmiruje finansijske obaveze u vezi sa izdavanjem potvrde. Narudžbenice za izdavanje digitalne potvrde dostupne su kod prijavnih službi Halcom CA i na web stranici Halcom CA. Cjenovnik usluga javno je objavljen na web stranicama Halcom CA.

3) Imaoc web stranice podnosi zahtjev u pisanoj formi.

4) Prije izdavanja narudžbenice, Halcom CA obavještava budućeg imaoca o CPS-u, politici i poslovanju pružatelja usluga od povjerenja Halcom CA.

(5) Kvalifikovana potvrda za vremenski pečat:

1) Kvalifikovane potvrde za vremensko pečatiranje namijenjene su isključivo pružaocima ili budućim pružaocima usluga povjerenja.

2) Pružaltelj usluga od povjerenja Halcom CA nije obavezan ugovorno sarađivati s drugim pružateljima usluga od povjerenja čak i ako drugi pružatelj usluga povjerenja ima status kvalifikovanog pružatelja usluga.

3) Pružatelj usluga od povjerenja Halcom CA garantuje da će potvrdu izdati isključivo nakon potpisivanja pisanog ugovora s drugim pružateljem ili budućim pružateljem usluga od povjerenja, koji mora ispunjavati nivo sigurnosnih zahtjeva koji je uporediv ili viši od onog koji propisuje pružatelj usluga od povjerenja Halcom CA.

4) Ako nije obezbijeđena eksterna i nezavisna procjena usklađenosti drugog pružatelja usluga od povjerenja, ovlaštena lica Halcom CA preispituju interna pravila drugog pružatelja usluga od povjerenja i njegovu usklađenost sa sigurnosnim zahtjevima.

5) Prije izdavanja narudžbenice, Halcom CA obavještava budućeg imaoca o CPS-u, politici i poslovanju pružatelja usluga od povjerenja Halcom CA.

(6) 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 potvrda

4.2.1 Provjera identiteta budućeg imaoca

(1) Ovlaštena osoba prijavne službe provjerava identitet zakonskog zastupnika i/ili imaoca važećim ličnim dokumentom sa fotografijom prilikom posjete prijavnoj službi ili putem kurirske službe ili sigurnog elektronskog portala prilikom dostave potvrde, PIN koda, lozinke za preuzimanje ili narudžbenice za cloud potvrdu.

(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 pravno lice ili budući imaoc odmah obavještava lično ili putem e-maila.

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

4.2.3 Vrijeme za izdavanje potvrda

Na osnovu odobrene narudžbenice ili ugovora 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 od povjerenja Halcom CA

(1) Proces proizvodnje za izdavanje potvrde zavisi od vrste potvrde:

- Napredna kvalifikovana potvrda

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

  1. predpersonalizacija sigurnog medija (generiranje ključeva na kartici, odabir lozinke za zaštitu potvrda),
  2. dobijanje elektronskog zahtjeva za izdavanje potvrda,
  3. obrada zahtjeva za izdavanje potvrda,
  4. priprema potvrde,
  5. personalizacija sigurnog medija (izdavanje i zapis potvrde, štampanje podataka imaoca),
  6. štampanje lične lozinke (PIN kod - samo u slučaju slanja preporučenom poštom),
  7. prosljeđivanje potvrda 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, ovlaštena lica prijavne službe mogu pošiljku imaocu predati i lično.

- Kvalifikovana 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 kvalificiranom 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.

- Standardna kvalifikovana digitalna potvrda

  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 referentnog koda i lozinke za preuzimanje,
  3. posredovanje referentnog koda i lozinke za preuzimanje i obavještavanje imaoca,
  4. preuzimanje potvrde.

  Referentni kod i lozinka za preuzimanje šalju se imaocu putem dva odvojena kanala, jedan putem e-maila, a drugi putem drugog kanala (lična dostava putem obične pošte, putem SMS-a, putem sigurnog web portala, gdje se imaoc identifikuje kvalifikovanom potvrdom ili podacima poznatim samo imaocu (npr. broj ličnog dokumenta, poreski broj imaoca, posljednje četiri cifre ili CVV kod platne ili kreditne kartice ili slično)). Izuzetno, ovlaštena osoba iz prijavne službe Halcom CA može i lično predati imaocu lozinku za preuzimanje.

- Kvalifikovana 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 (engl. »certificate request«),
3. personalizacija i izdavanje potvrde,
4. prosljeđivanje potvrde imaocu.

- 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.

- Kvalifikovana potvrda za vremenski pečat

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

1. pregled sigurnosnih zahtjeva i internih pravila drugog pružatelja usluga povjerenja,
2. razmatranje i potpisivanje ugovora za izdavanje potvrda,
3. dobijanje elektronskog zahtjeva (engl. »certificate request«),
4. priprema potvrde,
5. personalizacija potvrde,
6. izdavanje potvrde pružatelja usluga od 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 imaocu o izdavanju

Pogledajte prethodni odjeljak.

4.4. Preuzimanje potvrde

4.4.1 Postupak preuzimanja potvrde

(1) Postupak za preuzimanje potvrde zavisi od vrste potvrde:

- Napredna kvalifikovana potvrda

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

- Kvalifikovana potvrda u cloudu

  Kod cloud potvrda nije potrebno preuzimati potvrdu, jer je Halcom CA, pružatelj usluga od povjerenja, po odobrenju imaoca sigurno pohranjuje. Korisniku se dodjeljuju samo pristupni kodovi za sigurni cloud , pogledajte tačku 4.3.1.

- Standardna kvalifikovana potvrda

  Za standardne potvrde, budući korisnik preuzima potvrdu koristeći Halcom CA softver za preuzimanje digitalnih potvrda, u skladu s uputama. Korisniku se dostavljaju samo kodovi za preuzimanje standardne potvrde, pogledajte članak 4.3.1.

- Kvalifikovana potvrda za informacione sisteme, autentifikaciju web stranica i vremenski pečat

  Za potvrde za autentifikaciju web stranica, informacione sisteme i vremenski pečat, pravno lice lokalno inicira generiranje ključeva i postavlja lozinku za njihovu zaštitu. Pružatelj usluga od povjerenja Halcom CA generira potvrdu na osnovu primljenog elektronskog zahtjeva (»certificate request«) i prosljeđuje ga pravnom licu, koje koristi prethodno spomenutu lozinku za kreiranje potvrda s pripadajućim parom ključeva.

(2) Po prijemu potvrde, imaoc potvrde ili pravno lice mora odmah provjeriti podatke u potvrdi i

odmah obavijestiti pružatelja usluga od povjerenja Halcom CA o svim greškama ili problemima.

4.4.2 Objavljivanje potvrde

Proces je opisan u tački 2.

4.4.3 Obavještenje CA 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 potvrde 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 pridržavate prije izdavanja potvrde,
- postupati u skladu s politikom i drugim važećim propisima,
- nakon prijema potvrda ili aktivacije potvrda, provjeriti podatke u potvrdi i odmah obavijestiti Halcom CA o svim greškama ili problemima ili zatražiti opoziv potvrde,
- 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 potvrdom,
- 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 preuzimanje 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 potvrda, 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 namjenom politike i drugih važećih propisa,
- pažljivo razmotriti sve potencijalne rizike i odgovornosti pri korištenju potvrda i uspostaviti politiku o tome kako će se oni koristiti,
- obavijestiti Halcom CA ako sazna da su privatni ključevi imaoca potvrda na koji 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 li se potvrda nalazi u registru opozvanih potvrda,
- tokom korištenja potvrde, provjeriti da li je digitalni potpis/pečat kreiran u roku važenja i za odgovarajuću svrhu potvrde,
- tokom korištenja potvrde, provjeriti potpis potvrda pružatelja usluga od povjerenja Halcom CA, koji je objavljen u ovoj politici, a također i na web stranici Halcoma,
- pridržavati se drugih odredbi ako je zaključio ugovor s pružateljem usluga od povjerenja Halcom CA o korištenju potvrda.

(2) Da bi provjerila valjanost potpisa/pečata 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 potvrda

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

(2) Nakon isteka napredne potvrde, 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 važećim potvrdom.

(4) Ponovno izdavanje potvrda za autentifikaciju web stranice, informacione sisteme i vremenski pečat vrši se na isti način kao i početno pribavljanje potvrde (vidjeti tačku 4.1).

4.6.1 Okolnosti koje zahtijevaju ponovno izdavanje potvrde

Prije isteka važenja digitalne potvrde, imaoci standardnih, naprednih i cloud potvrda mogu osigurati kontinuitet korištenja digitalne potvrde podnošenjem elektronskog zahtjeva za ponovno izdavanje. Zahtjev za novo izdavanje može se podnijeti i nakon isteka važenja digitalne potvrde.

4.6.2 Osobe koje mogu zatražiti produženje potvrde

Produženje važenja potvrde moguće je samo na zahtjev imaoca standardne ili napredne kvalificirane digitalne potvrde i kvalificirane cloud potvrde.

4.6.3 Postupak za obradu zahtjeva za ponovno izdavanje potvrde

Procedura osigurava da je poslovni subjekt i/ili fizičko lice koje traži ponovno izdavanje potvrde bez promjene javnog ključa zapravo imaoc potvrde.

4.6.4 Obavještenje nosioca novoizdane potvrde

Pogledajte tačku 4.3.2.

4.6.5 Postupak za prihvatanje novoizdane potvrde

Pogledajte tačku 4.4.1.

4.6.6 Objavljivanje novoizdane potvrde

Proces je opisan u tački 2.

4.6.7 Obavještenje CA o izdavanju potvrda drugim subjektima

Halcom CA ne obavještava kompanije i druge organizacije o izdavanju pojedinačne potvrde imaocima potvrde.

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 Postupak preuzimanja

Nije podržano.

4.7.6 Objavljivanje potvrde pružatelja usluga povjerenja s novim parom ključeva

Nije podržano.

4.7.7 Obavještenje pružatelja usluga povjerenja o izdavanju potvrda trećim stranama

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 za dobijanje 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 novog potvrda

Nije podržano.

4.8.5 Prihvatanje izmijenjene potvrde

Nije podržano .

4.8.6 Objavljivanje izmijenjene potvrde

Nije podržano.

4.8.7 Obavještenje o promjenama drugih subjekata

Nije podržano.

4.9. Opoziv i suspenzija potvrde

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

1) promjene prepoznatljivog imena (DN),
2) kada poslovni subjekt ili imaoc potvrde promijeni ključne informacije vezane za potvrdu (ime ili prezime, naziv pravnog lica, adresu e-pošte, 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 potvrde ili sigurnog medija, 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, organa za prekršaje 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 direktoriju i dodana u registar opozvanih potvrda. Ako imaoc Halcom CA potvrde podnese nevažeći zahtjev za opoziv potvrde, bit će obaviješten o nevažećem zahtjevu za opoziv potvrde 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 potvrda 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:

- da su informacije u potvrdi netačne ili da je potvrda izdana 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 nosioca,
- da svi troškovi upravljanja digitalnom potvrdom nisu podmireni,
- da je infrastruktura pružatelja usluga povjerenja kompromitovana na način koji utječe na pouzdanost potvrde,
- da je privatni ključ imaoca potvrda 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 od povjerenja,
- da je opoziv naložio nadležni sud, prekršajni ili upravni organ.

(3) Imaoc digitalne potvrde može, u roku od trideset (30) dana od datuma izdavanja, zatražiti ponovno generiranje lične lozinke (PIN koda) za napredne potvrde ili referentne kodove i lozinke za preuzimanje za standardne potvrde ili registracijske i aktivacijske kodove za cloud potvrde u slučaju da je imaoc jednostavno zaboravio podatke za e-pristup i garantuje pod građanskom i krivičnom odgovornošću da ne postoji mogućnost da je/bi bio kompromitovan privatni ključ na način koji utiče na pouzdanost korištenja i da ne postoji rizik od zloupotrebe privatnog ključa ili potvrde imaoca.

4.9.2 Ko zahtjeva opoziv

Opoziv potvrde može zahtijevati:

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

4.9.3 Procedure opoziva

(1) Opoziv može zatražiti zakonski zastupnik poslovnog subjekta ili imaoc:

- 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 zahtjeva 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 potvrda. Tek na osnovu pismenog zahtjeva za opoziv potvrda, 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 poslovnog subjekta 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 opoziv, to čine u skladu sa zakonima koji uređuju postupak pred njima (krivični postupak, građanski postupak, opći upravni postupak i drugi).

(5) Odredbe o opozivu primjenjuju se smisleno i na postupke u vezi s ponovnim generiranjem PIN koda za napredne potvrde ili referentne kodove i lozinke za preuzimanje standardnih potvrda te registracijskih i aktivacijskih kodova 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 prijavnih službi (pogledajte sljedeći odjeljak).

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 od strane trećih lica

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

4.9.7 Učestalost objavljivanja registra opozvanih potvrda

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

- nakon svakog opoziva potvrda,
- 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 direktoriju na serveru ldap://ldap.halcom.si odmah (maksimalno pet (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 provjeru statusa potvrda u realnom vremenu (OCSP) podržan je u skladu s evropskim i međunarodnim standardima i preporukama (vidjeti odjeljak 7.3). Usluga provjere statusa potvrda u relanom vremenu (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 potvrde, treća lica bi uvijek trebala 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 za zloupotrebu privatnog ključa

Nisu specificirani.

4.9.13 Razlozi za suspenziju

(1) Ako imaoc potvrde zatraži opoziv potvrda telefonom ili elektronskim putem, potvrda će biti

privremeno suspendovan dok se ne primi originalni pisani zahtjev.

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

4.9.14 Ko traži suspenziju?

Pogledajte odjeljak 4.9.13.

4.9.15 Postupak suspenzije

Pogledajte odjeljak 4.9.13.

4.9.16 Vrijeme suspenzije

Pogledajte odjeljak 4.9.13.

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 odjeljcima 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 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 povjerenja 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 višeslojnim 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. Sigurnosne kopije se osiguravaju i za oporavak podataka i za arhiviranje važnih informacija, koje se pohranjuju na lokaciji koja nije softver za upravljanje potvrdama, kako bi se osiguralo ponovno korištenje u slučajevima uništenja podataka na primarnoj lokaciji.

(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 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 povjerenja i procedure za njeno upravljanje i sigurnost određeni su internim pravilima pružatelja usluga od povjerenja.

5.1.1 Lokacija i objekat pružatelja usluga od povjerenja

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

(2) Sav pristup je zaštićen 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 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 povjerenja Halcom CA.

5.1.5 Zaštita od požara

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

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

5.1.6 Pohranjivanje medija sa podacima

(1) Mediji sai podacima, bilo u papirnom ili elektronskom obliku, moraju se sigurno čuvati u zaštićenim objektima.

(2) Sigurnosne kopije softvera i šifriranih baza podataka pružatelja usluga 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) Detalji o ovome su navedeni u internim pravilima pružatelja usluga povjerenja Halcom CA.

5.1.8 Skladištenje na udaljenoj lokaciji

Pogledajte odjeljak 5.1.6.

5.2. Organizacijska struktura pružatelja usluga 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 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 povjerenja, • ovlaštenje podređenih pružatelja usluga povjerenja, • pristup protokolu za potpisivanje potvrda, • sigurno skladištenje i distribucija kopija i nadogradnji na zasebnu lokaciju.	2

Upravljanje potvrdama	Sistemski operater 1	• Priprema kopija sistema, nadogradnja i vraćanje softvera, sigurno skladištenje i distribucija kopija i nadogradnji, • administrativne funkcije vezane za održavanje, • Vršenje arhiviranja potrebnih sistemskih zapisa, • štampa PIN kodova, • dnevna provjera sistema.	2
	Operater za autorizaciju	• Potvrda izdavanja potvrde i generiranje lozinke.	2
	Operater za potvrde	• Predpersonalizacija sigurnih medija, • 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, • stručna pomoć menadžmentu i	1

		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 u pojedinačne organizacijske grupe:

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 distribuiranje kopije i nadogradnje na zasebnu lokaciju.

Organizaciona grupa: Upravljanje informacionim sistemom

Uloga: Sistemski administrator

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 kopije i nadogradnja na zasebnu lokaciju.

Organizacijska grupa: Upravljanje potvrdama

Uloga: Sistemski operater 1

Broj osoba: 2

Zadaci:

1. Priprema kopija sistema, nadogradnja i vraćanje 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 za autorizaciju

Broj osoba: 2

Zadaci:

1. Potvrđivanje izdavanja potvrda i generiranje lozinki

Organizacijska grupa: Upravljanje potvrdama

Uloga: Operater za potvrde

Broj osoba: 2

Zadaci:

1. Predpersonalizacija sigurnih medija.

2. Priprema potvrde (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 Autentifikacija korisnika radi izvršavanja specifičnih zadataka

Provjera 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 mora 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 osoblja

(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 nadgleda 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 nadgleda 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 Pogodnost 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 Dodatna obuka osoblja

Sva potrebna obuka obezbjeđuje 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 novinama 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 od povjerenja u skladu s važećim propisima i internim pravilima pružatelja usluga povjerenja Halcom CA.

5.3.7 Zahtjevi za vanjske izvođače radova

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

5.3.8 Pristup osoblja dokumentaciji

Ovlaštenim osobama pružatelja usluga od 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 u opremu ili podatke od strane neovlaštenih osoba.

(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

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

5.4.4 Zaštita logova

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

(2) Detalji su utvrđeni u internim pravilima pružatelja usluga od povjerenja u skladu s Uredbom.

5.4.5 Sigurnosne kopije logova

(1) Sigurnosne kopije logova se prave svakodnevno.

(2) Detalji su utvrđeni u internim pravilima pružatelja usluga povjerenja u skladu s Uredbom.

5.4.6 Prikupljanje podataka za logove

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

(2) Detalji su utvrđeni u internim pravilima pružatelja usluga povjerenja u skladu s Uredbom.

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 drugim sigurnosnim mehanizmima na svim informaciono-komunikacijskim uređajima pod odgovornošću pružatelja usluga od povjerenja.

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

(3) Detalji su utvrđeni u internim pravilima pružatelja usluga povjerenja u skladu s Uredbom.

5.5. Dugoročno čuvanje podataka

5.5.1 Vrste dugoročno pohranjenih 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,
- CPS,
- 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 potvrde 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 zadržani podaci se pohranjuju na siguran način.

(2) Detaljnija pravila utvrđena su 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 zadržanih podataka čuva se na sigurnom mjestu.

(2) Detaljnija pravila utvrđena su 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 Način prikupljanja podataka

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

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

5.7.2 Postupak u slučaju kvara softvera ili podataka

Detaljnija regulativa utvrđena je u internim pravilima pružatelja usluga od povjerenja Halcom CA, u skladu s važećim propisima, standardima i preporukama.

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

Detaljnija regulativa utvrđena je u internim pravilima pružatelja usluga od povjerenja Halcom CA, u skladu s važećim propisima, standardima i preporukama.

5.7.4 Plan oporavka

Detaljnija regulativa utvrđena je u internim pravilima pružatelja usluga od povjerenja Halcom CA, u skladu s važećim propisima, standardima i preporukama.

5.8. Prestanak rada Halcom CA

Detaljnija regulativa utvrđena je u internim pravilima pružatelja usluga od povjerenja Halcom CA, u skladu s važećim propisima, standardima i preporukama.

6. ZAHTJEVI TEHNIČKE SIGURNOSTI

6.1. Generisanje i instaliranje ključeva

6.1.1 Generisanje ključeva

(1) Par ključeva pružatelja usluga povjerenja Halcom CA za potpisivanje i provjeru valjanosti potpisa kreiran je prema najvišim sigurnosnim standardima u hardverskom sigurnosnom modulu, u sigurnom okruženju provajdera usluga od povjerenja Halcom CA.

(2) Ključevi imaoca se generiraju ovisno o vrsti potvrde prema donjoj tabeli.

Vrsta potvrda	Ključ	Ključ se generira.
Halcom CA root i intermediate potvrda	Par ključeva	u modulu hardverske sigurnosti pružatelja usluga od povjerenja
Napredna potvrda	Dva para ključeva	na sigurnom mediju, kod pružatelja usluga od povjerenja Halcom CA
Potvrda u cloudu	Par ključeva	u modulu hardverske sigurnosti pružatelja usluga od povjerenja
OT potvrda	Par ključeva	u modulu hardverske sigurnosti pružatelja usluga od povjerenja
Standardna potvrda	Par ključeva	kod imaoca potvrde
Potvrda o informacionim sistemima	Par ključeva	u sigurnom okruženju imaoca potvrde
Potvrda za autentifikaciju web stranice	Par ključeva	u sigurnom okruženju imaoca potvrde
Potvrda za vremenski pečat	Par ključeva	u modulu hardverske sigurnosti pružatelja usluga od povjerenja

6.1.2 Dostava privatnog ključa imaocima

Metoda za siguran prijenos privatnog ključa data je u donjoj tabeli.

Vrsta potvrda	Ključ	Dostava
Halcom CA root i intermediate potvrda	Privatni ključ	bez transfera
Napredna potvrda	Privatni ključevi	prenos sigurnog medija vrši se preporučenom poštom.
Standardna potvrda	Privatni ključ	nema prenosa

Potvrda u cloudu	Privatni ključ	nema prenosa
OT potvrda	Privatni ključ	nema prenosa
Potvrda o informacionim sistemima	Privatni ključ	nema prenosa
Potvrda za autentifikaciju web stranice	Privatni ključ	nema prenosa
Potvrda za vremenski pečat	Privatni ključ	nema prenosa

6.1.3 Dostavljanje javnog ključa pružatelju usluga od povjerenja za potvrde

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

(2) Za cloud 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 generiše imaoc. Zahtjev za PKCS#10 za izdavanje potvrde se prenosi sa računara korisnika do pružatelja usluga od povjerenja putem sigurne mrežne veze .

(4) Za standardne potvrde, ključeve generira imaoc. Zahtjev za PKCS#10 potvrdu (engl. »certificate request«) i izdavanje potvrde radi se putem softvera za preuzimanje digitalnih potvrda Halcom CA.

(5) Za potvrde s vremenskim žigom, ključevi se generiraju u hardverskom sigurnosnom modulu pružatelja usluga od povjerenja. Zahtjev PKCS#10 za izdavanje potvrde (angl. »certificate request«) prenosi se 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 stranama:

- u javnom direktoriju ldap://ldap.halcom.si koristeći LDAP protokol (vidi odjeljak 2.3),
- u PEM formatu na http://domina.halcom.si/crls , gdje je potrebno dodatno provjeriti autentičnost potvrde.

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
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 4096

6.1.6 Generisanje i kvalitet parametara javnog ključa

Kvalitet parametara ključa pružatelja usluga od povjerenja Halcom CA osigurava proizvođač softvera korištenjem visokokvalitetnih generatora slučajnih brojeva (engl. random number generator).

6.1.7 Namjena ključeva i potvrda

(1) Svrha korištenja ključeva ili potvrda navedena je u potvrdi u poljima 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 potvrde 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 odjeljku 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 u skladu sa 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 potvrda.

(2) Privatni ključevi za cloud 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 drugih potvrda kreira i pohranjuje imaoc.

6.2.7 Pohranjivanje privatnog ključa u kriptografskom modulu

(1) Privatni ključ pružatelja usluga od povjerenja pohranjuje Halcom CA u kriptografskom modulu certificiranom u skladu sa FIPS 140-2 nivo 3 i/ili Uobičajeno Kriteriji 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,
- Standardne potvrde kreira i pohranjuje imaoc,
- potvrde za informacione sisteme kreira i čuva imaoc,
- potvrde za sisteme autentifikacije web stranica kreira i pohranjuje imaoc,
- Potvrde s vremenskim pečatom kreiraju se i pohranjuju u kriptografskom modulu.

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

Postupak za deaktivacija privatnog ključa pružatelja usluga od povjerenja Halcom CA sigurno se generira 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 ga nije moguće restaurirati.

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

(3) Privatni ključ cloud i OT potvrda se automatski uništava nakon isteka potvrda. Halcom CA može uništiti privatni ključ cloud potvrde prije isteka potvrde na zahtjev imaoca potvrde. Privatni ključ se uništava na način da se ne može vratiti .

6.2.11 Svojstva kriptografskog modula

Sigurnosni moduli hardvera su u skladu sa standardima navedenim u odjeljku 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 odjeljku 5.5.

6.3.2 Period važenja javnih i privatnih ključeva

(1) Važenje zavisi od vrste potvrde.

Vrsta potvrda	Ključ	Validnost

Korjenska potvrda	Privatni/javni ključ	20 godina
Srednja (podređena) potvrda	Privatni/javni ključ	10 godina
Napredna potvrda	Privatni/javni ključ	3 godine
Standardna potvrda	Privatni/javni ključ	3 godine
Potvrda u cloudu	Privatni/javni ključ	1 - 3 godine
Potvrda za informacione sisteme	Privatni/javni ključ	3 godine
Potvrda za autentifikaciju web stranice	Privatni/javni ključ	1 - 3 godine
Potvrda za vremenski pečat	Privatni/javni ključ	5 godina
OT potvrda	Privatni/javni ključ	do 10 minuta

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

6.4. Lozinke za pristup do potvrda ili ključeva

6.4.1 Generisanje lozinke

(1) Napredna potvrda

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) Potvrda u cloudu

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) OT potvrda

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) Potvrda za elektronski pečat u cloudu

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) Standardni potvrda, potvrda za informacione sisteme i autentifikaciju web stranice

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) Napredna potvrda

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) Potvrda u cloudu

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) OT potvrda

Aktivacija OT potvrde može se vršiti 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 bosanskim propisima, standardima, preporukama, politikama i općim pravilima poslovanja 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 njenog trenutnog opoziva. Ako aplikacija ili njena autorizacija za pristup potvrdama u oblaku 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, politikama i općim pravilima poslovanja Halcom CA. Imaoc potvrde zaključenjem ugovora o izdavanju potvrde izričito dozvoljava tehničke provjere svoje upotrebe aplikacije u obimu potrebnom za osiguranje usklađenosti sa uslovima ovog CPS-a i važećom legislativom.

(4) Potvrda za elektronski pečat u cloudu

Aktivacija potvrde za elektronski pečat u oblaku moguća je samo putem kvalifikovane digitalne potvrde za pristup, koju izdaje pružalac usluga povjerenja Halcom CA, te preko IP adrese koju je ovlastio pružalac usluga povjerenja. Korištenje potvrde može se vršiti 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 njenog trenutnog opoziva. Ako aplikacija ili njena autorizacija za pristup potvrdama u oblaku 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, politikama i općim pravilima poslovanja Halcom CA. Imaoc potvrde zaključenjem ugovora o izdavanju potvrde izričito dozvoljava tehničke provjere svoje upotrebe aplikacije u obimu potrebnom za osiguranje usklađenosti sa uslovima ovog CPS-a i važećom legislativom.

(5) Standardna potvrda

Referentni kod i lozinka za dobijanje standardne potvrde sigurno se generiraju od strane pružatelja usluga od povjerenja Halcom CA. Tokom procesa dobijanja potvrde, korisnik određuje lozinku kako bi zaštitio pristup 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) Potvrda za informacione sisteme i autentifikaciju web stranice

Imaoci potvrda za informacione sisteme sami određuju lozinku kako bi zaštitili pristup 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 računarsku 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 su navedeni u 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. Vremenski pečat

Nije propisano.

7. PROFIL POTVRDA I REGISTRA OPOZVANIH POTVRDA

7.1. Profil potvrda

(1) Na osnovu CPS-a i politika, Halcom CA izdaje:

- napredne potvrde,
- potvrde u cloudu,
- OT potvrde,
- standardne potvrde,
- potvrde informacionih sistema,
- potvrde za autentifikaciju web stranice i
- potvrde za vremenski pečat.

(2) Sve potvrdae 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* , tačnije verziju 3.

7.1.2 Profil potvrda s ekstenzijama

Informacije u potvrdama navedene su u nastavku.

7.1.2.1 Profil korijenskih (root) potvrda

Nazivi polja	Vrijednost ili značenje
Osnovna polja u potvrdi	
Verzija, engleska verzija	V3
Identifikacijski kod potvrda, 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 RSA ili RSASSA-PSS algoritmom, 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	
Korištenje ključa, OID 2.5.29.15, engl. Key Usage	Certificate Signing, Off-line CRL Signing, CRL Signing
Identifikator ključa subjekta, 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 digitalne 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 FO e-signature 1

Nazivi polja	Vrijednost ili značenje
Osnovna polja u potvrdi	
Verzija, engl. Version	V3
Identifikacijski kod potvrde, engl. Serial Number	0cecac

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: <15.06.2016 10:34:15 GMT> Valid to: <15.06.2026 10:34:15 GMT>
Imaoc, engl. Subject	CN = Halcom CA FO e-signature 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 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	48fb3b1399c34ece
Osnovna ograničenja, OID 2.5.29.19, engl. Basic Constraints	Subject Type=CA Path Length Constraint=None
Dodatna identifikacija (nije dio digitalne potvrda)	
Identifikacijski otisak potvrde – SHA1, engl. Certificate Fingerprint – SHA1	Identifikacijski otisak potvrde prema SHA1

(2) Halcom CA FO e-signature 2

Nazivi polja	Vrijednost ili značenje
Osnovna polja u potvrdi	
Verzija, engl. Version	V3
Identifikacijski kod potvrde, engl. Serial Number	136c17
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 FO e-signature 2 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 3072 bit
X.509v3 ekstenzije	
Objava registra opozvanih potvrda, OID 2.5.29.31, engl. CRL Distribution Points	URI:ldap://ldap.halcom.si/cn=Halcom%20Root%20Certificate%20Authority,o=Halcom,c=SI?certificaterevocationlist;binary URL=http://domina.halcom.si/crls/halcom_root_certificate_authority.crl
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	48c427a66f6ef02e
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 FO e-sign 1 G2

Nazivi polja	Vrijednost ili značenje
Osnovna polja u potvrdi	
Verzija, engl. Version	V3
Identifikacijski kod potvrde, engl. Serial Number	63fde006151790064fdeecf32742e97c
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 FO 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 4096 bit
X.509v3 ekstenzije	
Objava registra opozvanih potvrda, OID 2.5.29.31, engl. CRL Distribution Points	URI:ldap://ldap.halcom.si/cn=Halcom%20Root%20Certificate%20Authority,o=Halcom,c=SI?certificaterevocationlist;binary URL=http://domina.halcom.si/crls/halcom_root_certificate_authority.crl
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	47902d7cbd318937
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 FO e-sig 1 G3

Nazivi polja	Vrijednost ili značenje
Osnovna polja u potvrdi	
Verzija, engl. Version	V3
Identifikacijski kod potvrde, engl. Serial Number	730ac4f1257e9b038804a9581dad91ea
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 09:00:00 GMT> Valid to: <02/04/2036 09:00:00 GMT>
Imaoc, engl. Subject	CN = Halcom CA FO 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 4096 bit
X.509v3 ekstenzije	
Objava registra opozvanih potvrda, OID 2.5.29.31, engl. CRL Distribution Points	URI: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 povjerenja, OID 2.5.29.35, engl. Authority Key Identifier	KeyID=4ba6657603985167
Identifikator ključa imaoca, OID 2.5.29.14, engl. Subject Key Identifier	46c21387d74ad8ae
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

(5) 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, 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	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

(6) Halcom CA PO e-signature 2

Nazivi polja	Vrijednost ili značenje
Osnovna polja u potvrdau	
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 od 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

(7) Halcom CA PO e-sign 1 G2

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

(8) Halcom CA PO e-sign 1 G3

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 podređenog potvrda 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 potvrdau	
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 digitalnog potvrda)	
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 podređenog potvrda za autentifikaciju web stranice

(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 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	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 potvrdau	
Verzija, engleska verzija	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 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	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 podređenog potvrda s vremenskim žigosanjem

(1) Halcom CA TSA 1

Nazivi polja	Vrijednost ili značenje
Osnovna polja u potvrdau	
Verzija, engl. Version	V3
Identifikacijski kod potvrde, engl. Serial Number	0e0ed1
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 TSA 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 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	438f8b569f441ed7
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 TSA 2

Nazivi polja	Vrijednost ili značenje
Osnovna polja u potvrdau	
Verzija, engl. Version	V3
Identifikacijska oznaka potvrde, engl. Serial Number	641bf7def92f969c8ca8bb049a033374
Algoritam potpisa, engl. Signature algorithm	Sha256RSA 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: <25.3.2025 09:00:00 GMT> Valid to: <25.3.2035 08:00:00 GMT>
Imaoc, engl. Subject	CN = Halcom CA TSA 2 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 3072 bita
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	ID ključa=42aea643c79828b0
Identifikator ključa imaoca, OID 2.5.29.14, engl. Subject Key Identifier	4fe0e1a9216e1bbe
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 TSA 1 G2

Nazivi polja	Vrijednost ili značenje
Osnovna polja u potvrdi	
Verzija, engl. Version	V3
Identifikacijski kod potvrde, engl. Serial Number	5e93f17167a040365fb93f24857e768f
Algoritam potpisa, engl. Signature algorithm	RSASSA-PSS
Izdavatelj, engl. Issuer	CN = Halcom Root CA G2 2.5.4.97 = VATSI-43353126 O = Halcom d.d. 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 TSA 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 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%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 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	4e1fe762246a1900
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 TSA 1 G3

Nazivi polja	Vrijednost ili značenje
Osnovna polja u potvrdi	
Verzija, engl. Version	V3
Identifikacijski kod potvrde, engl. Serial Number	4ae690c1d11e80fa7b11b976617ae68c
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 09:04:00 GMT> Valid to: <25.3.2036 09:04:00 GMT>
Imaoc, engl. Subject	CN = Halcom CA TSA 1 G3 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 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%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 povjerenja, OID 2.5.29.35, engl. Authority Key Identifier	KeyID=4ba6657603985167
Identifikator ključa imaoca, OID 2.5.29.14, engl. Subject Key Identifier	4599555173014e78
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

7.1.2.6 Profil potvrda krajnjeg 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,	dužine ključeva variraju (pogledajte tačku 6.1.5) G1: najmanje 2048 bit

šifriran RSA algoritmom, engl. RSA Public Key	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 FO e-signature 1: KeyID=48fb3b1399c34ece Halcom CA FO e-signature 2: KeyID=48c427a66f6ef02e 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 Halcom CA TSA 1: KeyID= 438f8b569f441ed7 Halcom CA TSA 2: KeyID= 4fe0e1a9216e1bbe
	G2: Halcom CA FO e-sig 1 G2: KeyID=47902d7cbd318937 Halcom CA PO e-sig 1 G2: KeyID=41753bf986c7cb9c Halcom CA e-seal 1 G2: KeyID=4125fcd8fad6662f Halcom CA web 1 G2: KeyID=4e9125213b702aca Halcom CA TSA 1 G2: KeyID= 4e1fe762246a1900
	G3: Halcom CA FO e-sig 1 G3: KeyID= 46c21387d74ad8ae Halcom CA PO e-sig 1 G3: KeyID=46b69ca3e4fa428d Halcom CA e-seal 1 G3: KeyID=462d8ba5e3c50364 Halcom CA web 1 G3: KeyID=4a4af4272960b712 Halcom CA TSA 1 G3: KeyID= 4599555173014e78
EŠEI	jedinstveni elektronski identifikacijski broj (pogledajte sljedeću tačku)

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

(5) 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

(6) Imaoc potvrde za elektronski pečat, informacione sisteme, autentifikaciju web stranica i vremenski pečat može imati više važećih potvrda.

7.1.2.7 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>

7.1.2.8 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,
- 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 odjeljak 3.1.1.

7.1.5 Ograničenja koja se tiču imena

Ograničenja imena (polje nameConstraints u potvrdau) nisu propisana.

7.1.6 Oznaka politike potvrda

Pogledajte odjeljak 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 FO e-signature 1
    O = Halcom
    C = SI
  - CN= Halcom CA FO e-signature 2
    O = Halcom
    C = SI
  - 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
  - CN = Halcom CA TSA 1
    O = Halcom
    C = SI
  - CN = Halcom CA TSA 2

O = Halcom
C = SI

- G2:
  - CN= Halcom CA FO e-sig 1 G2
    O = Halcom
    C = SI
  - 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
  - CN= Halcom CA TSA 1 G2
    O = Halcom
    C = SI
- G3:
  - CN= Halcom CA FO e-sig 1 G3
    O = Halcom
    C = SI
  - 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
  - CN= Halcom CA TSA 1 G3
    O = Halcom
    C = SI

(2) Registar opozvanih međupotvrda/podređenih potvrda osvježava se najmanje jednom godišnje, a ostali registri opozvanih potvrda osvježavaju se nakon svakog opoziva potvrde ili najmanje jednom dnevno, ako nema novih zapisa ili promjena u registrima opozvanih potvrda (24 sata nakon posljednjeg osvježavanja).

(3) Registri opozvanih potvrda sadrže jedinstveni interni serijski broj opozvane potvrde i vrijeme i datum opoziva.

7.2.1 Verzija

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

(2) Registri opozvanih potvrda su trajno dostupni u javnom direktoriju potvrda (vidjeti odjeljak 2.3):

- putem LDAP protokola i
- putem HTTP protokola.

7.2.2 Sadržaj registra i proširenja

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

- identifikacijske kodove 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-u	
Verzija, engl. Version	V2
Algoritam potpisa, engl. Signature Algorithm	G1: Sha256RSA
	G2: RSASSA-PSS
Potpis pružatelja usluga od povjerenja, engl. Signature	Potpis Halcom CA
Prepoznatljivo ime pružatelja usluga od 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 G2 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
	G1: Halcom Root Certificate Authority: KeyID=42aea643c79828b0

Identifikator ključa pružatelja usluga od povjerenja, engl. Authority Key Identifier (OID 2.5.29.35)	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-u	
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 FO e-signature 1: KeyID=48fb3b1399c34ece Halcom CA FO e-signature 2: KeyID=48c427a66f6ef02e 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 Halcom CA TSA 1: KeyID= 438f8b569f441ed7 Halcom CA TSA 2: KeyID= 4fe0e1a9216e1bbe

	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 Halcom CA FO e-sig 1 G2: KeyID=47902d7cbd318937 Halcom CA TSA 1 G2: KeyID= 4e1fe762246a1900
	G3: Halcom CA FO e-sig 1 G3: KeyID= 46c21387d74ad8ae Halcom CA PO e-sig 1 G3: KeyID=46b69ca3e4fa428d Halcom CA e-seal 1 G3: KeyID=462d8ba5e3c50364 Halcom CA web 1 G3: KeyID=4a4af4272960b712 Halcom CA TSA 1 G3: KeyID= 4599555173014e78
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 registre u javnom direktoriju na serveru ldap://ldap.hal com.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 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 obavljaju 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 druge usluge,
- sve povjerljive informacije koje se odnose na finansijske obaveze,
- bilo koje povjerljive informacije koje su predmet međusobnog ugovora s trećim stranama, i
- sva ostala pitanja koja su uključena u interna pravila pružatelja usluga od povjerenja Halcom CA u skladu s Uredbom.

(2) Pružatelj usluga od povjerenja Halcom CA obrađuje sve potencijalno povjerljive informacije o imaocima i trećim licima koje su strogo 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 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 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 po dizajnu i po zadanim postavkama. U Halcom d.d. radi ovlaštenik za privatnost kao službena osoba za zaštitu podataka.

9.4.2 Zaštićeni lični podaci

(1) 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 nosioca ili tokom pružanja usluga povjerenja.

(2) Zbog prirode upotrebe potvrda i odredbi važećih propisa i standarda, podaci u potvrdama i registru opozvanih potvrda dostupni su trećim licima koja 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 odjeljak), 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 o autorskim pravima, srodnim i drugim pravima intelektualnog vlasništva:

- sva prava na privatni ključ pripadaju imaocu potvrde,
- Sva prava na javne ključeve, svi podaci na potvrdai, direktorij potvrda i registar opozvanih potvrda, te ova politika pripadaju Halcom CA.

9.6. Obaveze i odgovornosti

9.6.1 Obaveze i odgovornosti pružatelja usluga od 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 usluga od 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 CPS

(1) Halcom CA zadržava pravo izmjene CPS-a i nadogradnje infrastrukture bez prethodne najave imaocima potvrda.

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

9.10.1 Period važenja

Nova verzija ili izmjene CPS-a objavljuju se osam (8) dana prije stupanja na snagu na web stranicama pružatelja usluga od povjerenja Halcom CA, uz navođenje datuma stupanja na snagu CPS-a.

9.10.2 Kraj važenja CPS-a

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

(2) Pružatelj usluga od povjerenja može izdati izmjene i dopune pojedinačnih odredbi CPS-a kako je navedeno u članu 9.12.

9.10.3 Posljedice isteka CPS-a

(1) Važenje potvrda regulirano je politikama.

(2) Novi CPS, a time i nova politika, ne utiču na važenje potvrda izdatih prema prethodnim politikama. Takve potvrdei će ostati važeće do datuma isteka i, gdje je to moguće, bit će tretirane prema novoj politici.

9.11. Komunikacija između subjekata

(1) Kontaktni podaci pružatelja usluga povjerenja objavljeni su na web stranicama i navedeni su u odjeljku 1.3.1.

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

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

9.12. Izmjene i dopune

9.12.1 Postupak za prihvatanje izmjena i dopuna

(1) Pružatelj usluga od povjerenja može objaviti izmjene ili dopune CPS-a u obliku izmjena i dopuna CPS-a, pod uslovom da ne uključuju značajne promjene u poslovanju pružatelja usluga od povjerenja.

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

(3) Način označavanja izmjena i dopuna 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.

9.13. Postupak rješavanja sporova

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

(2) Sve sporove između imaoca potvrda ili treća 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 zakonodavstvom i propisima provode nadležni inspektorat i akreditirana tijela za ocjenjivanje usklađenosti.

(2) Akreditovano tijelo za ocjenjivanje usklađenosti će vršiti reviziju pružaoca usluga od povjerenja Halcom CA najmanje svakih dvadeset četiri (24) mjeseca. Svrha revizije je potvrditi 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