Pripremio(la): Luka RIBIČIČ

Broj dokumenta: 400085-41-2/17

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

Izdanje: 02

Politika Halcom CA

Javni dio internih pravila Halcom CA

za EU kvalificirane digitalne potvrde za fizička lica

CPName: Halcom CA FO e-signature 2

Politika za EU kvalificirane digitalne potvrde za fizička lica
Napredne potvrde i potvrde u oblaku
CPOID: 1.3.6.1.4.1.5939.1.4.5
Standardne potvrde
CPOID:1.3.6.1.4.1.5939.1.5.4

Dokument važi od: 15.6.2024

Izdanje	br. dokumenta i prilog	Opis izmjene	Autor	Datum zadnje izmjene
1	400085-41-1/17	Početno izdanje	L. Ribičič	23.5.2023
2	400085-41-2/17	Godišnji pregled dokumenata, EŠEI	L.Ribičič	22.5.2024

1. UVOD

(1) Halcom CA je najstariji i najveći ponuđač usluga povjerenja u Sloveniji, koji za provođenje svojih usluga iz oblasti elektronskog potpisa, elektronskog pečata, elektronskog vremenskog pečata, validacije i drugih usluga, koristi naj sigurnije tehnologije, uključujući korištenje sigurnih nosioca podataka i sigurnog oblaka (cloud-a).

(2) Ova politika je javni dio unutrašnjih pravila Halcom CA za kvalificirane digitalne potvrde za fizička lica

(3) Oblik i sadržaj ove politike je usklađen sa uredbom eIDAS, međunarodnim preporukama IETF RFC i evropskim standardima ETSI i ostalim.

1.1. Pregled

(1) Ova politika predstavlja neodvojivu cjelinu opštih pravila djelovanja ponuđača usluga povjerenja Halcom CA u vezi izdavanja kvalificiranih digitalnih potvrda, uređuje svrhu, djelovanje i metodologiju upravljanja kvalificiranim digitalnim potvrdama te sigurnosne zahtjeve koji moraju ispunjavati ponuđači usluga povjerenja Halcom CA, vlasnici potvrda, treća lica, koja se odnose na te potvrde, te odgovornost nabrojanih lica.

(2) Halcom CA je ponuđač usluga povjerenja, koje izdaje i upravlja sa kvalificiranim digitalnim potvrdama za provjeru važnosti elektronskog potpisa. Ponuđač usluga povjerenja Halcom CA djeluje u okviru Halcom d.d.

(3) Halcom CA izdaje kvalificirane digitalne potvrde sa najmanje jednim parom ključeva i sa obaveznom korištenjem sigurnosnog prenosnika.

(4) Sve odredbe ove politike u vezi postupanja Halcom CA su odgovarajuće prenesene i detaljnije određene u javno objavljenim opštim pravilima djelovanja ponuđača usluga povjerenja (CPS) te određene u odredbama povjerljivih unutrašnjih pravila ponuđača usluga povjerenja, koje određuju infrastrukturu, odredbe u vezi osoblja Halcom CA (nadležnost, zadatke, punomoći i zahtijevani uslovi za pojedinačne članove osoblja), fizička zaštita (pristup prostorima, postupanje sa hardverskom i softverskom opremom), programska zaštita (sigurnosne postavke poslužitelja, sigurnosne kopije,...) i unutrašnji nadzor (kontrola fizičkih pristupa, punomoći,...).

(5) Halcom CA izdaje potvrde i obavlja ostale djelatnosti ponuđača usluga povjerenja u skladu sa važećim pravnim poretkom Republike Slovenije i Evropske unije, te u skladu sa uredbom eIDAS, tehničkim zahtjevima ETSI, standardom IETF RFC i familijom standarda ISO/IEC te drugim srodnim standardima.

(6) Spisak prijavnih službi koje omogućavaju dobivanje kvalificiranih digitalnih potvrda za poslovne subjekte, Halcom CA objavljuje na web stranici.

1.2. Identifikacijski podaci politike

(1) Oznake politika djelovanja Halcom CA FO e-signature 2:

- Napredne potvrde i potvrde u oblaku:

  CPOID: 1.3.6.1.4.1.5939.1.4.5

- Standardne potvrde:

  CPOID: 1.3.6.1.4.1.5939.1.5.5

U svakoj potvrdi je navod od politike u obliku oznake CPOID (vidi odjelj. 7.1.2.).

1.3. Subjekti

1.3.1 Ponuđač usluga povjerenja Halcom CA

Halcom CA je ponuđač usluga povjerenja, koji izdaje i upravlja sa kvalificiranim digitalnim potvrdama, koje povezuju podatke za potvrđivanje važenja kvalificiranog elektronskog potpisa sa fizičkim licem. Ponuđač usluga povjerenja Halcom CA djeluje u okviru Halcom d.d.

1.3.2 Prijavna služba Halcom CA

(1) Prijavna služba za ponuđača usluga povjerenja provodi sljedeće zadatke:

- Provjera identiteta fizičkog lica i ostalih, za upravljanje sa kvalificiranim digitalnim potvrdama, važnim podacima,
- Primanje zahtjeva za dobivanje potvrda,
- Praćenje zahtjeva za povlačenje potvrda,
- Izdavanje potrebne dokumentacije fizičkim licima, vlasnicima tj. budućim vlasnicima,
- posredovanje zahtjeva i ostalih podataka na siguran način ponuđačima usluga povjerenja Halcom CA.

(2) Ponuđač usluga povjerenja Halcom CA može pored svoje prijavne službe za obavljanje zadataka prijavne službe dati punomoć i drugim organizacijama u poslovnom i javnom sektoru. Svaku takvu organizaciju ponuđač usluga povjerenja Halcom CA ugovorno obaveže na ispunjavanje strogih sigurnosnih uslova u skladu sa važećim evropskim i slovenskim propisima te međunarodnim, evropskim i slovenskim standardima i preporukama te politikama, pravilima poslovanja i unutrašnjim pravilima Halcom CA.

(3) Ponuđač usluga povjerenja Halcom CA ima ispostavljenu geografski rasprostranjenu prijavnu službu, što budućim vlasnicima omogućava jednostavnu prijavu u svom ili obližnjem mjestu. Informacija o lokacijama prijavne službe su dostupne na web stranicama ponuđača usluga povjerenja Halcom CA.

1.3.3 Naručitelj i vlasnik potvrda

(1) Vlasnik potvrde, koji je fizičko lice, koristi svoje, od ponuđača usluga povjerenja dodijeljene podatke (par/parove ključeva) za kvalificirano elektronsko potpisivanje i kvalificirane digitalne potvrde za povezivanje tog elektronskog potpisa sa vlasnikom.

(2) Naručitelj potvrde je fizičko lice.

1.3.4 Treća lica

(1) Treća lica su lica koja se oslanjaju na izdate potvrde i druge usluge ponuđača usluga povjerenja Halcom CA, i mogu biti fizička ili pravna lica.

(2) Treća lica moraju postupati po uputama ponuđača usluga povjerenja Halcom CA i moraju uvijek provjeriti važnost potvrde, svrhu korištenja potvrde, vrijeme važnosti potvrde itd. Detaljnije obaveze i odgovornosti trećih lica su navedene u odjelj. 4.5.2 i 9.6.4.

(3) Treća lica nisu neophodno i vlasnici potvrda ponuđača usluga povjerenja Halcom CA ili digitalnih potvrda drugih ponuđača usluga povjerenja.

1.4. Svrha korištenja

Halcom CA upravlja (izdaje i provjerava, opoziva, produžava, čuva, objavljuje) sa kvalificiranim poslovnim digitalnim potvrdama za provjeru važenja elektronskog potpisa (u nastavku potvrde), koje su namijenjene fizičkim licima.

1.4.1 Pravilno korištenje potvrda i ključeva

(1) Potvrde su namijenjene za elektronsku potpis jednostrane ili međusobne komunikacije vlasnika potvrda te za korištenje u različitim aplikacijama i za različite svrhe, koje se pojavljuju na tržištu. Između ostalog se mogu potvrde koristiti u svrhu kao što je npr.:

1) Identifikacija vlasnika (fizičkog lica),
2) Iskazivanje identiteta vlasnika (fizičkog lica),
3) Potpisivanje dokumenata u elektronskom obliku,
4) Šifriranje i dešifriranje dokumenata u elektronskom obliku.

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

1) Elektronsko tj. mobilno bankarstvo,
2) Aplikacije e-uprave ili m-uprave,
3) Aplikacije e-liječnik ili m-zdravstvo,
4) Potpisivanje elektronskih ili mobilnih obrazaca,
5) Sigurno poslovanje sa organima i organizacijama javnog sektora te sa drugim pravnim ili fizičkim licima,
6) Ostale aplikacije odnosno usluge, u kojima se zahtjeva korištenje kvalificirane digitalne potvrde,
7) Kontrola pristupa.

1.4.2 Nedozvoljeno korištenje

(1) Zabranjena je upotrebna potvrde izdate u skladu sa ovom politikom koja je u suprotnosti sa odredbama ove politike ili važećim propisima ili van opsega dozvoljenog korištenja, određenog u prethodnom odjeljku.

(2) Potvrde nisu namijenjene daljoj prodaji.

1.5. Upravljanje politike

1.5.1 Upravitelj politika

(1) Sa ovim i drugim svojim politika upravlja ponuđač usluga povjerenja Halcom CA, koji djeluje u sklopu Halcom d.d.

(2) Adresa upravitelja: **Halcom d.d.**

Tržaška 118

1000 LJUBLJANA, Slovenija

1.5.2 Ovlaštene kontakt osobe

(1) (1) Za pitanja u vezi sa ovom politikom se možete obratiti ovlaštenim licima ponuđača usluga povjerenja, koja možete kontaktirati na dole navedenoj adresi i dole navedenim telefonskim brojevima.

(3) Adresa Halcom CA: **Halcom d.d.**

Tržaška 118

1000 LJUBLJANA

Slovenija

Tel.: (+386) 01 200 34 86

E-mail: ca@halcom.si

E-mail za opoziv: ca_preklici@halcom.si

1.5.3 Odgovorno lice u vezi usklađenosti rada ponuđača usluga povjerenja Halcom CA sa politikom

Za usklađenost djelovanja ponuđača usluga povjerenja Halcom CA sa ovom politikom su u skladu sa svojim nadležnostima odgovorna ovlaštena lica ponuđača usluga povjerenja.

1.5.4 Postupak za usvajanje nove politike

(1) Svaki prijedlog nove politike je prije potvrde glavnog izvršnog direktora Halcom d.d. sa svrhom osiguranja zakonitosti, sigurnosti i kvalitete podvrgnuti kako tehnološkom tako i pravnom pregledu.

(2) Ponuđač usluga povjerenja može za pojedine odredbe važeće politike izdati dopune, kako je to određeno u odjeljku 9.12.

1.6. Skraćenice i izrazi

1.6.1 Skraćenice

CA	Ponuđač usluga povjerenja, koji izdaje potvrde (engl.: Certificate Authority ali Certificate Agency).
CPName	Ime politike djelovanja ponuđača usluga povjerenja (engl.: Certification Policy Name), jedinstvenost povezano sa međunarodnim brojem politike djelovanja CPOID (engl.: Certification Policy Object Identifier).
CP	Politika ponuđača usluga povjerenja (engl. Certificate Policy). Politika uređuje svrhu, djelovanje i metodologiju upravljanja usluga te odgovornosti i sigurnosne zahtjeve koje moraju ispunjavati ponuđači usluga povjerenja, vlasnici potvrda (korisnici usluga) i treća lica, koja se pouzdaju u te potvrde/usluge.
CPS	CPS (engl. Certification Practice Statement) predstavlja opšta pravila djelovanja ponuđača usluga povjerenja.
CPOID	Međunarodni broj, koji jedinstvenosti određuje politiku djelovanja (engl.: Certification Policy Object IDentifier).
CRL	Certificate Revocation List – spisak povučenih digitalnih potvrda.
DN	Jedinstveno prepoznatljivo ime (prim. određivanje prepoznatljivog imena) (engl. Distinguished Name).
LDAP	Leightweight Directory Access Protocol je protokol, koji određuje pristup imeniku i specificiran je po IETF (Internet Engineering Task Force) preporukama IETF RFC 3494:.

S/MIME	Secure Multipurpose Internet Mail Extensions
SSL	Secure Sockets Layer
TLS	Transport Layer Security
PKI	Public Key Infrastructure je infrastruktura javnih ključeva.

1.6.2 Izrazi

Vlasnik potvrde	Imenik potvrda po preporuci X.500, gdje su sačuvane potvrde prema preporuci X.509 ver.3, do kojih je moguć pristup po protokolu LDAP.
Identifikacija	Identifikacija znači postupak korištenja identifikacijskih podataka lica u fizičkom ili elektronskom obliku, koji jedinstvenost predstavljaju bilo fizičko ili pravno lice bilo fizičko lice, koje zastupa pravno lice.
Ponuđač usluga povjerenja	Fizičko ili pravno lice koje izdaje potvrde ili obavlja druge usluge povjerenja (engl. Trust Service provider – TSP).
Prijavna služba	Služba ili lice koje prati zahtjeva za potvrde i preuzima identificiranje i provjeru identiteta budućih vlasnika u ime ponuđača usluga povjerenja potvrda (engl.: Registration Authority – RA).
Prepoznatljivo ime	Jedinstveno ime u potvrdi (prim. Određivanje DN), koji nedvosmisleno i jedinstveno definira korisnika u strukturi vlasnika.

2. OBJAVE INFORMACIJA I JAVNI IMENIK POTVRDA

2.1. Zbirka dokumenata

(1) Ponuđač usluga povjerenja Halcom CA sve u vezi sa svojim djelovanjem, obavještenja vlasnicima i trećim licima te druge važne dokumente javno objavi na web stranama Halcom CA na adresi http://www.halcom.si (kratak ključni sadržaj je dat i na engleskom jeziku).

(2) Dokumenti koji su javno dostupni, su:

- Cjenovnik
- Politika korištenja usluga povjerenja (CP),
- Pravila rada ponuđača usluga povjerenja (CPS)
- Narudžbenice i drugi ugovori za usluge ponuđača usluga povjerenja,
- Upute za sigurno korištenje digitalnih potvrda,
- Informacije o važećim propisima i standardima u vezi a radom ponuđača usluga povjerenja te
- Ostale informacije u vezi sa djelovanjem Halcom CA.

(3) Javno nisu dostupni dokumenti koji predstavljaju povjerljivi dio unutrašnjih pravila ponuđača usluga povjerenja Halcom CA.

2.2. Imenik potvrda

(1) Nove politike su objavljene u skladu sa uputama u odjeljku 9.10.

(2) Sve potvrde ponuđača usluga povjerenja se temelje na standardu X.509 i objavljena su u centralnom imeniku na serveru idap.halcom.si, koji je u nadležnosti HALCOM CA. Zbog zaštite podataka, javno je dostupan samo registar poništenih potvrda, koji je dio imenika.

(3) Poništene potvrde se u registru poništenih potvrda objave odmah (detaljno o tome u odjelj. 4.9.8.), ostale javno dostupne informacije tj. dokumenti se objave po potrebi.

(4) Pristup do imenika izdanih potvrda je omogućen samo ovlaštenim korisnicima, koji provjeravaju veći broj izdanih potvrda.

2.3. Učestalost objava

(1) Nova politika se objavi najkasnije sljedeći radni dan nakon prijema.

(2) Halcom CA osigura da se potvrde objave u centralnom imeniku odmah (najviše 5 sekundi) nakon njihovog izdavanja

(3) Spisak poništenih potvrda se ažurira odmah (najviše 5 sekundi) nakon poništenja potvrde u javnom imeniku poništenih potvrda Halcom CA. Sa nekoliko minuta zakašnjenja se to ažuriranje prenese i na web strane.

(4) Javno dostupne informacije tj. dokumenti (osim gore navedenih) se objave po potrebi.

2.4. Upravljanje pristupom do baze dokumenata

(1) Centralni imenik je dostupan na poslužitelju Idap.halcom.si, TCP 389 po protokolu LDAP. Javno dostupan je samo registar poništenih potvrda koji je dio imenika.

(2) Sa odgovarajućim tehničkim mjerama informacijske sigurnosti Halcom CA osigurava kontrole koje sprečavaju neovlašteno dodavanje, praćenje ili brisanje podataka u javnom imeniku potvrda

3. IDENTITET VLASNIKA POTVRDA

3.1. Dodjela imena

Prepoznavanje imena, koja sadrže potvrdu, nedvosmisleno i jedinstveno definiraju vlasnika potvrde, osim ako je drugačije zahtijevano bilo sa ovom politikom bilo sa sadržajem kvalificirane digitalne potvrde.

3.1.1 Prepoznatljiva imena

(1) U skladu sa IETF RFC 5280 svaka potvrda sadrži podatke o vlasniku te ponuđaču usluga povjerenja u obliku prepoznatljivog imena. Prepoznatljivo ime je oblikovano u skladu sa IETF RFC 5280 i standardom X501.

(2) Ponuđača usluga povjerenja potvrde je u izdanoj potvrdi naveden u polju Izdavatelj, engl. Issuer. Osnovni podaci o poslovnom subjektu i vlasniku, koji sadrži prepoznatljivo ime potvrda za poslovne subjekte, su u izdanoj potvrdi navedeni u polju Vlasnik engl. Subject.

(3) Serijski broj koji isto tako sadrži prepoznatljivo ime, odredi ponuđač usluga povjerenja Halcom CA. (više u odjelj. 3.1.5.).

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

(5) Prilikom izdavanja kvalificiranog digitalnog certifikata, ponuđač usluga povjerenja Halcom CA može u polje Imaoc (English Subject) također dodati atribut 1.3.6.1.4.1.5939.2.9, koji predstavlja vrstu certifikata (npr.označava da se radi o kvalificiranom digitalnom certifikatu u oblaku, na pametnoj kartici ili USB ključu itd.)

Vrsta potvrde	Naziv polja	Prepoznatljivo ime
Korijenska (Root) potvrda ponuđača usluga povjerenja Halcom CA	Izdavatelj, engl. Issuer i Vlasnik, engl. Subject	C= SI O= Halcom d.d. 2.5.4.97 = VATSI-43353126 CN= Halcom Root Certificate Authority
Ukliještena/podređena (Intermediate) potvrda ponuđača usluga povjerenja Halcom CA	Izdavatelj, engl. Issuer	C= SI O= Halcom d.d. 2.5.4.97 = VATSI-43353126 CN= Halcom Root Certificate Authority
	Vlasnik, engl. Subject	C= SI O= Halcom d.d. 2.5.4.97= VATSI-43353126 CN= Halcom CA FO e-signature 2
Kvalificirana digitalna potvrda korisnika	Izdavatelj, engl. Issuer	C= SI O= Halcom d.d. 2.5.4.97= VATSI-43353126 CN= Halcom CA FO e-signature 2
	Vlasnik, engl. Subject	C= SI CN=<ime in priimek> SN= <priimek> G= <ime> SERIALNUMBER=<TINSI-davčna št. imetnika> in/ali 1.3.6.1.4.1.5939.2.2= <davčna št. imetnika> E= <elektronska pošta>

3.1.2 Zahtjev pri kreiranju prepoznatljivog imena

Oznaka fizičkog lica koja je u skladu sa odredbama odjelj. 3.1.1. uključena u prepoznatljivo ime, mora ispunjavati sljedeće zahtjeve:

- Mora biti jedinstveno
- Mora biti sa značenjem povezano sa vlasnikom

- Najveća dužina može biti četrdesetdva (42) znaka.

3.1.3 Upotreba anonimnih imena ili pseudonima

Upotreba anonimnih imena ili pseudonima nije dozvoljena.

3.1.4 Pravila za interpretaciju prepoznatljivih imena

(1) (1) Podaci o vlasniku potvrde u prepoznatljivom imenu sadrže slova engleske abecede, preostali znakovi se promjene prema donjem pravilu:

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

(2) Sa odgovarajućom kombinacijom slova ponuđač usluga povjerenja osigura korištenje drugih nepredviđenih znakova.

3.1.5 Jedinstvenost prepoznatljivih imena

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

3.1.6 Zaštita imena tj. robne marke

(1) Poslovni subjekti tj. vlasnici ne smiju zahtijevati nazive državnih organa ili organa lokalnih zajednica, imena, oznaka, robnih marki ili druge elemente intelektualnog vlasništva, koji bi pripadala trećim licima i bila bi sa tim kršena prava intelektualnog vlasništva ili drugog prava trećih lica ili odredbe važećih propisa.

(2) Moguće sporove rješavaju isključivo ugrožena strana i vlasnik potvrde.

3.2. Provjera identiteta vlasnika pri prvom izdavanju potvrde

3.2.1 Metoda za posjedovanje pripadnosti privatnog ključa

Dokazivanje o posjedovanju privatnog ključa, koji pripada javnom ključu u potvrdi, je osigurano sa sigurnim postupcima prije i pri preuzimanju potvrde te standardom PKC2#10.

3.2.2 Provjera identiteta organizacije

Nije propisano.

3.2.3 Provjera identiteta vlasnika

(1) Prijavna služba ponuđača usluga povjerenja Halcom CA nesporno utvrdi identitet vlasnika potvrde u skladu sa važećim propisima (službeni dokument sa slikom) ili obezbjeđuje podatke o imaocima iz svojih baza podataka, dobivenih upotrebom postupka od strane prijavne službe koja se koristi u drugu svrhu, što pruža ekvivalentno uvjerenje.

(2) Ponuđač usluga povjerenja Halcom CA provjeri lične podatke vlasnika u odgovarajućim registrima, ako sa važećim propisima nije drugačije određeno.

3.2.4 Neprovjereni podaci u potvrdama

Halcom CA ne provjerava pravilnost i djelovanje adrese e-pošte vlasnika potvrde.

3.2.5 Provjera punomoći zaposlenih za dobivanje potvrda

Nije propisano.

3.2.6 Međusobno priznavanje

(1) Ponuđač usluga povjerenja Halcom CA nije dužan ugovorno sudjelovati ili jamčiti za druge ponuđače usluga povjerenja i ako ima drugi ponuđač status kvalificiranog ponuđača usluga povjerenja.

(2) Ponuđač usluga povjerenja Halcom CA osigurava, da će provoditi međusobno priznavanje isključivo nakon potpisa pismenog ugovora sa drugim ponuđačima usluga povjerenja, koji moraju ispunjavati nivo sigurnosnih zahtjeva, koji je usporediv ili viši od onoga koju propiše ponuđač usluga povjerenja Halcom CA.

(3) Ako nije osigurana vanjska i neovisna procjena usklađenosti drugog ponuđača usluga povjerenja, ovlaštena lica Halcom CA pregledaju unutrašnja pravila drugog ponuđača usluga povjerenja te njegovo ispunjavanje sigurnosnih zahtjeva.

(4) Troškove potrebne infrastrukture, koju zahtjeva ponuđač usluga povjerenja Halcom CA za međusobno priznavanje, pokriva drugi ponuđač usluga povjerenja.

3.3. Provjera vlasnika za ponovno izdavanje potvrde

3.3.1 Provjera vlasnika pri produženju potvrda

Identitet vlasnika pri ponovnom izdavanju potvrde se provjerava:

- Na prijavnoj službi ponuđača usluga povjerenja Halcom CA,

- Na osnovu već izdatog važećeg kvalificiranog digitalnog potpisa, kojeg je izdao kvalificiran ponuđača usluga povjerenja, pri čemu ponuđač usluga povjerenja Halcom CA provjeri podatke poslovnog subjekta i vlasnika u odgovarajućim registrima.

-

3.3.2 Provjera vlasnika za ponovno dobivanje potvrde nakon poništenja

Provjera vlasnika teče u skladu sa odredbama odjelj. 3.2.3.

3.4. Provjera identiteta pri zahtjevu za poništenje

(1) Zahtjev za poništenje potvrde vlasnik predaje:

- Lično na prijavnu službu, gdje ovlaštena lica provjere identitet podnosioca molbe,
- Elektronski, iako mora biti zahtjev digitalno potpisan sa kvalificiranom digitalnom potvrdom, sa tim je iskazan i identiteta podnosioca molbe,

- Ako vlasnik potvrde preko telefona ili elektronske pošte zahtjeva poništenje potvrde, ponuđač usluge povjerenja Halcom CA odredi suspenziju potvrde. Tek na osnovu pismenog zahtjeva za poništenje potvrde se stvarno izvede prekid potvrde.

(3) Detaljan postupak za poništenje: odjelj. 4.9.3.

4. UPRAVLJANJE SA POTVRDAMA

4.1. Dobivanje potvrde

4.1.1 Ko može dobiti potvrdu

Budući vlasnici potvrda izdanih po ovoj politici su fizička lica.

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

4.1.2 Postupak budućeg vlasnika za dobivanje potvrde i odgovornosti

(1) Potvrda se izdaje na osnovu pravilno ispunjenog i potpisanog zahtjeva za izdavanje potvrde (u nastavku narudžbenice) od strane budućeg vlasnika potvrde. Molbu zakoniti zastupnik predaje prijavnoj službi Halcom CA, te podmiri finansijske obaveze u vezi sa izdavanjem potvrde. Narudžbenice za izdavanje digitalne potvrde su na raspolaganju u prijavnim službama Halcom CA i na web strani Halcom CA. Cjenik usluga je javno objavljen na web stranicama Halcom CA.

(2) Prije izdavanja narudžbenice Halcom CA budućeg vlasnika upozna sa ovom politikom i opštim pravilima rada ponuđača usluga povjerenja Halcom CA.

(3) Halcom CA zadržava pravo na odbijanje zahtjeva za izdavanje potvrde bez posebnog pismenog obrazloženja zbog nedostatka podataka, dokumentacije ili previsokog rizika za sigurnost ili zakonitost djelovanja.

4.2. Postupak pri prijemu zahtjeva za dobivanje potvrde

4.2.1 Provjera identiteta budućeg vlasnika

(1) Ovlašteno lice prijavne službe provjerava identitet i vlasnika sa važećim ličnim dokumentom sa slikom pri posjeti prijavne službe ili preko kurirske službe pri uručenju pametne kartice koda PIN, autorizacijskog koda ili narudžbenice za potvrdu u oblaku.

(2) U slučaju izdavanja narudžbenice na elektronski način ovlašteno lice ili poslužitelj ponuđača usluga povjerenja Halcom CA obavlja provjeru važnosti elektronskog potpisa. Identitet zakonitog budućeg vlasnika se pokazuje sa važnosti njegove elektronske identifikacije ili njegovog kvalificiranog elektronskog potpisa.

(3) Opunomoćene osobe su dužne provjeriti identitet budućeg vlasnika tj. sve one podatke koji su navedeni u zahtjevu i dostupni su u službenim evidencijama tj. drugim službenim važećim dokumentima.

(4) (4) Prijavne službe provjere ispunjene zahtjeve i primaju originalnu dokumentaciju te je na siguran način posreduju u Halcom CA.

4.2.2 Odobrenje/odbijanje zahtjeva

(1) Opunomoćene osobe ponuđača usluga povjerenja Halcom CA narudžbenicu za dobivanje potvrde odobre tj. u slučaju nepravilnih ili nedostajućih podataka ili neispunjavanja obaveza odbiju, o čemu bude poslovni subjekt tj. budući vlasnik odmah obaviješten lično ili putem e-pošte.

(2) U slučaju odobrenja ponuđač usluga povjerenja Halcom CA prije izdavanja potvrde obavijesti budućeg vlasnika u skladu sa važećim propisima.

4.2.3 Vrijeme za izdavanje potvrde

Halcom CA na osnovu odobrene narudžbenice i podmirenih financijskih obaveza u vezi sa izdavanjem potvrde izdaje potvrdu najkasnije u pet (5) radnih dana od primljene uplate.

4.3. Izdavanje potvrde

4.3.1 Postupak ponuđača usluga povjerenja Halcom CA

(1) Proizvodni postupak je ovisan od vrste potvrde.

- Napredna kvalificirana digitalna potvrda:
  Proizvodni postupak za potvrde i za dva para ključeva je sastavljen iz jasno odvojenih dijelova (ili funkcija) sa njihovim odgovarajuće odvojenim podsistemima:
  1. Predažuriranje sigurnosnog prenosnika (generisanje ključeva na kartici/ključu USB i šifre za zaštitu potvrde),
  2. Obrada molbe za izdavanje potvrde,
  3. Priprema potvrde,
  4. Ažuriranje sigurnog prenosnika (izdavanje i zapis potvrde, štampanje podataka vlasnika),
  5. Štampanje osobne šifre (kod PIN),
  6. Posredovanje potvrde i osobne šifre (kod PIN) te obavještenja vlasniku.

Potvrda na sigurnom nosaču i pripadajuća lična šifra (kod PIN) vlasniku se posreduje sa preporučenom poštom, u dvije odvojene pošiljke, u razmaku od jednog radnog dana. Izuzetak može biti da pošiljke ovlaštene osobe prijavne službe predaju vlasniku i lično.

- Kvalificirana digitalna potvrda u oblaku:
  Proizvodni postupak za potvrde i za par ključeva je sačinjen iz jasno odvojenih dijelova (ili funkcija), sa njihovim odgovarajuće odvojenim podsistemima:
  1. Obrada zahtjeva za izdavanje potvrde
  2. Priprema potvrde i registracijskog te aktivacijskog koda
  3. Posredovanje registracijskog i aktivacijskog koda te obavijesti vlasniku,
  4. Generiranje ključeva na sigurnom prenosniku u oblaku i izdavanje potvrde.

  Registracijski i aktivacijski kod se vlasniku posreduje putem dva odvojena kanala, jednim sa elektronskom poštom, drugim putem drugog sigurnog kanala (siguran web portal dostupan sa kvalificiranom potvrdom, lično uručenje putem klasične pošte ili putem posebne web stranice na kojoj se imaoc identificira posebnim kodom primljenim putem SMS-a i drugim podacima koji su mu poznati (npr. porezni broj nositelja, posljednje četiri znamenke ili CVV kod uplate ili kreditne kartice ili slično)). Izuzetak može biti da jedan od navedenih kodova ovlaštena osoba prijavne službe Halcom CA preda vlasniku i lično.

- Standardna kvalificirana digitalna potvrda:

Proizvodni postupak za potvrde i za par ključeva je sačinjen iz jasno odvojenih dijelova (ili funkcija), sa njihovim odgovarajuće odvojenim podsistemima:

1. Obrada zahtjeva za izdavanje potvrde
2. Priprema potvrde i registracijskog te aktivacijskog koda
3. Posredovanje registracijskog i aktivacijskog koda te obavijesti vlasniku,
4. Preuzimanje potvrda.

Referentni kod se vlasniku posreduje sa elektronskom poštom, autorizacijski kod preporučeno putem pošte. Izuzetak može biti da jedan od navedenih kodova ovlaštena osoba prijavne službe Halcom CA preda vlasniku i lično.

(2) Naručitelj i vlasnik u pravilu nisu ista osoba kao Halcom CA ili prijavna služba Halcom CA. Ako prijavna služba Halcom CA naručuje potvrdu za sebe ili za svoje opunomoćene zaposlene, takvu narudžbu dodatno pažljivo provjeri osoblje Halcom CA.
(3) Ako Halcom CA naruči potvrdu za sebe ili za svoje opunomoćene, izdavanje svih takvih potvrda dodatno pažljivo provjeri opunomoćeni za unutrašnji nadzor i opunomoćeni za regulatornu usklađenost.
(4) Svi opisani postupci su utemeljeni tako da ih ne može obaviti pojedino lice samo.

4.3.2 Obavijest vlasnika o izdavanju
Vidi prethodni odjeljak.

4.4. Preuzimanje potvrde

4.4.1 Postupak preuzimanja potvrde
(1) Kod naprednih potvrda preuzimanje potvrde nije potrebno, jer budući vlasnik potvrdu na sigurnom prenosniku i pripadajuću osobnu šifru (kod PIN) prima preporučeno putem pošte tj. u izuzetnim slučajevima može uručiti ovlašteno lice Halcom CA, vidi odjelj. 4.3.1.
(2) Kod potvrda u oblaku preuzimanje potvrde nije potrebno, jer isto putem punomoći vlasnika, sigurno čuva ponuđač usluga povjerenja Halcom CA. Korisniku se posreduje samo kod za pristup do sigurnog oblaka, vidi odjelj. 4.3.1.

(3) Kod standardnih potvrda budući vlasnik u skladu sa uputama potvrdu preuzima uz pomoć Halcom CA programske opreme za preuzimanje kvalificirane digitalne potvrde. Korisniku se posreduje samo kod za preuzimanje standardne potvrde, vidi odjelj. 4.3.1.

4.4.2 Objava potvrde
Postupak je opisan u 2. odjeljku.

4.4.3 Obavijest ponuđača usluga povjerenja o izdavanju potvrda trećim licima
Ponuđač usluga povjerenja Halcom CA o izdavanju pojedine potvrde vlasnicima potvrde ne obavještava treća lica. Prijavna služba može dobiti podatak o izdavanju potvrda za koje je primila zahtjev za izdavanje.

4.5. Obaveze i odgovornost korisnika u vezi korištenja potvrda

4.5.1 Obaveze vlasnika potvrde
(1) Vlasnik odnosno budući vlasnik potvrde je dužan:

- Upoznati se i postupati u skladu sa politikom prije izdavanje potvrde,
- Postupati u skladu sa politikom i ostalim važećim propisima

- Po preuzimanju odnosno aktivaciji potvrde provjeri podatke u potvrdi i pri mogućim greškama ili problemima odmah obavijestiti Halcom CA odnosno zahtijevati poništiti potvrde,
- Pratiti sve obavijesti Halcom CA i postupati u skladu sa njima,
- U skladu sa obavijestima na odgovarajući način ažurirati potrebnu hardversku i softversku opremu za siguran rad sa potvrdama,
- Odmah izvijestiti Halcom CA o svim izmjenama koje su povezane sa potvrdom,
- Zahtijevati poništenje potvrde, ako je bio osobni ključ ugrožen na način, koji utiče na pouzdanost upotrebe, ali ako postoje opasnost zloupotrebe,
- Zahtijevati poništenje potvrde u oblaku pri gubitku ili krađi mobilnog telefona, ali ako postoji opasnost zloupotrebe istog
- Koristiti potvrdu za svrhu, određen u potvrdi (vidi odjeljak 7.1.) i na način koji je određen sa politikom Halcom CA.

(2) Vlasnik odnosno budući vlasnik potvrde je u vezi čuvanja osobnog ključa dužan i:

- Podatke za preuzimanje odnosno aktivaciju potvrde pažljivo čuvati od neovlaštenih lica,
- Čuvati osobni ključ i potvrdu na način i na sredstvima za sigurno čuvanje osobnih ključeva u skladu sa obavijesti i preporukama Halcom CA,
- Osobni ključ i sve druge povjerljive podatke štiti sa primjerenom šifrom u skladu sa preporukama Halcom CA ili na drugi način tako da ima pristup do njih samo vlasnik,
- Pažljivo čuvati šifre za zaštitu odnosno pristup osobnom ključu
- Nakon isteka važenja tj. poništenju potvrde postupati u skladu sa obavijesti Halcom CA.

4.5.2 Obaveze za treća lica

(1) Treće lice koji se oslanja na potvrdu, mora:

- Postupati i koristiti potvrde u skladu i svrhom politike i ostalim važećim propisima.
- Pažljivo proučavati sve moguće rizike i odgovornosti pri korištenju potvrda i odredbi politike za način korištenja,
- Obavijestiti Halcom CA, ako sazna da su bili osobni ključevi vlasnika potvrde, na kojeg se oslanja, ugroženi na način koji utiče na pouzdanost upotrebe, ili ako postoji opasnost zloupotrebe, ili ako su se izmijenili podaci, navedeni u potvrdi,
- Oslanjati se na potvrdu samo za svrhu određenu u potvrdi (vidi odjelj. 6.1.7.) na način koji je određen sa politikom,
- U vrijeme korištenja potvrde provjeriti da potvrda nije u registru poništenih potvrda,
- U vrijeme korištenja potvrde provjeriti, ako je bio digitalni potpis kreiran u vrijeme važenja i sa odgovarajućom svrhom potvrde,
- U vrijeme korištenja potvrde provjeriti potpis potvrde ponuđača usluga povjerenja Halcom CA, koji je objavljen u ovoj politici i na web stranama Halcom, tj. Drugim ponuđačima usluga povjerenja
- Uzeti u obzir druge odredbe u koliko je sa ponuđačem usluga povjerenja Halcom CA sklopio dogovor o upotrebi potvrda

(2) Treće lice mora za provjeru važenja potpisa tj. druge kriptografske operacije koristiti softversku i hardversku opremu, sa kojom može na vjerodostojan način provjeriti sve gore navedene zahtjeve za sigurnu upotrebu potvrda.

4.6. Ponovno izdavanje potvrde

(1) Produženje važenja potvrde je moguće samo na molbu vlasnika potvrde.

(2) Nakon isteka važenja napredne potvrde mora vlasnik na jednokratnom (1x) produženju ponovo zatražiti izdavanje potvrde.

(3) Vlasnik potvrde može prije isteka važenja potvrde elektronskim putem zamoliti za izdavanje nove digitalne potvrde, koju propiše još sa važećom potvrdom

4.6.1 Okolnosti, koje zahtijevaju ponovno izdavanje potvrde

Prije isteka važnosti digitalne potvrde sa elektronskim zahtjevom za ponovno izdavanje vlasnik potvrde osigurava kontinuitet korištenja digitalne potvrde. Zahtjev za novo izdavanje je moguće uložiti i nakon isteka važnosti digitalne potvrde.

4.6.2 Lica koja mogu zahtijevati ponovno izdavanje potvrde

Produženje važenja potvrde je moguće samo na molbu vlasnika potvrde.

4.6.3 Postupak obrade zahtjeva za ponovno izdavanje potvrde

Postupak osigurava da je opunomoćeno lice koje podnese molbu za ponovno izdavanje potvrde bez izmjene javnog ključa stvarno vlasnik potvrde.

4.6.4 Obavijest vlasniku o novo izdanoj potvrdi

Vidi odjelj. 4.3.1.

4.6.5 Postupak preuzimanja novo izdate potvrde

Vidi odjelj. 4.4.1.

4.6.6 Objava novo izdate potvrde

Postupak je opisan u 2. odjelu.

4.6.7 Obavijest ponuđača usluga povjerenja o izdavanju potvrde trećim licima

Ponuđač usluga povjerenja Halcom CA o izdavanju pojedine potvrde vlasnicima potvrde ne obavještava treća lica. Prijavna služba može dobiti podatak o izdavanju potvrda, za koje je primila zahtjeve za izdavanje.

4.7. Regenerisanje ključeva

4.7.1 Razlozi za regeneraciju

Nije podržano.

4.7.2 Ko zahtjeva regeneraciju

Nije podržano.

4.7.3 Postupak za izdavanje zahtjeva za regeneraciju

Nije podržano.

4.7.4 Obavijest vlasniku potvrde o novo izdanoj potvrdi

Nije podržano.

4.7.5 Postupak preuzimanja

Nije podržano.

4.7.6 Objava potvrde ponuđača usluga povjerenja sa novim parom ključeva

Nije podržano.

4.7.7 Obavijest ponuđača usluga povjerenja o izdavanju potvrde trećim licima

Nije podržano.

4.8. Izmjena potvrde

(1) U slučaju izmjene podataka koji utiču na važenje prepoznatljivog imena tj. drugih podataka u potvrdi, potrebno je potvrdu poništiti.

(2) Za dobivanje nove potvrde je važno ponoviti postupak za dobivanje nove potvrde, kako je navedeno u odjeljku 4.1.

4.8.1 Okolnosti za izmjenu potvrde

Nije podržano.

4.8.2 Ko zahtjeva izmjenu

Nije podržano.

4.8.3 Postupak pri zahtjevu za izmjenom

Nije podržano.

4.8.4 Obavijest o izdavanju nove potvrde

Nije podržano.

4.8.5 Preuzimanje izmijenjene potvrde

Nije podržano.

4.8.6 Objava izmijenjene potvrde

Nije podržano.

4.8.7 Obavijest drugih subjekata o izmjeni

Nije podržano.

4.9. Poništavanje i suspenzija potvrde

(1) Poništenje potvrde može zahtijevati vlasnik potvrde bilo kada, ipak mora ga zahtijevati u slučaju:

1. Izmjene prepoznatljivog imena (DN),
2. Kada vlasnik potvrde zamjeni ključne podatke, povezane sa potvrdom (ime ili prezime)
3. Kada se utvrdi, ili li se sumnja da je došlo bilo do razotkrivanja ključa za potpisivanje ili o zloupotrebi potvrde,
4. zamjena potvrde sa drugom potvrdom (npr. Pri gubitku sigurnosnog prenosnika, gubitka mobilnog telefona, gubitak šifre za pristup podacima na kartici i slično)

(2) Halcom CA može poništiti potvrdu i bez zahtjeva vlasnika u slučajevima iz prvog stava ili na osnovu zahtjeva nadležnog suda, prekršajnih ili upravnih organa.

(3) Poništenje potvrde je moguće uraditi 24 sata dnevno. Detaljne upute za poništenje potvrde su objavljene na web stranicama Halcom CA.

(4) Halcom CA će na osnovu pravilnog zahtjeva za poništenje potvrde, potvrdu poništiti najkasnije u roku od četiri (4) sata. U slučaju nastanka nepredviđenih okolnosti će Halcom CA sa izuzetkom poništiti potvrdu najkasnije u 8 (osam) sati nakon prijema pravilnog zahtjeva za poništenje potvrde. U tom vremenu će poništena potvrda u imeniku biti označena kao poništena i dodata u registar poništenih potvrda. Ako vlasnik potvrde Halcomu CA bude posredovao nepravilan zahtjev za poništenje potvrde, biće mu poslano upozorenje o nepravilnom zahtjevu za poništenje potvrde i biće upoznat sa uputama za predaju pravilnog zahtjeva za poništenje.

4.9.1 Razlozi za poništenje

(1) Poništenje potvrde mora vlasnik zahtijevati u slučaju:

- Ako je bio osobni ključ vlasnika potvrde ugrožen na način koji utiče na pouzdanost korištenja,
- Ako postoji opasnost zloupotrebe osobnog ključa ili potvrde vlasnika,
- Ako su se izmijenili tj. pogrešni su ključni podaci navedeni u potvrdi

(2) Ponuđač usluga povjerenja Halcom CA poništi potvrdu i bez zahtjeva vlasnika odmah kada sazna:

- Da je podatak u potvrdi pogrešan ili je bila potvrda izdata na osnovu pogrešnih podataka,
- Da je došlo do greške pri provjeri identiteta podataka na prijavnoj službi
- Da su se izmijenile druge okolnosti koje utiču na važnost potvrde,
- Za neispunjavanje obaveza vlasnika,
- Da nisu podmireni mogući troškovi za upravljanje digitalnim potvrdama,
- Da je bila infrastruktura ponuđača usluga povjerenja ugrožena na način koji utiče na pouzdanost korištenja,
- Da je bio osobni ključ vlasnika potvrde ugrožen na takav način koji utiče na pouzdanost korištenja
- Da će Halcom CA prestati sa izdavanjem potvrda ili da je bilo ponuđaču usluga povjerenja zabranjeno upravljanje sa potvrdama i njegovu djelatnost nije preuzeo neki drugi ponuđač usluga povjerenja,
- Da je poništenje odredio nadležan sud, prekršajni ili upravni organ.

(3) Vlasnik digitalne potvrde može zahtijevati, u roku od trideset (30) dana od izdavanja, ponovno generisanje koda PIN za napredne potvrde odnosno referentne te aktivacijske kodove za standardne potvrde ili registracijske te aktivacijske kodove za potvrde u oblaku, u slučaju da je e-dostupne podatke samo zaboravio te pod civilnom i kaznenom odgovornosti jamči da ne postoji mogućnost da je/bi bio osobni ključ ugrožen na način koji utiče na pouzdanost korištenja i da ne postoji opasnost od zloupotrebe osobnog ključa ili potvrde vlasnika

4.9.2 Ko zahtjeva poništenje

Poništenje potvrde može zahtijevati:

- Vlasnik
- Nadležni sud, prekršajni ili upravni organ.

4.9.3 Postupci za poništenje

(1) Poništenje može vlasnik zahtijevati:

- Lično u vrijeme službenih sati u prijavnoj službi,
- Elektronski dvadesetčetiri (24) sata na dan sve dane u godini, ako se radi o mogućnosti zloupotrebe ili nepouzdanosti potvrde, onda u vrijeme koje je po zakonu radno vrijeme državnih organa,
- Putem faksa dvadesetčetiri (24) sata na dan sve dane u godini, ako se radi o mogućnosti zloupotrebe ili nepouzdanosti potvrde, onda u vrijeme koje je po zakonu radno vrijeme državnih organa,

(2) Ako se poništenje zahtjeva:

- Lično, potrebno je ispuniti odgovarajući zahtjev za poništenje potvrde te ga predati na prijavnu službu,
- Elektronski, mora vlasnik poslati na Halcom CA elektronsku obavijest sa zahtjevom za poništenje, koje mora biti digitalno potpisano sa povjerenjem važećom potvrdom za njegovu provjeru,

- Ako vlasnik potvrde preko telefona ili elektronske pošte zahtjeva poništenje potvrde, ponuđač usluga povjerenja Halcom CA odredi suspenziju potvrde. Tek na osnovu pismenog zahtjeva za poništenje potvrde, se stvarno izvede poništenje potvrde.

(3) O datumu te vremenu poništenja, osobi koja predaje zahtjev za poništenje te uzrocima za poništenje moraju biti uvijek obavješteni vlasnik.

(4) Sudovi, prekršajni i upravni organi, koji mogu zahtijevati poništenje, čine to u skladu sa zakonima koji uređuju postupak pred njima (kazneni postupak, procesni postupak, opšti upravni postupak i drugi).

(5) Odredbe u vezi sa poništenjem se smisleno koriste i za postupke u vezi sa ponovnim generisanjem koda PIN za napredne potvrde odnosno referentne te autorizacijske kodove za standardne potvrde i registracijske te aktivacijske kodove za potvrde u oblaku.

4.9.4 Vrijeme za izdavanje zahtjeva za poništenje

Poništenje je potrebno zahtijevati odmah, ako se radi o mogućnosti zloupotrebe ili nepouzdanosti itd. hitne slučajeve. U ostalim slučajevima poništenje se može zahtijevati prvi radni dan u vrijeme koje važi za službeno radno vrijeme na prijavnoj službi (vidi sljedeći odjeljak).

4.9.5 Vrijeme od primljenog zahtjeva za poništenje do provođenja poništenja

(1) Ponuđač usluga povjerenja Halcom CA nakon prijema važećeg zahtjeva za poništenje:

- Najkasnije u četiri (4) sata poništi potvrdu, ako se radi o poništenju zbog opasnosti zloupotrebe ili nepouzdanosti i sl.,
- Inače prvi radni dan nakon primitka zahtjeva za poništenje

(2) Nakon poništenja je takva potvrda odmah (najviše 5 sekundi) dodata u registar poništenih potvrda.

4.9.6 Zahtjevi za provjerom registra poništenih potvrda za treća lica

(1) Prije korištenja moraju treća lica koja se oslanjaju na potvrdu provjeriti najnoviji objavljeni registar poništenih potvrda. Zbog vjerodostojnosti i cjelovitosti je uvijek potvrđeno provjeriti i vjerodostojnost ovog registra, koji je digitalno potpisan od strane Halcom CA.

(2) Treće lice mora za svaku korištenu digitalnu potvrdu provesti potpuni postupak provjere lanca povjerenja u skladu sa evropskim i međunarodnim standardima i preporukama.

4.9.7 Učestalost objave registra poništenih potvrda

Registar poništenih potvrda se osvježava (za pristup registru vidi odjelj. 7.2.3.):

- Nakon svakog poništenja potvrde,
- Jednom dnevno, ako nema novih zapisa tj. izmjena, u registru poništenih potvrda i to približno dvadesetčetiri (24) sata nakon zadnjeg osvježenja

4.9.8 Vrijeme objave registra poništenih potvrda

(1) Objava novog registra poništenih potvrda se izvodi:

- U javnom imeniku na poslužitelju ldap://ldap.halcom.si odmah (najviše 5 sekundi),
- Na web strani http://domina.halcom.si/crls sa kašnjenjem najviše deset (10) minuta.

(2) Ponuđač usluga povjerenja Halcom CA osigurava što veću dostupnost svojih usluga, i to svim danima u godini, pri čemu se ne uzimaju u obzir nepredviđene okolnosti. Halcom CA će u slučaju nepredviđenih kvarova i planiranih tehničkih ili servisnih zahvata na infrastrukturu objavio registar poništenih potvrda najkasnije u 8 (osam) sati. U slučaju nastanka nepredviđenih okolnosti kao

posljedica više sile ili vanrednih događaja će Halcom CA izuzetno objaviti registar poništenih potvrda najkasnije u 24 sata, iako još prije isteka zadnjeg važećeg registra poništenih potvrda.

4.9.9 Paralelna provjera statusa potvrda

Podržan je protokol za provjeru statusa potvrda (OCSP) u skladu sa evropskim i međunarodnim standardima i preporukama (vidi odjelj. 7.3.). Provjera statusa certifikata u stvarnom vremenu može raditi s odgodom do jedne minute od objave novog registra.

4.9.10 Zahtjevi za paralelnu provjeru statusa potvrda

Treća lica moraju pri korištenju potvrde uvijek provjeriti da li je potvrda na koju se oslanjaju poništena.

4.9.11 Drugi načini za pristup statusu potvrda

Nisu podržani.

4.9.12 Posebni zahtjevi pri zloupotrebi privatnog ključa

Nisu određeni.

4.9.13 Razlozi za suspenziju

(1) Ako vlasnik potvrde telefonski ili elektronski zahtjeva poništenje potvrde, do prijema originalnog pismenog zahtjeva potvrdu privremeno suspendira.

(2) Ako vlasnik potvrde, trećeg ili drugog lica, državni ili srodni organ odnosno ponuđač usluga povjerenja sam, izrazi sumnju da se u vezi sa potvrdom postupa u suprotnosti sa ovom politikom odnosno važećim propisima, potvrda se privremeno suspendira do krajnje odluke.

4.9.14 Ko zahtjeva suspenziju

Vidi odjelj. 4.9.13.

4.9.15 Postupak za suspenziju

Vidi odjelj. 4.9.13.

4.9.16 Vrijeme suspenzije

Vidi odjelj. 4.9.13.

4.10. Provjeravanje statusa potvrda

4.10.1 Pristup za provjeru

(1) Registar poništenih potvrda je javno objavljen na poslužitelju ldap: //ldap.halcom.si/ putem protokola LDAP i na http://domina.halcom.si/crls putem HTTP protokola.

(2) Paralelna provjera statusa potvrde je dostupna na adresi http://ocsp.halcom.si.

(3) Detalji o objavi i pristupu su u odjeljcima 7.1 i 7.3

4.10.2 Raspoloživost

(1) Provjera statusa potvrde je stalno na raspolaganju dvadesetčetiri (24) sata sve dane u godini.

(2) Ponuđač usluga povjerenja Halcom CA osigurava što veću dostupnost svojih usluga, i to sve dane u godini, pri čemu se ne uzimaju u obzir nepredviđene okolnosti. Halcom CA će u slučaju nepredviđenih kvarova i neplaniranih tehničkih ili servisnih zahvata na infrastrukturi ponovo omogućiti provjeru statusa potvrda najkasnije u 8 (osam) sati. U slučaju nastanka nepredvidivih okolnosti kao posljedica više sile ili vanrednih događaja Halcom CA će sa izuzetkom omogućiti provjeru statusa potvrde najkasnije u 24 sata, a prije isteka zadnjeg važećeg registra poništenih potvrda.

4.10.3 Ostale informacije za provjeru statusa
Nisu propisane.

4.11. Prekid odnosa između vlasnika i ponuđača usluga povjerenja

Odnos između vlasnika tj. poslovnog subjekta i ponuđača usluga povjerenja Halcom CA se prekida ako:

- Potvrda istekne i vlasnik je ne produži
- Potvrda je poništena, vlasnik ne zahtjeva novu

4.12. Otkrivanje kopije ključeva za dešifriranje

4.12.1 Razlozi za otkrivanje kopije ključeva za dešifriranje
Nije podržano.

4.12.2 Ko zahtjeva otkrivanje kopije ključeva za dešifriranje
Nije podržano.

4.12.3 Postupak pri zahtjevu za otkrivanje kopije ključeva za dešifriranje
Nije podržano.

5. UPRAVLJANJE I SIGURNOSNI NADZOR INFRASTRUKTURE

(1) Halcom CA planira i izvodi sve sigurnosne mjere u skladu sa familijom standarda ISO/IEC 27000 i sa FIPS 140-2 nivo 3 te sa tehničkim zahtjevima ETSI.

(2) Oprema Halcom CA je postavljena u posebnim, odvojenim prostorijama i osigurana je sa višestepenim sistemom fizičke zaštite i tehničke zaštite protiv upada. Oprema je zaštićena od neovlaštenog pristupa. Isto tako je osigurana i zaštićena sa protupožarnim sistemom, sa sistemom protiv poplave, sistemom za prozračivanje i višestepenim sistemom neprekidnog napajanja.

(3) Halcom CA čuva rezervne i distribucijske prenosnike podataka tako da je u najvećoj mjeri spriječen gubitak, prodor ili neovlašteno korištenje ili mijenjanje pohranjenih informacija. Kako za ažuriranje podataka tako i za arhiviranje važnih informacija su osigurane rezervne kopije koje su pohranjene na drugom mjestu, kao što je pohranjena programska oprema z upravljanje sa potvrdama, za osiguranje ponovnog djelovanja u slučajevima, kada bi bili uništeni podaci na osnovu lokacija.

(4) Detaljan opis infrastrukture Halcom CA, operativni rad, postupci upravljanja sa infrastrukturom te nadzor nad sigurnosnom politikom njegovog djelovanja je određen sa njegovim unutrašnjim pravilima.

5.1. Fizička zaštita

(1) Oprema ponuđača usluga povjerenja je čuvana sa višestrukim sistemom fizičke i elektronske zaštite.

(2) Zaštita infrastrukture ponuđača usluga povjerenja se provodi u skladu sa preporukama struke za najviši nivo zaštite.

(3) Cjelokupan opis infrastrukture ponuđača usluga povjerenja i postupci upravljanja te zaštita istog su određeni sa unutrašnjim pravilima ponuđača usluga povjerenja.

5.1.1 Lokacija i struktura ponuđača usluga povjerenja

(1) Oprema ponuđača usluga povjerenja na Halcom CA je postavljena u posebnim, čuvanim, odvojenim prostorima.

(2) Osigurana je sa višestepenim sistemom fizičke i elektronske zaštite.

(3) Slične odredbe su u unutrašnjim pravilima ponuđača usluga povjerenja Halcom CA.

5.1.2 Fizički pristup do infrastrukture ponuđača usluga povjerenja

(1) Pristup do infrastrukture ponuđača usluga povjerenja je omogućen samo ovlaštenim licima ponuđača usluga povjerenja u skladu sa njihovim zadacima i punomoćima, vidi odjelj. 5.2.1.

(2) svi pristupi su čuvani u skladu sa zakonodavstvom i preporukama.

(3) Detaljne odredbe su u unutrašnjim pravilima ponuđača usluga povjerenja Halcom CA

5.1.3 Napajanje i prozračivanje

(1) Infrastruktura ponuđača usluga povjerenja ima osigurano neprekidno napajanje i odgovarajuće sisteme klima.

(2) Detaljno o tome je određeno u unutrašnjim pravilima ponuđača usluga povjerenja Halcom CA.

5.1.4 Zaštita od poplave

(1) Infrastruktura ponuđača usluga povjerenja nije izložena opasnosti poplava, osim u slučaju više sile.

(2) Detaljno o tome je određeno u unutrašnjim pravilima ponuđača usluga povjerenja Halcom CA

5.1.5 Zaštita od požara

(1) Prostori ponuđača usluga povjerenja su čuvani od moguće pojave požara.

(2) Detaljno o tome je određeno u unutrašnjim pravilima ponuđača usluga povjerenja Halcom CA.

5.1.6 Čuvanje prenosnika podataka

(1) Prenosnici podataka, bilo u papirnatom ili elektronskom obliku čuvaju se sigurno u zaštićenim objektima.

(2) Sigurnosne kopije softvera i šifriranih baza podataka ponuđača usluga povjerenja Halcom CA se redovno obnavljaju i čuvaju u dva odvojena i fizički zaštićena prostora, na različitim lokacijama.

5.1.7 Odstranjivanje otpadaka

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

(2) Odstranjivanje otpadaka izvodi posebna komisija u skladu sa unutrašnjim pravilima ponuđača usluga povjerenja Halcom CA.

(3) Detaljno o tome je određeno u Opštim pravilima djelovanja i unutrašnjim pravilima ponuđača usluga povjerenja Halcom CA.

5.1.8 Čuvanje na udaljenoj lokaciji

Vidi odjelj. 5.1.6.

5.2. Organizacijska struktura ponuđača usluga povjerenja

5.2.1 Organizacijske grupe

(1) Operativno, organizacijsko i stručno pravilno djelovanje ponuđača usluga, povjerenja Halcom CA vodi opunomoćeni za unutrašnji nadzor, koji je odgovoran za upravljanje potvrdama.

(2) Među opunomoćene osobe ponuđača usluga povjerenja Halcom CA spadaju:
- Zaposleni kod ponuđača usluga povjerenja Halcom CA i
- Prijavne službe.

(3) Zaposleni kod ponuđača usluga povjerenja na Halcom CA su raspoređeni u četiri organizacijske grupe, koje pokrivaju sljedeća područja:
- Upravljanje sa informacijskim sistemom,
- Upravljanje sa potvrdama,
- Zaštita i kontrola
- Regulativno.

Organizacijska grupa	Uloga	Osnovni zadaci	Broj osoba
Upravljanje sa informacijskim sistemom	Glavni sistemski administrator	• Priprema početne konfiguracije sistema, • Početna postavka parametara novih podređenih ponuđača usluga povjerenja • Postavljanje početne konfiguracije mreže • Priprema prenosnika podataka za restart sistema u slučaju katastrofalnog gubitka sistema • Sigurno pohranjivanje i distribucija kopija i nadogradnji na odvojenu lokaciju.	2
	Sistemski administrator	• Upravljanje postupaka za izdavanje potvrda • Pomoć podređenim ponuđačima usluga povjerenja • Opunomoćenje podređenih ponuđača usluga povjerenja • Pristup do protokola potpisivanja potvrda • Sigurno čuvanje i distribucija kopija i nadogradnji na odvojenu lokaciju.	2
Upravljanje sa potvrdama	Sistemski operater 1	• Priprema sistemskih kopija, nadogradnja i obnavljanje programske opreme, sigurno čuvanje i distribucija kopija i nadogradnji Administrativne funkcije povezane sa održavanjem	2

		• Provođenje arhiviranja zahtijevanih sistemskih zapisa • Ispis koda PIN • Dnevni pregled sistema.	
	Operater za autorizacijo	• Potvrđivanje izdavanja potvrda i davanje šifri.	2
	Operater za potvrde	• Predažuriranje potvrda i davanje šifri, • Priprema potvrda (obrada potpisanih zahtjeva za potvrde) • Ažuriranje (izrada potvrda, zapis na sigurni prenosnik, štampanje vlasnikovih podataka na siguran prenosnik) • Distribucija potvrda.	2
	Operater za kodove	• Distribucija koda PIN kod.	2
	Službenik za prijavu	• Identifikacija vlasnika potvrda.	2
	Službenik za poništenje	• Priprava zahtjeva za poništenje, • Poništenje potvrde.	2
Zaštita i kontrola	Administrator za sigurnost	• Određivanje sigurnosnih pravila i nadzor njihove implementacije • Pregled sistemske dokumentacije i kontrolnih dnevnika za nadzor rada • Lična saradnja i pomoć pri godišnjoj inventuri dokumentacije podređenih ponuđača usluga povjerenja.	2
	Opunomoćeni za unutrašnji nadzor	• Nadzor sigurnosnih pravila i nadzor njihove implementacije • Nadzor sistemske dokumentacije i kontrolnih dnevnika za nadzor rada.	2
Regulativno	Opunomoćeni za privatnost i usklađenost sa regulativama	• Samostalno i neovisno usmjeravanje, procjena čuvanja privatnosti i zaštite ličnih podataka	1

		• Osiguranje usklađenosti sa važećim evropskim i slovenskim propisima, međunarodnim standardima i preporukama • Stručna pomoć poslovodstvu i zaposlenim pri operativnom provođenju mjera zaštite privatnosti i osigurane usklađenosti sa regulativama.	

5.2.2 Broj osoba za pojedine zadatke

(1) Operativne radne uloge su planirane tako da u najvećoj mogućoj mjeri sprečavaju mogućnost zloupotrebe i podijeljene su među pojedinačne, organizacijske grupe:

Organizacijska grupa: Upravljanje sa informacijskim sistemom

Uloga: glavni sistemski administrator

Broj osoba: 2

Zadaci:

1. Priprema početne konfiguracije sistema, uključujući sigurno pokretanje i zaustavljanje rada sistema
2. Početna postavka parametara novih podređenih ponuđača usluga povjerenja
3. Postavljanje početne konfiguracije mreže
4. Priprema prenosnika podataka za restart sistema u slučaju katastrofalnog gubitka sistema
5. Sigurno pohranjivanje i distribucija kopija i nadogradnji na odvojenu lokaciju

Organizacijska grupa: Upravljanje sa informacijskim sistemom

Uloga: glavni sistemski administrator

Broj osoba: 2

Zadaci:

1. Upravljanje postupaka za izdavanje potvrda
2. Pomoć podređenim ponuđačima usluga povjerenja
3. Opunomoćenje podređenih ponuđača usluga povjerenja
4. Pristup do protokola potpisivanja potvrda
5. Sigurno čuvanje i distribucija kopija i nadogradnji na odvojenu lokaciju.

Organizacijska grupa: Upravljanje sa potvrdama

Uloga: sistemski operater 1

Broj osoba: 2

Zadaci:

1. Priprema sistemskih kopija, nadogradnja i obnavljanje softverske opreme, sigurno čuvanje i distribucija kopija i nadogradnji
2. Administrativne funkcije povezane sa održavanjem baze podataka ponuđača usluga povjerenja i koji pomažu pri istragama odstupanja od pravila
3. Izmjene imena poslužitelja i/ili mrežne adrese
4. Provođenje arhiviranja zahtijevanih sistemskih zapisa
5. Ispis koda PIN
6. Dnevni pregled sistema

Organizacijska grupa: Upravljanje sa potvrdama

Uloga: operater za autorizaciju

Broj osoba: 2

Zadaci:

1. Potvrđivanje izdavanja potvrda i davanje šifri

Organizacijska grupa: Upravljanje sa potvrdama

Uloga: operater za potvrde

Broj osoba: 2

Zadaci:

1. Predažuriranje potvrda i davanje šifri
2. Priprema potvrda (obrada potpisanih zahtjeva za potvrde)
3. Ažuriranje (izrada potvrda, zapis na sigurni prenosnik, štampanje vlasnikovih podataka na siguran prenosnik)
4. Distribucija potvrda

Organizacijska grupa: Upravljanje sa potvrdama

Uloga: operater za kodove

Broj osoba: 2

Zadaci:

1. Distribucija kod PIN

Organizacijska grupa: Upravljanje sa potvrdama

Uloga: službenik za prijavu

Broj osoba: 2

Zadaci:

1. Identifikacija vlasnika potvrda

Organizacijska grupa: Upravljanje sa potvrdama

Uloga: operater za poništenje

Broj osoba: 2

Zadaci:

1. Priprema zahtjeva za poništenje
2. Poništenje potvrde

Organizacijska grupa: Zaštita i kontrola

Uloga: administrator sigurnosti

Broj osoba: 2

Zadaci:

1. Određivanje sigurnosnih pravila i nadzor njihove implementacije
2. Pregled sistemske dokumentacije i kontrolnih dnevnika za nadzor rada
3. Lična saradnja i pomoć pri godišnjoj inventuri dokumentacije podređenih ponuđača usluga povjerenja

Organizacijska grupa: Zaštita i kontrola

Uloga: opunomoćeni za unutrašnji nadzor

Broj osoba: 2

Zadaci:

1. Nadzor sigurnosnih pravila i nadzor njihove implementacije
2. Nadzor sistemske dokumentacije i kontrolnih dnevnika za nadzor rada

Organizacijska grupa: Regulativno

Uloga: opunomoćeni za privatnost i usklađenost sa regulativom

Broj osoba: 1

Zadaci:

1. Samostalno i neovisno usmjeravanje, procjena čuvanja privatnosti i zaštite ličnih podataka

2. Osiguranje usklađenosti sa važećim evropskim i slovenskim propisima, međunarodnim standardima i preporukama

3. Stručna pomoć poslovodstvu i zaposlenim pri operativnom provođenju mjera zaštite privatnosti i osigurane usklađenosti sa regulativama.

(2) Navedeno je minimalan broj zaposlenih za pojedine uloge.

5.2.3 Dokazivanje identiteta za obavljanje pojedinih zadataka

Dokazivanje identiteta i prava pristupa za obavljanje pojedinih zadataka u skladu sa ulogom pojedine organizacijske grupe kao i za obavljanje zadataka prijavne službe, osiguran je zaštitnim mehanizmima i kontrolnim postupcima u skladu sa unutrašnjim pravilima ponuđača usluga povjerenja Halcom CA.

5.2.4 Nespojivost zadataka

Za svaku ulogu je unutrašnjim pravilima Halcom CA detaljno određeno, sa kojom se smije tj. ne smije udružiti. Za neke je potrebna prisutnost bar dvije za to ovlaštene osobe. U drugom slučaju nepredviđene odsutnosti određenih zaposlenih njihove uloge preuzimaju drugi zaposleni ako to po unutrašnjim pravilima nije nespojivo.

5.3. Nadzor nad osobljem

(1) Operativno, organizacijski i stručno pravilno djelovanje ponuđača usluga povjerenja Halcom CA vodi opunomoćeni za unutrašnji nadzor, koji ne obavljaju zadatke u vezi sa upravljanjem potvrdama.
(2) Opunomoćeni za unutrašnji nadzor vrši nadzor nad poslom Halcom CA. Opunomoćeni za unutrašnji nadzor u slučaju otkrivenih nedostataka odredi odgovarajuće mjere za otklanjanje tih nedostataka, koje je Halcom CA dužan izvesti, te vrši nadzor nad provođenjem određenih mjera.

5.3.1 Potrebne kvalifikacije i iskustva osoblja

Halcom CA zapošljava pouzdano i stručno osposobljeno osoblje, koje provjereno nije bilo kažnjavano za bilo koje kazneno djelo. Svo osoblje se redovno educira i stiče dodatna znanja iz svoje stručne oblasti.

5.3.2 Primjerenost osoblja

Osoblje ponuđača usluga povjerenja ima u skladu sa zahtjevima važećih propisa te tehničkim standardima i preporukama odgovarajuće kvalifikacije i iskustva.

5.3.3 Dodatni trening osoblja

Osobama koje obavljaju zadatke gore navedenih organizacijskih skupina i zadataka prijavne službe, se osigura sav potreban trening.

5.3.4 Zahtjevi za redovnim treninzima

Osoblje se trenira u odnosu na potrebe tj. novosti u vezi sa djelovanjem infrastrukture ponuđača usluga povjerenja Halcom CA.

5.3.5 Zamjena zadataka

Nije propisana.

5.3.6 Sankcije

Sankcije u slučaju neovlaštenog ili nemarnog provođenja zadataka se za ovlaštena lica ponuđača usluga povjerenja provode u skladu sa važećim propisima i unutrašnjim pravilima ponuđača usluga povjerenja Halcom CA.

5.3.7 Zahtjevi za vanjske izvođače

Za potencijalne vanjske izvođače vrijede jednaki zahtjevi kao za ovlaštena lica ponuđača usluga povjerenja Halcom CA.

5.3.8 Pristup osoblja dokumentaciji

Opunomoćenim osobama ponuđača usluga povjerenja je na raspolaganju sva potrebna dokumentacija u skladu sa važećim zaduženjima i zadacima.

5.4. Sigurnosni pregledi sistema

5.4.1 Vrste dnevnika

(1) Ponuđač usluga povjerenja Halcom CA redovno provjerava i evidentira sve što bitno utiče na:

- sigurnost infrastrukture,
- nesmetano djelovanje svih sigurnosnih sistema i
- da li je u međuvremenu došlo do upada ili probe upada neovlaštenih osoba do opreme ili podataka.

(2) Detaljni podaci o tome su u skladu sa Uredbom određeni u unutrašnjim pravilima ponuđača usluga povjerenja Halcom CA

5.4.2 Učestalost pregleda dnevnika

Ponuđač usluga povjerenja Halcom CA obavlja sigurnosne preglede svoje infrastrukture tj. dnevnika dnevno.

5.4.3 Vrijeme čuvanja dnevnika

Dnevnici se čuvaju bar deset (10) godina nakon njihovog nastanka, ako poseban zakon ne određuje duži rok.

5.4.4 Zaštita dnevnika

Dnevnici se čuvaju u skladu sa sigurnosnim mehanizmima, koji osiguravaju najviši nivo sigurnosti.

5.4.5 Sigurnosne kopije dnevnika

Sigurnosne kopije dnevnika se provode dnevno.

5.4.6 Skupljanje podataka za dnevnike

Podaci se skupljaju bilo automatski ili ručno, ovisno od vrste podataka.

5.4.7 Obavještavanje osobe koja je prouzrokovala događaj

Osobu koja je prouzrokovala događaj nije potrebno obavještavati.

5.4.8 Procjena ranjivosti sistema

(1) Analiza dnevnika i nadzor nad provođenjem svih postupaka izvodi se redovno od strane ovlaštenih lica ponuđača usluga povjerenja ili automatski sa drugim sigurnosnim mehanizmima na svim informacijsko-komunikacijskim uređajima ponuđača usluga povjerenja.

(2) Procjena ranjivosti se provodi na osnovu analize dnevnika, sigurnosnih događaja i drugih važnih podataka.

5.5. Dugoročno čuvanje podataka

5.5.1 Vrste dugoročno čuvanih podataka

Ponuđač usluga povjerenja Halcom CA u skladu sa odredbama važećih propisa čuva sljedeću dokumentaciju:

- Dnevnike
- Zapisnike
- Sve dokaze o obavljenoj provjeri identiteta vlasnika tj. poslovnih subjekata,
- Sve zahtjeve
- Potvrde i registar poništenih potvrda,
- Politike djelovanja
- Objave i obavijesti ponuđača usluga povjerenja Halcom CA te
- Ostale dokumente u skladu sa važećim propisima.

5.5.2 Rok čuvanja

(1) Dugoročno čuvani podaci u vezi sa ključevima i digitalnim potvrdama se čuvaju bar deset (10) godina nakon isteka potvrde, na koju se podaci odnose, ako poseban zakon ne određuje duži rok.

(2) Ostali dugoročni čuvani podaci se čuvaju bar deset (10) godina nakon njihovog nastanka, ako poseban zakon ne određuje duži rok.

5.5.3 Zaštita dugoročno čuvanih podataka

(1) Dugoročno čuvani podaci su sigurno pohranjeni.

(2) Detaljnije uređenje je u skladu sa važećim propisima, standardima i preporukama određena u Općim pravilima djelovanja i unutrašnjim pravilima ponuđača usluga povjerenja Halcom CA.

5.5.4 Sigurnosna kopija dugoročno čuvanih podataka

(1) Kopija dugoročno čuvanih podataka sigurno se čuva.

(2) Detaljnije uređenje je u skladu sa važećim propisima, standardima i preporukama određena u Općim pravilima djelovanja i unutrašnjim pravilima ponuđača usluga povjerenja Halcom CA.

5.5.5 Zahtjev za vremensko žigosanje

Nije propisano.

5.5.6 Način skupljanja podataka

(1) Podaci se skupljaju na način, usklađen sa vrstom dokumenta.

(2) Detaljnije uređenje je u skladu sa važećim propisima, standardima i preporukama određeno u Općim pravilima djelovanja i unutrašnjim pravilima ponuđača usluga povjerenja Halcom CA.

5.5.7 Postupak za pristup dugoročno čuvanim podacima i njihova verifikacija

(1) Pristup do dugoročno čuvanih podataka je moguć samo ovlaštenim licima.

(2) Detaljnije uređenje je u skladu sa važećim propisima, standardima i preporukama određeno u Opštim pravilima djelovanja i unutrašnjim pravilima ponuđača usluga povjerenja Halcom CA.

5.6. Izmjena javnog ključa ponuđača usluga povjerenja Halcom CA

U slučaju nove izdate vlastite potvrde ponuđača usluga Halcom CA postupak se objavi na web strani ponuđača usluga povjerenja Halcom CA.

5.7. Plan oporavka od katastrofe

5.7.1 Postupak u slučaju upada i zloupotrebe

Detaljnije uređenje je u skladu sa važećim propisima, standardima i preporukama određeno u Opštim pravilima djelovanja i unutrašnjim pravilima ponuđača usluga povjerenja Halcom CA.

5.7.2 Postupak u slučaju kvara softvera, podataka

Detaljnije uređenje je u skladu sa važećim propisima, standardima i preporukama određeno u Opštim pravilima djelovanja i unutrašnjim pravilima ponuđača usluga povjerenja Halcom CA.

5.7.3 Postupak u slučaju ugroženog privatnog ključa ponuđača usluga povjerenja Halcom CA

Detaljnije uređenje je u skladu sa važećim propisima, standardima i preporukama određeno u Opštim pravilima djelovanja i unutrašnjim pravilima ponuđača usluga povjerenja Halcom CA.

5.7.4 Plan oporavka od katastrofe

Osigurano je duplanje kritičnih sistema i čuvanje podataka na geografski udaljenoj lokaciji. Detaljnije uređenje je u skladu sa važećim propisima, standardima i preporukama određeno u Opštim pravilima djelovanja i unutrašnjim pravilima ponuđača usluga povjerenja Halcom CA.

5.8. Prestanak rada Halcom CA

Detaljnije uređenje je u skladu sa važećim propisima, standardima i preporukama određeno u Opštim pravilima djelovanja i unutrašnjim pravilima ponuđača usluga povjerenja Halcom CA.

6. TEHNIČKI SIGURNOSNI ZAHTJEVI

6.1. Generisanje i podešavanje ključeva

6.1.1 Generisanje ključeva

(1) Par ključeva ponuđača usluga povjerenja Halcom CA za potpisivanje i provjeru važenja potpisa je bio kreiran po najvišim sigurnosnim standardima, u sigurnom okruženju ponuđača usluga povjerenja Halcom CA.

(2) Par ključeva vlasnika naprednih kvalificiranih potvrda se generišu na sigurnom prenosniku u sigurnom okruženju ponuđača usluga povjerenja Halcom CA.

(3) Par ključeva vlasnika kvalificiranih potvrda u obliku se generišu u hardverskom sigurnosnom modulu, u sigurnom okruženju ponuđača usluga povjerenja Halcom CA

(4) Par ključeva vlasnika standardnih kvalificiranih potvrda se generišu kod vlasnika.

6.1.2 Dostava privatnog ključa vlasnicima

(1) Privatne ključeve naprednih potvrda vlasniku se posreduje na sigurnom prenosniku sa preporučenom poštom. Sa izuzetkom može pošiljku ovlašteno lice Halcom Ca vlasniku predati i lično.

(2) Privatni ključ potvrde u oblaku vlasniku se ne posreduje, isti po punomoći vlasnika sigurno čuva ponuđača usluga povjerenja Halcom Ca

(3) Privatni ključ standardne potvrde se generiše kod vlasnika, ne posreduje se, naime isti se putem punomoći vlasnika sigurno čuva ponuđač usluga povjerenja Halcom CA.

6.1.3 Dostava javnog ključa ponuđaču usluga povjerenja

(1) Kod naprednih potvrda se ključevi generišu na sigurnom prenosniku u sigurnom okruženju ponuđača usluga Halcom Ca.

(2) Kod potvrda u oblaku ključevi se generišu u kriptografskom modulu, u sigurnom okruženju ponuđača usluga povjerenja Halcom CA.

(3) Kod standardnih potvrda se ključevi generišu kod vlasnika. Izdavanje potvrde se odvija preko Halcom CA softverske opreme za preuzimanje digitalne potvrde.

6.1.4 Dostava javnog ključa ponuđača usluga povjerenja

Potvrda sa javnim ključem ponuđača usluga povjerenja Halcom CA je vlasniku dostavljeno tj. trećim licima dostupno:

- U javnom imeniku ldap://ldap.halcom.si putem LDAP protokola (vidi odjeljak 2.3.)
- U obliku PEM na adresi http://www.halcom.si/si/produkti/digitalno-potrdilo/politike-in-dokumenti/, pri čemu mora dodatno provjeriti vjerodostojnost potvrde.

6.1.5 Dužina ključeva

Potvrda	Dužina ključa po RSA [bit]
Korijenska (Root) potvrda ponuđača usluga povjerenja Halcom CA	Najmanje 2048
Ugniježdena/podređena (Intermediate) potvrda ponuđača usluga povjerenja Halcom CA	Najmanje 3072
Kvalificirana digitalna potvrda korisnika	Najmanje 2048

6.1.6 Generisanje i kvaliteta parametara javnih ključeva

Kvalitet parametara ključa ponuđača usluga povjerenja Halcom CA je osigurana na strani proizvođača softvera sa korištenjem kvalitetnim generatora slučajnih brojeva (engl. Random number generator).

6.1.7 Svrha ključeva i potvrda

(1) Namjena korištenja ključeva tj. potvrda je u skladu sa X.509 v.3 određen u potvrdi u polju korištenja ključa (engl. keyUsage) i proširena upotreba ključa (engl. Extenden keyUsage).

(2) Za potpis potvrda i registra poništenih potvrda je namijenjen privatni ključ ponuđača usluga povjerenja Halcom Ca, za provjeru važenja potpisa javni ključ u potvrdi ponuđača usluga povjerenja.

(3) Profil potvrda je dat u odjeljku 7.1

6.2. Zaštita privatnog ključa

6.2.1 Standardi za kriptografski modul

Privatni ključ ponuđača usluga povjerenja HALCOM CA je zaštićen u kriptografskom modulu, koji je certificiran u skladu sa FIPS 140-2 nivo 3 i/ili Common Criteria EAL4+.

6.2.2 Nadzor privatnog ključa od strane ovlaštenih lica

Odredbe u vezi pristupa privatnom ključu ponuđača usluga povjerenja Halcom CA su u skladu sa važećim propisima i Opštim pravilima rada određena u unutrašnjim pravilima ponuđača usluga povjerenja Halcom CA.

6.2.3 Otkrivanje kopije privatnog ključa

Odredbe u vezi otkrivanja privatnog ključa ponuđača usluga povjerenja Halcom CA su u skladu sa važećim propisima i Opštim pravilima rada određena u unutrašnjim pravilima ponuđača usluga povjerenja Halcom CA.

6.2.4 Sigurnosna kopija privatnog ključa

Odredbe u vezi sigurnosnog kopiranja privatnog ključa ponuđača usluga povjerenja Halcom CA su u skladu sa važećim propisima i Opštim pravilima rada određena u unutrašnjim pravilima ponuđača usluga povjerenja Halcom CA.

6.2.5 Arhiviranje privatnog ključa

(1) Privatne ključeve Halcom CA može kopirati i čuvati samo ovlaštena osoba ponuđača usluga povjerenja Halcom CA. Sigurnosne kopije ključeva se čuvaju sa jednakim stepenom zaštite kao ključevi u upotrebi.

(2) Detaljnije odredbe kopiranja privatnog ključa ponuđača usluga povjerenja Halcom CA su u skladu sa važećim propisima i Opštim pravilima rada određena u unutrašnjim pravilima ponuđača usluga povjerenja Halcom Ca.

6.2.6 Prijenos privatnog ključa iz/u kriptografski modul

(1) Privatni ključevi kod naprednih potvrda se kreiraju u sigurnom prenosniku sa kojim se naknadno prenesu vlasniku potvrde.

(2) Privatni ključevi kod potvrda u oblaku se kreiraju i čuvaju u kriptografskom modulu koji je certificiran u skladu sa FIPS 140-2 nivo 3 i/ili Common Criteria EAL4+.

(3) Privatni ključevi standardnih potvrda se kreiraju i čuvaju kod vlasnika.

6.2.7 Čuvanje privatnog ključa u kriptografskom modulu

(1) Privatni ključevi ponuđača usluga povjerenja Halcom CA se čuvaju u kriptografskom modulu koji je certificiran u skladu sa FIPS 140-2 nivo 3 i/ili Common Criteria EAL4+.

(2) Privatni ključevi korisnika:

- Napredne potvrde se kreiraju i čuvaju na sigurnom prenosniku
- Potvrde u oblaku se kreiraju i čuvaju u kriptografskom modulu
- Standardne potvrde se kreiraju i čuvaju kod vlasnika.

6.2.8 Postupak za aktiviranje privatnog ključa

(1) Postupak za aktiviranje privatnog ključa ponuđača usluga povjerenja Halcom CA teče na siguran način u skladu sa odredbama unutrašnjih pravila ponuđača usluga povjerenja Halcom Ca.

(2) Halcom CA vlasnicima preporučuju korištenje softverskog okruženja koje pri odjavi ili nakon određenog vremena onemogućava pristup njihovom privatnom ključu bez unosa odgovarajuće šifre

(3) Vlasnik potvrde za potpisivanje u oblaku može koristiti usluge kvalificiranog elektronskog potpisa u oblaku. U takvom slučaju vlasnik ili u njegovo ime neki drugi pošiljatelj posreduje na siguran način ponuđaču usluga povjerenja Halcom CA elektronski dokument, koji se kvalificirano elektronski potpiše. Vlasnik zatim na siguran način preko mobilnog uređaja i sa korištenjem od strane ponuđača usluga povjerenja Halcom CA propisanog sigurnosnog postupka (korištenje PIN i mobilnih sigurnosnih

postupaka) odobrava kvalificirani elektronski potpis u oblaku. Na osnovu odobrenja vlasnika ponuđača usluga povjerenja Halcom CA koristi osobni ključ vlasnika u oblaku i kvalificirano elektronski potpiše dokument te potpisan dokument dostavi vlasniku ili drugom pošiljatelju dokumenta.

(4) Zbog zaštite povjerljivosti elektronskih dokumenata vlasnika, može vlasnik pri narudžbi potvrde izričito pismeno zahtijevati, da ponuđač usluga povjerenja Halcom CA pri potpisivanju u oblaku, kako je opisano u prethodnom stavu, ne zahtjeva prijem cjelokupnog dokumenta za kvalificiran elektronski potpis u oblaku, nego samo hash vrijednosti (engl. Hash value) takvog dokumenta i vlasniku ili drugom pošiljatelju posreduje samo kvalificirani elektronski potpis. Halcom CA u takvom slučaju ne osigurava provjeru proračuna hash vrijednosti ili drugih sigurnosnih mehanizama u vezi elektronskog dokumenta te je odgovornost u cijelosti na strani vlasnika.

6.2.9 Postupak za deaktiviranje privatnog ključa

Postupak za deaktiviranje privatnog ključa ponuđača usluga povjerenja Halcom CA teče na siguran način u skladu sa odredbama unutrašnjih pravila ponuđača usluga povjerenja Halcom CA.

6.2.10 Postupak za uništavanje privatnog ključa

(1) Postupak za uništavanje privatnog ključa ponuđača usluga povjerenja Halcom CA teče na siguran način u skladu sa odredbama unutrašnjih pravila ponuđača usluga povjerenja Halcom CA i uputa proizvođača hardverskog sigurnosnog modula. Privatni ključ se uništava tako da ga nije moguće restaurirati.

(2) Uništenje privatnih ključeva od strane vlasnika je u nadležnosti vlasnika. Koristiti moraju odgovarajuće aplikacije za sigurno brisanje naprednih potvrda.

(3) Privatni ključ potvrde u oblaku se nakon isteka važnosti potvrde automatski uništava. Privatni ključ potvrde u oblaku može na zahtjev vlasnika potvrde Halcom CA uništiti i prije isteka važnosti. Privatni ključ se uništava tako da ga nije moguće restaurirati.

6.2.11 Svojstva kriptografskog modula

Hardverski sigurnosni moduli odgovaraju standardima datim u odjelj. 6.2.1.

6.3. Ostali aspekti upravljanja ključevima

6.3.1 Arhiviranje javnog ključa

Ponuđač usluga povjerenja Halcom CA arhivira svoj javni ključ i javne ključeve vlasnika, kako je dato u odjeljku 5.5.

6.3.2 Period važenja za javne i privatne ključeve

(1) Važnost potvrde je jasna iz donje tabele

Tip potvrde	Potvrda	Ključ	Važenje
Napredna potvrda	Par ključeva za digitalno potpisivanje/provjeru važnosti potpisa	Privatni ključ za potpisivanje	3 godine
		Javni ključ za provjeru važnosti potpisa	3 godine
		Privatni ključ za dešifrovanje	3 godine

	Par ključeva za dešifriranje/šifriranje	Javni ključ za šifriranje	3 godine
Potvrda u oblaku	Par ključeva za digitalno potpisivanje/provjeru važnosti potpisa	Privatni ključ za potpisivanje	1 - 3 godine
		Javni ključ za provjeru važnosti potpisa	1 - 3 godine

(2) Halcom CA može u posebnim slučajevima za pojedinu potvrdu odrediti i drugačiji rok važenja potvrde.

6.4. Šifre za pristup potvrdama tj. ključevima

6.4.1 Generisanje šifara

(1) Osobni broj (kod PIN) za korištenje napredne potvrde i broj za otključavanje sigurnog prenosnika (kod PUK) se kreiraju na strani Halcom CA. Osobni broj mora vlasnik prije prvog korištenja promijeniti.

(2) Registracijski i aktivacijski kod za potvrde u oblaku se kreiraju na strani Halcom CA. U procesu aktivacije korisnik postavi svoj osobni broj (kod PIN) za pristup potvrdi u oblaku

(3) Referentne i autorizacijske kodove za preuzimanje standardne potvrde se kreiraju sigurno kod ponuđača usluga povjerenja Halcom CA. U procesu preuzimanja potvrde korisnik sam odredi šifru sa kojom zaštiti pristup do svojih osobnih ključeva. Halcom CA preporučuje da se šifra za pristup osobnom ključu ne čuva tj. pohrani se na sigurno mjesto i da tom mjestu pristup ima samo vlasnik.

6.4.2 Zaštita šifara

(1) Osobna šifra za korištenje napredne potvrde i šifra za otključavanje sigurnog prenosnika se kreiraju kod ponuđača usluga povjerenja Halcom CA. Halcom CA posreduje obje šifre vlasniku potvrde preporučeno putem pošte, u izuzetnom slučaju preda je lično. Halcom CA preporučuje da se obje šifre čuvaju na sigurnom mjestu do kojeg pristup ima samo vlasnik.

(2) Registracijski i aktivacijski kod se kreiraju sigurno kod ponuđača usluga povjerenja Halcom Ca. Kodovi se vlasniku posreduju putem dva odvojena kanala, jednim putem elektronske pošte, drugi putem drugog sigurnog kanala (siguran web portal dostupan sa kvalificiranom potvrdom, osobno uručenje putem klasične pošte i drugi sličan siguran način). Izuzetak može biti da aktivacijske kodove ovlašteno lice prijavne službe Halcom CA vlasniku preda osobno. Kodovi su namijenjeni samo za aktivaciju pristupa potvrdi u oblaku, za koji si korisnik sam postavi svoj osobni broj (kod PIN).

(3) Referentne i autorizacijske kodove za preuzimanje standardne potvrde se kreiraju sigurno kod ponuđača usluga povjerenja Halcom CA. Referentni kod se vlasniku posreduje sa elektronskom poštom, autorizacijski kod putem preporučene pošte. Izuzetak može biti da aktivacijske kodove ovlašteno lice prijavne službe Halcom CA vlasniku preda osobno. Kodovi su namijenjeni samo za preuzimanje standardne potvrde. U procesu preuzimanja potvrde korisnik sam odredi šifru sa kojom štiti pristup svojim osobnim ključevima.

6.4.3 Ostali aspekti šifara

Nisu propisani

6.5. Sigurnosni zahtjevi za informacijsko-komunikacijsku opremu ponuđača usluga povjerenja

6.5.1 Specifični tehnički zahtjevi sigurnosti

Detaljnije određenje je u skladu sa važećim propisima, standardima i preporukama određeno u Opštim pravilima djelovanja i unutrašnjim pravilima ponuđača usluga povjerenja Halcom CA.

6.5.2 Nivo sigurnosne zaštite

Detaljnije uređenje je u skladu sa važećim propisima, standardima i preporukama određena u Opštim pravilima djelovanja i unutrašnjim pravilima ponuđača usluga povjerenja Halcom CA.

6.6. Tehnički nadzor životnog ciklusa ponuđača usluga povjerenja

6.6.1 Nadzor razvoja sistema

Halcom CA koristi softversku i hardversku opremu koja je certificirana u skladu sa FIPS 140-2 nivo 3 i/ili Common Criteria EAL4+.

6.6.2 Upravljanje sigurnosti

Detaljnije uređenje je u skladu sa važećim propisima, standardima i preporukama određena u Opštim pravilima djelovanja i unutrašnjih pravila ponuđača usluga povjerenja Halcom CA.

6.6.3 Nadzor životnog ciklusa

Detaljni tehnički zahtjevi su određeni u Opštim pravilima djelovanja i unutrašnjim pravilima ponuđača usluga povjerenja Halcom CA.

6.7. Sigurnosna kontrola mreže

Detaljnije određenje je u skladu sa važećim propisima, standardima i preporukama određeno u Opštim pravilima djelovanja i unutrašnjim pravilima ponuđača usluga povjerenja Halcom CA.

6.8. Vremenski žig

Nije propisan.

7. PROFIL POTVRDA I REGISTRA PONIŠTENIH POTVRDA

7.1. Profil potvrda

(1) Na osnovu ove politike Halcom CA izdaje napredne potvrde i potvrde u oblaku za poslovne subjekte.

(2) Sve potvrde uključuju podatke koji su u skladu sa uredbom eIDAS određena na kvalificirane potvrde.

(3) Potvrde ponuđača usluga povjerenja Halcom CA prate standard X.509.

7.1.1 Verzija potvrde

Sve potvrde ponuđača usluga povjerenja Halcom CA slijede standard X.509, i to verziju 3.

7.1.2 Profil potvrda sa proširenjima

(1) Profil korijenske (root) potvrde – Halcom Root Certificate Authority.

Nazivi polja	Vrijednost tj. značenje
Osnovna polja u potvrdi	

Verzije, engl. Version	V3
Identifikacijska oznaka potvrde, engl. Serial Number	Jedinstven interni broj potvrde
Algoritam za potpis, engl. Signature algorithm	Sha256RSA (OID 1.2.840.113549.1.1.11)
Izdavatelj, engl. Issuer	CN = Halcom Root Certificate Authority 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Važenje, engl. Validity	Valid from: <10.6.2016 07:07:50 GMT > Valid to: <10.6.2036 07:07:50 GMT >
Vlasnik, engl. Subject	CN = Halcom Root Certificate Authority 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Algoritam za javni ključ, engl. Subject Public Key Algorithm	rsaEncryption (OID 1.2.840.113549.1.1.1)
Javni ključ, engl. Public Key (... bits)	modul, eksponent,...
Vlasnikov javni ključ, koji pripada odgovarajućem paru ključeva, šifriran sa alg. RSA, engl. RSA Public Key	dužina ključa je 2048 bita
Proširenje X.509v3	
Upotreba ključa, OID 2.5.29.15, engl. Key Usage	Certificate Signing, Off-line CRL Signing, CRL Signing
Identifikator vlasnikovog ključa, OID 2.5.29.14, engl. Subject Key Identifier	42 ae a6 43 c7 98 28 b0
Osnovna ograničenja, OID 2.5.29.19, engl. Basic Constraints	Subject Type=CA Path Length Constraint=None

Dodatna identifikacija (nije dio digitalne potvrde)	
Prepoznatljivi otisak potvrde - SHA1 engl. Certificate Fingerprint – SHA1	Prepoznatljivi otisak potvrde po SHA1

(2) Profil ugniježdene/podređene (intermediate) potvrde – Halcom CA FO e-signature 2

Nazivi polja Osnovna polja u potvrdi	Vrijednost tj. značenje
Verzija, engl. Version	V3
Identifikacijska oznaka potvrde, engl. Serial Number	jedinstven interni broj potvrde
Algoritam za potpis, engl. Signature algorithm	Sha256RSA (1.2.840.113549.1.1.11)
Izdavatelj, engl. Issuer	CN = Halcom Root Certificate Authority 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Važenje, engl. Validity	Valid from: <03.04.2023 07:00:00 GMT > Valid to: <03.04.2033 07:00:00 GMT >
Vlasnik, 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	rsaEncryption (OID 1.2.840.113549.1.1.1)
Javni ključ, engl. Public Key (... bits)	modul, eksponent,...
Vlasnikov javni ključ, koji pripada odgovarajućem paru ključeva, šifriran sa alg. RSA, engl. RSA Public Key	dužina ključa 3072 bita
Proširenje X.509v3	

Objava registra poništenih 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
Upotreba ključa, OID 2.5.29.15, engl. Key Usage	Certificate Signing, Off-line CRL Signing, CRL Signing
Identifikator ključa ponuđača usluga povjerenja, OID 2.5.29.35, engl. Authority Key Identifier	KeyID=42 ae a6 43 c7 98 28 b0
Identifikator vlasnikovog ključa, OID 2.5.29.14, engl. Subject Key Identifier	48 c4 27 a6 6f 6e f0 2e
Osnovna ograničenja, OID 2.5.29.19, engl. Basic Constraints	Subject Type=CA Path Length Constraint=None
Dodatna identifikacija (nije dio digitalne potvrde)	
Prepoznatljivi otisak potvrde - SHA1 engl. Certificate Fingerprint – SHA1	Prepoznatljivi otisak potvrde po SHA1

(3) Profil potvrda krajnjih korisnika

Nazivi polja Osnovna polja u potvrdi	Vrijednost tj. značenje
Verzija, engl. Version	V3
Identifikacijska oznaka potvrde, engl. Serial Number	jedinstven interni broj potvrde
Algoritam za potpis, engl. Signature algorithm	Sha256RSA (OID 1.2.840.113549.1.1.11)

Izdavatelj, engl. Issuer	CN = Halcom CA FO e-signature 2 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Važenje, engl. Validity	Valid from: <početak važenja po GMT> Valid to: <kraj važenja po GMT>
Vlasnik, engl. Subject	prepoznatljivo ime vlasnika, vidi odjelj. 3.1.1.
Algoritam za javni ključ, engl. Subject Public Key Algorithm	rsaEncryption (OID 1.2.840.113549.1.1.1)
Javni ključ, engl. Public Key (... bits)	modul, eksponent,...
Vlasnikov javni ključ, koji pripada odgovarajućem paru ključeva, šifriran sa alg. RSA, engl. RSA Public Key	dužina ključa je min 2048 bita, vidi odjelj. 6.1.5.
Proširenja X.509v3	
Objava registra poništenih potvrda, OID 2.5.29.31, engl. CRL Distribution Points	URI:ldap://ldap.halcom.si/cn=Halcom%20CA%20FO%20e-signature%202,o=Halcom,c=SI?certificaterevocationlist;binary URL=http://domina.halcom.si/crls/halcom_ca_fo_e-signature_2.crl
Upotreba ključa, OID 2.5.29.15, engl. Key Usage	Napredne potvrde: Digital Signature, Non Repudiation, Key Encipherment Standardne potvrde: Digital Signature, Key Encipherment Potvrde u oblaku: Digital Signature, Non Repudiation
Identifikator ključa ponuđača usluga povjerenja, OID 2.5.29.35, engl. Authority Key Identifier	KeyID=48 c4 27 a6 6f 6e f0 2e
EŠEI	Jedinstveni broj elektronske identifikacije (vidi odjeljak 7.1.2.1)

(4) Polje svrha upotrebe (engl. Key Usage) je označena kao kritično (engl. critical).
(5) Vlasnik može imati jednu važeću identičnu potvrdu, osim u vremenu od šestdeset (60) dana prije isteka važnosti ove potvrde, kada može vlasnik dobiti novu potvrdu.

7.1.2.1 Jedinstveni broj elektronske identifikacije

U skladu s člankom 24. Zakona o elektronskoj identifikaciji i uslugama povjerenja (Službeni list Republike Slovenije, br.121/21 i 189/21 – ZDU-1M), člankom 52. Uredbe o određivanju načina

elektronske identifikacije i korištenju centralnog servisa za online registraciju i elektronski potpis (Službeni list RS, br. 29/22) Jedinstveni broj elektronske identifikacije (EŠEI) imaoca kvalificirane digitalne potvrde za elektronski potpis, elektronski pečat ili autentifikaciju web stranica se zapiše kao zasebno proširenje kvalificirane potvrde.

Ovo posljednje se zapiše kao nezavisno prošireno polje zapisano u ASN.1 notaciji:

SEQUENCE :

OBJECT_IDENTIFIER : '1.3.6.1.4.1.58536.1.1.1.1.1' <OID proširenje za vrijednost EŠEI fizičke osobe>

OCTET_STRING :

IA5String : 'xxxxxxxxxxxx' <vrijednost>

SEQUENCE :

OBJECT_IDENTIFIER : '1.3.6.1.4.1.58536.1.1.1.1.2' <OID proširenje za vrijednost EŠEI poslovnog subjekta>

OCTET_STRING :

IA5String : 'xxxxxxxxxxxx' <vrijednost>

7.1.2.2 Zahtjevi za elektronsku adresu

(1) Halcom CA zadržava pravo da odbije zahtjev za dobivanje potvrde, ako utvrdi da je elektronska adresa:

- neprimjerena tj. uvredljiva,
- obmanjujuća sa treće stranke
- je u suprotnosti sa važećim propisima i standardima.

(2) Ostala ograničenja u vezi elektronskih adresa nisu propisana.

7.1.3 Identifikacijske oznake algoritama

(1) Potvrde koje izdaje Halcom CA su sa strane ponuđača usluga povjerenja potpisani sa algoritmom, određenim u polju signature algorithm: vrijednost »sha256RSA, identifikacijska oznaka: OID 1.2.840.113549.1.1.11.

(2) Cjelokupan skup algoritama, formata podataka i protokola je na raspolaganju kod ovlaštenih lica ponuđača usluga povjerenja Halcom CA.

7.1.4 Oblik prepoznatljivih imena

Vidi odjelj. 3.1.1.

7.1.5 Ograničenja u vezi imena

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

7.1.6 Oznake politike potvrde

Vidi odjelj. 7.1.2.

7.1.7 Ograničenja upotrebe

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

7.1.8 Sintaksa i značenje oznaka politike potvrda

U potvrdama koje izdaje ponuđač usluga povjerenja Halcom CA, koristi se specifični podataka policyQualifiers, koji se obrađuje u skladu sa IETF RFC i ETSI standardom.

7.1.9 Značenje ključnih dodataka politike

Nije podržano.

7.2. Profil registra poništenih potvrda

(1) Registar poništenih potvrda Halcom CA je spisak poništenih potvrda (CRL) i nalazi se u grani:

CN= Halcom CA PO e-signature 2

O = Halcom

C = SI

(2) Registar poništenih potvrda se ažurira nakon svakog poništenja potvrde odnosno najmanje jednom dnevno, ako nema novih zapisa tj. izmjena u registru poništenih potvrda (24 sata nakon zadnjeg ažuriranja).

(3) Registar poništenih potvrda sadrži jedinstven interni serijski broj poništenih potvrda te vrijeme i datum poništenja.

7.2.1 Verzija

(1) Registar poništenih potvrda odgovara preporuci ITU-T za X.509 (2005) i ISO/IEC 95948:2014.

(2) Registar poništenih potvrda je stalno dostupan u javnom imeniku potvrda (vidi odjeljak 2.3.):

- po protokolu LDAP i
- po protokolu HTTP.

7.2.2 Sadržaj registra i proširenje

(1) Registar poništenih potvrda pored ostalih podataka u skladu sa preporukom X.509 sadrži (osnovna polja i proširenja koja su kasnije prikazana u tabeli ispod)::

- identifikacijske oznake poništenih potvrda i
- vrijeme i datum poništenja.

Korijenski (Root) registar poništenih potvrda (CRL ugniježdenih/podređenih tj. intermediate potvrda)

Naziv polja Osnovna polja u CRL	Vrijednost tj. značenje
Verzija, engl. Version	V2
Algoritam za potpis, engl. Signature Algorithm	Sha256RSA
Potpis ponuđača usluga povjerenja, engl. Signature	potpis Halcom CA

Prepoznatljivo ime ponuđača usluga povjerenja, engl. Issuer	CN = Halcom Root Certificate Authority 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Vrijeme izdavanja CRL, engl. thisUpdate	Effective date: <vrijeme izdanja po GMT>
Vrijeme izdavanja CRL, engl. nextUpdate	Next Update: <vrijeme narednog izdanja po GMT>
identifikacijske oznake poništenih potvrda i vrijeme poništenja, engl. revokedCertificate	Serial Number: <identifikacijska oznaka poništene ditigalne potvrde > Revocation Date: <vrijeme poništenja po GMT>
Proširenja X.509v2 CRL	
Broj VRL list Engl. CRL number	Redni broj CRL liste
identifikator ključa poniđača usluga povjerenja, engl. Authority Key Identifier (OID 2.5.29.35)	KeyID=42 ae a6 43 c7 98 28 b0
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

(3) Ugniježdeni/podređeni (Intermediate) registar poništenih potvrda (CRL korisničkih potvrda)

Naziv polja Osnovna polja u CRL	Vrijednost tj. značenje
Verzija, engl. Version	V2
Algoritam za potpis, engl. Signature Algorithm	Sha256RSA
Potpis ponuđača usluga povjerenja, engl. Signature	potpis Halcom CA

Prepoznatljivo ime ponuđača usluga povjerenja, engl. Issuer	CN = Halcom CA FO e-signature 2 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Vrijeme izdavanja CRL, engl. thisUpdate	Effective date: <vrijeme izdavanja po GMT>
Vrijeme sljedećeg izdavanja CRL, engl. nextUpdate	Next Update: <vrijeme sljedećeg izdavanja po GMT>
identifikacijske oznake poništenih potvrda i vrijeme poništenja, engl. revokedCertificate	Serial Number: <identifikacijska oznaka poništene dig. potvrde> Revocation Date: <vrijeme poništenja po GMT>
Proširenja X.509v2 CRL	
Broj VRL list Engl. CRL number	Redni broj CRL liste
identifikator ključa ponuđača usluga povjerenja, engl. Authority Key Identifier (OID 2.5.29.35)	KeyID= 48 c4 27 a6 6f 6e f0 2e
engl. issuerAltName (OID 2.5.28.18)	Ne koristi se
engl. deltaCRLindicator (OID 2.5.29.27)	Ne koristi se
engl. issuingDistribuitionPoint (OID 2.5.29.28)	Ne koristi se

7.2.3 Objava registra poništenih potvrda

Halcom CA objavljuje registar u javnom imeniku na poslužitelju ldap://ldap.halcom.si po protokolu LDAP i http://domina.halcom.si/crls po protokolu HTTP.

7.3. Profil paralelne provjere statusa potvrda

(1) Paralelna provjera statusa digitalnih potvrda je dostupna na adresi http://ocsp.halcom.si

(2) Profil izvještaja OCSP (zahtjev/odgovor) usluge za paralelnu provjeru statusa potvrda je u skladu sa preporukom IETF RFC.

7.3.1 Verzija paralelne provjere statusa

Ponuđač usluga povjerenja Halcom CA koristi izvještaje OCSP verzije 1 u skladu sa preporukom IETF RFC.

7.3.2 Profil paralelne provjere statusa

Izvještaji OCSP (zahtjev/odgovor) usluge za paralelnu provjeru statusa potvrda daju podršku za proširenje Nonce, koja nije označena kao kritična.

8. NADZOR

(1) U Halcom CA radi opunomoćeni za unutrašnji nadzor i sa odgovarajućim tehnološkim i pravnim znanjima koji ne obavlja zadatke u vezi sa upravljanjem potvrda.

(2) Opunomoćeni za unutrašnji nadzor vrši nadzor nad radom Halcoma CA. Opunomoćeni za unutrašnji nadzor u slučaju otkrivenih nedostataka odredi odgovarajuće mjere za otklanjanje tih nedostataka, koje je Halcom CA dužan izvesti, te vrši nadzor nad provođenjem određenih mjera.

(3) Halcom CA je jednom godišnje prolazi kroz vanjsku neovisnu procjenu, koju provodi Akreditirani organ

8.1. Učestalost nadzora

(1) Opunomoćeni za unutrašnji nadzor obavlja nadzor najmanje jednom godišnje.

(2) Opunomoćeni za vanjski nadzor na ISO 9001 i ISO 27001 obavlja nadzor jednom godišnje. Opunomoćeni za vanjski nadzor nad radom u skladu sa ETSI standardima obavlja nadzor jednom u dvije godine.

(3) Svi relevantni ETSI standardi su na raspolaganju na web stranici Halcom CA.

8.2. Vrsta i osposobljenost nadzora

(1) Opunomoćeni za unutrašnji nadzor ima odgovarajuća tehnološka i pravna znanja.

(2) Opunomoćeni za vanjski nadzor ima odgovarajuća tehnološka i pravna znanja.

8.3. Neovisnost nadzora

(1) Opunomoćeni za unutrašnji nadzor ne obavlja zadatke u vezi sa upravljanjem potvrdama.

(2) Opunomoćeni za vanjski nadzor ne obavlja zadatke u vezi sa upravljanjem potvrdama.

8.4. Područja nadzora

Područja nadzora su određena u unutrašnjim pravilima ponuđača usluga povjerenja Halcom CA.

8.5. Mjere ponuđača usluga povjerenja

U slučaju utvrđenih nedostataka ili grešaka opunomoćeni za unutrašnji/vanjski nadzor odredi odgovarajuće mjere za otklanjanje tih nedostataka, koje je Halcom CA dužan provesti, te vrši nadzor nad provođenjem određenih mjera. Detaljno je provođenje mjera određeno u unutrašnjim pravilima ponuđača usluga povjerenja Halcom CA.

8.6. Objava rezultata nadzora

Rezultati provođenja nadzora se čuvaju kod ponuđača usluga povjerenja Halcom CA.

9. FINANSIJSKI I OSTALI PRAVNI POSLOVI

9.1. Cjenovnik

Halcom CA odredi cjenovnik korištenja potvrda, svojih usluga, potrebne opreme i infrastrukture te cjenik objavljuje na svojim web stranicama.

9.1.1 Cijena izdavanja potvrda i produženja
Cijena izdavanja potvrda i produženje je određeno sa važećim cjenovnikom.

9.1.2 Cijena pristupa do potvrde
Pristup do javnog vlasnika potvrda je besplatan, osim ako se stranke ne dogovore drugačije.

9.1.3 Cijena pristupa statusima potvrda i registra poništenih potvrda
Registar poništenih potvrda je besplatan i dostupan svim licima.

9.1.4 Cijene drugih usluga
Cijene drugih usluga, opreme i infrastrukture su određene sa važećim cjenovnikom.

9.1.5 Povrat troškova
Nije propisano.

9.2. Finansijska odgovornost

9.2.1 Pokriće osiguranja
Halcom CA ima na odgovarajući način osiguranu svoju odgovornost. Detaljnije informacije su objavljene na web stranicama.

9.2.2 Ostalo pokriće
Nije propisano.

9.2.3 Osiguranje vlasnika
Nije propisano.

9.3. Zaštita poslovnih podataka

9.3.1 Zaštićeni podaci
(1) Ponuđač usluga povjerenja Halcom CA postupa sa povjerenjem prema sljedećim podacima:

- Sa svim zahtjevima za dobivanje potvrde ili druge usluge
- Sve moguće povjerljive podatke u vezi sa finansijskim obavezama
- Sve moguće povjerljive podatke koji su predmet međusobnog ugovora sa trećim licima te
- Svi ostali poslovi koji su u skladu sa Uredbom zavede u unutrašnjim pravilima rada ponuđača usluga povjerenja Halcom CA.

(2) Sa svim mogućim povjerljivim podacima o poslovnim subjektima, vlasnicima i trećim licima, koji su neophodno potrebno za usluge upravljanja sa potvrdama, ponuđač usluga povjerenja Halcom CA postupa u skladu sa važećim zakonodavstvom.

9.3.2 Nezaštićeni podaci
Ponuđač usluga povjerenja Halcom CA javno objavljuje samo takve poslovne podatke koji u skladu sa važećim zakonodavstvom nisu povjerljive prirode (lični podaci poslovne tajne i slično).

9.3.3 Odgovornost u vezi zaštite
(1) Halcom CA ne preuzima nikakvu odgovornost za sadržaj podataka, koje je vlasnik potvrde elektronski šifrirao ili potpisao, također i u slučaju da je vlasnik ili treće lice poštovao sve važeće propise, sve odredbe ove politike i drugih pravila Halcom CA odnosno poštivao sve njegove upute.

(2) Halcom CA ne preuzima nikakvu odgovornost za posljedice, koji nastaju jer vlasnik potvrde nije postupak u skladu sa sigurnosnim zahtjevima iz tačke 4.5.1. ove politike.

9.4. Zaštita ličnih podataka

9.4.1 Plan zaštite ličnih podataka

Halcom CA pažljivo čuva lične podatke u skladu sa evropskim i slovenskim važećim propisima, međunarodnim standardima i preporukama, provodi redovne pismene procjene učinaka te osigurava ugrađenu i prema zadatim postavkama privatnost. Kod Halcoma d.d. djeluje opunomoćeni za privatnost kao službena osoba za zaštitu podatka.

9.4.2 Zaštićeni lični podaci

Zaštićeni podaci su svi osobni podaci koje ponuđač usluga povjerenja Halcom CA dobija na zahtjev za svoju uslugu ili u odgovarajućim registrima za dokazivanje identiteta vlasnika ili tokom provođenja usluge povjerenja.
Podaci u potvrdama i registru poništenih potvrda su zbog prirode korištenja potvrda i odredbi važećih propisa i standarda dostupni trećim licima, koji se oslanjaju na potvrde ili provjeravaju njihovu važnost.

9.4.3 Nezaštićeni lični podaci

Ostalih mogućih nezaštićenih ličnih podataka, osim onih koji su navedeni u potvrdi i registru poništenih potvrda nema.

9.4.4 Odgovornost u vezi zaštite ličnih podataka

Ponuđač usluga povjerenja Halcom CA je za zaštitu podataka odgovaran u skladu sa važećim propisima o zaštiti podataka i odredbi internog Pravilnika o zaštiti podataka.

9.4.5 Punomoć u vezi korištenja ličnih podataka

Vlasnik punomoći ponuđača usluga povjerenja Halcom CA za korištenje ličnih podataka na zahtjevu za dobivanje potvrde, posebno pismeno da suglasnost za obradu ličnih podataka ili za druge slučajeve kasnije u drugom pismenom obliku

9.4.6 Posredovanje ličnih podataka

(1) Ponuđač usluga povjerenja Halcom CA ne posreduje druge podatke o vlasnicima potvrda, koji nisu navedeni u potvrdi, osim ako se određeni podaci posebno zahtijevaju za provođenje specifičnih usluga tj. aplikacija, povezanih sa potvrdama, te je ponuđača usluga povjerenja Halcom CA vlasnik punomoći za to (vidi prijašnji odjeljak), ili na zahtjev nadležnog suda, prekršajnog, organa progona, upravnog organa ili druge ovlaštene osobe. Svaki takav zahtjev Halcom CA pažljivo provjeri te posreduje podatke samo u neophodnom opsegu, određenom sa važećim propisima.

(2) Podaci se posreduju bez pismene suglasnosti samo u slučajevima ako tako određuju važeći evropski ili slovenski propisi sa zakonskom snagom.

9.4.7 Druge odredbe u vezi zaštite ličnih podataka

Nije propisano.

9.5. Odredbe u vezi prava intelektualnog vlasništva

Odredbe u vezi autorskih, srodnih i drugih prava intelektualnog vlasništva:

- Na privatnom ključu pripadaju sva prava poslovnom subjektu tj. vlasniku potvrde,
- Na javnim ključevima, svih podataka na potvrdi, na imeniku potvrda i registru poništenih potvrda te na ovoj politici pripadaju sva prava Halcom CA.

9.6. Obaveze i odgovornosti

9.6.1 Obaveze i odgovornosti ponuđača usluga povjerenja Halcom CA

(1) Ponuđač usluga povjerenja Halcom CA je dužan:

- Djelovati u skladu sa svojim unutrašnjim pravilima i ostalim važećim propisima i zakonodavstvom,
- Djelovati u skladu sa međunarodnim preporukama,
- Objavljivati sve važne dokumente, koji određuju njegovo djelovanje (politike djelovanja, zahtjeve, cjenik, upute za sigurno korištenje kvalificiranih digitalnih potvrda i sl.)
- Objavljivati na svojim web stranicama sve informacije o onim izmjenama u vezi djelatnosti ponuđača usluga povjerenja, koji bilo kada utiču na vlasnike potvrda i treća lica,
- Osigurati djelovanje prijavnih službi u skladu sa odredbama HALCOM CA i ostalim važećim propisima,
- Poštovati odredbe u vezi sigurnog postupanja sa ličnim, poslovnim i povjerljivim podacima o ponuđaču usluga povjerenja, vlasnika potvrda ili trećih lica,
- Poništiti potvrdu i objaviti poništenu potvrdu u registru poništenih potvrda, kada utvrdi da su dati razlozi po ovoj politici ili drugim važećim propisima,
- Izdati kvalificirane digitalne potvrde u skladu sa ovom politikom i ostalim propisima te preporukama.

(2) Ponuđač usluga povjerenja Halcom CA je dužan:

- Osigurati pravilnost podataka izdatih potvrda,
- Osigurati pravilnost objave registra poništenih potvrda,
- Osigurati jedinstvenost prepoznatljivih imena,
- Osigurati primjerenu fizičku sigurnost prostora i pristupa do samih prostora ponuđača usluga povjerenja,
- Kao dobar gospodar brinuti za nesmetano djelovanje i što veću raspoloživost usluga,
- Kao dobar gospodar brinuti za što veću dostupnost usluga,
- Kao dobar gospodar brinuti za nesmetan rad svih ostalih pratećih usluga,
- Pokušati otkloniti nastale probleme u najvećoj moći i u najkraćem vremenu,
- Brinuti za optimizaciju hardverske i softverske opreme i
- Obavještavati korisnike o važnim stvarima te
- Ispunjavati sve druge zahtjeve u skladu sa ovom politikom.

(3) Ponuđač usluga povjerenja Halcom CA osigurava što veću dostupnost svojih usluga, i to sve dane u godini, pri čemu se ne uzimaju u obzir sljedeći slučajevi:

- Planirane i unaprijed najavljene tehničke ili servisne zahvate na infrastrukturi,
- Neplanirane tehničke ili servisne zahtjeve na infrastrukturi kao posljedica nepredviđenih kvarova
- Tehničke i servisne zahvate zbog kvara infrastrukture van nadležnosti ponuđača usluga povjerenja Halcom CA i
- Nedostupnosti kao posljedica više sile ili vanrednih događaja.

(4) Održavanje ili ažuriranje infrastrukture mora ponuđač usluga povjerenja Halcom CA najaviti bar tri (3) dana prije početka poslova.

(5) Ponuđač usluga povjerenja Halcom CA je odgovoran za sve navode u ovom dokumentu i za provođenje svih odredbi iz ove politike.

(6) Ostale obaveze tj. odgovornosti ponuđača usluga povjerenja Halcom CA su određene sa mogućim međusobnim dogovorom sa trećim licem.

9.6.2 Obaveze i odgovornosti prijavne službe

(1) Prijavna služba je dužna:

- Provjeravati identitet vlasnika tj. budućih vlasnika
- Primati zahtjeve za usluge Halcom CA,
- Provjeravati zahtjeve,
- Izdavati potrebnu dokumentaciju poslovnim subjektima, vlasnicima tj. budućim vlasnicima,
- Posredovati zahtjeve i ostale podatke na siguran način na Halcom CA.

(2) Prijavna služba je odgovorna za provođenje svih odredbi iz ove politike i drugih zahtjeva koje dogovaraju sa ponuđačem usluga povjerenja Halcom CA.

9.6.3 Obaveze i odgovornost vlasnika potvrda

(1) Vlasnik potvrde odgovara za:

- Nastalu štetu u slučaju zloupotrebe potvrde od prijave poništenja do poništenja,
- Svaku štetu, koja je ili posredno ili neposredno prouzrokovana zato jer je bila omogućeno korištenje tj. zloupotreba vlasnikove potvrde od strane neovlaštenog lica,
- Svaku drugu štetu koja slijedi iz nepoštivanja odredbi ove politike i drugih obavijesti Halcom CA te važećih propisa.

(2) Obaveze vlasnika su u vezi korištenja potvrda određene u odjelj. 4.5.1.

9.6.4 Obaveze i odgovornosti trećih lica

(1) Pri prvom korištenju potvrde Halcom CA po ovoj politici mora treće lice koji se pouzda u potvrdu, pažljivo pročitati ovu politiku i od tada redovno prati sve obavijesti Halcom Ca.

(2) Treće lice mora uvijek u vrijeme korištenja potvrde tačno provjeriti da li je potvrda u registru poništenih potvrda.

(3) Ako bi potvrda sadržavala podatke o trećem licu, isto je dužno zahtijevati poništenje potvrde ako sazna da je bio osobni ključ ugrožen na način koji utiče na pouzdanost korištenja, ili ako postoji opasnost zloupotrebe, ili ako su se promijenili podaci koji su navedeni u potvrdi.

(4) Treće lice može do poništenja potvrde da se pouzda na takvu potvrdu.

(5) Treće lice može bilo kada zahtijevati sve informacije u vezi važenja bilo koje izdate potvrde, u vezi odredbi ove politike te u vezi obavijesti Halcom CA.

9.6.5 Obaveze i odgovornosti drugih lica

Nije propisano.

9.7. Ograničenje odgovornosti

Ponuđač usluga povjerenja Halcom CA nije odgovoran za štetu koja bi nastala zbog:

- Korištenje potvrda za svrhu i na način koji nije izričito predviđen u ovoj politici,
- Nepravilno ili nedovoljno čuvanje šifara ili privatnih ključeva vlasnika, izdanja povjerljivih podataka ili ključeva trećim licima i neodgovornog postupanja vlasnika
- Zloupotrebe tj. provale u informacijski sistem vlasnika potvrde odnosno do podataka o potvrdama od strane neovlaštenih lica
- Nefunkcionisanje ili loše funkcionisanje informacijske infrastrukture vlasnika potvrde ili trećih lica,
- Neprovjeravanja podataka i važnosti potvrda u registru poništenih potvrda,
- Neprovjeravanje vremena važnosti potvrde,
- Postupanje vlasnika potvrde ili trećeg lica u suprotnosti sa obavještenjem Halcom CA, politikom i drugim propisima,

- Omogućenog korištenja tj. zloupotrebe vlasničke potvrde neovlaštenim licima,
- Izdate potvrde sa pogrešnim podacima i nevjerodostojnim podacima ili drugim aktivnostima vlasnika ili ponuđača usluga povjerenja,
- Korištenje potvrda te važenje potvrda pri promjenama podataka iz potvrde, elektronskih adresa ili izmjena imena vlasnika,
- Ispada infrastrukture koja nije u domenu upravljanja ponuđača usluga povjerenja Halcom CA,
- Podataka koji se šifriraju ili potpisuju sa korištenjem potvrda,
- Postupanje vlasnika pri korištenju potvrda i to u slučaju da je vlasnik ili treće lice poštovao sve odredbe ove politike, obavještenja Halcom CA ili druge važeće propise,
- Korištenje i pouzdanost rada hardvera i softvera vlasnika potvrde.
- Grešaka pri izračunu hash vrijednosti (engl. hash value), provjeravanju te vrijednosti ili drugih sigurnosnih postupaka u vezi elektronskog dokumenta, koji se potpisuje, ako je vlasnih zahtijevao potpis u oblaku samo na osnovu hash vrijednosti i bez prilaganja cjelokupnog elektronskog dokumenta ponuđaču usluga povjerenja Halcom CA.

9.8. Ograničenja u vezi korištenja

Nije propisano

9.9. Podmirenje štete

Za štetu odgovara stranka koja istu prouzrokuje zbog nepoštivanja odredbi iz ove politike i važećeg zakonodavstva.

9.10. Važnost politike

(1) Halcom CA zadržava pravo na izmjene politike djelovanja i nadgradnje infrastrukture bez prethodnog obavještavanja vlasnika potvrda. Važeće potvrde pri tome ostaju u važnosti do kraja isteka važnosti i za njih još i dalje vrijedi ona politika djelovanja, koja je vrijedila pri njihovom izdavanju. Sve potvrde izdate na početku važnosti nove politike, vrijedi nova politika

(2) Ova politika počinje da važi sa danom kada je usvoji Halcom CA.

9.10.1 Vrijeme važnosti

(1) Nova verzija tj. izmjene politike ponuđača usluge povjerenja Halcom CA se osam (8) dana prije važenja prethodno objavi na web stranicama ponuđača usluga povjerenja Halcom CA, pod novim identifikacijskim brojem (CPOID) i označenim datumom početka njene važnosti.

(2) Kraj važnosti politike nije određen i povezan sa važenjem potvrda, izdatih na osnovu politike.

9.10.2 Kraj važenja politike

(1) Pri objavi nove politike ostaju za sve potvrde, izdate na osnovu ove politike, u važnosti one odredbe koje se smisleno ne moraju nadoknaditi sa odgovarajućim odredbama po novoj politici (na primjer postupak koji određuje način po kojem je bila ova potvrda izdata i sl.).

(2) Ponuđač usluga povjerenja može za pojedine odredbe važeće politike izdati dopune, kako je to određeno u odjeljku 9.12.

9.10.3 Dejstvo isteka važenja politike

(1) Pri izdavanju nove politike se sve kvalificirane digitalne potvrde izdate nakon tog datuma obrađuju po novoj politici.

(2) Nova politika ne utiče na važnost potvrda koje su izdate prema prethodnim politikama. Takve potvrde ostaju u važnosti do kraja isteka važnosti, pri čemu se, gdje je to moguće, obrađuju po novoj politici.

9.11. Komuniciranje među subjektima

(1) Kontakt podaci ponuđača usluga povjerenja su objavljeni na web stranicama i dati u odjelj 1.3.1.

(2) Kontakt podaci vlasnika su dati u zahtjevima u vezi sa potvrdama.

(3) Kontakt podaci trećih lica su dati u mogućem međusobnom dogovoru između trećeg lica i ponuđača usluga povjerenja Halcom CA.

9.12. Izmjene i dopune

9.12.1 Postupak za prijem izmjena i dopuna

(1) Izmjene i dopune ove politike može ponuđač usluga povjerenja objaviti u obliku izmjena i dopuna ovoj politici, kada se ne radi o ključnim izmjenama u radu ponuđača usluga povjerenja.

(2) Dopune usvajaju po jednakom postupku kao i politika.

(3) Ako izmjene i dopune bitno utiču na rad ponuđača usluga povjerenja, o tome se obavijesti nadležno ministarstvo po jednakom postupku kako to vrijedi za politiku.

(4) Način za označavanje dopuna odredi ponuđač usluga povjerenja Halcom CA

9.12.2 Važenje i objava izmjena i dopuna

(1) Ponuđač usluga povjerenja Halcom CA odredi početak i kraj važenja izmjena i dopuna.

(2) Izmjene i dopune se osam (8) dana prije početka važenja objave na web stranama Halcom CA.

9.12.3 Izmjena identifikacijskog broja politike

Ako usvojene izmjene i dopune utiču na korištenje potvrda, može ponuđač usluga povjerenja Halcom CA odredi novu identifikacijsku oznaku politike (CP_{OID}) tj. izmjena i dopuna.

9.13. Postupak u slučaju sporova

(1) Sve žalbe vlasnika potvrda rješava opunomoćeni za privatnost i regulatornu usklađenost

(2) Moguće sporove između vlasnika potvrda ili treće osobe i Halcoma CA rješava stvarno nadležan sud u Ljubljani.

9.14. Važeće zakonodavstvo

Za odlučivanje o ovoj politici koristi se pravo Evropske unije i Republike Slovenije.

9.15. Usklađenost sa važećim zakonodavstvom

(1) Nadzor nad usklađenosti rada ponuđača usluga povjerenja Halcom CA sa važećim propisima provodi nadležni inspektorat i akreditirani organi za utvrđivanje usklađenosti.

(2) Akreditiran organ za utvrđivanje usklađenosti ponuđača usluga povjerenja Halcom CA revidira najmanje svaka 24 mjeseca. Svrha revizije je da potvrdi da li ponuđač kvalificiranih usluga povjerenja i kvalificirane usluga povjerenja, koje osigurava, ispunjava zakonske zahtjeve.

(3) Unutrašnju provjeru usklađenosti rada provode ovlaštena lica u okviru ponuđača usluga povjerenja Halcom CA.

9.16. Opšte odredbe

(1) Sa ostalim subjektima ponuđač usluga povjerenja Halcom CA može sklopiti međusobne dogovore, ako to određuje važeće zakonodavstvo tj. drugi propisi.

(2) Ako bilo koja od odredbi ove politike jeste ili postaje nevažeća, to ne utiče na ostale odredbe. Nevažeće odredbe se nadomjeste sa važećom, koja mora što više odgovaraju namjeni koju je željela postići nevažeća odredba.

9.17. Ostale odredbe

Nisu propisane.

Mjesto i datum:

Gravni izvršni direktor:

Tomi Šefman

Ljubljana, 26.5.2023.