Pripremio: Luka RIBIČIČ

Broj dokumenta: 400085-43-1/17

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

Izdanje: 02

Politika Halcom CA

Javni dio internih pravila Halcom CA za EU kvalificirane digitalne potvrde za fizičke osobe

Dokument važi od: 15.6.2026.

Naziv CP-a: Halcom CA FO

Politika	CPOID	Vrsta certifikata	Generacija
Halcom CA FO e-signature 1	1.3.6.1.4.1.5939.1.4.4 1.3.6.1.4.1.5939.1.5.4	QCert za ESig QRemManage for Cert for Esig	G1 G1
Halcom CA FO e-signature 2	1.3.6.1.4.1.5939.1.4.5 1.3.6.1.4.1.5939.1.5.5	QCert za ESig QRemManage for Cert for Esig	G1 G1
Halcom CA FO e-sig 1 G2	1.3.6.1.4.1.5939.1.4.7 1.3.6.1.4.1.5939.1.5.7	QCert za ESig QRemManage for Cert for Esig	G2 G2
Halcom CA FO e-sig 1 G3	1.3.6.1.4.1.5939.1.4.8 1.3.6.1.4.1.5939.1.5.8	QCert for ESig QRemManage for QSigCD Cert for ESig	G3 G3

Izdanje	broj dokumenta i priloga	Opis promjene	Autor	Datum posljednje izmjene
1	400085-43-1/17	Početno izdanje (spajanje svih CP-ova za fizičke osobe)	L. Ribičič	2 2 .5.2025
2	400085-43-2/17	Nova CA generacija – G3, OT potvrde	L. Ribičič	20.5.2026

Sadržaj

1. UVOD 12
1.1. Pregled 12
1.2. Identifikacijski podaci politike 12
1.3. Subjekti 13
1.3.1 Pružatelj usluga povjerenja Halcom CA 13
1.3.2 Prijavna služba Halcom CA 13
1.3.3 Naručioci i vlasnici potvrda 13
1.3.4 Treće osobe 14
1.4. Svrha upotrebe 14
1.4.1 Pravilna upotreba potvrda i ključeva 14
1.4.2 Neovlaštena upotreba 14
1.5. Upravljanje politikama 15
1.5.1 Upravitelj politika 15
1.5.2 Ovlaštene kontakt osobe 15
1.5.3 Osoba odgovorna za usklađenost pružatelja usluga povjerenja Halcom CA s politikom 15
1.5.4 Postupak za usvajanje nove politike 15
1.6. Skraćenice i termini 15
1.6.1 Skraćenice 15
1.6.2 17
Izrazi 17
2. OBJAVLJIVANJE INFORMACIJA I JAVNI IMENIK POTVRDA 17
2.1. Prikupljanje dokumenata 17
2.2. Imenik potvrda 17
2.3. Učestalost objavljivanja 18
2.4. Upravljanje pristupom do zbirke dokumenata 18
3. IDENTITET IMAOCA POTVRDE 18

3.1. Imenovanje 18
3.1.1 Prepoznatljivo ime 18
3.1.2 Zahtjevi za formiranje prepoznatljivog imena 20
3.1.3 Korištenje anonimnih imena ili pseudonima 21
3.1.4 Pravila za tumačenje prepoznatljivih imena 21
3.1.5 Jedinstvenost prepoznatljivih imena 21
3.1.6 Zaštita imena ili robnih marki 21
3.2. Provjera identiteta imaoca prilikom prvog izdavanja potvrde 21
3.2.1 Metoda za posjedovanje vlasništva nad privatnim ključem 22
3.2.2 Provjera identiteta organizacije 22
3.2.3 Provjera identiteta imaoca 22
3.2.4 Neprovjereni podaci u potvrdama 22
3.2.5 Provjera ovlaštenja zaposlenika za dobijanje potvrde 22
3.2.6 Uzajamno priznavanje 22
3.3. Provjera imaoca za ponovno izdavanje potvrde 23
3.3.1 Provjera vlasnika prilikom obnavljanja potvrde 23
3.3.2 Provjera imaoca za ponovno dobijanje potvrde nakon opoziva 23
3.4. Provjera identiteta prilikom zahtjeva za opoziv 23
4. UPRAVLJANJE POTVRDAMA 23
4.1. Dobijanje potvrde 23
4.1.1 Ko može dobiti potvrdu? 23
4.1.2 Postupak za budućeg imaoca da dobije potvrdu i odgovornosti 23
4.2.1 Provjera identiteta budućeg imaoca 24
4.2.2 Odobrenje/odbijanje zahtjeva 24
4.2.3 Vrijeme za izdavanje potvrde 24
4.3. Izdavanje potvrda 24
4.3.1 Postupak pružatelja usluga povjerenja Halcom CA 25
4.3.2 Obavještenje imaoca o izdavanju 27
4.4. Preuzimanje potvrda 27
4.4.1 Postupak preuzimanja potvrde 27
4.4.2 Objavljivanje potvrde 27

4.4.3 Obavještenje pružatelja usluga povjerenja o izdavanju potvrde trećim licima 27
4.5. Obaveze i odgovornosti korisnika u vezi s korištenjem potvrda 27
4.5.1 Obaveze imaoca potvrda 28
4.5.2 Obaveze trećih lica 28
4.6. Ponovno izdavanje potvrde 29
4.6.1 Okolnosti koje zahtijevaju ponovno izdavanje potvrde 29
4.6.2 Osobe koje mogu zatražiti ponovno izdavanje potvrde 29
4.6.3 Postupak za obradu zahtjeva za ponovno izdavanje potvrde 29
4.6.4 Obavještenje nosioca novoizdane potvrde 29
4.6.5 Postupak za prihvatanje novoizdane potvrde 29
4.6.6 Objavljivanje novoizdane potvrde 29
4.6.7 Obavještenje pružatelja usluga povjerenja o izdavanju potvrde trećim licima 29
4.7. Regeneracija ključa 30
4.7.1 Razlozi za regeneraciju 30
4.7.2 Kome je potrebna regeneracija? 30
4.7.3 Postupak za izdavanje zahtjeva za regeneraciju 30
4.7.4 Obavještenje imaocu potvrde o novoizdanoj potvrdi 30
4.7.5 Proces prihvatanja 30
4.7.6 Objavljivanje certifikata pružatelja usluga povjerenja s novim parovima ključeva 30
4.7.7 Obavještenje pružatelja usluga povjerenja o izdavanju certifikata trećim stranama 30
4.8. Promjena potvrde 30
4.8.1 Okolnosti za promjenu potvrde 30
4.8.2 Ko traži promjenu? 30
4.8.3 Postupak za podnošenje zahtjeva za promjenu 30
4.8.4 Obavještenje o izdavanju novog certifikata 30
4.8.5 Prihvatanje izmijenjenog certifikata 31
4.8.6 Objavljivanje izmijenjenog certifikata 31
4.8.7 Obavještenje o promjenama drugih entiteta 31
4.9. Opoziv i suspenzija potvrde 31
4.9.1 Razlozi za opoziv 31
4.9.2 Ko zahtjeva opoziv 32
4.9.3 Procedure opoziva 32

4.9.4 Vrijeme za izdavanje zahtjeva za opoziv....33
4.9.5 Vrijeme od prijema zahtjeva za opoziv do izvršenja opoziva....33
4.9.6 Zahtjevi za provjeru Registra opozvanih potvrda od strane trećih lica....33
4.9.7 Učestalost objavljivanja registra opozvanih potvrda....33
4.9.8 Vrijeme objave registra opozvanih potvrda....33
4.9.9 Provjera statusa potvrda u stvarnom vremenu....34
4.9.10 Zahtjevi za provjeru statusa potvrda u stvarnom vremenu....34
4.9.11 Drugi načini pristupa statusu potvrde....34
4.9.12 Posebni zahtjevi pri zloupotrebi privatnog ključa....34
4.9.13 Razlozi za suspenziju....34
4.9.14 Ko traži suspenziju?....34
4.9.15 Postupak suspenzije....34
4.9.16 Vrijeme suspenzije....34
4.10. Provjera statusa potvrda....34
4.10.1 Pristup za provjeru....35
4.10.2 Dostupnost....35
4.10.3 Ostale informacije za provjeru statusa....35
4.11. Prekid odnosa između vlasnika i pružatelja usluga povjerenja....35
4.12. Otkrivanje kopije ključeva za dešifriranje....35
4.12.1 Razlozi za otkrivanje kopije ključeva za dešifriranje....35
4.12.2 Ko traži otkrivanje kopije ključeva za dešifriranje....35
4.12.3 Postupak za podnošenje zahtjeva za otkrivanje kopije ključeva za dešifriranje....35
5. UPRAVLJANJE INFRASTRUKTUROM I NADZOR SIGURNOSTI....35
5.1. Fizička sigurnost....36
5.1.1 Lokacija i struktura pružatelja usluga povjerenja....36
5.1.2 Fizički pristup infrastrukturi pružatelja usluga povjerenja....36
5.1.3 Napajanje i ventilacija....36
5.1.4 Zaštita od poplava....36
5.1.5 Zaštita od požara....37
5.1.6 Pohranjivanje nosača podataka....37
5.1.7 Odlaganje otpada....37

5.1.8 Skladištenje na udaljenoj lokaciji....37
5.2. Organizacijska struktura pružatelja usluga povjerenja....37
5.2.1 Organizacijske grupe....37
5.2.2 Broj ljudi za pojedinačne zadatke....39
5.2.3 Identifikacija za obavljanje pojedinačnih zadataka....42
5.2.4 Nekompatibilnost zadataka....42
5.3. Nadzor osoblja....42
5.3.1 Potrebne kvalifikacije i iskustvo osoblja....43
5.3.2 Prikladnost osoblja....43
5.3.3 Dodatna obuka osoblja....43
5.3.4 Zahtjevi za redovnu obuku....43
5.3.5 Promjena zadataka....43
5.3.6 Sankcije....43
5.3.7 Zahtjevi za vanjske izvođače radova....43
5.3.8 Pristup osoblja dokumentaciji....43
5.4. Sigurnosne provjere sistema....43
5.4.1 Vrste zapisnika....43
5.4.2 Učestalost pregleda logova....44
5.4.3 Period čuvanja logova....44
5.4.4 Zaštita logova....44
5.4.5 Sigurnosne kopije logova....44
5.4.6 Prikupljanje podataka za logove....44
5.4.7 Obavještavanje osobe koja je izazvala incident....44
5.4.8 Procjena ranjivosti sistema....44
5.5. Dugoročno čuvanje podataka....44
5.5.1 Vrste dugoročno pohranjenih podataka....44
5.5.2 Period čuvanja....45
5.5.3 Zaštita dugoročno pohranjenih podataka....45
5.5.4 Sigurnosna kopija dugoročno pohranjenih podataka....45
5.5.5 Zahtjev za vremenskim žigom....45
5.5.6 Metoda prikupljanja podataka....45
5.5.7 Postupak za pristup i provjeru dugoročno pohranjenih podataka....45

5.6. Promjena javnog ključa pružatelja usluga povjerenja Halcom CA..45
5.7. Plan oporavka 45
5.7.1 Postupak u slučaju upada i zloupotrebe.....45
5.7.2 Postupak u slučaju kvara programske opreme ili podataka 46
5.7.3 Postupak u slučaju kompromitovanja privatnog ključa pružatelja usluga povjerenja Halcom CA.....46
5.7.4 Plan oporavka.....46
5.8. Prekid rada Halcom CA..... 46
6. ZAHTJEVI TEHNIČKE SIGURNOSTI 46
6.1. Generisanje i instaliranje ključeva 46
6.1.1 Generisanje ključeva 46
6.1.2 Dostava privatnog ključa vlasnicima.....46
6.1.3 Dostava javnog ključa pružatelju usluga povjerenja.....47
6.1.4 Dostava javnog ključa pružatelja usluga povjerenja 47
6.1.5 Dužina ključa.....47
6.1.6 Generisanje i kvalitet parametara javnog ključa.....47
6.1.7 Svrha ključeva i potvrda 47
6.2. Zaštita privatnog ključa 48
6.2.1 Standardi kriptografskih modula 48
6.2.2 Kontrola privatnog ključa od strane ovlaštenih osoba 48
6.2.3 Detekcija kopije privatnog ključa.....48
6.2.4 Sigurnosna kopija privatnog ključa.....48
6.2.5 Arhiviranje privatnog ključa 48
6.2.6 Prijenos privatnog ključa iz/u kriptografski modul.....48
6.2.7 Pohranjivanje privatnog ključa u kriptografskom modulu 48
6.2.8 Postupak za aktiviranje privatnog ključa 49
6.2.9 Postupak za deaktivaciju privatnog ključa 50
6.2.10 Postupak uništavanja privatnog ključa.....50
6.2.11 Svojstva kriptografskog modula.....50
6.3. Ostali aspekti upravljanja ključevima 50
6.3.1 Arhiviranje javnog ključa 50
6.3.2 Period važenja javnih i privatnih ključeva.....50

6.4. Lozinke za pristup potvrdama ili ključevima 50
6.4.1 Generisanje lozinke 50
6.4.2 Zaštita lozinkom 51
6.4.3 Ostali aspekti lozinki 52
6.5. Sigurnosni zahtjevi za informacionu i komunikacijsku opremu pružatelja usluga povjerenja 52
6.5.1 Specifični tehnički sigurnosni zahtjevi 52
6.5.2 Nivo sigurnosne zaštite 52
6.6. Tehnička kontrola životnog ciklusa pružatelja usluga povjerenja 52
6.6.1 Kontrola razvoja sistema 52
6.6.2 Upravljanje sigurnošću 53
6.6.3 Kontrola životnog ciklusa 53
6.7. Kontrola sigurnosti mreže 53
6.8. Vremensko označavanje 53
7. PROFIL POTVRDE I REGISTRA OPOZVANIH POTVRDA 53
7.1. Profil potvrde 53
7.1.1 Verzija potvrde 53
7.1.2 Profil potvrde s ekstenzijama 53
7.1.3 Identifikacijske oznake algoritma 61
7.1.4 Format prepoznatljivog imena 61
7.1.5 Ograničenja imena 61
7.1.6 Oznaka politike potvrde 61
7.1.7 Ograničenja korištenja 61
7.1.8 Sintaksa i značenje oznaka politike potvrde 61
7.1.9 Važnost bitnih dopuna politika 61
7.2. Profil registra opozvanih potvrda 61
7.2.1 Verzija 62
7.2.2 Sadržaj i proširenja registra 62
7.2.3 Objavljivanje registra opozvanih potvrda 64
7.3. Profil provjere statusa potvrde u stvarnom vremenu 64

7.3.1 Verzija provjere statusa u stvarnom vremenu....64
7.3.2 Profil provjere statusa u stvarnom vremenu....64
8. NADZOR....64
8.1. Učestalost kontrole....65
8.2. Vrsta i osposobljenost nadzora....65
8.3. Nezavisnost nadzora....65
8.4. Područja kontrole....65
8.5. Mjere pružatelja usluga povjerenja....65
8.6. Objavljivanje rezultata kontrole....65
9. FINANSIJSKA I DRUGA PRAVNA PITANJA....65
9.1. Cjenovnik....65
9.1.1 Cijena izdavanja i obnavljanja potvrde....65
9.1.2 Cijena pristupa do potvrda....66
9.1.3 Cijena pristupa do statusa potvrda i registra opozvanih potvrda....66
9.1.4 Cijene ostalih usluga....66
9.1.5 Povrat troškova....66
9.2. Finansijska odgovornost....66
9.2.1 Osiguranje....66
9.2.2 Ostalo pokriće....66
9.2.3 Osiguranje imaoca....66
9.3. Zaštita poslovnih podataka....66
9.3.1 Zaštićeni podaci....66
9.3.2 Nezaštićeni podaci....66
9.3.3 Odgovornost za sigurnost....67
9.4. Zaštita ličnih podataka....67
9.4.1 Plan zaštite ličnih podataka....67
9.4.2 Zaštićeni lični podaci....67
9.4.3 Nezaštićeni lični podaci....67
9.4.4 Odgovornost za zaštitu ličnih podataka....67
9.4.5 Ovlaštenje u vezi s korištenjem ličnih podataka....67

9.4.6 Proslijeđivanje ličnih podataka 67
9.4.7 Ostale odredbe u vezi sa zaštitom ličnih podataka 68
9.5. Odredbe o pravima intelektualnog vlasništva 68
9.6. Obaveze i odgovornosti 68
9.6.1 Obaveze i odgovornosti pružatelja usluga povjerenja Halcom CA 68
9.6.2 Obaveza i odgovornost prijavne službe 69
9.6.3 Obaveze i odgovornost imaoca potvrda 69
9.6.4 Obaveze i odgovornost trećih lica 70
9.6.5 Obaveze i odgovornost drugih osoba 70
9.7. Odricanje odgovornosti 70
9.8. Ograničenje upotrebe 71
9.9. Naplata štete 71
9.10. Važenje politike 71
9.10.1 Period važenja 71
9.10.2 Kraj važenja politike 71
9.10.3 Posljedice isteka politike 71
9.11. Komunikacija između subjekata 72
9.12. Izmjene i dopune 72
9.12.1 Postupak za prihvatanje izmjena i dopuna 72
9.12.2 Važenje i objavljivanje izmjena i dopuna 72
9.12.3 Promjena identifikacijskog broja politike 72
9.13. Postupak rješavanja sporova 72
9.14. Primjenjivo zakonodavstvo 72
9.15. Usklađenost s važećim zakonodavstvom 72
9.16. Opće odredbe 73
9.17. Ostale odredbe 73

1. UVOD

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

(2) Ova politika je javni dio internih pravila Halcom CA za kvalifikovane digitalne certifikate za fizička lica.

(3) Oblik i sadržaj ove politike su u skladu s uredbom eIDAS, uredbom eIDAS 2.0, međunarodnom preporukom IETF RFC i evropskim ETSI standardima, između ostalog.

1.1. Pregled

(1) Ova politika predstavlja nedjeljivu cjelinu općih pravila poslovanja pružatelja usluga povjerenja Halcom CA u vezi s izdavanjem kvalificiranih digitalnih certifikata, uređuje svrhu, rad i metodologiju upravljanja kvalificiranim digitalnim certifikatima, kao i sigurnosne zahtjeve koje mora ispunjavati pružatelj usluga povjerenja Halcom CA, vlasnici certifikata, treće strane koje se oslanjaju na te certifikate, te odgovornost svih navedenih osoba.

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

(3) Halcom CA izdaje kvalifikovane digitalne potvrde sa najmanje jednim parom ključeva i uz obaveznu upotrebu sigurnog medija.

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

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

(6) Halcom CA objavljuje popis prijavinh službi koji omogućavaju sticanje kvalificiranih digitalnih certifikata za fizička lica na internetu.

1.2. Identifikacijski podaci politike

(1) Oznake operativne politike Halcom CA FO:

Politika	CPOID	Vrsta certifikata

Halcom CA FO e-signature 1	1.3.6.1.4.1.5939.1.4.4 1.3.6.1.4.1.5939.1.5.4	QCert for ESig Cert for Esig
Halcom CA FO elektronski potpis 2	1.3.6.1.4.1.5939.1.4.5 1.3.6.1.4.1.5939.1.5.5	QCert for ESig Cert for Esig
Halcom CA FO e-sign 1G2	1.3.6.1.4.1.5939.1.4.7 1.3.6.1.4.1.5939.1.5.7	QCert for ESig Cert for Esig

(2) Svaka potvrda sadrži referencu politike u obliku CPOID-a (pogledajte odjeljak 7.1.2).

1.3. Subjekti

1.3.1 Pružatelj usluga povjerenja Halcom CA

Halcom CA je pružatelj usluga povjerenja koji izdaje i upravlja kvalificiranim digitalnim potvrdama koje povezuju podatke za validaciju kvalificiranog elektroničkog potpisa s fizičkom osobom. Pružatelj usluga 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 fizičkog lica i drugih podataka važnih za upravljanje kvalifikovanim digitalnim potvrdama,
- primanje zahtjeva za dobijanje potvrda,
- prihvatanje zahtjeva za opoziv potvrda,
- izdavanje potrebne dokumentacije fizičkim licima, vlasnicima ili budućim vlasnicima,
- prosljeđivanje zahtjeva i ostalih podataka na siguran način pružatelju usluga povjerenja Halcom CA.

(2) Pored svoje prijavne službe, pružatelj usluga 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 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 povjerenja Halcom CA uspostavio je geografski raspršenu uslugu registracije, koja potencijalnim vlasnicima omogućava jednostavnu registraciju u svom mjestu ili obližnjoj lokaciji. Informacije o lokacijama prijavnih službi dostupne su na web stranici pružatelja usluga povjerenja Halcom CA.

1.3.3 Naručioci i vlasnici potvrda

(1) Vlasnik potvrde, koji je fizičko lice, koristi svoje podatke (par ključeva/parove ključeva) koje mu je dodijelio pružatelj usluga povjerenja za kvalificirano elektroničko potpisivanje i kvalificirane digitalne potvrde kako bi povezao taj elektronički potpis s vlasnikom.

(2) Naručioc potvrde je fizičko lice.

1.3.4 Treće osobe

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

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

(3) Treće osobe ne moraju nužno biti vlasnici potvrda pružatelja usluga povjerenja Halcom CA ili digitalnih potvrda drugih pružatelja usluga povjerenja. .

1.4. Svrha upotrebe

Halcom CA upravlja (izdaje i provjerava, opoziva, produžava, pohranjuje, objavljuje) kvalificiranim digitalnim potvrdama fizičkih osoba za provjeru valjanosti elektroničkih potpisa (u daljnjem tekstu potvrde), koje su namijenjene fizičkim osobama.

1.4.1 Pravilna upotreba potvrda i ključeva

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

1) identifikacija imaoca (fizičkog lica),
2) pokazivanja identiteta imaoca (fizičkog lica),
3) elektronsko potpisivanje dokumenata,
4) šifriranje i dešifriranje dokumenata u elektronskom obliku.

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

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

1.4.2 Neovlaštena upotreba

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

(2) Potvrde nisu namijenjene za preprodaju.

1.5. Upravljanje politikama

1.5.1 Upravitelj politika

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

(2) Adresa upravitelja:

Halcom d.d.
Dunajska cesta 123
1000 LJUBLJANA
Slovenija

1.5.2 Ovlaštene kontakt osobe

(1) Za pitanja u vezi s ovom politikom, možete se obratiti ovlaštenim osobama pružatelja usluga 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-pošta: ca@halcom.si
E-mail za otkazivanje : ca_preklici@halcom.si

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

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

1.5.4 Postupak za usvajanje nove politike

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

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

1.6. Skraćenice i termini

1.6.1 Skraćenice

CA	Pružatelj usluga povjerenja koji izdaje potvrde (Certificate Authority ili Certificate Agency).

CPName	Naziv politike pružatelja usluga povjerenja (engl.: Certification Policy Name), jedinstveno povezan s međunarodnim CPOID brojem politike (engl.: Certification Policy Object Identifier).
CP	Politika pružatelja usluga povjerenja (engl.: Certificate Policy). Politika uređuje svrhu, rad i metodologiju upravljanja uslugom, kao i odgovornosti i sigurnosne zahtjeve koje moraju ispuniti pružatelj usluga povjerenja, vlasnici potvrda (korisnici usluga) i treće osobe koje se oslanjaju na ove potvrde/usluge.
CPS	CPS (engl.: Certification Practice Statement) predstavlja opšta pravila poslovanja pružatelja usluga povjerenja.
CPOID	Međunarodni broj koji jedinstveno identificira politiku poslovanja (engl.: Certification Policy Object IDentifier).
CRL	Certificate Revocation List – lista opozvanih digitalnih potvrda.
DN	Jedinstveno prepoznatljivo ime (uporedi definiciju prepoznatljivog imena) (engl.: Distinguished Name).
LDAP	Lightweight Directory Access Protocol je protokol koji definira pristup direktoriju i specificiran je prema preporuci IETF-a (Internet Engineering Task Force) IETF RFC 3494:.
S/MIME	Secure Multipurpose Internet Mail Extensions
SSL	Secure Sockets Layer
TLS	Transport Layer Security
PKI	Public Key Infrastructure je infrastruktura javnog ključa.
EŠEI	Jedinstveni elektronski identifikacijski broj
HSM	Modul hardverske sigurnosti (engl.: Hardware Security Module).
G1, G2, G32	Prva, druga ili treća generacija Halcom CA root i podređenih potvrda.
QCert for ESig/ESeal	Kvalifikovana digitalna potvrda izdana na sigurnom mediju (engl.: QSCD – Qualified signature creation device). Halcom CA može izdati portvrdu na pametnoj kartici, USB pametnom ključu ili u cloudu (HSM). Potvrda je namijenjena za kvalifikovani elektronski potpis/pečat (engl.: Qualified electronic signature/seal).
Certificate for Esig/Eseal	Kvalifikovana digitalna potvrda izdana u datoteci namijenjenoj za napredni elektronski potpis/pečat (engl.: Advanced electronic signature/seal).
QRemManage for QSigCD/ QSealCD	Upravljanje uređajima za kreiranje kvalifikovanog elektronskog potpisa/pečata na daljinu (eng. Management of remote qualified electronic signature/seal creation devices).
OT Potvrda	OT potvrda (eng. One Time Certificate) je potvrda sa kratkom važnošću, namijenjena za jednokratno potpisivanje dokumenta ili grupe dokumenata.

1.6.2 Izrazi

Imenik potvrda	Imenik X.500 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.
Pružatelj usluga povjerenja	Fizičko ili pravno lice koje izdaje potvrde ili obavlja druge usluge povjerenja (engl.: Trust Service provider - TSP).
Prijavna služba	SLužba ili osoba koja prihvata zahtjeve za potvrde i vrši identifikaciju i provjeru identiteta potencijalnih vlasnika u ime pružatelja usluga 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 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 (sažeci bitnih komponenti i na engleskom jeziku).

(2) Dokumenti koji su javno dostupni su:

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

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

2.2. Imenik potvrda

(1) Nove politike su objavljene kako je naznačeno u tački 9.10.

(2) Sve potvrde pružatelja usluga 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 član 4.9.8.), a po potrebi se objavljuju i druge javno dostupne informacije ili dokumenti.

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

2.3. Učestalost objavljivanja

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

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

(3) Lista opozvanih potvrda se osvježava odmah (maksimalno pet (5) sekundi) nakon što je potvrda opozvana u javnom 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 imenik je dostupan na serveru ldap.halcom.si, TCP port 389 putem LDAP protokola. Javno je dostupan samo registar opozvanih potvrda, koji je dio imenika.

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

3. IDENTITET IMAOCA POTVRDE

3.1. Imenovanje

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

3.1.1 Prepoznatljivo ime

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

(2) Pružatelj usluga 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 povjerenja Halcom CA (više o tome u članu 3.1.5).

(4) U skladu sa eIDAS uredbom, eIDAS uredbom 2.0 i ETSI standardima, Halcom CA može koristiti i druge semantičke identifikatore fizičkih lica i poslovnih subjekata prilikom kreiranja prepoznatljivog

imena stranih fizičkih lica i/ili stranih poslovnih subjekata, kao što su "PNO", "IDC" ili "PAS" i ISO 3161-1 kod države za identifikaciju na osnovu nacionalnog registracijskog broja ili broja pasoša ili lične karte za fizička lica, a za poslovne subjekte "NTR" i ISO 3161-1 kod države za identifikaciju na osnovu identifikatora iz nacionalnog registra poslovnih subjekata ili lokalnog koda (dva znaka u skladu sa lokalnom definicijom u određenoj zemlji, koji se smatra prikladnim za nacionalni i evropski nivo).

(5) Halcom CA može prilikom formiranja prepoznatljivog imena stranih fizičkih osoba i/ili stranih poslovnih subjekata koristiti i druge semantičke identifikatore fizičkih osoba i poslovnih subjekata, kao što su „PNO“, „IDC“, „PAS“ ili „EID“, zajedno sa ISO 3166-1 oznakom države za identifikaciju na osnovu nacionalnog matičnog broja ili broja pasoša, lične karte ili sredstva za elektronsku identifikaciju za fizičke osobe. Za poslovne subjekte koristi se „NTR“ i ISO 3166-1 oznaka države za identifikaciju na osnovu identifikatora iz nacionalnog registra poslovnih subjekata ili lokalna oznaka (dva znaka u skladu s lokalnom definicijom u određenoj državi, koja se smatra prikladnom na nacionalnom i evropskom nivou).

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

(7) Pružalac usluga povjerenja Halcom CA može prilikom izdavanja kvalifikovane digitalne potvrde u polje *Imaoc* (eng. *Subject*) dodati i atribut 1.3.6.1.4.1.5939.2.9, koji predstavlja vrstu potvrde (npr. označava da se radi o kvalifikovanoj digitalnoj potvrdi u cloudu, na pametnoj kartici ili USB ključu i sl.).

(8) Potvrde pružatelja usluga povjerenja Halcom CA:

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

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

3.1.2 Zahtjevi za formiranje prepoznatljivog imena

Oznaka fizičke osobe uključena u prepoznatljivo ime u skladu s odredbama člana 3.1.1 mora ispunjavati sljedeće zahtjeve:

- mora biti jedinstven,
- mora biti semantički povezan sa vlasnikom,

- maksimalna dužina može biti četrdeset dva (42) znaka.

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 vlasniku potvrde u prepoznatljivom imenu G1 potvrde 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) Podatke o imaocu potvrde u prepoznatljivom imenu G2 i G3 potvrda sadrže znakove iz UTF-8 kodne tabele.

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

3.1.5 Jedinstvenost prepoznatljivih imena

Prepoznatljiva imena su jedinstvena za svaku izdanu potvrdu i nedvosmisleno i jedinstveno identificiraju vlasnika u strukturi direktorija.

3.1.6 Zaštita imena ili robnih marki

(1) Imaoci ne mogu zahtijevati nazive državnih organa ili organa lokalne zajednice, imena, oznake, žigove 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.

3.2. Provjera identiteta imaoca prilikom prvog izdavanja potvrde

3.2.1 Metoda za posjedovanje vlasništva nad privatnim ključem

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

3.2.2 Provjera identiteta organizacije

Nije propisano.

3.2.3 Provjera identiteta imaoca

(1) Prijavna služba pružaoca usluga povjerenja Halcom CA nesporno utvrđuje identitet imaoca potvrde u skladu s važećim propisima (službeni dokument sa slikom) ili pruža podatke o imaocima iz svojih baza podataka dobijene 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 provjeravati i u skladu s nacionalnim propisima te države članice, pod uslovom da ti propisi osiguravaju jednaku razinu pouzdanosti i da se smatraju prikladnim na nacionalnom i evropskom nivou.

(3) Identitet imaoca potvrda može se provjeriti putem evropskog novčanika za digitalni identitet ili na osnovu prijavljenog sredstva elektronske identifikacije koje ispunjava zahtjeve u vezi s visokom razinom pouzdanosti.

(4) Pružalac usluga povjerenja Halcom CA provjerava lične podatke imatelja potvrde u odgovarajućim registrima, osim ako važeći propisi ne određuju drugačije.

3.2.4 Neprovjereni podaci u potvrdama

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

3.2.5 Provjera ovlaštenja zaposlenika za dobijanje potvrde

Nije propisano.

3.2.6 Uzajamno priznavanje

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

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

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

(4) Troškove potrebne infrastrukture koju pružatelj usluga povjerenja Halcom CA zahtijeva za

međusobno priznavanje snosi drugi pružatelj usluga povjerenja.

3.3. Provjera imaoca za ponovno izdavanje potvrde

3.3.1 Provjera vlasnika prilikom obnavljanja potvrde

Identitet vlasnika prilikom ponovnog izdavanja potvrde se provjerava:

- u prijavnoj službi pružatelja usluga povjerenja Halcom CA,
- na osnovu već izdate važeće kvalifikovane digitalne potvrde koji je izdao kvalifikovani pružalac usluga povjerenja, pri čemu pružalac usluga povjerenja Halcom CA provjerava podatke vlasnika u odgovarajućim registrima.

3.3.2 Provjera imaoca za ponovno dobijanje potvrde nakon opoziva

Provjera imaoca se vrši u skladu sa odredbama člana 3.2.3.

3.4. Provjera identiteta prilikom zahtjeva za opoziv

(1) Zahtjev za opoziv imaoc potvrde podnosi:

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

(2) Detaljan postupak opoziva: član 4.9.3.

4. UPRAVLJANJE POTVRDAMA

4.1. Dobijanje potvrde

4.1.1 Ko može dobiti potvrdu?

(1) Budući imaoci potvrda izdatih u skladu s ovom politikom su fizička lica.

(2) Potvrda se neće izdati potencijalnom imaocu ako je uvršten 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 budućeg imaoca da dobije potvrdu i odgovornosti

(1) Potvrda se izdaje na osnovu pravilno popunjene i potpisane narudžbenice za izdavanje potvrde od strane budućeg imatelja potvrde ili na osnovu dostavljenih podataka iz baza prijavne službe, pribavljenih postupkom koji prijavna služba koristi za druge svrhe, a koji u skladu s važećim propisima osigurava jednaku razinu pouzdanosti.

(2) Imaoc potvrde podnosi ili potvrđuje zahtjev u prijavnoj službi Halcom CA te izmiruje finansijske obaveze u vezi s izdavanjem potvrde. Narudžbenice za izdavanje digitalne potvrde dostupne su u

prijavnim službama 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 upoznaje budućeg imaoca potvrde sa CPS-om, politikom i obavještenjem o djelovanju pružatelja usluga povjerenja Halcom CA.4.2. Postupak po prijemu zahtjeva za dobijanje potvrde

4.2.1 Provjera identiteta budućeg imaoca

(1) Ovlaštena osoba u prijavnoj službi provjerava identitet imaoca važećim ličnim dokumentom sa slikom prilikom posjete prijavnoj službi ili putem kurirske službe ili sigurnog elektronskog portala prilikom dostave pametne kartice, PIN koda, lozinke za preuzimanje ili narudžbenice za potvrdu u cloudu.

(2) Prijavna služba pružatelja usluga povjerenja Halcom CA može također pružiti podatke iz svojih baza podataka dobivene postupkom koji servis registracije 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 potvrde (državljana te države) može se provjeriti i u skladu s nacionalnim propisima te države članice, koji osiguravaju jednaku razinu pouzdanosti i smatraju se primjerenim za nacionalni i evropski nivo.

(4) Identitet nositelja potvrda može se provjeriti putem evropskog novčanika za digitalni identitet ili na osnovu prijavljenog sredstva elektronske identifikacije koje ispunjava zahtjeve u vezi s visokim nivoom pouzdanosti.

(5) Ovlaštene osobe su dužne provjeriti identitet budućeg imaoca i sve podatke navedene u zahtjevu i dostupne 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 povjerenja Halcom CA odobravaju narudžbenicu za dobijanje potvrde ili, u slučaju netačnih ili nepotpunih podataka ili neispunjavanja obaveza, istu odbijaju, o čemu se budući imaoc odmah obavještava lično ili putem e-maila.

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

4.2.3 Vrijeme za izdavanje potvrde

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

4.3. Izdavanje potvrda

4.3.1 Postupak pružatelja usluga povjerenja Halcom CA

(1) Proces proizvodnje zavisi od vrste potvrde.

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

  1. prije personalizacije sigurnog medija (generiranje ključeva na kartici/USB ključu i lozinke za zaštitu potvrde),
  2. obrada zahtjeva za izdavanje potvrde,
  3. priprema potvrde,
  4. personalizacija sigurnog medija (izdavanje i snimanje potvrde, štampanje podataka imaoca),
  5. štampanje lične lozinke (PIN kod – samo ako se šalje preporučenom poštom),
  6. prosljeđivanje potvrde, lične lozinke (PIN koda) i obavještavanje vlasnika.

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

- Kvalifikovana digitalna potvrda u cloudu:

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

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

  Registracijski i aktivacijski kodovi šalju se vlasniku putem dva odvojena kanala, jednog putem e-maila, a drugog putem drugog sigurnog kanala (siguran web portal dostupan sa kvalificiranom potvdrom, 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 vlasnika, posljednje četiri cifre ili CVV kod platne ili kreditne kartice ili slično)). Izuzetno, jedan od navedenih kodova vlasniku 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):

  Proizvodni postupak za potvrde i za par 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.

OT potvrda je namijenjena jednokratnom potpisu dokumenta ili skupa dokumenata u različitim mobilnim ili web aplikacijama na tržištu. Pri svakom kreiranju elektronskog potpisa u sistemu za digitalno potpisivanje na daljinu stvara se novi privatni potpisni ključ i izdaje nova OT potvrda.

- 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. prijem potvrde.

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

(2) Imaoc kvalifikovane potvrde može za pristup svojoj potvrdi i aktivacijskim podacima koristiti isključivo mobilne ili web aplikacije pružatelja usluga 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 poslovanja Halcom CA.
Imaoc potvrde sklapanjem ugovora o izdavanju potvrde izričito dozvoljava tehničke provjere korištenja aplikacije u obimu potrebnom za osiguravanje usklađenosti s uslovima ove politike i važećom zakonskom regulativom.

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

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

4.3.2 Obavještenje imaoca o izdavanju

Pogledajte prethodni član.

4.4. Preuzimanje potvrda

4.4.1 Postupak preuzimanja potvrde

(1) Postupak preuzimanja zavisi od vrste potvrde

- Napredna kvalifikovana potvrda

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

- Kvalifikovana potvrda za elektronski potpis u cloudu

Za potvrde u cloudu nije potrebno preuzeti potvrdu, jer je sigurno pohranjuje Halcom CA, pružatelj usluga povjerenja, po odobrenju imaoca. Imaocu se dodjeljuju samo pristupni kodovi za pristup do sigurnog clouda, pogledajte član 4.3.1.

- OT potvrda

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

- Standardna kvalifikovana potvrda

Za standardne potvrde, budući imaoc potvrdu preuzima u skladu s uputama za korištenje Halcom CA softvera za dobijanje kvalificiranih digitalnih potvrda. Korisniku se dostavljaju samo kodovi za dobijanje standardne potvrde, vidjeti član 4.3.1.

(2) Imaoc potvrde, odnosno poslovni subjekt, mora prilikom preuzimanja potvrde odmah provjeriti podatke u potvrdi i u slučaju eventualnih grešaka ili problema bez odlaganja obavijestiti pružatelja usluga povjerenja Halcom CA.

4.4.2 Objavljivanje potvrde

Proces je opisan u članu 2.

4.4.3 Obavještenje pružatelja usluga povjerenja o izdavanju potvrde trećim licima

Pružatelj usluga povjerenja Halcom CA ne obavještava treća lica o izdavanju pojedinačnih potvrda imaoca 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 pridržava prije izdavanja potvrde,
- postupati u skladu s politikom i drugim važećim propisima,
- nakon prijema ili aktivacije potvrde, provjeriti podatke u potvrdi i odmah obavijestiti Halcom CA o 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 potvrdama,
- odmah obavijestiti Halcom CA o svim promjenama vezanim za potvrde,
- zatražiti opoziv potvrde ako je privatni ključ kompromitovan na način koji utiče na pouzdanost korištenja ili ako postoji rizik od zloupotrebe,
- zatražiti opoziv potvrde u cloud-u ako je mobilni telefon izgubljen ili ukraden ili ako postoji rizik od zloupotrebe,
- koristiti potvrdu u svrhu navedenu u potvrdi (vidjeti odjeljak 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,
- zaštitite privatni ključ i sve ostale povjerljive podatke odgovarajućim PIN kodom u skladu s preporukama Halcom CA ili na drugi način tako da samo vlasnik ima pristup njima,
- Pažljivo zaštitite PIN kod radi zaštite ili pristupa privatnom ključu,
- nakon isteka ili opoziva potvrde, postupite 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 sa i u svrhu 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 vlasnika potvrde na koju 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 odjeljak 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 kreiran u roku važenja i za odgovarajuću svrhu potvrde,

- tokom korištenja potvrde, provjeriti potpis potvrde pružatelja usluga povjerenja Halcom CA, koji je objavljen u ovoj politici, a također i na web stranicama Halcom CA ili drugih pružatelja usluga povjerenja,
- pridržavati se drugih odredbi ako je zaključen ugovor s pružateljem usluga povjerenja Halcom CA o korištenju potvrde.

(2) Da bi provjerio valjanost potpisa ili druge kriptografske operacije, treće lice mora koristiti softver i hardver koji može pouzdano provjeriti sve gore navedene zahtjeve za sigurnu upotrebu potvrde.

4.6. Ponovno izdavanje potvrde

(1) Važenje potvrde može se produžiti samo na zahtjev imaoca potvrde.

(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 važećom potvrdom.

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

4.6.1 Okolnosti koje zahtijevaju ponovno izdavanje potvrde

Prije isteka važenja digitalne potvrde, imaoci potvrde mogu osigurati kontinuitet korištenja digitalne potvrde podnošenjem elektronskog zahtjeva za ponovno izdavanje. Međutim, zahtjev za novo izdavanje može se podnijeti i nakon isteka važenja digitalne potvrde.

4.6.2 Osobe koje mogu zatražiti ponovno izdavanje potvrde

Važenje potvrde može se produžiti samo na zahtjev imaoca potvrde.

4.6.3 Postupak za obradu zahtjeva za ponovno izdavanje potvrde

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

4.6.4 Obavještenje nosioca novoizdane potvrde

Pogledajte član 4.3.1.

4.6.5 Postupak za prihvatanje novoizdane potvrde

Pogledajte član 4.4.1.

4.6.6 Objavljivanje novoizdane potvrde

Proces je opisan u članu 2.

4.6.7 Obavještenje pružatelja usluga povjerenja o izdavanju potvrde trećim licima

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

4.7. Regeneracija ključa

4.7.1 Razlozi za regeneraciju

Nije podržano.

4.7.2 Kome je potrebna regeneracija?

Nije podržano.

4.7.3 Postupak za izdavanje zahtjeva za regeneraciju

Nije podržano.

4.7.4 Obavještenje imaocu potvrde o novoizdanoj potvrdi

Nije podržano.

4.7.5 Proces prihvatanja

Nije podržano.

4.7.6 Objavljivanje certifikata pružatelja usluga povjerenja s novim parovima ključeva

Nije podržano.

4.7.7 Obavještenje pružatelja usluga povjerenja o izdavanju certifikata 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 dobijanja nove potvrde, kako je navedeno u tački 4.1.

4.8.1 Okolnosti za promjenu potvrde

Nije podržano.

4.8.2 Ko traži promjenu?

Nije podržano.

4.8.3 Postupak za podnošenje zahtjeva za promjenu

Nije podržano.

4.8.4 Obavještenje o izdavanju novog certifikata

Nije podržano.

4.8.5 Prihvatanje izmijenjenog certifikata

Nije podržano.

4.8.6 Objavljivanje izmijenjenog certifikata

Nije podržano.

4.8.7 Obavještenje o promjenama drugih entiteta

Nije podržano.

4.9. Opoziv i suspenzija potvrde

(1) Vlasnik potvrde može zatražiti opoziv potvrde u bilo kojem trenutku, ali to mora učiniti u sljedećim slučajevima:

1. Promjene razlikovnog imena (DN),
2. kada vlasnik potvrde promijeni ključne podatke povezane s potvrdom (ime ili prezime),
3. kada se utvrdi ili posumnja da je ključ za potpisivanje otkriven ili da je potvrda zloupotrijebljena,
4. zamjena potvrde drugom potvrdom (npr. u slučaju gubitka sigurnog medija, gubitka mobilnog telefona, gubitka lozinki za pristup podacima na kartici itd.).

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

(3) Potvrda se može opozvati 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, opozvane potvrde će biti označene kao opozvane u direktoriju i dodate u registar opozvanih potvrda. Ako imaoc Halcom CA potvrde podnese nevažeći zahtjev za opoziv potvrde, bit će obaviješten o zahtjevu za opoziv nevažeće potvrde i bit će obaviješten o uputama za podnošenje važećeg zahtjeva za opoziv.

4.9.1 Razlozi za opoziv

(1) Imaoc mora zatražiti opoziv potvrde u sljedećim slučajevima:

- ako je privatni ključ vlasnika 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 povjerenja Halcom CA opoziva potvrdu i bez zahtjeva vlasnika u slijedećem slučaju:

- da su informacije u potvrdi netačne ili da je potvrda izdata na osnovu netačnih informacija,
- da je došlo do greške prilikom provjere identiteta podataka u prijavnoj službi,
- da su se promijenile druge okolnosti koje utiču na važenje potvrde,
- zbog neispunjavanja obaveza nosioca,
- da svi troškovi upravljanja digitalnim potvrdama nisu podmireni,
- da je infrastruktura pružatelja usluga povjerenja kompromitovana na način koji utječe na pouzdanost potvrde,
- da je privatni ključ vlasnika potvrde kompromitovan na način koji utiče na pouzdanost korištenja,
- da će Halcom CA prestati izdavati potvrde ili da je pružatelju usluga povjerenja zabranjeno upravljanje potvrdama i da njegove aktivnosti nije preuzeo drugi pružatelj usluga povjerenja,
- da je opoziv naložio nadležni sud, prekršajni ili upravni organ.

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

4.9.2 Ko zahtjeva opoziv

Opoziv potvrde može zahtijevati:

- imaoc,
- nadležni sud, prekršajni ili upravni organ.

4.9.3 Procedure opoziva

(1) Imaoc može zatražiti opoziv:

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

(2) Ako se traži opoziv:

- lično, potrebno je popuniti odgovarajući zahtjev za opoziv potvrde i podnijeti ga prijavnoj službi,
- elektronski, imaoc mora poslati elektronsku poruku Halcom CA sa zahtjevom za opoziv, koji mora biti digitalno potpisan pouzdanom potvrdom radi njegove provjere,
- Ako vlasnik potvrde zatraži opoziv potvrde putem telefona ili e-pošte, pružatelj usluga

povjerenja Halcom CA nalaže suspenziju potvrde. Tek na osnovu pismenog zahtjeva za opoziv potvrde, potvrda se zapravo opoziva.

(3) Imaoc mora uvijek biti obaviješten o datumu i vremenu opoziva. Pružalac usluga povjerenja, na pisani zahtjev poslovnog subjekta ili nosioca, dužan je dostaviti i dodatne informacije o opozivu (podaci o podnosiocu zahtjeva za 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 prijavne službe (pogledajte sljedeći član).

4.9.5 Vrijeme od prijema zahtjeva za opoziv do izvršenja opoziva

(1) Po prijemu valjanog zahtjeva za opoziv, pružatelj usluga 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 pet (5) sekundi) dodaje u registar opozvanih potvrda.

4.9.6 Zahtjevi za provjeru Registra opozvanih potvrda od strane trećih lica

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

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

4.9.7 Učestalost objavljivanja registra opozvanih potvrda

Registar opozvanih potvrda se osvježava (za pristup registru, pogledajte član7.2.3):

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

4.9.8 Vrijeme objave registra opozvanih potvrda

(1) Objavljivanje novog registra opozvanih potvrda vrši se:

- u javnom 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 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 stvarnom vremenu

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

4.9.10 Zahtjevi za provjeru statusa potvrda u stvarnom vremenu

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

4.9.11 Drugi načini pristupa statusu potvrde

Nisu podržani.

4.9.12 Posebni zahtjevi pri zloupotrebi privatnog ključa

Nisu specificirani.

4.9.13 Razlozi za suspenziju

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

(2) Ako vlasnik potvrde, treće lice ili druge osobe, državni ili srodni organi, ili sam pružatelj usluga povjerenja, izraze sumnju da se s potvrdom postupa kršeći ovu politiku ili važeće propise, potvrdaće biti privremeno suspendirana do donošenja konačne odluke.

4.9.14 Ko traži suspenziju?

Pogledajte član 4.9.13.

4.9.15 Postupak suspenzije

Pogledajte član 4.9.13.

4.9.16 Vrijeme suspenzije

Pogledajte član 4.9.13.

4.10. Provjera statusa potvrda

4.10.1 Pristup za provjeru

(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 stvarnom 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 potvrde dostupna je dvadeset četiri (24) sata dnevno, svakog dana u godini.

(2) Pružatelj usluga 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 provjeru statusa 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 vlasnika i pružatelja usluga povjerenja

Odnos između nosioca i pružatelja usluga povjerenja Halcom CA prestaje ako:

- potvrda vlasnika ističe i nije obnovljena,
- potvrda je opozvana i vlasnik ne traži novu.

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 INFRASTRUKTUROM I NADZOR SIGURNOSTI

(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-ja.

(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 sistemom neprekidnog napajanja na više nivoa.

(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 sistemom fizičke i elektronske sigurnosti na više nivoa.

(2) Sigurnost infrastrukture pružatelja usluga 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 povjerenja.

5.1.1 Lokacija i struktura pružatelja usluga povjerenja

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

(2) Osiguran je sistemom fizičke i elektronske sigurnosti na više nivoa.

(3) Detaljne odredbe sadržane su u internim pravilima pružatelja usluga 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 povjerenja u skladu s njihovim zadacima i ovlaštenjima, vidjeti član 5.2.1.

(2) Sav pristup je zaštićen u skladu sa zakonodavstvom i preporukama.

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

5.1.4 Zaštita od poplava

(1) Infrastruktura pružatelja usluga 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 nosača podataka

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

(2) Sigurnosne kopije softvera i šifriranih baza podataka pružatelja usluga 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 povjerenja Halcom CA.

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

5.1.8 Skladištenje na udaljenoj lokaciji

Pogledajte član 5.1.6.

5.2. Organizacijska struktura pružatelja usluga povjerenja

5.2.1 Organizacijske grupe

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

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

- zaposleni kod pružatelja usluga povjerenja Halcom CA i
- prijavne službe .

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

- upravljanje informacionim sistemom,

- upravljanje potvrdama,
- sigurnost i kontrola,
- regulatorni.

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 operator 1	• Priprema kopija sistema, nadogradnja i vraćanje softvera, sigurno skladištenje i distribucija kopija i nadogradnji, • administrativne funkcije vezane za održavanje, • obavljanje arhiviranja potrebnih sistemskih zapisa, • štampa PIN kodova, • dnevna provjera sistema.	2
	Operator autorizacije	• Potvrđivanje izdavanja potvrda i generiranje lozinke.	2
	Operator za potvrde	• Predpersonalizacija sigurnih	2

		pametnih kartica, • priprema potvrda (obrada potpisanih zahtjeva za potvrde), • personalizacija (izrada potvrda, snimanje na siguran medij, štampanje podataka vlasnika na siguran medij), • distribucija potvrda.	
	Operator za kodove	• Distribucija PIN kodova.	2
	Službenik za registraciju	• Identifikacija vlasnika potvrda.	2
	Službenik za opoziv	• Priprema zahtjeva za opoziv, • opoziv potvrda.	2
Sigurnost i kontrola	Administrator sigurnosti	• 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 povjerenja.	2
	Službenik za internu kontrolu	• Praćenje sigurnosnih pravila i njihovog poštivanja, • kontrola sistemske dokumentacije i kontrolnih dnevnika za nadzor 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 zaposlenima u operativnoj implementaciji mjera zaštite privatnosti i osiguravanju usklađenosti s propisima.	1

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 povjerenja.
3. Postavljanje početne konfiguracije mreže.
4. Priprema nosača podataka za hitno ponovno pokretanje sistema u slučaju katastrofalnog gubitka sistema.
5. Sigurno pohranite i distribuirajte kopije i nadogradnje na zasebnu lokaciju.

Organizaciona grupa: Upravljanje informacionim sistemom

Uloga: Administrator sistema

Broj osoba: 2

Zadaci:

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

Organizacijska grupa: Upravljanje potvrdama

Uloga: Sistemski operator 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 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: Operator autorizacije

Broj osoba: 2

Zadaci:

1. Potvrda izdavanja potvrda i generiranja lozinke.

Organizacijska grupa: Upravljanje potvrdama

Uloga: Operator za potvrde

Broj osoba: 2

Zadaci:

1. Predpersonalizacija sigurnih nosioca.
2. Priprema potvrda (obrada potpisanih zahtjeva za potvrde).
3. Personalizacija (izrada potvrda, snimanje na siguran medij, štampanje podataka vlasnika na siguran medij).
4. Distribucija potvrda.

Organizacijska grupa: Upravljanje potvrdama

Uloga: Operator za kodove

Broj osoba: 2

Zadaci:

1. Distribucija PIN kodova

Organizacijska grupa: Upravljanje potvrdama

Uloga: Službenik za registraciju

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: Administrator sigurnosti

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 povjerenja.

Organizacijska grupa: Sigurnost i kontrola

Uloga: Službenik za internu kontrolu

Broj osoba: 2

Zadaci:

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

Organizacijska grupa: Regulatorna

Uloga: Službenik za zaštitu privatnosti i usklađenost s propisima

Broj osoba: 1

Zadaci:

1. Nezavisno i autonomno vođenje, procjena privatnosti i zaštite ličnih podataka.
2. Osiguranje usklađenosti s važećim evropskim i slovenačkim propisima, međunarodnim standardima i preporukama.
3. Stručna pomoć menadžmentu i zaposlenima u operativnoj implementaciji mjera zaštite privatnosti i osiguravanju usklađenosti s propisima.

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

5.2.3 Identifikacija za obavljanje pojedinačnih zadataka

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

5.2.4 Nekompatibilnost zadataka

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

5.3. Nadzor osoblja

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

(2) Službenik za unutrašnju kontrolu nadzire rad Halcom CA. U slučaju uočenih nedostataka,

Službenik za unutrašnju kontrolu nalaže odgovarajuće mjere za otklanjanje tih nedostataka, koje je Halcom CA dužan provesti, te nadzire provođenje naloženih mjera.

5.3.1 Potrebne kvalifikacije i iskustvo osoblja

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

5.3.2 Prikladnost osoblja

Osoblje pružatelja usluga 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 inovacijama vezanim za rad infrastrukture pružatelja usluga povjerenja Halcom CA.

5.3.5 Promjena zadataka

Nije propisano.

5.3.6 Sankcije

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

5.3.8 Pristup osoblja dokumentaciji

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

5.4. Sigurnosne provjere sistema

5.4.1 Vrste zapisnika

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

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

podatke .

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

5.4.2 Učestalost pregleda logova

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

5.4.3 Period čuvanja logova

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

5.4.4 Zaštita logova

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

5.4.5 Sigurnosne kopije logova

Sigurnosne kopije logova se vrše svakodnevno.

5.4.6 Prikupljanje podataka za logove

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

5.4.7 Obavještavanje osobe koja je izazvala incident

Nije potrebno obavijestiti osobu koja je uzrokovala događaje.

5.4.8 Procjena ranjivosti sistema

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

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

5.5. Dugoročno čuvanje podataka

5.5.1 Vrste dugoročno pohranjenih podataka

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

- logovi,
- zapisnici,
- sve dokaze o provjeri identiteta imaoca,
- sve zahtjeve,
- potvrde i registar opozvanih potvrda,

- politike rada,
- publikacije i obavještenja pružatelja usluga 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 koju 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 pohranjeni podaci se čuvaju na siguran način.

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

5.5.4 Sigurnosna kopija dugoročno pohranjenih podataka

(1) Kopija dugoročno pohranjenih podataka čuva se na sigurnom mjestu.

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

5.5.5 Zahtjev za vremenskim žigom

Nije propisano.

5.5.6 Metoda prikupljanja podataka

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

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

5.5.7 Postupak za pristup i provjeru dugoročno pohranjenih podataka

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

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

5.6. Promjena javnog ključa pružatelja usluga povjerenja Halcom CA

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

5.7. Plan oporavka

5.7.1 Postupak u slučaju upada i zloupotrebe

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

5.7.2 Postupak u slučaju kvara programske opreme ili podataka

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

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

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

5.7.4 Plan oporavka

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

5.8. Prekid rada Halcom CA

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

6. ZAHTJEVI TEHNIČKE SIGURNOSTI

6.1. Generisanje i instaliranje ključeva

6.1.1 Generisanje ključeva

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

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

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

(4) Par ključeva imaoca standardnih kvalificiranih potvrda generira vlasnik.

6.1.2 Dostava privatnog ključa vlasnicima

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

(2) Privatni ključ cloud potvrda se ne dostavlja vlasniku, jer ga sigurno čuva pružatelj usluga povjerenja Halcom CA, nakon odobrenja vlasnika.

(3) Privatni ključ OT potvrde se imaocu ne dostavlja, jer ga po ovlaštenju imaoca generira pružatelj usluga povjerenja Halcom CA. Privatni ključ OT potvrde se nakon jednokratne upotrebe briše iz hardverskog sigurnosnog modula.

(4) Privatni ključ standardne potvrde ne generira vlasnik i ne prenosi se, jer ga sigurno pohranjuje pružatelj usluga povjerenja Halcom CA, nakon ovlaštenja imaoca.

6.1.3 Dostava javnog ključa pružatelju usluga povjerenja

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

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

(3) Za standardne potvrde, ključeve generira vlasnik. Potvrda se izdaje putem Halcom CA softvera za dobijanje digitalnih potvrda.

6.1.4 Dostava javnog ključa pružatelja usluga povjerenja

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

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

6.1.5 Dužina ključa

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

6.1.6 Generisanje i kvalitet parametara javnog ključa

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

6.1.7 Svrha ključeva i potvrda

(1) Svrha korištenja ključeva ili potvrde 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 povjerenja Halcom CA koristi se za potpisivanje potvrde i registra

opozvanih potvrda, a javni ključ u potvrdi pružatelja usluga povjerenja koristi se za provjeru valjanosti potpisa.

(3) Profil potvrde dat je u članu 7.1.

6.2. Zaštita privatnog ključa

6.2.1 Standardi kriptografskih modula

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

6.2.2 Kontrola privatnog ključa od strane ovlaštenih osoba

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

6.2.3 Detekcija kopije privatnog ključa

Odredbe u vezi s otkrivanjem privatnog ključa pružatelja usluga povjerenja Halcom CA utvrđene su internim pravilima pružatelja usluga 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 povjerenja Halcom CA utvrđene su u internim pravilima pružaoca usluga 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 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 povjerenja Halcom CA utvrđene su u internim pravilima pružatelja usluga 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 vlasniku potvrde.

(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 standardnih potvrda kreira i pohranjuje vlasnik.

6.2.7 Pohranjivanje privatnog ključa u kriptografskom modulu

(1) Privatni ključ pohranjuje HALCOM CA pružatelj usluga povjerenja u kriptografskom modulu

certificiranom u skladu s FIPS 140-2 Level 3 i/ili Common Criteria EAL4+.

(2) Privatni ključevi korisnika:

- napredne potvrde se kreiraju i pohranjuju na sigurnom mediju,
- Potvrde u cloudu i OT potvrde se kreiraju i pohranjuju u kriptografskom modulu,
- Standardne potvrde kreira i pohranjuje vlasnik.

6.2.8 Postupak za aktiviranje privatnog ključa

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

(2) Halcom CA imaocima preporučuje da 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 cloud-u može koristiti uslugu kvalificiranog elektroničkog potpisa u cloudu. U takvom slučaju, imaoc ili drugi pošiljatelj u njegovo ime dužan je sigurno prenijeti pružatelju usluga povjerenja Halcom CA elektronički dokument koji će biti kvalificirano elektronički potpisan. Imaoc je zatim dužan sigurno odobriti kvalificirani elektronički potpis u cloud-u putem mobilnog uređaja i koristeći sigurnu proceduru koju je propisao pružatelj usluga povjerenja Halcom CA (korištenje PIN-a i mobilnih sigurnosnih procedura). Na temelju odobrenja imaoca, pružatelj usluga povjerenja Halcom CA će koristiti privatni ključ vlasnika u cloud-u i izvršiti kvalificirani elektronički potpis na dokumentu te dostaviti potpisani dokument vlasniku ili drugom pošiljatelju dokumenta.

(4) maoc OT potvrde odobrava kvalificirani elektronski potpis u oblaku putem mobilne ili web aplikacije, koju potpisnik s visokim stepenom povjerenja može koristiti isključivo pod vlastitom kontrolom. Na osnovu odobrenja imaoca, pružatelj usluga povjerenja Halcom CA generira i koristi privatni ključ imaoca u oblaku te kvalificirano elektronski potpisuje dokument, a potpisani dokument dostavlja imaocu ili drugom pošiljaocu dokumenta.

(5) 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 poslovanja Halcom CA.

(6) Radi zaštite povjerljivosti elektronskih dokumenata imaoca, imaoc ili u njegovo ime drugi pošiljalac može zahtijevati da pružatelj usluga povjerenja Halcom CA prilikom potpisivanja u oblaku, kako je opisano u prethodnim odlomcima, ne zahtijeva dostavljanje cijelog dokumenta za kvalificirani elektronski potpis u oblaku, već samo saženu vrijednost (engl. hash value) takvog dokumenta. U takvom slučaju korisnik je prije potpisivanja obaviješten. Potvrdom potpisa imaoc prihvata da Halcom CA ne osigurava nikakvu provjeru izračuna zgošćene vrijednosti niti drugih sigurnosnih mehanizama u vezi s elektronskim dokumentom te da je za to u potpunosti odgovoran sam.

6.2.9 Postupak za deaktivaciju privatnog ključa

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

6.2.10 Postupak uništavanja privatnog ključa

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

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

(3) Privatni ključ cloud i OT potvrde se automatski uništava nakon isteka potvrde. Halcom CA može uništiti privatni ključ cloud potvrde prije isteka, a na zahtjev vlasnika potvrde. Privatni ključ se uništava na način koji ga čini nemogućim za vraćanje.

6.2.11 Svojstva kriptografskog modula

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

6.3. Ostali aspekti upravljanja ključevima

6.3.1 Arhiviranje javnog ključa

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

6.3.2 Period važenja javnih i privatnih ključeva

(1) Važenje potvrda prikazano je u donjoj tabeli.

Vrsta potvrde	Ključ	Validnost
Korjenska (root) potvrda	Privatni/javni ključ	20 godina
Podređena (intemediate) potvrda	Privatni/javni ključ	10 godina
Napredna potvrda	Privatni/javni ključ	3 godine
Potvrda u cloudu	Privatni/javni ključ	1-3 godine
OT potvrda	Privatni/javni ključ	Do 10 minuta

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

6.4. Lozinke za pristup potvrdama ili ključevima

6.4.1 Generisanje lozinke

(1) Lični identifikacijski broj (PIN kod) za korištenje napredne potvrde i broj za otključavanje sigurnog medija (PUK kod) generiraju se na strani Halcom CA. Vlasnik mora promijeniti lični identifikacijski broj prije prve upotrebe potvrde.

(2) Registracijski i aktivacijski kod za potvrde za elektronski potpis u cloudu kreiraju 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 svojom kontrolom. Imaoc potvrde može za pristup svojoj potvrdi i aktivacijskim podacima koristiti isključivo mobilne ili web aplikacije ponuđača Halcom d.d. ili trećih ponuđača 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 potvrda te može dovesti do trenutnog opoziva potvrde. Ako aplikacija ili njena autorizacija za pristup potvrdama u cloudu ne funkcioniše u okviru Halcom d.d., ponuđač usluga povjerenja Halcom CA takvu organizaciju ugovorno obavezuje na ispunjavanje strogih sigurnosnih uslova u skladu sa važećim evropskim, slovenačkim i bosanskohercegovačkim propisima, standardima, preporukama, politikama i općim pravilima rada Halcom CA. Vlasnik potvrde sklapanjem ugovora o izdavanju potvrde izričito dozvoljava tehničke provjere korištenja aplikacije u obimu potrebnom za osiguravanje usklađenosti sa uslovima ovog CPS-a i važećom zakonskom regulativom.

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

(4) Referentni kod i lozinka za dobijanje standardne potvrde sigurno generira pružatelj usluga 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 vlasnik ima pristup njoj .

6.4.2 Zaštita lozinkom

(1) Ličnu lozinku za korištenje napredne potvrde (PIN kod) i lozinku za otključavanje sigurnog medija (PUK kod) sigurno generira pružatelj usluga povjerenja Halcom CA. Halcom CA šalje obje lozinke vlasniku potvrde preporučenom poštom ili putem drugog sigurnog kanala (lična dostava redovnom poštom, sigurni web portal ili druga slična sigurna metoda) ili ih, izuzetno, dostavlja lično. Halcom CA preporučuje da se obje lozinke čuvaju na sigurnom mjestu kojem samo vlasnik ima pristup.

(2) Registracijski i aktivacijski kod za potvrde za elektronski potpis u oblaku kreiraju se sigurno kod pružaoca usluga povjerenja Halcom CA. Kodovi se imaocu dostavljaju putem dva odvojena kanala – jedan putem elektronske pošte, a drugi putem drugog sigurnog kanala (lična dostava klasičnom poštom, siguran web portal ili 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 oblaku, tokom koje korisnik sam postavlja svoju ličnu šifru (PIN kod). Aktivacija potvrde u oblaku može se obaviti i putem različitih mobilnih i web aplikacija, koje potpisnik sa visokim nivoom povjerenja koristi isključivo pod svojom kontrolom. Imaoc potvrde može za pristup svojoj potvrdi i aktivacijskim podacima koristiti isključivo mobilne ili web aplikacije ponuđača Halcom d.d. ili trećih ponuđača 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., 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 rada Halcom CA. Imaoc potvrde sklapanjem ugovora o

izdavanju potvrde izričito dozvoljava tehničke provjere korištenja aplikacije u obimu potrebnom za osiguravanje usklađenosti sa uslovima ovog CPS-a i važećom zakonskom regulativom.

(3) Aktivacija OT potvrde može se obaviti putem različitih mobilnih i web aplikacija, koje potpisnik sa visokim nivoom povjerenja koristi isključivo pod svojom 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 rada Halcom CA. Imaoc potvrde može za pristup svojoj potvrdi i aktivacijskim podacima koristiti isključivo mobilne ili web aplikacije ponuđača Halcom d.d. ili trećih ponuđača 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., 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 rada Halcom CA. Imaoc potvrde sklapanjem ugovora o izdavanju potvrde izričito dozvoljava tehničke provjere korištenja aplikacije u obimu potrebnom za osiguravanje usklađenosti sa uslovima ovog CPS-a i važećom zakonskom regulativom.

(4) Referentni kod i lozinku za standardnu potvrdu sigurno generira pružatelj usluga povjerenja Halcom CA. Referentni kod i lozinka za preuzimanje šalju se vlasniku putem dva odvojena kanala, jedan putem e-pošte, a drugi putem drugog kanala (lična dostava redovnom poštom, kratka SMS poruka, sigurni web portal ili druga slična metoda). Izuzetno, lozinku za preuzimanje vlasniku može dati i lično ovlaštena osoba u Halcom CA. Kodovi su namijenjeni samo za preuzimanje standardne potvrde. U procesu preuzimanja potvrde, korisnik određuje lozinku, sa
kojom štiti pristup njihovim privatnim ključevima.

6.4.3 Ostali aspekti lozinki

Nisu propisani.

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

6.5.1 Specifični tehnički sigurnosni zahtjevi

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

6.5.2 Nivo sigurnosne zaštite

Detaljnija regulativa utvrđena je u Opštim pravilima poslovanja i Internim pravilima pružaoca usluga povjerenja Halcom CA, u skladu sa važećim propisima, standardima i preporukama.

6.6. Tehnička kontrola životnog ciklusa pružatelja usluga 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 poverenja Halcom CA, u skladu sa važećim propisima, standardima i preporukama.

6.6.3 Kontrola životnog ciklusa

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

6.7. Kontrola sigurnosti mreže

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

6.8. Vremensko označavanje

Nije propisano.

7. PROFIL POTVRDE I REGISTRA OPOZVANIH POTVRDA

7.1. Profil potvrde

(1) Na osnovu ove politike, Halcom CA izdaje napredne, standardne, cloud i OT potvrde za pojedince.

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

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

7.1.1 Verzija potvrde

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

7.1.2 Profil potvrde s ekstenzijama

7.1.2.1 Profil korijenske (root) potvrde

Nazivi polja	Vrijednost ili značenje
Osnovna polja u potvrdi	
Verzija, engl. Version	V3
Identifikacijski kod potvrde, engl. Serial Number	G1: 0cdf9b
	G2: 6fb450b4a6bbeebb983055e81d53c040
	G3: 7539c53f6170763fb3c445b870ef6174

Algoritam potpisa, engl. Signature algorithm	G1: Sha256RSA
	G2: RSASSA-PSS
	G3: RSASSA-PSS
Izdavatelj, engl. Issuer	G1: C=SI, O=Halcom dd, 2.5.4.97 = VATSI-43353126 CN=Halcom Root Certificate Authority
	G2: C=SI, O=Halcom dd, 2.5.4.97 = VATSI-43353126 CN=Halcom Root CA G2
	G3: C=SI, O=Halcom d.d., 2.5.4.97 = VATSI-43353126 CN=Halcom Root CA G3
Validnost, engl. Validity	G1: Valid from: <10.6.2016 07:07:50 GMT > Valid to: <10.6.2036 07:07:50 GMT >
	G2: Valid from: < 19.3. 2025 09:00:00 GMT> Valid to: <19.3.2045 09:00:00 GMT>
	G3: Valid from: < 19.3. 2026 10:00:00 GMT> Valid to: < 19.3. 2046 10:00:00 GMT>
Imaoc, engl. Subject	G1: C=SI, O=Halcom dd, 2.5.4.97 = VATSI-43353126 CN=Halcom Root Certificate Authority
	G2: C=SI, O=Halcom dd, 2.5.4.97 = VATSI-43353126 CN=Halcom Root CA G2
	G3: C=SI, O=Halcom d.d., 2.5.4.97 = VATSI-43353126 CN=Halcom Root CA G3
Algoritam javnog ključa subjekta, engl. Subject Public Key Algorithm	G1: RSA
	G2: RSASSA-PSS
	G3: RSA
Javni ključ, angl. 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 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 potvrde)	
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 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-sig 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, angl. 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 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

7.1.2.3 Profil potvrde krajnjeg korisnika

Nazivi polja	Vrijednost ili značenje
Osnovna polja u potvrdi	
Verzija, engl. Version	V3
Identifikacijska oznaka 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 članove 3.1.1 i 7.1.2.2.
Validnost, engl. Validity	Validm from: <datum važenja po GMT> Valid to: <kraj važenja po GMT>
Imaoc, angl. Subject	Ime i prezime imaoca, pogledajte odjeljak 3.1.1.
Algoritam za javni ključ, engl. Subject Public Key Algorithm	RSA

Javni ključ, engl. Public Key (... bits)	modul, eksponent,...
Javni ključ imaoca, koji pripada odgovarajućem paru ključeva, šifriran RSA algoritmom, engl. RSA Public Key	Dužine ključeva variraju (pogledajte član 6.1.5) G1: minimalno 2048 bit
	G2: minimalno 3072 bit
	G3: minimalno 3072 bit
X.509v3 ekstenzije	
Objava registra opozvanih certifikata, OID 2.5.29.31, engl. CRL Distribution Points	U zavisnosti od izdavaoca, pogledajte član 7.2.2
Korištenje ključa, OID 2.5.29.15, engl. Key Usage	Digital Signature, Non Repudiation, Key Encipherment
Identifikator ključa pružatelja usluga 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
	G2: Halcom CA FO e-sig 1 G2: KeyID=47902d7cbd318937
	G3: Halcom CA FO e-sig 1 G3: KeyID= 46c21387d74ad8ae
EŠEI	jedinstveni elektronski identifikacijski broj (pogledajte sljedeći član)

(4) Polje svrha korištenja (engl. Key Usage) je označeno kao kritično (engl. critical).

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

7.1.2.4 Jedinstveni elektronski identifikacijski broj

U skladu sa članom 24. Zakona o elektronskoj identifikaciji i uslugama 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) vlasnika se upisuje u kvalifikovani certifikat za elektronski potpis, elektronski pečat ili autentifikaciju web stranice kao privatno proširenje kvalifikovanog certifikata. 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: 'xxxxxxxxxxxxxxx' <vrijednost>

7.1.2.5 Zahtjevi za e-mail adresu

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

- neprikladan ili uvredljiv,

- da obmanjuje treća lica,
- u suprotnosti s važećim propisima i standardima.

(2) Nisu propisana nikakva druga ograničenja u vezi e-maila.

7.1.3 Identifikacijske oznake algoritma

(1) Potvrde koje izdaje Halcom CA su na strani pružatelj usluga povjerenja potpisani algoritmom navedenim u polju signature algorithm vrijednost:

- G1: sha256RSA, identifikacijska oznaka: OID 1.2.840.113549.1.1.11 ili
- G2: RSASSA-PSS, identifikacijska oznaka: OID 1.2.840.113549.1.1.10,
- G3: RSASSA-PSS, identifikacijska oznaka: OID 1.2.840.113549.1.1.10.

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

7.1.4 Format prepoznatljivog imena

Pogledajte član 3.1.1.

7.1.5 Ograničenja imena

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

7.1.6 Oznaka politike potvrde

Pogledajte član 7.1.2.

7.1.7 Ograničenja korištenja

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

7.1.8 Sintaksa i značenje oznaka politike potvrde

Potvrde koje izdaje Halcom CA pružatelj usluga 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) Registar opozvanih potvrda Halcom CA je lista opozvanih potvrda (CRL) i nalazi se u grani:

- G1:
  - CN= Halcom CA FO e-signature 1
    O = Halcom
    C = SI
  - CN= Halcom CA FO e-signature 2
    O = Halcom

C = SI

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

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

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

7.2.1 Verzija

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

(2) Registar opozvanihpotvrda je trajno dostupan u javnom imeniku potvrda (vidjeti član 2.3):

- putem LDAP protokola i
- putem HTTP protokola.

7.2.2 Sadržaj i proširenja registra

(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 oznakei opozvanih potvrda i
- vrijeme i datum otkazivanja.

7.2.2.1 Korjenski (Root) registar opozvanih potvrda (CRL podređenih ili intermediate potvrda)

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

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

7.2.2.2 Podređeni (intermediate) registar opozvanih potvrda (CRL korisničkih potvrda)

Naziv polja	Vrijednost ili značenje
Osnovna polja u CRL-u	
Verzija, engl. Version	V2
Algoritam za potpis, engl. Signature Algorithm	G1: Sha256RSA
	G2: RSASSA-PSS
	G3: RSASSA-PSS
Potpis pružatelja usluga povjerenja, engl. Signature	potpis Halcom CA
Prepoznatljivo ime pružatelja usluga povjerenja, engl. Issuer	prepoznatljivo ime izdavatelja, pogledajte članove 3.1.1 i 7.1.2.2.
Vrijeme izdavanja CRL, engl. thisUpdate	Effective date: <vrijeme izdavanja po GMT>

Vrijeme izdavanja sljedećeg CRL, engl. nextUpdate	Next Update: <vrijeme sljedećeg izdanja po GMT>
identifikacijske oznake opozvanih potvrda i vrijeme opoziva, angl. 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
lidentifikator ključa pružatelja usluga 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
	G2: Halcom CA FO e-sig 1 G2: KeyID=47902d7cbd318937
	G3: Halcom CA FO e-sig 1 G3: KeyID= 46c21387d74ad8ae
angl. issuerAltName (OID 2.5.28.18)	Ne koristi se
angl. deltaCRLindicator (OID 2.5.29.27)	Ne koristi se
angl. issuingDistribuitionPoint (OID 2.5.29.28)	Ne koristi se

7.2.3 Objavljivanje registra opozvanih potvrda

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

7.3. Profil provjere statusa potvrde u stvarnom vremenu

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

(2) Profil OCSP poruke (zahtjev/odgovor) za uslugu provjere statusa potvrde 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 poruke OCSP verzije 1 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 i 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 obavi pregled najmanje jednom godišnje.

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

(3) Vanjski revizor provodi reviziju poslovanja u skladu sa ETSI standardima jednom godišnje.

8.2. Vrsta i osposobljenost 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 povjerenja Halcom CA.

8.5. Mjere pružatelja usluga povjerenja

U slučaju uočenih nedostataka ili grešaka, službenik za internu/eksternu kontrolu nalaže odgovarajuće mjere za otklanjanje ovih nedostataka, koje je Halcom CA dužan provesti, te nadzire provođenje naloženih mjera. Provođenje mjera detaljno je precizirano u internim pravilima pružatelja usluga povjerenja Halcom CA.

8.6. Objavljivanje rezultata kontrole

Rezultati kontrola se čuvaju kod pružatelja usluga 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 potvrde

Cijena izdavanja i obnavljanja potvrde određena je važećim cjenovnikom.

9.1.2 Cijena pristupa do potvrda

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

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

9.1.3 Cijena pristupa do statusa potvrda i registra 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 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 licima i
- Sva ostala pitanja koja su uključena u interna pravila poslovanja pružatelja usluga povjerenja Halcom CA u skladu s Uredbom.

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

9.3.2 Nezaštićeni podaci

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

9.3.3 Odgovornost za sigurnost

(1) Halcom CA ne preuzima nikakvu odgovornost za sadržaj podataka koje imaoc potvrde elektronski šifrira ili potpisuje, čak i ako je imaoc ili treće lice postupio u skladu sa svim važećim propisima, svim odredbama ove politike i drugih pravila 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 potvrde navedenih u tački 4.5.1 ove politike.

9.4. Zaštita ličnih podataka

9.4.1 Plan zaštite ličnih podataka

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

9.4.2 Zaštićeni lični podaci

Zaštićeni podaci su svi lični podaci koje pružalac usluga povjerenja Halcom CA prikupi u zahtjevima za svoje usluge ili u relevantnim registrima radi dokazivanja identiteta vlasnika ili u toku pružanja usluga povjerenja. Podaci u potvrdama i registru opozvanih potvrda dostupni su trećim licima koja se oslanjaju na potvrde ili provjeravaju njihovu validnost zbog prirode upotrebe potvrda i odredbi važećih propisa i standarda.

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 povjerenja Halcom CA odgovoran je za zaštitu podataka u skladu s važećim propisima o zaštiti podataka i odredbama interne Politike zaštite podataka.

9.4.5 Ovlaštenje u vezi s korištenjem ličnih podataka

Imaoc ovlašćuje pružaoca usluga povjerenja Halcom CA da koristi lične podatke na zahtjevu za dobijanje potvrde, sa posebnom pisanom saglasnosti za obradu ličnih podataka ili za druge slučajeve kasnije u drugom pisanom obliku.

9.4.6 Proslijeđivanje ličnih podataka

(1) Pružatelj usluga povjerenja Halcom CA ne daje druge podatke o vlasnicima 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 povjerenja Halcom CA je za to ovlašten (vidjeti prethodni član), ili na zahtjev nadležnog suda, prekršajnog organa, organa za provođenje zakona,

upravnog organa ili druge ovlaštene osobe. Halcom CA pažljivo provjerava svaki takav zahtjev i daje podatke samo u mjeri u kojoj je to potrebno, kako je određeno važećim propisima.

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

9.4.7 Ostale odredbe u vezi sa zaštitom ličnih podataka

Nisu propisani.

9.5. Odredbe o pravima intelektualnog vlasništva

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

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

9.6. Obaveze i odgovornosti

9.6.1 Obaveze i odgovornosti pružatelja usluga povjerenja Halcom CA

(1) Pružalac usluga 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 kvalificiranih digitalnih potvrda itd.),
- objavljuje na svojim web stranicama sve informacije o promjenama u vezi s aktivnostima pružatelja usluga povjerenja koje na bilo koji način utječu na vlasnike 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 i povjerljivim podacima o pružaocu usluga povjerenja, vlasnicima 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,
- izdaje kvalifikovane digitalne potvrde u skladu s ovom politikom i drugim propisima i preporukama.

(2) Pružalac usluga 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 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 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 povjerenja Halcom CA i
- nedostupnost kao rezultat više sile ili vanrednih događaja.

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

(5) Pružatelj usluga 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 povjerenja Halcom CA utvrđuju se eventualnim međusobnim dogovorom s trećim licem..

9.6.2 Obaveza i odgovornost prijavne službe

(1) Prijavna služba je dužna:

- provjeriti identitet imaoca ili budućih imaoca,
- primaju zahtjeve za usluge Halcom CA,
- provjeriti zahtjeve,
- izdavati potrebnu dokumentaciju imaocima ili budućim imaocima,
- proslijediti zahtjeve i ostale podatke na siguran način Halcom CA.

(2) Služba za registraciju je odgovorna za sprovođenje svih odredbi ove politike i drugih zahteva dogovorenih sa pružaocem usluga poverenja Halcom CA.

9.6.3 Obaveze i odgovornost imaoca potvrda

(1) Imaoc potvrde je odgovoran za:

- štetu nastalu u slučaju zloupotrebe potvrde od prijave opoziva 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 potvrde 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 koja se oslanja na potvrdu mora pažljivo pročitati ovu politiku i od tada redovno pratiti sva obavještenja od Halcom CA.

(2) Treće lice mora uvijek pažljivo provjeriti, prilikom korištenja certifikata, 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. Odricanje odgovornosti

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

- korištenja potvrde u svrhu i na način koji nije izričito predviđen ovom politikom,
- nepravilne ili neadekvatne zaštite lozinki ili privatnih ključeva nosioca, izdavanje povjerljivih podataka ili ključeva trećim licima i neodgovornog ponašanja imaoca,
- zloupotrebe ili upada u informacioni sistem vlasnika potvrde, a time i u podatke potvrde, od strane neovlaštenih osoba,
- nefunkcionalnosti ili lošeg funkcionisanja informacione infrastrukture vlasnika potvrde ili trećih lica,
- neprovjeravanja podataka i validnosti potvrde u registru opozvanih potvrda,
- neprovjeravanja roka važenja potvrde,
- radnji imaoca potvrde ili trećeg lica koje krše obavještenja, politike i druge propise Halcom CA,
- omogućavanja korištenja ili zloupotrebe potvrde imaoca od strane neovlaštenih osoba,
- potvrde izdane s netačnim ili nepouzdanim podacima ili drugim radnjama imaoca ili pružatelja usluga povjerenja,
- korištenja potvrde i važenja potvrde u slučaju promjene podataka potvrde, e-mail adresa ili promjene imena imaoca,

- prekida infrastrukture koji nije u domenu upravljanja pružatelja usluga povjerenja Halcom CA,
- potpisivanja ili šifriranja podataka pomoću potvrde,
- ponašanja imaoca prilikom korištenja potvrde, 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,
- grešaka u izračunavanju hash vrijednosti, provjeri ove vrijednosti ili drugim sigurnosnim procedurama u vezi s potpisivanjem elektronskog dokumenta, ako je vlasnik zatražio potpis u cloudu isključivo na osnovu hash vrijednosti, a bez dostavljanja cijelog elektronskog dokumenta pružatelju usluga povjerenja Halcom CA.

9.8. Ograničenje upotrebe

Nije propisano.

9.9. Naplata štete

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

9.10. Važenje politike

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

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

9.10.1 Period važenja

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

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

9.10.2 Kraj važenja politike

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

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

9.10.3 Posljedice isteka politike

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

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

9.11. Komunikacija između subjekata

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

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

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

9.12. Izmjene i dopune

9.12.1 Postupak za prihvatanje izmjena i dopuna

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

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

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

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

9.12.2 Važenje i objavljivanje izmjena i dopuna

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

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

9.12.3 Promjena identifikacijskog broja politike

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

9.13. Postupak rješavanja sporova

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

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

9.14. Primjenjivo zakonodavstvo

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

9.15. Usklađenost s važećim zakonodavstvom

(1) Nadzor nad usklađenošću poslovanja pružatelja usluga povjerenja Halcom CA s važećim

propisima provode nadležni inspektorat i akreditirana tijela za ocjenjivanje usklađenosti.

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

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

9.16. Opće odredbe

(1) Pružatelj usluga 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.

Generalni direktor:
Gregor Pelhan