FINA

PRAVILNIK O POSTUPCIMA CERTIFICIRANJA ZA NEKVALIFICIRANE CERTIFIKATE

Verzija 1.2

Datum stupanja na snagu: 12.09.2018.

OID Dokumenta: 1.3.124.1104.5.0.4.2.1.2

Informacije o dokumentu

Ime dokumenta:	Pravilnik o postupcima certificiranja za nekvalificirane certifikate
OID dokumenta:	1.3.124.1104.5.0.4.2.1.2
Tip dokumenta:	Pravilnik o postupcima certificiranja (*Certification Practice Statement*, CPS)
Oznaka distribucije	Javno
Vlasnik dokumenta	Financijska agencija, Fina
Kontakt	pma@fina.hr

Povijest izmjena

Verzija	Datum	Razlog izmjene
1.0	22.05.2017.	Inicijalna verzija
1.1	19.04.2018.	Ažuriranje referente liste zakonske regulative, proširenje primjerene uporabe certifikata u točkama 1.4.1.2. i 1.4.1.4., dopuna postupka registracije korisnika u točki 3.2.2., izmjene u načinima dostave zahtjeva za opoziv, suspenziju i reaktivaciju certifikata u točkama 3.4., 4.9.3. i 4.9.15., dopuna razloga za opoziv certifikata u točki 4.9.1. te ispravljanje prepoznatih grešaka.
1.2	11.09.2018.	Ažuriranje referente liste zakonske regulative, dodavanje izjave o usklađenosti strukture dokumenta s RFC 3647, dodavanje SHA-256 *fingerprint*-a CA certifikata, dopuna odredbi vezanih uz prestanak pružanja usluga povjerenja, poboljšanja u postupcima prihvaćanja certifikata, reduciranje potrebnih podataka koji se prikupljaju prilikom opoziva certifikata, dodavanje izjave o postupcima vezanim za upravljanje kritičnim ranjivostima, dodavanje izjave o obavljanju opoziva i suspenzije certifikata bez obzira na status naplate i dodavanje izjave o dostupnosti usluga osobama s invaliditetom.

SADRŽAJ

AUTORSKA PRAVA

REFERENTNE DOKUMENTIRANE INFORMACIJE

Temeljni zakon

[1] Uredba (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ

[2] Zakon o provedbi Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ (NN 62/2017)

Podzakonski akti

[3] Provedbena uredba komisije (EU) 2015/1505 od 8. rujna 2015. o utvrđivanju tehničkih specifikacija i formata koji se odnose na pouzdane popise u skladu s člankom 22. stavkom 5. Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu

[4] Provedbena uredba komisije (EU) 2016/650 od 25. travnja 2016. utvrđivanju normi za ocjenu sigurnosti kvalificiranih sredstava za izradu potpisa i pečata u skladu s člankom 30. stavkom 3. i člankom 39. stavkom 2. Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu

Ostali zakoni

[5] Zakon o provedbi Opće uredbe o zaštiti podataka (NN 42/2018)

Normizacijski dokumenti

[6] ISO/IEC 27001:2013 – Information technology – Security techinques – Information security management

[7] ISO/IEC 27002:2013 – Information technology – Security techinques – Code of practice for information security management

[8] ETSI EN 319 401 V2.1.1. (2016-02) – Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

[9] ETSI EN 319 411-1 V1.1.1. (2016-02) – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements

[10] ETSI EN 319 412-1 V1.1.1. (2016-02) – Electronic Signatures and Infrastructures (ESI);Certificate Profiles; Part 1: Overview and common data structures

[11] ETSI EN 319 412-2 V2.1.1. (2016-02) – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons

[12] ETSI EN 319 412-3 V1.1.1. (2016-02) – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons

[13] ETSI EN 319 403 V 2.2.2 (2015-08) - Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers

[14] ETSI TS 119 312 – Electronic Signatures and Infrastructures (ESI); Cryptographic Suites

[15] HRN EN 419 211-1:2014 – Obrasci zaštite sredstava za izradu elektroničkog potpisa – 1. dio: Pregled (EN 419211-1:2014); Protection profiles for secure signature creation device – Part 1: Overview (EN 419211-1:2014)

[16] HRN EN 419 211-2:2013 – Obrasci zaštite sredstava za izradu elektroničkog potpisa – 2. dio: Sredstvo za generiranje ključa (EN 419211-1:2013); Protection profiles for secure signature creation device – Part 2: Device with key generation (EN 419211-2:2013)

[17] HRN EN 419 211-4:2013 – Obrasci zaštite sredstava za izradu elektroničkog potpisa – 4. dio: Dodatna zaštita sredstava za generiranje ključa i povjerljivi kanal do aplikacije za generiranje certifikata (EN 419211-4:2013); Protection profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted channel to certificate generation application (EN 419211-4:2013)

[18] HRN EN 419 211-5:2013 – Obrasci zaštite sredstava za izradu elektroničkog potpisa – 5. dio: Dodatna zaštita sredstava za generiranje ključa i povjerljivi kanal do aplikacije za izradu elektroničkog potpisa (EN 419211-5:2013); Protection profiles for secure signature creation device – Part 5: Extension for device with key generation and trusted channel to signature creation application (EN 419211-5:2013)

[19] NIST FIPS PUB 140-2 (2001) – Security Requirements for Cryptographic Modules

[20] IETF RFC 3647 – Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework

[21] IETF RFC 5280 (2008) – Internet X.509 Public Key Infrastructure; Certificate and Certificate Revocation List (CRL) Profile

[22] IETF RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP (2013)

[23] HRN ISO/IEC 9594-8:2015 - Informacijska tehnologija – Međusobno povezivanje otvorenih sustava – Imenik – 8. dio: Okviri certifikata javnog ključa i atributnog certifikata (ISO/IEC 9594-8:2014); Information technology – Open

Systems Interconnection – The Directory – Part 8: Public-key and attribute certificate frameworks (ISO/IEC 9594-8:2014)

[24] CA/Browser Forum - Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates

Finini dokumenti

[25] Opća pravila pružanja usluga certificiranja i Pravilnik o postupcima certificiranja za Fina Root CA, CP/CPS_{ROOT}

[26] Opća pravila pružanja usluga certificiranja za nekvalificirane certifikate, $CP_{NQC\text{-}eIDAS}$

[27] Pravilnik o postupcima certificiranja za certifikate za autentikaciju mrežnih stranica, $CPS_{WSA\text{-}eIDAS}$

1 UVOD

Kao treća strana od povjerenja, Fina svoje usluge certificiranja pruža od 2003. godine. Usluge povjerenja koje pruža Fina usklađene su sa zakonskom regulativom [1] – [5] te s mjerodavnim međunarodnim normama iz djelokruga pružanja usluga povjerenja. Fina neprekidno prati potrebe korisnika, razvoj tehnologije i promjene u normama iz područja pružanja usluga povjerenja te sukladno tome unapređuje i usklađuje svoj PKI sustav kako bi svoje proizvode i usluge prilagodila zahtjevima za prekograničnu interoperabilnost.

1.1 Pregled

Fina PKI je PKI infrastruktura uspostavljena u Fini kojom Fina pruža usluge povjerenja, a koje se odnose na izdavanje i upravljanje životnom ciklusom produkcijskih certifikata (u daljnjem tekstu: usluge certificiranja) i izdavanje elektroničkih vremenskih žigova.

Hijerarhijska struktura Fina PKI zasnovana je na Fina Root CA te se temelji na dvorazinskoj arhitekturi produkcijskih certifikacijskih tijela (engl.: *Certification Authorities,* u daljem tekstu: CA ili CA-ovi).

Dvorazinsku arhitekturu produkcijskih certifikacijskih tijela Fine čine:

- korijensko certifikacijsko tijelo (root CA): Fina Root CA
- dva subordinirana certifikacijska tijela:
    - Fina RDC 2015,
    - Fina RDC-TDU 2015.

Fina Root CA je izdao samopotpisani Fina Root CA certifikat te je certifikate izdao njemu subordiniranim Fina RDC 2015 i Fina RDC-TDU 2015 CA-ovima.

Opća pravila i postupci certificiranja koja se odnose na Fina Root CA i Fina PKI hijerarhiju zasnovanu na Fina Root CA opisana su u dokumentu Opća pravila pružanja usluga certificiranja i Pravilnik o postupcima certificiranja za Fina Root CA [25].

Fina RDC 2015 i Fina RDC-TDU 2015 su CA-ovi koji izdaju certifikate za krajnje korisnike (u daljnjem tekstu: korisnički certifikati).

1.1.1 Opseg i namjena

Ovaj Pravilnik o postupcima certificiranja za nekvalificirane certifikate (engl. C*ertification Practice Statement for Non-Qualified Certificates*, u daljnjem tekstu: $CPS_{NQC\text{-}eIDAS}$) opisuje postupke i procedure koje primjenjuje Fina PKI na izdavanje i upravljanje životnim ciklusom produkcijskih digitalnih certifikata koji se ne smatraju kvalificiranim u smislu Uredbe (EU) br. 910/2014 [1] (u daljnjem tekstu: nekvalificirani certifikati ili certifikati), a sukladno zahtjevima iz Općih pravila pružanja usluga certificiranja za nekvalificirane certifikate (u daljnjem tekstu: Opća pravila) [26].

Opseg ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta su usluge povjerenja koje pruža Fina, a koje se odnose na izdavanje i upravljanje životnom ciklusom produkcijskih nekvalificiranih certifikata koji se izdaju kao softverski certifikati čiji je privatni ključ zaštićen softverskim tokenom, kao certifikati na sigurnim kriptografskim ili QSCD uređajima i certifikati koji se izdaju za korištenje u HSM modulima.

Produkcijski certifikati iz opsega ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta sastavni su dio Registra digitalnih certifikata (Fina RDC), a koji se sastoji od dva certifikacijska tijela (CA) iz opsega ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta: Fina RDC 2015 i Fina RDC-TDU 2015. U daljem tekstu, gdje je to primjenjivo, radi jednostavnosti Fina RDC 2015 i Fina RDC-TDU 2015 označavaju se zajedničkim nazivom subordinirani Fina CA-ovi ili samo Fina CA-ovi.

Ovaj $CPS_{NQC\text{-}eIDAS}$ dokument usklađen je s dokumentom Opća pravila [26], a koji je objavljen na internetskim stranicama http://www.fina.hr/finadigicert.

Namjena ovog dokumenta je definiranje postupaka iz područja određenog opsegom ovog dokumenta, a koje provode sudionici Fina PKI navedeni u točki 1.3. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

Struktura ovog dokumenta temelji se na normizacijskom dokumentu IETF RFC 3647 [20].

1.1.2 Tipovi certifikata

Fina kao pružatelj usluga povjerenja izdaje tipove nekvalificiranih certifikata koji su sljedećim tablicama prikazani po svojim grupama i Fininim razinama sigurnosti. U tablicama su za svaki tip certifikata navedeni i pripadajući Finini te ETSI OID-ovi općih pravila certificiranja (u daljnjem tekstu: CP OID). Tablica 1.1. prikazuje grupe i tipove nekvalificiranih certifikata koje izdaje Fina RDC 2015 CA, a Tablica 1.2. prikazuje grupu i tip nekvalificiranog certifikata koje izdaje Fina RDC-TDU 2015 CA.

Nekvalificirani certifikati koje izdaje Fina RDC 2015 CA			
Naziv grupe certifikata	**Naziv tipa certifikata**	**Finin i ETSI CP OID**	**Razina sigurnosti**
Fina RDC 2015 osobni certifikati	Osobni autentikacijski certifikat (NCP+)	Fina CP OID: 1.3.124.1104.5.12.11.4.2 ETSI CP OID: 0.4.0.2042.1.2	Srednja
	Osobni soft certifikat (NCP)	Fina CP OID: 1.3.124.1104.5.12.11.3.1 ETSI CP OID: 0.4.0.2042.1.1	Standardna
Fina RDC 2015 poslovni certifikati	Poslovni autentikacijski certifikat (NCP+)	Fina CP OID: 1.3.124.1104.5.12.12.4.2 ETSI CP OID: 0.4.0.2042.1.2	Srednja
	Poslovni soft certifikat (NCP)	Fina CP OID: 1.3.124.1104.5.12.12.3.1 ETSI CP OID: 0.4.0.2042.1.1	Standardna
	Poslovni soft certifikat (LCP)	Fina CP OID: 1.3.124.1104.5.12.12.5.1 ETSI CP OID: 0.4.0.2042.1.3	Standardna
Fina RDC 2015 poslovni certifikati za IT opremu	Aplikacijski certifikat razine 1 (NCP)	Fina CP OID: 1.3.124.1104.5.12.15.3.1 ETSI CP OID: 0.4.0.2042.1.1	Standardna

Nekvalificirani certifikati koje izdaje Fina RDC 2015 CA			
	Aplikacijski certifikat razine 2 (NCP)	Fina CP OID: 1.3.124.1104.5.12.15.3.2 ETSI CP OID: 0.4.0.2042.1.1	Srednja
	Aplikacijski certifikat razine 2 (NCP+)	Fina CP OID: 1.3.124.1104.5.12.15.4.2 ETSI CP OID: 0.4.0.2042.1.2	Srednja
	Aplikacijski certifikat razine 3 (NCP+)	Fina CP OID: 1.3.124.1104.5.12.15.4.3 ETSI CP OID: 0.4.0.2042.1.2	Visoka
Certifikat za e-pečat Trusted liste	Certifikat za e-pečat *Trusted* liste (NCP+)	Fina CP OID: 1.3.124.1104.5.12.17.4.2 ETSI CP OID: 0.4.0.2042.1.2	Srednja
Fina RDC 2015 administrativni certifikati	Administrativni certifikat (NCP+)	Fina CP OID: 1.3.124.1104.5.12.16.4.2 ETSI CP OID: 0.4.0.2042.1.2	N/A

Tablica 1.1. Grupe i tipovi nekvalificiranih certifikata koje izdaje Fina RDC 2015

Nekvalificirani certifikati koje izdaje Fina RDC-TDU 2015 CA			
Naziv grupe certifikata	**Naziv tipa certifikata**	**Finin i ETSI CP OID**	
Fina RDC-TDU 2015 certifikati	TDU autentikacijski certifikat (NCP+)	Fina CP OID: 1.3.124.1104.5.22.12.4.2 ETSI CP OID: 0.4.0.2042.1.2	Srednja

Tablica 1.2. Grupe i tipovi nekvalificiranih certifikata koje izdaje Fina RDC-TDU 2015

1.1.2.1 Fina RDC 2015 osobni certifikati

Fina RDC 2015 osobni certifikati namijenjeni su Fizičkim osobama – građanima. Fina RDC 2015 CA izdaje sljedeće tipove osobnih nekvalificiranih certifikata:

- ***Osobni autentikacijski certifikat (NCP+)*** – Osobni autentikacijski certifikat srednje razine sigurnosti čiji se pripadajući privatni ključ čuva u sigurnom kriptografskom uređaju ili QSCD uređaju, sukladno točki 6.2.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta. Ovaj tip certifikata sukladan je s „NCP+“ općim pravilima za certifikate iz norme ETSI EN 319 411-1.
- ***Osobni soft certifikat (NCP)*** – Osobni autentikacijski certifikat standardne razine sigurnosti čiji se pripadajući privatni ključ čuva u softverskom zaštićenom tokenu, sukladno točki 6.2.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta. Ovaj tip certifikata sukladan je s „NCP“ općim pravilima za certifikate iz norme ETSI EN 319 411-1.

1.1.2.2 Fina RDC 2015 poslovni certifikati

Fina RDC 2015 poslovni certifikati namijenjeni su za poslovnu uporabu, a izdaju se fizičkim osobama povezanim s poslovnim subjektom (u daljnjem tekstu: Pripadajuća osoba).

Fina RDC 2015 poslovni certifikati ne izdaju se tijelima državne uprave, već certifikate za tijela državne uprave Fina izdaje na zasebnom Fina RDC-TDU 2015 CA sukladno točki 1.1.2.6. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

Fina RDC 2015 CA izdaje sljedeće tipove poslovnih certifikata:

- ***Poslovni autentikacijski certifikat (NCP+)*** – Poslovni autentikacijski certifikat srednje razine sigurnosti čiji se pripadajući privatni ključ čuva u sigurnom kriptografskom uređaju ili QSCD uređaju, sukladno točki 6.2.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta. Ovaj tip certifikata sukladan je s „NCP+“ općim pravilima za certifikate iz norme ETSI EN 319 411-1.
- ***Poslovni soft certifikat (NCP)*** – Poslovni autentikacijski certifikat standardne razine sigurnosti čiji se pripadajući privatni ključ čuva u softverskom zaštićenom tokenu, sukladno točki 6.2.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta. Ovaj tip certifikata sukladan je s „NCP“ općim pravilima za certifikate iz norme ETSI EN 319 411-1.
- ***Poslovni soft certifikat (LCP)*** – Poslovni autentikacijski certifikat za e-potpis, srednje razine sigurnosti čiji se pripadajući privatni ključ čuva u softverskom zaštićenom tokenu, sukladno točki 6.2.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta. Ovaj tip certifikata sukladan je s „LCP“ općim pravilima za certifikate iz norme ETSI EN 319 411-1.

1.1.2.3 Fina RDC 2015 poslovni certifikati za IT opremu

Fina RDC 2015 poslovni certifikati za IT opremu izdaju se za IT sustave, aplikacije ili servise povezane s poslovnim subjektom. Certifikati za autentikaciju mrežnih stranica ne smatraju se poslovnim certifikatima za IT opremu iz opsega ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta. Fina RDC 2015 CA izdaje sljedeći tipovi poslovnih certifikati za IT opremu:

- ***Aplikacijski certifikat razine 1 (NCP)*** – Certifikat standardne razine sigurnosti čiji se pripadajući privatni ključ čuva u softverskom zaštićenom tokenu, sukladno točki 6.2.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta. Ovaj tip certifikata sukladan je s „NCP“ općim pravilima za certifikate iz norme ETSI EN 319 411-1.
- ***Aplikacijski certifikat razine 2 (NCP)*** – Certifikat srednje razine sigurnosti čiji se pripadajući privatni ključ čuva u softverskom zaštićenom tokenu, sukladno točki 6.2.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta. Ovaj tip certifikata sukladan je s „NCP“ općim pravilima za certifikate iz norme ETSI EN 319 411-1.
- ***Aplikacijski certifikat razine 2 (NCP+)*** – Certifikat srednje razine sigurnosti čiji se pripadajući privatni ključ čuva u sigurnom kriptografskom uređaju ili QSCD uređaju, sukladno točki 6.2.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta. Ovaj tip certifikata sukladan je s „NCP+“ općim pravilima za certifikate iz norme ETSI EN 319 411-1.
- ***Aplikacijski certifikat razine 3 (NCP+)*** – Certifikat visoke razine sigurnosti čiji se pripadajući privatni ključ čuva u HSM modulu, sukladno točki 6.2.1. ovog $CPS_{NQC\text{-}eIDAS}$

dokumenta. Ovaj tip certifikata sukladan je s „NCP+“ općim pravilima za certifikate iz norme ETSI EN 319 411-1.

1.1.2.4 Certifikat za e-pečat Trusted liste

Certifikat za e-pečat Trusted liste (NCP+) **–** koristi se za elektronički pečat Pouzdanog popisa (engl. *Trusted List*, u daljnjem tekstu. Truste lista), a izdaje se središnjem tijelu državne uprave nadležnom za poslove gospodarstva. Pripadajući privatni ključ čuva se u sigurnom kriptografskom uređaju ili QSCD uređaju, sukladno točki 6.2.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta. Ovaj tip certifikata sukladan je s „NCP+“ općim pravilima za certifikate iz norme ETSI EN 319 411-1.

1.1.2.5 Fina RDC-TDU 2015 administrativni certifikati

Administrativni certifikat (NCP+) **–** koristi ovlašteno osoblje Fine. Pripadajući privatni ključ ovog certifikata čuva se u sigurnom kriptografskom uređaju ili QSCD uređaju, sukladno točki 6.2.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta. Ovaj tip certifikata sukladan je s „NCP+“ općim pravilima za certifikate iz norme ETSI EN 319 411-1.

1.1.2.6 Fina RDC-TDU 2015 certifikati

Fina RDC-TDU 2015 certifikati namijenjeni su za uporabu u TDU, a izdaju se državnim dužnosnicima i zaposlenicima u tijelima državne uprave (u daljnjem tekstu: TDU).

- ***TDU autentikacijski certifikat (NCP+)*** – TDU autentikacijski certifikat srednje razine sigurnosti, koji se izdaje Pripadajućim osobama, a čiji se pripadajući privatni ključ sigurnom kriptografskom uređaju ili QSCD uređaju, sukladno točki 6.2.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta. Ovaj tip certifikata sukladan je s „NCP+“ općim pravilima za certifikate iz norme ETSI EN 319 411-1.

1.2 Naziv dokumenta i identifikacijski podaci

OID za Finu dodijeljen je od strane *British Standards Institution* (BSI) *International Code Designator* (ICD). Na temelju tog OID-a Fina je za potrebe Fina PKI dodijelila OID: 1.3.124.1104.5.

U nastavku je naveden naziv ovog dokumenta i pripadajući identifikacijski podaci.

- Naziv: Pravilnik o postupcima certificiranja za nekvalificirane certifikate
- Verzija: 1.2
- Datum stupanja na snagu: 12.09.2018.
- OID: 1.3.124.1104.5.0.4.2.1.2
- Internetske adrese na kojima je objavljen ovaj $CPS_{NQC\text{-}eIDAS}$ dokumenta su:
  - http://rdc.fina.hr/RDC2015/FinaRDC2015-CPSNQC1-2-hr.pdf i
  - http://rdc.fina.hr/RDC-TDU2015/FinaRDC-TDU2015-CPSNQC1-2-hr.pdf

1.3 Sudionici u PKI

Sudionici unutar Fina PKI su:

- certifikacijska tijela (*Certification Authorities*, CA-ovi),
- registracijska mreža (RA mreža) koja se sastoji od registracijskih ureda (*Registration Authority*, RA) i lokalnih registracijskih ureda (*Local Registration Authority*, LRA),
- Korisnici,
- Pouzdajuće strane.

1.3.1 Certifikacijska tijela

Certifikacijska tijela u Fina PKI iz opsega ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta su Fina RDC 2015 i Fina RDC-TDU 2015 (Fina CA-ovi).

Pojedini Fina CA se u izdanom certifikatu identificira kao izdavatelj (eng. *Issuer*). Fina CA koji izdaje certifikat potpisuje certifikat koristeći svoj privatni ključ.

1.3.1.1. Fina Root CA

Fina Root CA je izdao samopotpisani Fina Root CA certifikat te CA certifikate za njemu subordinirane Fina CA-ove (Fina RDC 2015 CA i Fina RDC-TDU 2015 CA). Fina Root CA ne izdaje certifikate Korisnicima.

Osnovni podaci o Fina Root CA certifikatu dani su u Tablici 1.3.

Polje	Atribut	Vrijednost
Issuer	commonName	Fina Root CA
	organizationName	Financijska agencija
	countryName	HR
Validity	notBefore	*Vrijeme izdavanja certifikata*
	notAfter	*Vrijeme izdavanja certifikata + 20 godina*
Subject	commonName	Fina Root CA
	organizationName	Financijska agencija
	countryName	HR
SHA-1 *fingerprint*: 62:02:bf:16:9a:f2:7f:a6:7e:d0:ce:c6:6b:78:2b:83:22:61:26:e9		
SHA-256 *fingerprint*:5a:b4:fc:db:18:0b:5b:6a:f0:d2:62:a2:37:5a:2c:77:d2:56:02:01:5d:96:64:87:56:61:1e:2e:78:c5:3a:d3		

Tablica 1.3. Osnovni podaci o Fina Root CA certifikatu

Fina Root CA certifikat dostupan je na sljedećoj internetskoj adresi: http://rdc.fina.hr/Root/FinaRootCA.cer.

1.3.1.1 Fina RDC 2015 CA

Fina RDC 2015 izdaje nekvalificirane certifikate za javnost koji su navedeni u Tablici 1.1 u točki 1.1.2. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

Administrativni certifikati i certifikati za elektronički pečat *Trusted* liste iz opsega ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta ne smatraju se certifikatima koje Fina izdaje za javnost.

Fina RDC 2015 izdaje nekvalificirane certifikate po istim pravilima za ovlaštene osobe Fine te za osobe s povjerljivim ulogama u Fina PKI.

Osnovni podaci o Fina RDC 2015 CA certifikatu dani su u Tablici 1.4.

Polje	Atribut	Vrijednost
Issuer	commonName	Fina Root CA
	organizationName	Financijska agencija
	countryName	HR
Validity	notBefore	25. studenog 2015. 11:13:30
	notAfter	25. studenog 2025. 11:43:30
Subject	commonName	Fina RDC 2015
	organizationName	Financijska agencija
	countryName	HR
SHA-1 fingerprint: d8:86:43:90:c7:6c:9b:71:f0:40:4f:f3:76:fc:38:fd:73:78:7d:08		
SHA-256 fingerprint: 85:7b:fc:e4:3b:1b:b4:60:1f:f4:54:3b:46:d3:fb:2e:21:3b:f9:b4:fe:eb:6f:13:be:9e:f4:5c:04:ff:6f:8b		

Tablica 1.4. Osnovni podaci o Fina RDC 2015 CA certifikatu

Fina RDC 2015 CA certifikat dostupan je na sljedećoj internetskoj adresi: http://rdc.fina.hr/RDC2015/FinaRDCCA2015.cer.

1.3.1.2 Fina RDC-TDU 2015 CA

Fina RDC-TDU 2015 izdaje nekvalificirane certifikate državnim dužnosnicima i zaposlenicima u TDU. Nekvalificirani certifikati koje izdaje Fina RDC 2015 navedeni su u Tablici 1.2. u točki 1.1.2. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

Osnovni podaci o Fina RDC-TDU 2015 certifikatu dani su u Tablici 1.5.

Polje	Atribut	Vrijednost
Issuer	commonName	Fina Root CA
	organizationName	Financijska agencija
	countryName	HR
Validity	notBefore	25. studenog 2015. 17:10:09
	notAfter	25. studenog 2025. 17:40:09
Subject	commonName	Fina RDC-TDU 2015
	organizationName	Financijska agencija
	countryName	HR
SHA-1 *fingerprint*: 1c:f5:2f:38:06:4b:fa:95:1e:45:b2:f3:9c:de:3f:d5:13:31:35:cd		
SHA-256 *fingerprint*: 0a:af:b7:83:43:b5:30:ba:06:17:c0:9a:70:ab:28:5b:30:42:59:f4:96:e0:19:af:ef:84:08:f2:a6:dd:00:f3		

Tablica 1.5. Osnovni podaci o Fina RDC-TDU 2015 CA certifikatu

Fina RDC-TDU 2015 CA certifikat dostupan je na sljedećoj internetskoj adresi: http://rdc.fina.hr/RDC-TDU2015/FinaRDC-TDUCA2015.cer.

1.3.2 Registracijski uredi

Poslovi registracije korisnika za Fina CA-ove obavljaju se u registracijskim uredima Fine. Za potrebe registracije korisnika za Fina CA-ove, Fina može s drugim poslovnim subjektom ugovoriti obavljanje usluge registracije.

Mrežu registracijskih ureda (u daljnjem tekstu: RA mreža) čine Fina RA mreža i mreža pojedinog vanjskog ugovorenog RA.

Fina RA mrežu čini mreža lokalnih registracijskih ureda (u daljnjem tekstu: Fina LRA) u poslovnoj mreži Fine te Središnji RA Fine. Registraciju korisnika u Fina RA mreži provodi Fina LRA, a može je provoditi i Središnji RA Fine. Poslovima registracije u Fina RA mreži koordinira Središnji RA Fine koji je središnja komunikacijska točka Fina RA mreže. Popis aktualnih registracijskih ureda Fina LRA nalazi se na internetskoj adresi http://www.fina.hr/finadigicert.

Mreža vanjskog ugovorenog RA je mreža lokalnih registracijskih ureda poslovnog subjekta s kojim je Fina sklopila ugovor o obavljanju usluga registracije za Fina CA-ove. RA mreža obvezna je poslove registracije obavljati u skladu s ovim $CPS_{NQC\text{-}eIDAS}$ dokumentom.

Registraciju korisnika u RA mreži provode ovlaštene osobe kojima je dodijeljena povjerljiva uloga Službenik za registraciju.

Poslovima registracije u RA mreži koordinira Središnji RA Fine.

RA mreža je obvezna registraciju korisnika za izdavanje certifikata provoditi sukladno postupcima opisanim u ovom $CPS_{NQC\text{-}eIDAS}$ dokumentu.

Obveze i odgovornosti Fina RA mreže i vanjskih ugovorenih RA navedene su u točki 9.6.2. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

1.3.3 Korisnici

Korisnik je poslovni subjekti ili fizička osoba koja je sklapanjem ugovora s Finom kao pružateljem usluga povjerenja preuzela ugovorne obveze Korisnika.

Korisnici Fina PKI mogu biti:

- Fizičke osobe – građani i
- poslovni subjekti.

Posebna kategorija poslovnih subjekata u okviru ovog dokumenta su TDU. Certifikate za pripadajuće osobe u TDU izdaje Fina RDC-TDU 2015, a za sve druge Korisnike certifikate izdaje Fina RDC 2015.

Za korištenje usluge certificiranja Korisnici obavljaju postupak predaje zahtjeva i registracije te prihvaćaju obaveze i odgovornosti Korisnika koje su navedene u točki 9.6.3. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta. Korisnici s Finom sklapaju ugovor o obavljanju usluga certificiranja.

1.3.3.1 Subjekti certificiranja

Subjekt certificiranja je u certifikatu identificiran kao Subjekt te je nositelj privatnog ključa koji je povezan s javnim ključem sadržanim u certifikatu.

Subjekt certificiranja u certifikatima koje izdaje Fina RDC 2015:

- u osobnim certifikatima je Fizička osoba – građanin,
- u poslovnim certifikatima je Pripadajuća osoba poslovnog subjekta,
- u poslovnim certifikatima za IT opremu je IT sustav, aplikacija ili uređaj,
- u certifikatima za elektronički pečat *Trusted* liste je tijelo državne uprave nadležno za poslove gospodarstva.

Subjekt certificiranja u certifikatima koje izdaje Fina RDC-TDU 2015 je Pripadajuća osoba TDU.

1.3.4 Pouzdajuće strane

Pouzdajuće strane su fizičke osobe ili poslovni subjekti koji se oslanjaju na uslugu povjerenja. Certifikat omogućuje pouzdajućoj strani provjeru identiteta Subjekta te validaciju elektroničkog potpisa.

Obaveze i odgovornosti Pouzdajuće strane navedene su u točki 9.6.4. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

1.3.5 Ostali sudionici

Nema odredbi.

1.4 Uporaba certifikata

Na temelju namjene, dozvoljene uporabe i ograničenja uporabe tipa certifikata Pouzdajuća strana odlučuje je li pojedini tip certifikata prikladan i pouzdan za korištenje i prihvaćanje. Pouzdajuća strana odgovorna je za prihvaćanje i ostvarivanje razumnog pouzdanja u certifikat koji ima određenu razinu sigurnosti. Pri donošenju odluke o prihvaćanju certifikata pouzdajuća strana treba razmotriti sljedeće:

- sve podatke koji se nalaze u certifikatu ili činjenice o kojima je pouzdajuća strana obaviještena, uključujući i ovaj $CPS_{NQC\text{-}eIDAS}$ dokument,
- ekonomsku vrijednost transakcije ili podataka, ako je to primjenjivo,
- potencijalne gubitke ili štetu koja može biti uzrokovana pogrešnom identifikacijom Subjekta certificiranja od strane Pouzdajuće strane,
- primjenjivost zakonske regulative,

- bilo koji pokazatelj prikladnosti ili neprikladnosti, ili druge činjenice koje Pouzdajuća strana zna, a odnose se na Subjekt certificiranja, primijenjeno rješenje ili transakciju,
- preporučeni financijski limit povezan s razinom sigurnosti certifikata.

U Tablici 1.6. opisane su razine sigurnosti za nekvalificirane certifikate koje izdaju Fina CA-ovi. Za pojedinu razinu sigurnosti u tablici je prikazan pripadajući opis područja primjene i preporučeni financijski limit.

Razina sigurnosti	Područje primjene	Preporučeni financijski limiti
Standardna	Ova razina je prikladna za transakcije manje vrijednosti i u okolinama u kojima potencijalna zlouporaba certifikata može nanijeti manju štetu ili je rizik od zlouporabe certifikata mali.	do 8.000,00 kn
Srednja	Ova razina je prikladna za transakcije koje imaju umjerenu vrijednost i u okolinama u kojima potencijalna zlouporaba certifikata može nanijeti umjerenu štetu ili je rizik od zlouporabe certifikata umjeren.	do 80.000,00 kn
Visoka	Ova razina je prikladna za transakcije koje imaju visoku vrijednost i u okolinama u kojima potencijalna zlouporaba certifikata može nanijeti veliku štetu ili je rizik od zlouporabe certifikata velik.	do 400.000,00 kn

Tablica 1.6. Razine sigurnosti za nekvalificirane certifikate

1.4.1 Primjerena uporaba certifikata

1.4.1.1 Primjerena uporaba osobnih certifikata

Osobne certifikate navedene u Tablici 1.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta upotrebljavaju Fizičke osobe – građani za podršku u elektroničkim potpisima, za jaku autentikaciju i enkripciju ključa. Ovi certifikati i pripadajući privatni ključevi prikladni su za podršku i izradu naprednog elektroničkog potpisa koji nije zasnovan na kvalificiranom certifikatu.

1.4.1.2 Primjerena uporaba poslovnih certifikata

Poslovne certifikate navedeni u Tablici 1.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta upotrebljavaju Pripadajuće osobe za podršku u elektroničkim potpisima, za jaku autentikaciju i enkripciju ključa. Ovi certifikati i pripadajući privatni ključevi prikladni su za podršku i izradu naprednog elektroničkog potpisa koji nije zasnovan na kvalificiranom certifikatu. Poslovni certifikati koriste se u poslovne svrhe, a Potpisnici ih mogu koristiti i u osobne svrhe ukoliko to ne priječe interni akti poslovnog subjekta.

1.4.1.3 Primjerena uporaba poslovnih certifikata za IT opremu

Poslovni certifikati za IT opremu navedeni u Tablici 1.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta pravila upotrebljavaju poslovni subjekti za podršku u elektroničkim potpisima, za jaku autentikaciju i enkripciju ključa. Ovi certifikati upotrebljavaju su u poslovne svrhe.

1.4.1.4 Primjerena uporaba TDU certifikata

TDU autentikacijski certifikat (NCP+) naveden u Tablici 1.2. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta pravila upotrebljavaju Pripadajuće osobe u TDU za podršku u elektroničkim potpisima, za jaku autentikaciju i enkripciju ključa. Ovi certifikati i pripadajući privatni ključevi prikladni su za podršku i izradu naprednog elektroničkog potpisa koji nije zasnovan na kvalificiranom certifikatu. Ovaj tip certifikata koristi se za potrebe tijela državne uprave. TDU certifikate Potpisnici mogu koristiti i u osobne svrhe ukoliko to ne priječe interni akti tijela državne uprave.

1.4.2 Zabrane uporabe certifikata

Osim uporaba navedenih u točki 1.4.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta, sve ostale uporabe nekvalificiranih certifikata su zabranjene.

1.5 Administracija dokumenta Opća pravila

1.5.1 Organizacija odgovorna za održavanje dokumenta Opća pravila

Za izradu i održavanje dokumenta Općih pravila [26] i ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta ovlaštena je i odgovorna Fina.

Ovlaštene osobe iz organizacijskih jedinica Fine koje sudjeluju u izradi, održavanju, implementaciji i odobravanju pravila i postupaka u Fina PKI koja se primjenjuju u pružanju usluga povjerenja u daljnjem tekstu nazivaju se zajedničkim nazivom Fina PMA.

Promjene sadržaja dokumenta obavljaju se na temelju internih prijedloga i zahtjeva za usklađivanjem sa zakonskom regulativom i mjerodavnim normama.

1.5.2 Kontakt podaci

Kontakt podaci za administraciju i sadržaj ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta dani su u nastavku.

Poštanska adresa:

Fina
Sektor komercijalnih digitalnih rješenja
Ured za upravljanje politikama e-poslovanja
Koturaška cesta 43
10000 Zagreb
Hrvatska

Telefon: +385-1-6128-171
Telefaks: +385-1-6304-081
E-mail: pma@fina.hr

1.5.3 Tijelo koje utvrđuje usklađenost CPS-a s Općim pravilima

Usklađenost ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta s Općim pravilima [26] utvrđuje Fina PMA.

Fina PMA odgovoran je za usklađenost ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta s Općim pravilima [26].

1.5.4 Procedure odobravanja CPS-a

Izrada, odobravanje i stupanje na snagu $CPS_{NQC\text{-}eIDAS}$ dokumenta kojom se potvrđuje njegova sukladnost s Općim pravilima [26] opisana je u točki 9.12.1 ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

1.6 Definicije i kratice

1.6.1 Definicije

POJAM	ZNAČENJE
Aktivacijski podaci	Tajni podaci potrebni za pristup ili aktivaciju kriptografskog modula. Aktivacijski podatak može biti PIN, zaporka ili elektronički ključ kojeg osoba zna ili posjeduje.
Autentikacija	Elektronički postupak koji omogućava da elektronička identifikacija Fizičke ili pravne osobe, ili izvornost i cjelovitost podataka u elektroničkom obliku budu potvrđeni.
Autor pečata	Pravna osoba koja izrađuje elektronički pečat.
CA certifikat	Certifikat javnog ključa za CA kojeg je izdao drugi CA ili kojeg je izdao isti CA.
Certifikacijsko tijelo (CA)	Tijelo koje izrađuje i dodjeljuje certifikate javnog ključa, a kojem vjeruje jedan ili više Korisnika. Certifikacijsko tijelo može biti: 1. pružatelj usluga povjerenja koji izrađuje i dodjeljuje certifikate javnog ključa, ili 2. tehnički servis izrade certifikata kojeg upotrebljava pružatelj usluga certificiranja koji izrađuje i dodjeljuje certifikate javnog ključa.
Certifikat	Vidi pojam „certifikat javnog ključa“.
Certifikat javnog ključa	Javni ključ Subjekta koji je zajedno s drugim informacijama zaštićen od krivotvorenja digitalnim potpisom izrađenim privatnim ključem certifikacijskog tijela koje je izdalo certifikat.
Certifikat za elektronički pečat	Elektronička potvrda koja povezuje podatke za validaciju elektroničkog pečata s pravnom osobom i potvrđuje naziv te osobe.

POJAM	ZNAČENJE
Certifikat za elektronički potpis	Elektronička potvrda koja povezuje podatke za validaciju elektroničkog potpisa s Fizičkom osobom i potvrđuje barem ime ili pseudonim te osobe.
Elektronički pečat	Podaci u elektroničkom obliku koji su pridruženi drugim podacima u elektroničkom obliku ili su logički povezani s njima radi osiguravanja izvornosti i cjelovitosti tih podataka.
Elektronički potpis	Podaci u elektroničkom obliku koji su pridruženi ili su logički povezani s drugim podacima u elektroničkom obliku i koje Potpisnik koristi za potpisivanje.
Elektronički vremenski žig	Podaci u elektroničkom obliku koji povezuju druge podatke u elektroničkom obliku s određenim vremenom i na taj način dokazuju da su ti podaci postojali u to vrijeme.
Fina LRA	Lokalni registracijski ured u Fina poslovnoj mreži.
Fina PKI	Infrastruktura javnog ključa (PKI) uspostavljena u Fini koja je namijenjena za pružanje usluga certificiranja Fizičkim osobama – građanima, Poslovnim subjektima i tijelima državne uprave, a koja je uspostavljena kao treća strana od povjerenja (engl. *Trusted Third Party*).
Fina RA mreža	Mreža registracijskih ureda u Fini, a sastoji se od Središnjeg RA Fine i Fina LRA ureda.
Fizička osoba - građanin	Fizička osoba koja uslugu certificiranja traži sa svrhom korištenja certifikata u vlastito ime i za vlastiti račun i isključuje Fizičku osobu s registriranom djelatnošću, Fizičku osobu u obavljanju slobodnog zanimanja te Fizičku osobu koja nastupa u ime i za račun druge Fizičke ili pravne osobe (Pripadajuća osoba).
Infrastruktura javnog ključa (PKI)	Infrastruktura za upravljanje javnim ključevima koji podržavaju usluge autentikacije, enkripcije, cjelovitosti i neporecivosti.
Javni imenik	Informatički sustav koji služi za *online* objavu informacija vezanih uz certifikate, uključujući i informacije o opozvanosti certifikata.
Javni ključ	U kriptografskom sustavu javnog ključa, javno poznati ključ iz Subjektovog para ključeva.
Koordinirano svjetsko vrijeme (UTC)	Vremenska ljestvica koja se temelji na sekundi kako je definirana ITU-R preporukom TF.460-5. Za većinu primjena u praksi UTC je ekvivalentan srednjem sunčevom vremenu na nultom meridijanu (0°). Točnije, UTC je kompromis između vrlo stabilnog atomskog vremena (*Temps Atomique International* - TAI) i sunčevog vremena koje se izvodi iz nepravilne rotacije Zemlje (u odnosu na dogovoreno Greenwich srednje zvjezdano vrijeme (GMST).

POJAM	ZNAČENJE
Korisnik	Poslovni subjekt ili fizička osoba koja je sklapanjem ugovora s pružateljem usluga povjerenja preuzela ugovorne obveze Korisnika.
Kriptografski modul	Softver ili uređaj određene razine sigurnosti koji: ▪ generira par ključeva i/ili, ▪ štiti kriptografske informacije i/ili, ▪ obavlja kriptografske funkcije.
Kvalificirani certifikat za elektronički potpis	Certifikat za elektroničke potpise koji izdaje kvalificirani pružatelj usluga povjerenja i koji ispunjava zahtjeve utvrđene u Prilogu I. Uredbe (EU) br. 910/2014 [1].
Kvalificirani elektronički potpis	Napredan elektronički potpis koji je izrađen pomoću kvalificiranih sredstava za izradu elektroničkog potpisa i temelji se na kvalificiranom certifikatu za elektroničke potpise.
Kvalificirani elektronički vremenski žig	Elektronički vremenski žig koji ispunjava sljedeće zahtjeve: (a) povezuje datum i vrijeme s podacima na način kojim se u razumnoj mjeri isključuje mogućnost nezapažene promjene podataka, (b) temelji se na izvoru točnog vremena povezanom s koordiniranim svjetskim vremenom, i (c) potpisan je pomoću naprednog elektroničkog potpisa ili pečaćen pomoću naprednog elektroničkog pečata kvalificiranog pružatelja usluga povjerenja ili jednakovrijednom metodom.
Kvalificirani ocjenitelj	Fizička ili pravna osoba koja zadovoljava zahtjeve navedene u dokumentu Baseline Requirements [24] kojeg objavljuje CA/Browser Forum.
Kvalificirani pružatelj usluga povjerenja	Pružatelj usluga povjerenja koji pruža jednu ili više kvalificiranih usluga povjerenja i kojemu je nadzorno tijelo odobrilo kvalificirani status.
Kvalificirano sredstvo za izradu elektroničkog potpisa	Sredstvo za izradu elektroničkog potpisa koje ispunjava zahtjeve utvrđene u Prilogu II Uredbe (EU) br. 910/2014 [1].
LCP certifikat	Certifikat usklađen s *Lightweight* općim pravilima pružanja usluge certificiranja (*Lightweight Certificate Policy*).
Lista opozvanih certifikata (CRL)	Potpisana lista u kojoj su naznačeni certifikati koje izdavatelj certifikata više ne smatra valjanim.

POJAM	ZNAČENJE
Napredan elektronički potpis	Elektronički potpis koji ispunjava sljedeće zahtjeve: (a) na nedvojben način je povezan s Potpisnikom, (b) omogućava identificiranje Potpisnika, (c) izrađen je korištenjem podacima za izradu elektroničkog potpisa koje Potpisnik može, uz visoku razinu pouzdanja, koristiti pod svojom isključivom kontrolom, i (d) povezan je s njime potpisanim podacima na način da se može otkriti bilo koja naknadna izmjena podataka.
NCP certifikat	Certifikat usklađen s normaliziranim općim pravilima pružanja usluge certificiranja (*Normalized Certificate Policy*).
Opća pravila pružanja usluge certificiranja - *Certificate Policy* (CP)	Imenovani skup pravila koji ukazuje na primjenjivost certifikata za određenu skupinu i/ili klasu primjena sa zajedničkim zahtjevima na sigurnost.
Opoziv certifikata	Radnja koja certifikat nepovratno čini nevažećim od trenutka opoziva.
Osoba ovlaštena za zastupanje	Osoba koja je po zakonu ovlaštena zastupati Korisnika koji je Poslovni subjekt.
Ovlašteni predstavnik	Fizička osoba koja je po zakonu ili na temelju punomoći ovlaštena zastupati Autora pečata u postupku izdavanja i /ili opoziva certifikata za elektronički pečat.
Par ključeva	Dva jedinstveno povezana kriptografska ključa, od kojih je jedan privatni ključ, a drugi javni ključ.
Podaci za izradu elektroničkog pečata	Jedinstveni podaci koje autor elektroničkog pečata koristi za izradu elektroničkog pečata.
Podaci za izradu elektroničkog potpisa	Jedinstveni podaci koje Potpisnik koristi za izradu elektroničkog potpisa
Podaci za validaciju	Podaci koji se koriste za validaciju elektroničkog potpisa ili elektroničkog pečata.
Podaci za verifikaciju potpisa	Podaci, poput kodova ili javnih kriptografskih ključeva koji se koriste u svrhu verificiranja potpisa.

POJAM	ZNAČENJE
Poslovni subjekt	1. Pravne osobe, primjerice ▪ trgovačka društva, ▪ kreditne i financijske institucije, ▪ javne i privatne ustanove, ▪ udruge s pravnom osobnošću, ▪ neprofitne i nevladine organizacije s pravnom osobnošću, ▪ fondovi s pravnom osobnošću, ▪ jedinice lokalne i područne (regionalne) samouprave (općine, gradovi i županije) i dr. 2. Tijela javne vlasti, primjerice ▪ tijela državne vlasti, ▪ tijela državne uprave, ▪ državne agencije i dr. 3. Fizičke osobe s registriranom djelatnošću, primjerice ▪ obrtnici, ▪ odvjetnici, ▪ javni bilježnici i dr.
Potpisnik	Fizička osoba koja izrađuje elektronički potpis.
Pouzdajuća strana	Fizička osoba ili Poslovni subjekt koji se oslanja na elektroničku identifikaciju ili uslugu povjerenja.
Pouzdani popis	Popis države članice EU koji pruža informacije o statusu i povijesti statusa usluga povjerenja pružatelja usluga povjerenja u odnosu na usklađenost s važećim zahtjevima i odgovarajućim odredbama važećih propisa (engl. *Trusted List*).
Povjerljive uloge	Uloge o kojima ovisi sigurnost rada pružatelja usluga povjerenja. Povjerljive uloge (engl. *Trusted Roles*) i pripadajuće odgovornosti pružatelj usluga povjerenja jasno opisuje u opisu posla djelatnika.
Pravilnik o postupcima certificiranja (CPS)	Pravilnik operativnih postupaka koje certifikacijsko tijelo provodi u izdavanju, upravljanju, opozivu ili obnovi certifikata.
Pripadajuća osoba	Fizička osoba zaposlena u Poslovnom subjektu ili na drugi način povezana s Poslovnim subjektom, a koja je od strane istog poslovnog subjekta autorizirana za dobivanje certifikata. Takav certifikat identificira osobu i Poslovni subjekt te naznačuje da je ta osoba povezana s Poslovnim subjektom.
Privatni ključ	U kriptografskom sustavu javnog ključa, ključ iz Subjektovog para ključeva koji je poznat samo Subjektu.
Pružatelj usluga povjerenja	Fizička ili pravna osoba koja pruža jednu ili više usluga povjerenja bilo kao kvalificirani ili nekvalificirani pružatelj usluga povjerenja.

POJAM	ZNAČENJE
QSCD uređaj	Kvalificirano sredstvo za izradu elektroničkog potpisa/pečata (vidi pojam „kvalificirano sredstvo za izradu elektroničkog potpisa“, odnosno „sredstvo za izradu kvalificiranog elektroničkog pečata“.
RA mreža	Cjelokupna mreža registracijskih tijela, a sastoji se od Fina RA mreže te od vanjskih ugovorenih RA s kojima Fina ima sklopljen ugovor o obavljanju poslova registracije.
Razlikovno ime (DN)	Jedinstveno ime Subjekta upisano u certifikat. Razlikovno ime subjekta jedinstveno identificira Subjekt kojem je izdan certifikat i jedinstveno je unutar jednog CA.
Reaktivacija certifikata	Radnja koja suspendirani certifikat ponovno čini važećim od trenutka reaktivacije.
Redovna obnova certifikata	Obnova certifikata u FINA PKI podrazumijeva izdavanje novog certifikata čiji su parametri jednaki kao i parametri certifikata na koji se zahtjev odnosi, ali s novim javnim ključem, novim serijskim brojem certifikata, novim vremenskim periodom valjanosti i novim potpisom istog CA, a provodi se u definiranom periodu prije datuma isteka valjanosti certifikata.
Registracijski ured (RA)	Tijelo odgovorno za identifikaciju i autentikaciju subjekata certificiranja, kao i drugih osoba ili organizacija.
Root CA	Certifikacijsko tijelo najviše razine unutar domene pružatelja usluga povjerenja i koje potpisuje certifikate subordiniranih CA-ova.
Root CA certifikat	CA certifikat kojeg je samom sebi izdao root CA.
Siguran kriptografski uređaj	Uređaj koji čuva privatni Korisnički ključ, štiti ga protiv kompromitiranja i obavlja potpisne ili dekripcijske funkcije u ime Korisnika.
Skrbnik	Fizička osoba zaposlena u Poslovnom subjektu ili na drugi način povezana s Poslovnim subjektom, a koja je od strane istog poslovnog subjekta ovlaštena za podnošenje zahtjeva za izdavanje poslovnih certifikata za sustave, uređaje i autentikaciju mrežnih stranica te za preuzimanje certifikata i pripadajućih aktivacijskih podataka. Skrbnik je ovlašten za podnošenje zahtjeva za upravljanje životnim ciklusom certifikata. Skrbnik je kontakt osoba poslovnog subjekta prema pružatelju usluge povjerenja za predmetni certifikat.
Službenik za opoziv certifikata	Osoba koja je odgovorna za promjenu operativnog statusa certifikata.
Službenik za registraciju	Osoba odgovorna za potvrđivanje podataka koji su potrebni za izdavanje certifikata i za odobravanje zahtjeva za izdavanje certifikata.

POJAM	ZNAČENJE
Središnji RA	Središnji registracijski ured koji je primarno je zadužen za koordiniranje cjelokupne RA mreže, ali može i izravno obavljati registriranje Korisnika
Sredstvo za izradu elektroničkog pečata	Konfigurirani softver ili hardver koji se koristi za izradu elektroničkog pečata.
Sredstvo za izradu elektroničkog potpisa	Konfigurirani softver ili hardver koji se koristi za izradu elektroničkog potpisa.
Subjekt	Entitet identificiran u certifikatu kao nositelj privatnog ključa koji je povezan s javnim ključem sadržanim u certifikatu.
Suspenzija certifikata	Radnja koja certifikat čini nevažećim od trenutka suspenzije. Suspendirani certifikat se reaktivacijom može ponovno učiniti važećim.
Sustav certificiranja	Sustav IT proizvoda i komponenti organiziranih za pružanje usluga certificiranja.
Tijelo državne uprave (TDU)	Tijelo državne vlasti nadležno za obavljanje poslova državne uprave u upravnom području za koje je nadležno. Tijela državne uprave su ministarstva, državni uredi, državne upravne organizacije i uredi državne uprave u županijama ili druga tijela državne uprave utvrđena mjerodavnim važećim zakonom.
Tijelo za ocjenjivanje sukladnosti	Tijelo u smislu članka 2. točke 13. Uredbe (EZ) br. 765/2008 koje je u skladu s tom Uredbom ovlašteno kao nadležno za provedbu ocjenjivanja sukladnosti kvalificiranog pružatelja usluga povjerenja i kvalificiranih usluga povjerenja koje on pruža.
Tijelo za upravljanje pravilima certificiranja (PMA)	Tijelo s konačnom ovlašću i odgovornošću za određivanje i odobravanje pravila pružanja usluga povjerenja (engl. *Policy Management Authority*)
Usluge certificiranja	Usluge izdavanje i upravljanje životnom ciklusom certifikata.
Validacija	Postupak verifikacije i potvrđivanja da su elektronički potpis ili pečat valjani.
Validacija certifikata	Postupak verificiranja i potvrđivanja da je certifikat valjan.
Verifikacija potpisa	Proces provjere kriptografske vrijednosti potpisa korištenjem podataka za verifikaciju potpisa.

Tablica 1.7. Definicije

1.6.2 Kratice

KRATICA	PUNI NAZIV	ZNAČENJE
CA	*Certification Authority*	Certifikacijsko tijelo
CP	*Certificate Policy*	Opća pravila pružanja usluga certificiranja
$CP_{NQC\text{-}eIDAS}$	*Certificate Policy for Non-Qualified Certificates*	Opća pravila pružanja usluga certificiranja za nekvalificirane certifikate
CPS	*Certification Practice Statement*	Pravilnik o postupcima certificiranja
$CPS_{NQC\text{-}eIDAS}$	*Certification Practice Statement for Non-Qualified Certificates*	Pravilnik o postupcima certificiranja za nekvalificirane certifikate
CRL	*Certificate Revocation List*	Lista opozvanih certifikata
DN	*Distinguished Name*	Razlikovno ime
LCP	*Lightweight Certificate Policy*	Opća pravila certificiranja za *lightweight* certifikate
LDAP	*Lightweight Directory Access Protocol*	Protokol za pristup informacijskim direktorijima
LRA	*Local Registration Authority*	Lokalni registracijski ured
NCP	*Normalized Certificate Policy*	Opća pravila certificiranja za normalizirane certifikate
NCP+	*Extended Normalized Certificate Policy*	Opća pravila certificiranja za proširene normalizirane certifikate
OCSP	*Online Certificate Status Protocol*	Protokol *on-line* provjere statusa certifikata
OID	*Object Identifier*	Identifikator objekta
PIN	*Personal Identification Number*	Osobni tajni broj za aktivaciju smart kartice, USB tokena ili sličnog uređaja
PKI	*Public Key Infrastructure*	Infrastruktura javnog ključa
PMA	*Policy Management Authority*	Tijelo za upravljanje pravilima certificiranja
QSCD	*Qualified electronic Signature/Seal Creation Device*	Kvalificirano sredstvo za izradu elektroničkog potpisa/pečeta
RA	*Registration Authority*	Registracijski ured
TDU	Tijelo (ili tijela) državne uprave	Tijelo (ili tijela) državne uprave
UTC	*Coordinated Universal Time*	Koordinirano svjetsko vrijeme

Tablica 1.7. Kratice

2 OBJAVE I ODGOVORNOSTI ZA REPOZITORIJ

2.1 Identifikacija tijela koje vodi repozitorij

Fina PKI repozitorij vodi Fina kao pružatelj usluga certificiranja. Fina je odgovorna za rad Fina PKI repozitorija te za objavu dokumenata i informacija na repozitoriju.

Fina osigurava dostupnost repozitorija uz raspoloživost 24 sata na dan, 7 dana u tjednu.

2.2 Objava informacija o certificiranju

Na Fina PKI repozitoriju javno su objavljeni dokumenti i informacije o pružanju usluga certificiranja.

Repozitorij se sastoji od dijela dostupnog na internetskim stranicama i dijela dostupnog preko javnog LDAP imenika.

2.2.1 Sadržaji repozitorija

Na internetskim stranicama Fina PKI repozitorija objavljuju se:

- aktualna opća pravila pružanja usluga certificiranja,
- pravilnik o postupcima certificiranja,
- prijašnje verzije općih pravila pružanja usluga certificiranja i pravilnika o postupcima certificiranja,
- uvjeti i izjave o pružanju usluga izdavanja certifikata (engl. *Terms and conditions* i *PKI disclosure statement*),
- opis važećih profila certifikata,
- cjenik usluga certificiranja,
- obrasci zahtjeva za izdavanje certifikata,
- obrasci ugovora o obavljanju usluga certificiranja,
- obrasci zahtjeva za opoziv, suspenziju, reaktivaciju ili oporavak certifikata,
- obrasci punomoći,
- Fina Root CA certifikat i certifikati subordiniranih Fina CA-ova,
- objedinjene CRL pojedinog Fina CA,
- informacije o zakonskoj regulativi iz područja elektroničkog potpisa i pružanja usluga certificiranja,
- informacije o postojanju dokumenata važnim za poslovanje koji ne mogu biti u cijelosti ili uopće objavljeni zbog osjetljivosti ili tajnosti sadržaja,
- aktualne lokacije Fina LRA ureda,
- korisničke upute,
- certifikati namijenjeni za provjeru i testiranje,
- obavijesti Korisnicima i Pouzdajućim stranama vezane uz davanje usluga certificiranja,
- ostale informacije vezane uz rad Fina CA-ova.

Preko internetske stranice repozitorija moguće je pretraživanje javnog imenika i preuzimanje certifikata koje je izdao pojedini Fina CA. Za pronalaženje traženog certifikata potrebno je poznavanje i upis osnovnih podataka o subjektu.

Objavljeni sadržaj na internetskim stranicama dostupan je s adrese http://www.fina.hr/finadigicert na hrvatskom i engleskom jeziku.

U strukturi javnog imenika javno se objavljuju:

- certifikati subordiniranih Fina CA-ova,
- objedinjena CRL i segmentirana CRL za pojedini Fina CA.

Adresa javnog LDAP imenika:

- za Fina RDC 2015 je ldap://rdc-ldap2.fina.hr,
- za Fina RDC-TDU je ldap://rdc-tdu-ldap2.fina.hr.

Putem Fina OCSP servisa dostupne su informacije o statusu izdanih certifikata koje izdaju Fina CA-ovi. Adresa Fina OCSP servisa je http://ocsp.fina.hr.

Adrese na kojima se objavljuju CRL pojedinog Fina CA navedene su u točki 4.10.1 ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

U Fina PKI repozitoriju ne objavljuju se povjerljivi podaci.

2.2.2 Postupci objave sadržaja i upravljanja repozitorijem

Objavu dokumenata na repozitoriju po odobrenju obavlja ovlaštena osoba zadužena za upravljanje sadržajem internetskog dijela repozitorija.

Obavijesti korisnicima, informacije o zakonskim aktima objavljuju se po početku primjene zakonskih akata u Fina PKI. Certifikati Fina CA-ova i pripadajuće informacije objavljuju se po njihovu izdavanju.

Certifikati Fina CA-ova i pripadajuće informacije objavljuju se po njihovu izdavanju.

Objavu dokumenata uvjeta pružanja usluga, korisničkih uputa, obrazaca zahtjeva, ugovora i punomoći odobrava Fina PMA. Objava ovih dokumenata se obavlja bez prethodne najave, a starije verzije dokumenata brišu se iz repozitorija.

Fina CA automatski objavljuje pripadajuće CRL na javnom imeniku i na internetskim stranicama repozitorija nakon njihova izdavanja.

Obavijesti i informacije korisnicima se mogu objaviti na internetskim stranicama repozitorija i bez odobrenja Fina PMA, ali Fina PMA mora biti pravodobno obaviješten o svakoj objavi obavijesti i informacija.

2.3 Vrijeme ili učestalost objavljivanja

Fina na godišnjoj razini održava i ažurira dokumente Opća pravila i ovaj $CPS_{NQC\text{-}eIDAS}$ dokument te ih odobrava, objavljuje i primjenjuje. Prijašnje verzije ovih dokumenata ostaju objavljene na repozitoriju najmanje do isteka certifikata izdanih sukladno tim dokumentima.

Drugi Fina PKI dokumenti i ostale relevantne informacije iz točke 2.2.1. ovog $CSP_{NQC\text{-}eIDAS}$ dokumenta objavljuju se po potrebi, nakon odobrenja Fina PMA.

Korisnički certifikati su za preuzimanje s repozitorija raspoloživi odmah po njihovom izdavanju.

Učestalost objave CRL za certifikate koje izdaju Fina CA definirana je u točki 4.9.7 ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

Online informacije o statusu izdanih certifikata dostupne su putem Fina OCSP servisa koji je opisan u točki 4.9.9. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

2.4 Kontrole pristupa repozitoriju

Dokumenti i informacije objavljene na Fina PKI repozitoriju su besplatne i javno dostupne svim sudionicima Fina PKI.

Fina na repozitoriju ima uspostavljene kontrole pristupa u cilju sprječavanja neautoriziranog dodavanja, promjene ili brisanja informacija te zaštite njihove cjelovitosti i autentičnosti. Pristup objavljenim dokumentima i informacijama na repozitoriju omogućen je samo za čitanje.

Pravo dodavanja, promjene ili brisanja informacija na Fina PKI repozitoriju imaju ovlaštene osobe Fine.

3 IDENTIFIKACIJA I POTVRĐIVANJE IDENTITETA SUBJEKTA

Postupke identifikacije i potvrđivanja identiteta subjekta za Fina PKI provodi RA mreža koju čine Fina RA mreža i mreža pojedinog vanjskog ugovorenog RA. Fina RA mrežu čine Središnji RA Fine i Fina LRA. Djelatnici ovlašteni za registraciju u RA mreži obavljaju poslove registracije sukladno ovom $CPS_{NQC\text{-}eIDAS}$ dokumentu.

3.1 Određivanje imena

3.1.1 Tipovi imena

U svaki certifikat upisuju se podaci o imenu, odnosno nazivu Subjekta certificiranja te podatak o mjestu prebivališta fizičke osobe, odnosno mjestu sjedišta poslovnog subjekta. Podaci o imenu ili nazivu koji se upisuju u certifikat odnose se na autentično ime ili naziv subjekta. Polje *Subject* u certifikatu usklađeno je s preporukom IETF RFC 5280 [21].

Polje *Subject* u osobnim certifikatima i poslovnim certifikatima koji se izdaju Pripadajućim osobama sadrži ime i prezime osobe te serijski broj kojim se osigurava jedinstvenost polja *Subject*. U poslovnim certifikatima za Pripadajuće osobe polje *Subject* dodatno sadrži puni registrirani naziv poslovnog subjekta i njegov identifikator.

Polje *Subject* u aplikacijskim certifikatima sadrži naziv za IT sustav, aplikaciju ili servis (u daljnjem tekstu: naziv aplikacije). Polje Subject u aplikacijskim certifikatima dodatno sadrži i puni registrirani naziv poslovnog subjekta i njegov identifikator.

Polje *Subject* u certifikatima za elektronički pečat *Trusted* liste sadrži puni registrirani naziv i identifikator središnjeg tijela državne uprave nadležnog za poslove gospodarstva.

Polje *Subject* u Administrativnim certifikatima koji se izdaju ovlaštenim zaposlenicima Fine za internu uporabu sadrži ime i prezime osobe te serijski broj kojim se osigurava jedinstvenost polja *Subject*, a dodatno sadrži i puni registrirani skraćeni naziv Fine i njen OIB.

Ukoliko bilo koji podatak koji se unosi u polje „Subjekt“ sadrži posebne znakove ili slova koja nisu sadržana u engleskoj ili hrvatskoj abecedi, takvi znakovi se zamjenjuju najbližim znakom engleske abecede sukladno Fininim pravilima korištenja zamjenskih znakova.

3.1.2 Smislenost imena

Imena i nazivi u atributima polja *Subject* koji identificiraju fizičku osobu i poslovni subjekt su smisleni.

Za atribute u polju *Subject* u certifikatima koje izdaju Fina CA-ovi primjenjuju se sljedeća pravila:

- identifikatori moraju biti smisleni,
- osobno ime i prezime moraju biti kako su navedeni u identifikacijskoj ispravi, odnosno u službenim matičnim registrima,

- naziv poslovnog subjekta mora biti kako je naveden u službenim nadležnim nacionalnim registrima,
- naziv aplikacije mora biti kako je naveden u zahtjevu za izdavanje certifikata.

Naziv grupe certifikata	Pravilo za smislenost elemenata polja *Subject*
Fina RDC 2015 osobni certifikati	• commonName: Ime i prezime potpisnika • givenName: Ime Potpisnika • surname: Prezime Potpisnika • localityName: Mjesto prebivališta Potpisnika • countryName: HR
Fina RDC 2015 poslovni certifikati	• commonName: Ime i prezime Potpisnika • givenName: Ime Potpisnika • surname: Prezime Potpisnika • localityName: Mjesto sjedišta poslovnog subjekta • organizationIdentifier: „HR“, jedanaesteroznamenkasti identifikator (OIB ili interni Finin identifikator) • organizationName: Puni registrirani skraćeni naziv poslovnog subjekta • countryName: HR
Fina RDC 2015 aplikacijski certifikati	• commonName: Naziv aplikacije • localityName: Mjesto sjedišta poslovnog subjekta • organizationIdentifier: „HR“, jedanaesteroznamenkasti identifikator (OIB ili interni Finin identifikator) • organizationName: Puni registrirani skraćeni naziv poslovnog subjekta • countryName: HR
Fina RDC 2015 certifikat za e-pečat Trusted liste	• commonName: Naziv kojeg određuje središnje tijelo državne uprave nadležno za poslove gospodarstva • localityName: Zagreb • organizationIdentifier: „VATHR-“ OIB središnjeg tijela državne uprave nadležnog za poslove gospodarstva • organizationName: Naziv središnjeg tijela državne uprave nadležnog za poslove gospodarstva • countryName: HR
Fina RDC 2015 administrativni certifikati	• commonName: Ime i prezime Potpisnika • givenName: Ime Potpisnika • surname: Prezime Potpisnika • localityName: ZAGREB • organizationIdentifier: HR85821130368 • organizationName: FINA • countryName: HR

Naziv grupe certifikata	Pravilo za smislenost elemenata polja *Subject*
Fina RDC-TDU 2015 certifikati	• commonName: Ime i prezime potpisnika • givenName: Ime potpisnika • surname: Prezime potpisnika • localityName: Mjesto sjedišta TDU • organizationalUnit: Naziv organizacijske jedinica TDU 2. razine (opcionalno) • organizationalUnit: Naziv organizacijske jedinica TDU 1. razine (opcionalno) • organizationIdentifier: „HR“, OIB • organizationName: Puni registrirani skraćeni naziv TDU • countryName: HR

Tablica 3.1. Pravila za određivanje elemenata polja „Subject“

Sadržaj ekstenzije certifikata *Subject Alternative Name* može biti e-mail adresa Subjekta koja ne mora biti smislena.

3.1.3 Anonimnost korisnika ili pseudonimi

Anonimnost i pseudonimi korisnika nisu podržani.

3.1.4 Pravila tumačenja raznih oblika imena

Tumačenje oblika imena u polju *Subject* po normi X.520 u Fina PKI određeno je na sljedeći način:

Pravila tumačenja raznih oblika imena		
Osobni nekvalificirani certifikati		
Atribut po X.520	**Fina RDC 2015**	**Pojašnjenje**
serialNumber	HR OIB, ili ISO kod države prebivališta Potpisnika i jedanaesteroznamenkasti jedinstveni identifikator fizičke osobe, te dva broja W i Z koji predstavljaju Finine interne oznake.	Jedanaesteroznamenkasti jedinstveni identifikator fizičke osobe je OIB ako fizička osoba ima dodijeljen OIB u Republici Hrvatskoj. Ako fizička osoba nema dodijeljen OIB, tada jedanaesteroznamenkasti jedinstveni identifikator fizičke osobe generira Fina.
commonName (CN)	Ime i prezime Potpisnika	Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi
givenName	Ime(na) Potpisnika	Ime(na) potpisnika kako je navedeno u identifikacijskoj ispravi
surname (SN)	Prezime(na) Potpisnika	Prezime(na) potpisnika kako je navedeno u identifikacijskoj ispravi
localityName (L)	Mjesto prebivališta Potpisnika	Mjesto prebivališta fizičke osobe-građanina

organizationName (O)	OSOBNI	U certifikatima izdanim fizičkim osobama koje nisu povezane s poslovnim subjektom atribut Organization Name sadrži vrijednost „OSOBNI“ koja predstavlja internu klasifikaciju osobnog certifikata.
countryName (C)	HR	Dvoslovčani ISO kod države, HR za Hrvatsku.

Poslovni nekvalificirani i TDU certifikati

Atribut po X.520	Fina RDC 2015	Fina RDC-TDU 2015	Pojašnjenje
serialNumber	HR OIB, ili ISO kod države prebivališta Potpisnika i jedanaesteroznamenkasti jedinstveni identifikator, te dva broja W i Z koji predstavljaju Finine interne oznake.	HR OIB, ili ISO kod države prebivališta Potpisnika i jedanaesteroznamenkasti jedinstveni identifikator, te dva broja W i Z koji predstavljaju Finine interne oznake.	Jedanaesteroznamenkasti jedinstveni identifikator fizičke osobe je OIB ako fizička osoba ima dodijeljen OIB u Republici Hrvatskoj. Ako fizička osoba nema dodijeljen OIB, tada jedanaesteroznamenkasti jedinstveni identifikator fizičke osobe generira Fina.
commonName (CN)	Ime i prezime Potpisnika	Ime i prezime Potpisnika	Ime i prezime Potpisnika kako je navedeno u identifikacijskoj ispravi
givenName	Ime(na) Potpisnika	Ime(na) Potpisnika	Ime(na) Potpisnika kako je navedeno u identifikacijskoj ispravi
surname (SN)	Prezime(na) Potpisnika	Prezime(na) Potpisnika	Prezime(na) Potpisnika kako je navedeno u identifikacijskoj ispravi
localityName (L)	Mjesto sjedišta poslovnog subjekta	Mjesto sjedišta TDU	Mjesto sjedišta poslovnog subjekta
organizationIdentifier	Dvoslovčani ISO kod države sjedišta poslovnog subjekta te jedanaesteroznamenkasti broj. Za poslovne subjekte kojima je dodijeljen OIB u Republici Hrvatskoj: „HR“, OIB.	„HR“, OIB	Za poslovne subjekte kojima nije dodijeljen OIB u Republici Hrvatskoj jedinstveni jedanaesteroznamenkasti broj dodjeljuje Fina CA i ne predstavlja OIB.
organizationName (O)	Puni registrirani skraćeni naziv poslovnog subjekta	Puni registrirani skraćeni naziv TDU	Puni registrirani skraćeni naziv bez OIB-a

Atribut po X.520	Fina RDC 2015	Fina RDC-TDU 2015	Pojašnjenje
Organization Unit (OU)	Ne primjenjuje se.	Ovaj atribut je opcionalan, a sadrži naziv organizacijske jedinice TDU	Certifikati koje izdaje Fina RDC-TDU 2015 podržavaju do dvije podorganizacijske jedinice unutar TDU
countryName (C)	HR	Ne primjenjuje se.	Dvoslovčani ISO kod Republike Hrvatske
Aplikacijski certifikati			
Atribut po X.520	**Fina RDC 2015**	**Fina RDC-TDU 2015**	**Pojašnjenje**
commonName (CN)	Naziv aplikacije	Ne primjenjuje se.	Naziv za IT sustav, aplikaciju ili servis.
localityName (L)	Mjesto sjedišta poslovnog subjekta	Ne primjenjuje se.	Mjesto sjedišta poslovnog subjekta
organizationIdentifier	Dvoslovčani ISO kod države sjedišta poslovnog subjekta te jedanaesteroznamenkasti broj. Za poslovne subjekte kojima je dodijeljen OIB u Republici Hrvatskoj: „HR“, OIB.	Ne primjenjuje se.	Za poslovne subjekte kojima nije dodijeljen OIB u Republici Hrvatskoj jedinstveni jedanaesteroznamenkasti broj dodjeljuje Fina CA i ne predstavlja OIB.
organizationName (O)	Puni registrirani skraćeni naziv poslovnog subjekta	Ne primjenjuje se.	Puni registrirani skraćeni naziv bez OIB-a
countryName (C)	HR	HR	Dvoslovčani ISO kod Republike Hrvatske

Tablica 3.2. Tumačenje oblika imena za osobne, poslovne i TDU nekvalificirane certifikate po X.520 normi

Certifikat za elektronički pečat *Trusted* liste		
Atribut po X.520	**Fina RDC 2015**	**Pojašnjenje**
serialNumber	„P“ i dva broja W i Z koji su Finini interni broj.	Atribut *Serial Number* sastoji se od dvije komponente: W i Z odijeljene točkom. W i Z su brojevi koji imaju interno značenje za Fina PKI.
commonName (CN)	Prepoznatljivi naziv	Naziv kojeg određuje središnje tijelo državne uprave nadležno za poslove gospodarstva

Atribut po X.520	Fina RDC 2015	Pojašnjenje
localityName (L)	Mjesto sjedišta TDU.	Mjesto sjedišta središnjeg tijela državne uprave nadležnog za poslove gospodarstva.
organizationIdentifier	„VAT“, HR, "-", OIB	„VATHR-“ OIB središnjeg tijela državne uprave nadležnog za poslove gospodarstva
organizationName (O)	Naziv središnjeg tijela državne uprave nadležnog za poslove gospodarstva	Puni registrirani skraćeni naziv pravne osobe, bez OIB-a
countryName (C)	HR	Dvoslovčani ISO kod Republike Hrvatske

Tablica 3.3. Tumačenje oblika imena za certifikat za potpis Trusted liste po X.520 normi

Subject Alternative Name je opcionalna ekstenzija certifikata koja može sadržavati e-mail adresu Subjekta.

3.1.5 Jedinstvenost imena

Razlikovno ime Subjekta jedinstveno je unutar Fina PKI produkcijske hijerarhije zasnovane na Fina Root CA.

Jedinstvenost razlikovnog imena u osobnim certifikatima i poslovnim certifikatima izdanim Pripadajućim osobama osigurana je vrijednošću atributa *Serial Number* u polju *Subject* certifikata.

U aplikacijskim certifikatima jedinstvenost imena osigurana je vrijednošću atributa *Common Name* u polju *Subject* certifikata na način da naziv aplikacije koji se upisuje u ovo polje mora biti jedinstven unutar istog poslovnog subjekta.

U certifikatima za elektronički pečat *Trusted* liste jedinstvenost imena osigurana je vrijednošću atributa *Serial Number* u polju *Subject* certifikata.

Jedinstvenost razlikovnog imena u Administrativnim certifikatima osigurana je vrijednošću atributa *Serial Number* u polju *Subject* certifikata.

Fina CA kontrolira vrijednost atributa *SerialNumber* u razlikovnom imenu da bi ostvarila jedinstvenost imena subjekata

3.1.6 Prepoznavanje, potvrđivanje identiteta i uloga zaštitnog znaka

U slučaju da Korisnik traži izdavanje certifikata koji sadrži zaštitni znak RA mreža provjerava legitimnu uporabu zaštitnog znaka, te u slučaju utemeljenog prigovora ima pravo opozvati takav certifikat.

U slučaju kada Korisnik traži izdavanje certifikata koji sadrži zaštitni znak RA mreža može tražiti dokaz o registraciji zaštitnog znaka kod nadležnog tijela.

3.2 Inicijalno utvrđivanje identiteta

Provjeru podataka koji se prikupljaju u postupku registracije korisnika Fina provodi njihovom usporedbom s podacima iz dostavljene dokumentacije te ukoliko je primjenjivo korištenjem komunikacijskih kanala sukladno važećoj zakonskoj regulativi.

Pri izdavanju certifikata usklađenih s NCP i NCP+ općim pravilima certificiranja iz opsega ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta Fina provjerava i potvrđuje identitet fizičke osobe temeljem neposredne fizičke identifikacije ili korištenjem metoda koje pružaju jednaku razinu sigurnosti utvrđivanja identiteta.

Pri izdavanju LCP certifikata iz opsega ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta Fina provjerava i potvrđuje identitet Potpisnika postupkom posredne identifikacije temeljem provjere podataka iz prikupljene propisane dokumentacije i preslika identifikacijskih isprava s fotografijom Potpisnika.

3.2.1 Metoda dokazivanja posjeda privatnog ključa

3.2.1.1 Dokazivanje posjeda privatnog ključa za NCP+ tipove certifikata navedene u točki 6.1.1.3.a)

Korisnički par ključeva certifikata iz točke 6.1.1.3.a) ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta generira se unutar sigurnog kriptografskog odnosno QSCD uređaja. Fina podržava generiranje ključeva na sigurnom kriptografskom odnosno QSCD uređaju na lokaciji Fina RA mreže i na korisničkoj lokaciji.

a) Par ključeva generira Fina RA mreža na svojoj lokaciji

Ukoliko se generiranje para ključeva obavlja na lokaciji Fina RA mreže dokazivanje da Potpisnik, Skrbnik, odnosno Ovlašteni predstavnik posjeduje privatni ključ čiji je javni ključ dostavljen na certificiranje osigurava se sljedećim postupkom:

- Generiranje para ključeva na registriranom QSCD uređaju ili sigurnom kriptografskom uređaju, uporabom Fina CMS-a pokreće autenticirani Službenik za registraciju, sukladno postupku opisanom u točki 4.3.1.1.a) ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.
- Javni ključ se PKCS#10 zahtjevom i uporabom sigurnog TLS kanala prosljeđuje u određeni Fina CA na certificiranje, na način koji osigurava da je javni ključ koji se dostavlja na certificiranje iz para ključeva generiranog u registriranom QSCD uređaju, odnosno sigurnom kriptografskom uređaju.
- Nakon izdavanja i preuzimanja certifikata sigurnim TLS kanalom na QSCD uređaju, odnosno sigurnom kriptografskom uređaju Službenik za registraciju, uz neposrednu identifikaciju Potpisnika, Skrbnika ili Ovlaštenog predstavnika, uručuje QSCD uređaj, odnosno sigurni kriptografski uređaj s parom ključeva i certifikatom registriranom Potpisniku, Skrbniku ili Ovlaštenom predstavniku te time Potpisnik, odnosno Ovlašteni predstavnik dolazi u posjed privatnog ključa.

Fina CA prije izdavanja certifikata provjerava izvornost i cjelovitost PKCS#10 zahtjeva verifikacijom potpisa u PKCS#10 zahtjevu te tako utvrđuje da Potpisnik posjeduje pripadajući privatni ključ.

b) Par ključeva generira Potpisnik ili Skrbnik na korisničkoj lokaciji

Ukoliko par ključeva generira Potpisnik, odnosno Skrbnik na korisničkoj lokaciji dokazivanje da Potpisnik, odnosno Skrbnik posjeduje privatni ključ čiji je javni ključ dostavljen na certificiranje osigurava se sljedećim postupkom:

- Generiranje para ključeva na registriranom QSCD uređaju ili sigurnom kriptografskom uređaju sa korisničke lokacije uporabom Fina CMS-a pokreće registrirani i autenticirani Potpisnik, odnosno Skrbnik sukladno postupku opisanom u točki 4.3.1.1.b) ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta,
- Javni ključ se PKCS#10 zahtjevom koji je potpisan pripadajućim privatnim ključem iz generiranog para ključeva uporabom sigurnog TLS kanala prosljeđuje u određeni Fina CA na certificiranje, na način koji osigurava da je javni ključ koji se dostavlja na certificiranje iz para ključeva generiranog u QSCD uređaju ili sigurnom kriptografskom uređaju.
- Fina CA prije izdavanja certifikata verifikacijom potpisa u PKCS#10 zahtjevu utvrđuje da Potpisnik, odnosno Skrbnik posjeduje pripadajući privatni ključ.

Ukoliko se u postupku koristi CMS sustav vanjskog ugovorenog RA, dokazivanje da Potpisnik posjeduje privatni ključ čiji je javni ključ dostavljen na certificiranje osigurava se sljedećim postupkom:

- Generiranje para ključeva na registriranom QSCD uređaju ili sigurnom kriptografskom uređaju sa lokacije poslovnog subjekta uporabom CMS-a vanjskog ugovorenog RA pokreće registrirani i autenticirani Potpisnik, odnosno Skrbnik sukladno postupku opisanom u točki 4.3.1.1.b) ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta,
- Javni ključ se PKCS#10 zahtjevom koji je potpisan pripadajućim privatnim ključem iz generiranog para ključeva uporabom sigurnog TLS kanala vanjski ugovoreni RA prosljeđuje u određeni Fina CA na certificiranje, na način koji osigurava da je javni ključ koji se dostavlja na certificiranje proslijeđen iz vanjskog ugovorenog RA te da je iz para ključeva generiranog u QSCD uređaju ili sigurnom kriptografskom uređaju.
- Fina CA prije izdavanja certifikata verifikacijom potpisa u PKCS#10 zahtjevu utvrđuje da Potpisnik, odnosno Skrbnik posjeduje pripadajući privatni ključ.

3.2.1.2 Dokazivanje posjeda privatnog ključa za NCP+ tip certifikata navedenog u točki 6.1.1.3.b)

Par ključeva za *Aplikacijski certifikat razine 3 (NCP+)* uvijek generira Skrbnik unutar HSM modula na lokaciji poslovnog subjekta. Dokazivanje da Skrbnik posjeduje privatni ključ čiji je javni ključ dostavljen na certificiranje osigurava se sljedećim postupkom:

- Generiranje para ključeva provodi Skrbnik uvijek unutar HSM modula, sukladno certifikacijskoj dokumentaciji HSM modula na lokaciji poslovnog subjekta,

- Javni ključ se PKCS#10 zahtjevom koji je potpisan pripadajućim privatnim ključem iz generiranog para ključeva uporabom sigurnog TLS kanala prosljeđuje u određeni Fina CA na certificiranje. Odgovornost je Skrbnika da je javni ključ koji se dostavlja na certificiranje iz para ključeva generiranog unutar HSM modula.
- Fina CA prije izdavanja certifikata verifikacijom potpisa u PKCS#10 zahtjevu utvrđuje da Skrbnik posjeduje pripadajući privatni ključ.

3.2.1.3 Dokazivanje posjeda privatnog ključa za NCP i LCP tipove certifikata navedenih u točki 6.1.1.4.

Par ključeva za tipove certifikata iz točke 6.1.1.4. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta generira Fina.

Par ključeva za tipove certifikata Aplikacijski certifikat razine 1 i Aplikacijski certifikat razine 2 može generirati Skrbnik na lokaciji poslovnog subjekta.

a) Par ključeva generira Fina

Ukoliko generiranje para ključeva obavlja Fina dokazivanje da Potpisnik, odnosno Skrbnik posjeduje privatni ključ čiji je javni ključ dostavljen na certificiranje osigurava se sljedećim postupkom:

- Generiranje para ključeva putem Fina CMS-a pokreće registrirani i autenticirani Potpisnik, odnosno Skrbnik, sukladno postupku opisanom u točki 4.3.1.3.a) ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta,
- Generiranje para ključeva i izdavanje certifikata u Fini provodi se sukladno točkama 6.1.1.4. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta,
- Potpisnik, odnosno Skrbnik uporabom Fina CMS-a i sigurnog TLS kanala preuzima izdani par ključeva i certifikat u PKCS#12 datoteci zaštićenoj svojim aktivacijskim podatkom i time dolazi u posjed privatnog ključa.

b) Par ključeva generira Skrbnik na lokaciji poslovnog subjekta

Ukoliko par ključeva generira Skrbnik na lokaciji poslovnog subjekta dokazivanje da Skrbnik posjeduje privatni ključ čiji je javni ključ dostavljen na certificiranje osigurava se sljedećim postupkom:

- Skrbnik na lokaciji poslovnog subjekta provodi generiranje para ključeva sukladno točki 6.1.1.4. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.
- Skrbnik na lokaciji poslovnog subjekta izrađuje PKCS#10 zahtjev u kojem se nalazi javni ključ iz generiranog para ključeva, a zahtjev potpisuje privatnim ključem iz istog generiranog para ključeva.
- Registrirani i autenticirani Skrbnik uporabom Fina CMS-a i sigurnog TLS kanala u određeni Fina CA šalje PKCS#10 zahtjev za izdavanje certifikata.
- Fina CA prije izdavanja certifikata verifikacijom potpisa u PKCS#10 zahtjevu utvrđuje da Skrbnik posjeduje pripadajući privatni ključ.

3.2.2 Potvrda identiteta poslovnog subjekta

Podnositelj zahtjeva za izdavanje certifikata navodi točno i cjelovito popunjene podatke o poslovnom subjektu u zahtjevu za izdavanje certifikata, koji mora biti potpisan od strane osobe ovlaštene za zastupanje.

Dodatno, poslovni subjekti, ovisno o važećim zakonima i propisima Republike Hrvatske koji reguliraju obavljanje aktivnosti poslovnog subjekta, prilažu sljedeću dokumentaciju za utvrđivanje pravnog subjektiviteta i identiteta:

- izvornik ili presliku, uz predočenje izvornika, važećeg izvatka, ne starijeg od šest mjeseci, iz nadležnog registra, sukladno zakonima i propisima Republike Hrvatske zbog dokaza upisa u nadležni registar poslovne djelatnosti ili zakon, odnosno drugi propis temeljem kojeg je poslovni subjekt osnovan ako nije određeno da se poslovni subjekt upisuje u registar,

- obavijest Državnog zavoda za statistiku o razvrstavanju prema nacionalnoj klasifikaciji djelatnosti - NKD,

- presliku identifikacijske isprave fizičke osobe ovlaštene za zastupanje poslovnog subjekta.

Obavijest Državnog zavoda za statistiku o razvrstavanju prema nacionalnoj klasifikaciji djelatnosti (NKD) prikuplja se jednokratno, tj. samo prilikom inicijalne registracije poslovnog subjekta.

Za poslovne subjekte osnovane izvan Republike Hrvatske, potrebno je dostaviti odgovarajući ovjereni prijevod važećeg izvatka izdanog od nadležnog tijela u zemlji sjedišta pravnog subjekta.

Po inicijalnom prikupljanju podataka sa zahtjeva i zaprimanju priložene dokumentacije obavlja se identifikacija i potvrda identiteta poslovnog subjekta na sljedeći način:

- provjerava se cjelovitost, autentičnost i valjanost dokumentacije za registriranje poslovnog subjekta,
- provjerava se je li poslovni subjekt upisan u nadležni registar ako je po propisima dužan upisati se u isti, odnosno akt nadležnog organa ili propis o osnivanju poslovnog subjekta, ako poslovni subjekt nije dužan upisati se u registar,
- ako je podnositelj zahtjeva za izdavanje certifikata za TDU u zahtjevu naveo naziv organizacijske jedinice TDU tada se točnost tog naziva organizacijske jedinice provjerava u odnosu na naziv upisan u važećem zakonu odnosno drugom propisu temeljem kojeg je TDU osnovan, a u kojem je određen naziv organizacijske jedinice, ili TDU prilaže izvornik, ili presliku, uz predočenje izvornika, važećeg internog dokumenta, kojim dokazuje postojanje organizacijske jedinice pod tim nazivom,
- RA mreža dodatno provjerava točnost provjerljivih podataka upisanih u zahtjevu. Provjera se provodi temeljem upita na nacionalni OIB sustav kroz Fina RA aplikaciju za podatke koji su dohvatljivi iz OIB sustava,

- provjerava se ovlaštenje osobe ovlaštene za zastupanje poslovnog subjekta i točnost njenih osobnih podataka. Ukoliko ovlaštena osoba za zastupanje ovlasti opunomoćenika, provjerava se dokument punomoći na osnovu potpisa s preslike identifikacijske isprave fizičke osobe ovlaštene za zastupanje, te se provjeravaju podaci opunomoćenika na osnovu dostavljene preslike njegove identifikacijske isprave uz prethodnu provjeru ovlaštenja osobe ovlaštene za zastupanje poslovnog subjekta.

Registracija poslovnog subjekta i identifikacija osobe ovlaštene za zastupanje obavlja se jednokratno, odnosno ne provodi se ukoliko je poslovni subjekt već registriran u RA mreži, a traži certifikat za sljedeću pripadajuću osobu. U tom se slučaju provjerava je li osoba ovlaštena za zastupanje poslovnog subjekta koja je potpisala zahtjev navedena u izvatku iz nadležnog registra kao osoba ovlaštena za zastupanje, te je li pri podnošenju inicijalnog zahtjeva za izdavanje certifikata bila registrirana i provjerena na način opisan u točki 3.2.5. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

U slučaju promjene podataka o poslovnom subjektu sadržanih u certifikatu Korisnik je dužan u roku od sedam dana dostaviti dokaze o promjeni podataka, a Službenik za registraciju, uz prethodnu provjeru, unosi izmjenu podataka o poslovnom subjektu.

U slučaju već registriranog poslovnog subjekta kojem novi zahtjev za izdavanje certifikata ili ugovor potpisuje ovlaštena osoba koja nije registrirana u RA mreži, prilikom podnošenja zahtjeva za izdavanje certifikata nužno je dostaviti novi, valjani izvod iz nadležnog registra kojim se potvrđuju ovlasti navedene osobe ovlaštene za zastupanje, te presliku osobne iskaznice te ovlaštene osobe. Procedura provjere tada je istovjetna inicijalnoj proceduri provjere identiteta poslovnog subjekta. Ukoliko u novom rješenju nadležnog registra, već registrirana ovlaštena osoba više nije navedena, istu Službenik za registraciju briše iz liste registriranih ovlaštenih osoba tog poslovnog subjekta u Fina RA aplikaciji.

U slučaju promjene podataka o poslovnom subjektu koji nisu sadržani u certifikatu podnositelj zahtjeva je dužan dostaviti dokaze o promjeni podataka prilikom predaje slijedećeg zahtjeva za izdavanje ili obnovu certifikata, a Službenik za registraciju, uz prethodnu provjeru, unosi izmjenu podataka o poslovnom subjektu.

Poslovni subjekt odgovara za točnost i ispravnost dostavljenih podataka.

3.2.3 Potvrda identiteta fizičke osobe

Inicijalna identifikacija i potvrđivanje identiteta fizičke osobe provodi se prikupljanjem i provjerom osobnih podataka postupcima neposredne ili posredne identifikacije.

Inicijalnu identifikaciju i potvrđivanje identiteta fizičke osobe u Fina PKI provodi RA mreža.

Za potrebe inicijalne identifikacija i potvrđivanje identiteta fizičke osobe Fina prikuplja i provjerava sljedeće osobne podatke:

- ime i prezime,
- datum, mjesto i zemlja rođenja,

- OIB (ako je OIB dodijeljen),
- podatke o identifikacijskoj ispravi iz točke 3.2.3.3. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta,
- poštansku adresu,
- e-mail adresu,
- broj telefona.

Za izdavanje certifikata koji se izdaju fizičkim osobama povezanim s poslovnim subjektom Fina prikuplja i dokaz o povezanosti fizičke osobe s poslovnim subjektom.

Za izdavanje certifikata za elektroničke pečate Fina prikuplja i dokaz o povezanosti Ovlaštenog predstavnika s pravnom osobom kojoj se izdaje certifikat za elektronički pečat.

Podaci u zahtjevu koje dostavlja Potpisnik, odnosno Ovlašteni predstavnik moraju sadržavati ime i prezime, OIB, broj identifikacijske isprave s datumom do kada isprava vrijedi, državljanstvo i broj telefona ili mobitela. Ukoliko Potpisnik, odnosno Ovlašteni predstavnik traži dostavu aktivacijskih podataka elektroničkom poštom i SMS porukom, zahtjev mora sadržavati i podatke o e-mail adresi i broju mobitela.

Dodatno, za hrvatske državljane, prikupljaju se podaci o datumu i mjestu rođenja, te mjesto prebivališta. Ove dodatni podaci prikupljaju se upitom na nacionalni OIB sustav te ih potpisnik u zahtjevu ne mora unositi.

Identifikacija fizičkih osoba koji su strani državljani se može provesti na dva načina, ovisno o tome je li stranom državljaninu dodijeljen OIB u Republici Hrvatskoj. U slučaju da strani državljanin ima dodijeljen OIB, identifikacija se obavlja na način identičan identifikaciji hrvatskih građana.

Dodatno, za Potpisnike koji su strani državljani, prikupljaju se podaci o datumu i mjestu rođenja, te mjestu prebivališta. Ove dodatne podatke Fina RA mreža prikuplja i provjerava njihovu točnost usporedbom istih u priloženoj dokumentaciji.

Neposredna identifikacija fizičke osobe u svojstvu Potpisnika i Ovlaštenog predstavnika obvezna je u slučajevima podnošenja zahtjeva za inicijalno izdavanje certifikata, izdavanje certifikata nakon njegova isteka te u slučajevima podnošenja zahtjeva za izdavanje certifikata nakon opoziva.

Službenik za registraciju provjerava sve provjerljive podatke iz dokumenata koje prilaže potpisnik i potvrđuje točnost i cjelovitost informacija u zahtjevu za izdavanje certifikata. Službenik za registraciju potpisom na zahtjevu za izdavanje certifikata ovjerava uspješnu i pravilnu identifikaciju potpisnika, odnosno Ovlaštenog predstavnika te podatke upisuje ili ih na zaštićeni način dostavlja u Finin sustav za registraciju korisnika.

3.2.3.1 Postupak neposredne identifikacije

Neposredna identifikacija fizičke osobe provodi se u njenoj fizičkoj prisutnosti temeljem važeće identifikacijske isprave iz točke 3.2.3.3. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

Postupak neposredne identifikacije i potvrde identiteta fizičke osobe se provodi na sljedeći način:

- provjerava se cjelovitost, autentičnost i važenje identifikacijske isprave,
- na temelju provjerene identifikacijske isprave provjerava se cjelovitost i točnost podataka o fizičkoj osobi u zahtjevu za izdavanje certifikata,
- provjerava se identitet fizičke osobe neposrednom identifikacijom licem u lice temeljem identifikacijske isprave i usporedbom sa slikom iz identifikacijske isprave,
- uspoređuje se preslika identifikacijske isprave s originalom u cilju provjere autentičnosti preslike,
- provjerava se točnost podataka o fizičkoj osobi te njen potpis u zahtjevu za izdavanje certifikata s podacima i potpisom iz identifikacijske isprave. Dodatno se obavlja provjera podataka iz važeće identifikacijske isprave upitom na nacionalni OIB sustav, osim za strane državljane koji nemaju dodijeljen OIB u Republici Hrvatskoj.

3.2.3.2 Postupak posredne identifikacije

Postupak posredne identifikacije fizičke osobe provodi se na način koji pruža jednaku razinu sigurnosti utvrđivanja identiteta fizičke osobe kao i postupak neposredne identifikacije.

Fina provodi postupak posredne identifikacije fizičke osobe validacijom kvalificiranog elektroničkog potpisa zasnovanog na kvalificiranom certifikatu izdanom temeljem neposredne identifikacije fizičke osobe.

3.2.3.3 Prihvatljive vrste identifikacijskih isprava

Podnositelji zahtjeva za izdavanje certifikata usklađenih s NCP i NCP+ općim pravilima certificiranja iz opsega ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta te certifikata za elektronički pečat *Trusted* liste dokazuju svoj identitet valjanom osobnom iskaznicom ili putovnicom.

Podnositelji zahtjeva za izdavanje LCP certifikata dokazuju svoj identitet valjanom osobnom iskaznicom, putovnicom, vozačkom dozvolom ili jednakovrijednom identifikacijskom ispravom sa slikom, potpisom i svojim osobnim podacima izdanom od strane nadležnog državnog tijela u zemlji izdavanja isprave, sukladno zakonskoj regulativi te zemlje.

Fizičke osobe koje nemaju osobnu iskaznicu ili putovnicu izdanu u Republici Hrvatskoj svoj identitet dokazuju valjanom identifikacijskom ispravom za ulazak u Republiku Hrvatsku.

Za odobrenje dokazivanja identiteta drugim vrstama identifikacijskih isprava s fotografijom izdanim od nadležnog nacionalnog tijela potrebno je kontaktirati Fina PMA.

3.2.4 Informacije o korisniku koje se ne provjeravaju

Fina ne provjerava telefonski broj za kontakt korisnika u slučajevima podnošenja zahtjeva za izdavanje NCP+ i NCP certifikata.

Napomena! Telefonski brojevi za kontakt provjeravaju se u postupku provjere prikupljene dokumentacije za izdavanje LCP certifikata

Za točnost i cjelovitost informacija o telefonskom broju za kontakt korisnika u slučajevima podnošenja zahtjeva za izdavanje NCP+ i NCP certifikata jamči i odgovara:

- Potpisnik, ukoliko se radi o osobnim certifikatima,
- Pripadajuća osoba i osoba ovlaštena za zastupanje poslovnog subjekta ili TDU, ukoliko se radi o poslovnim certifikatima izdanim Pripadajućim osobama, certifikatima za TDU ili poslovnim certifikatima za IT opremu,
- Autor pečata, ukoliko se radi o certifikatima certifikata za elektronički pečat Trusted liste.

3.2.5 Provjera identiteta ovlaštenih osoba

Prije izdavanja poslovnih certifikata, poslovni certifikati za IT opremu i TDU certifikata provodi se utvrđivanje identiteta osobe ovlaštene za zastupanje provjerom podataka iz dostavljene dokumentacije za utvrđivanje pravnog subjektiviteta poslovnog subjekta navedene u točki 3.2.2. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta, i usporedbom s podacima iz preslike važeće identifikacijske isprave osobe ovlaštene za zastupanje.

Ako je rješenjem o upisu poslovnog subjekta u nadležni registar, odnosno drugog akta u slučajevima kad upis u registar nije propisan, više osoba određeno za samostalno i pojedinačno zastupanje, zahtjev i ugovor potpisuje bilo koja od osoba ovlaštenih za takvo zastupanje.

Ako je više osoba određeno za zajedničko, odnosno skupno zastupanje, zahtjev i ugovor potpisuju osobe ovlaštene za zastupanje sukladno rješenju, odnosno drugom aktu u slučajevima kad upis u registar nije propisan ili jedna ovlaštena osoba za zastupanje uz pisanu suglasnost ostalih osoba koje zajednički ili skupno zastupaju poslovni subjekt.

Službenik za registraciju iz rješenja o upisu u nadležni registar, odnosno drugog akta ako upis u registar nije propisan, utvrđuje je li osoba koja je potpisala zahtjev ili ugovor osoba ovlaštena za zastupanje. U slučaju kada zahtjev ili ugovor potpisuje opunomoćenik ovlaštene osobe, RA mreža iz odgovarajuće punomoći utvrđuje je li osoba koja je potpisala zahtjev ili ugovor opunomoćenik te je li punomoć potpisana od strane osobe ovlaštene za zastupanje.

Službenik za registraciju dužan je utvrditi identitet osobe ovlaštene za zastupanje, odnosno opunomoćenika osobe ovlaštene za zastupanje poslovnog subjekta koja je potpisala zahtjev ili ugovor. Utvrđivanje identiteta osobe ovlaštene za zastupanje, odnosno njenog opunomoćenika, provodi se provjerom podataka iz dostavljene dokumentacije za utvrđivanje pravnog subjektiviteta i identiteta navedene u točki 3.2.2. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta i usporedbom s podacima iz preslike prihvatljive i važeće identifikacijske isprave osobe ovlaštene za zastupanje, odnosno njenog opunomoćenika. Vrste prihvatljivih identifikacijskih isprava navedene su u točki 3.2.3.3. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta. Dodatno, vrši se upit na nacionalni OIB sustav i provjeravaju se svi podaci koje OIB sustav sadrži u odnosu na podatke iz preslike identifikacijske isprave.

Utvrđivanje identiteta opunomoćenika osobe ovlaštene za zastupanje provodi se na jednak način kao i provjera identiteta osobe ovlaštene za zastupanje.

3.2.6 Kriteriji interoperabilnosti

Nema odredbi.

3.3 Identifikacija i potvrđivanje identiteta kod podnošenja zahtjeva za obnovu certifikata uz generiranje novog para ključeva

Fina provodi postupke identifikacije i potvrde identiteta podnositelja zahtjeva za:

- redovnu obnovu certifikata uz generiranje novog para ključeva,
- izdavanje certifikata nakon isteka,
- ponovno izdavanje certifikata nakon opoziva i
- oporavak certifikata.

Ako su od izdavanja certifikata koji je predmet obnove ili ponovnog izdavanja mijenjani pripadajući uvjeti pružanja usluga certificiranja iz točke 9.16. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta, aktualni se uvjeti pružanja usluga certificiranja komuniciraju Potpisniku, Skrbniku, odnosno Ovlaštenom predstavniku koji ih prihvaćaju prije izdavanja certifikata.

3.3.1 Identifikacija i potvrđivanje identiteta kod redovne obnove certifikata uz generiranje novog para ključeva

Redovna obnova certifikata obavlja se pred kraj životnog vijeka certifikata te uključuje postupak generiranja novog para Subjektovih ključeva (vidi točke 4.6. i 4.7. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta).

Certifikat se obnavlja redovnom obnovom ako su zadovoljeni uvjeti iz točke 4.7.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

3.3.1.1 Identifikacija pri podnošenju zahtjeva u RA mreži

Postupak identifikacije i potvrđivanja identiteta podnositelja zahtjeva kod obnove certifikata provodi se na lokaciji RA mreže ili dolaskom Službenika za registraciju na lokaciju Potpisnika, Skrbnika, odnosno Ovlaštenog predstavnika. Postupak identifikacije i potvrđivanja identiteta Potpisnika, Skrbnika, odnosno Ovlaštenog predstavnika provodi se sukladno odredbama točke 3.2.3. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

Provjera poslovnog subjekta provodi se na način da se utvrdi je li došlo do promjena u podacima poslovnog subjekta u odnosu na podatke kojima trenutno raspolaže Fina RA sustav. Ova provjera se obavlja uvidom u podatke iz dostavljenog zahtjeva za izdavanje certifikata i upitom na nacionalni OIB sustav, ukoliko je poslovnom subjektu dodijeljen OIB. Ukoliko se podaci o poslovnom subjektu koji su sadržani u certifikatu razlikuju od važećih podataka u Fina RA sustavu, provodi se postupak izmjene podataka u certifikatu sukladno točki 4.8. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

Ukoliko je zahtjev potpisala osoba ovlaštena za zastupanje koja za taj poslovni subjekt još nije registrirana u Fina RA aplikaciji, obavlja se postupak opisan u točki 3.2.5. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

Fizičkim osobama, koje su u ulozi opunomoćenika Potpisnika, odnosno Ovlaštenog predstavnika dopušteno je podnošenje zahtjeva u postupcima obnove certifikata, uz uvjet da se aktivacijski podaci dostavljaju isključivo Potpisniku, odnosno Ovlaštenom predstavniku na siguran način.

3.3.1.2 Identifikacija pri podnošenju online zahtjeva

Za identifikaciju i potvrđivanje identiteta podnositelja zahtjeva kod redovne obnove certifikata koja se provodi podnošenjem *online* zahtjeva koristiti se dokumentacija i podaci za provjeru identiteta fizičke osobe koji su prikupljeni pri zadnjoj neposrednoj identifikaciji podnositelja zahtjeva u RA mreži sukladno točki 3.3.1.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta, pod uvjetom da od zadnje neposredne identifikacije podnositelja zahtjeva nije prošlo više od šest godina. Skup podataka iz zahtjeva za obnovu certifikata elektronički se potpisuje naprednim elektroničkim potpisom uz korištenje certifikata čija se obnova traži.

Na temelju verifikacije naprednog elektroničkog potpisa u elektroničkom zahtjevu za obnovu certifikata i obavljene provjere podataka iz tog zahtjeva upitom na Fina RA sustav i nacionalni OIB sustav provodi se udaljena identifikacija i potvrđivanje identiteta Potpisnika, odnosno Skrbnika te se omogućuje iniciranje procesa obnove certifikata s generiranjem novog para ključeva.

U suprotnom provodi se postupak sukladno točki 3.3.1.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

3.3.2 Identifikacija i potvrđivanje identiteta korisnika za ponovno izdavanje certifikata nakon opoziva

Identifikacija i potvrđivanje identiteta podnositelja zahtjeva za ponovno izdavanje certifikata nakon opoziva provodi se sukladno proceduri inicijalnog utvrđivanja identiteta iz točke 3.2. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

Po pozitivnoj identifikaciji, potvrdi identiteta i zaprimanju točnog i cjelovitog zahtjeva za izdavanje certifikata, Korisniku se izdaje certifikat čiji su parametri jednaki kao i parametri certifikata na koji se zahtjev odnosi, ali s novim ključem, novim serijskim brojem certifikata, novim vremenskim periodom valjanosti i novim potpisom istog Fina CA.

3.3.3 Identifikacija i potvrđivanje identiteta korisnika za ponovno izdavanje certifikata nakon isteka

Identifikacija i potvrđivanje identiteta podnositelja zahtjeva za ponovno izdavanje certifikata nakon isteka provodi se sukladno proceduri inicijalnog utvrđivanja identiteta iz točke 3.2. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

3.3.4 Identifikacija i potvrđivanje identiteta korisnika za oporavak certifikata

Oporavak certifikata provodi se iz razloga i uz uvjete navedene u točki 4.7.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

Identifikacija i potvrđivanje identiteta podnositelja zahtjeva za oporavak certifikata provodi se sukladno proceduri inicijalnog utvrđivanja identiteta iz točke 3.2. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

3.4 Identifikacija i potvrđivanje identiteta kod zahtjeva za opoziv i suspenziju certifikata

Fina provodi opoziv, suspenziju i reaktivaciju certifikata na temelju podnesenog zahtjeva. Potvrđivanje identiteta podnositelja zahtjeva provodi se kako bi se utvrdio identitet fizičke osobe u svojstvu podnositelja zahtjeva te je li ta osoba ovlaštena za njegovo podnošenje.

3.4.1 Identifikacija i potvrđivanje identiteta podnositelja zahtjeva kod opoziva i suspenzije certifikata

Fina ili vanjski ugovoreni RA provodi identifikaciju i potvrđivanje identiteta podnositelja zahtjeva za opoziv ili suspenziju certifikata ovisno o načinu dostave zahtjeva:

- Osobno podnošenje zahtjeva za opoziv ili suspenziju u registracijskom uredu RA mreže

  Identifikacija i potvrđivanje identiteta provodi se u uredovno vrijeme registracijskih ureda RA mreže na jedan od sljedećih načina:

  - postupkom neposredne identifikacije podnositelja zahtjeva uz predočenje identifikacijske isprave podnositelja zahtjeva iz točke 3.2.3.3. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta, ili
  - usporedbom potpisa podnositelja zahtjeva i podataka na zahtjevu s potpisom i podacima prikupljenih prilikom registracije.
- Podnošenje zahtjeva za opoziv ili suspenziju poštanskom dostavom ili dostavom preko dostavljača

  Identifikacija i potvrđivanje identiteta podnositelja zahtjeva provodi se u registracijskom uredu RA mreže usporedbom potpisa podnositelja zahtjeva i podataka na zahtjevu s potpisom i podacima prikupljenih prilikom registracije.

- Elektronička dostava zahtjeva za opoziv ili suspenziju zaštićenim komunikacijskim kanalom

  Identifikacija i potvrđivanje identiteta podnositelja zahtjeva provodi se verifikacijom i validacijom zahtjeva potpisanog naprednim elektroničkim potpisom, odnosno naprednim elektroničkim pečatom ili jakom autentikacijom podnositelja zahtjeva prilikom elektroničke dostave zahtjeva.

- Podnošenje zahtjeva za opoziv ili suspenziju telefonskim putem

  Identifikacija podnositelja zahtjeva provodi se predstavljanjem podnositelja svojim imenom i prezimenom te navođenjem naziva poslovnog subjekta ukoliko je certifikat

za koji se podnosi zahtjev povezan s poslovnim subjektom. Potvrđivanje identiteta podnositelja zahtjeva provodi se dokazivanjem njegovog poznavanja zaporke za opoziv i suspenziju certifikata. Ovlašteni službenik koji je zaprimio telefonski poziv provjerava istovjetnost zaporke koju izgovara podnositelj zahtjeva i zaporke koja je predana u RA mrežu prilikom podnošenja zahtjeva za izdavanje tog certifikata.

3.4.2 Identifikacija i potvrđivanje identiteta podnositelja zahtjeva kod reaktivacije certifikata

Potvrđivanje identiteta podnositelja zahtjeva provodi se kako bi se utvrdio identitet fizičke osobe u svojstvu podnositelja zahtjeva te je li ta osoba ovlaštena za podnošenje zahtjeva.

Fina ili vanjski ugovoreni RA provodi identifikaciju i potvrđivanje identiteta podnositelja zahtjeva za reaktivaciju certifikata postupkom neposredne identifikacije podnositelja zahtjeva temeljem identifikacijske isprave podnositelja zahtjeva iz točke 3.2.3.3. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta, u uredovno vrijeme registracijskih ureda RA mreže.

4 OPERATIVNI ZAHTJEVI NA ŽIVOTNI CIKLUS CERTIFIKATA

4.1 Podnošenje zahtjeva za izdavanje certifikata

4.1.1 Tko može podnijeti zahtjev za izdavanje certifikata

Zahtjev za izdavanje certifikata, podnose sljedeći subjekti, osim ako im propisi, odnosno akti donijeti temeljem propisa isto priječe.

Zahtjev za izdavanje osobnih certifikata mogu podnijeti fizičke osobe – građani.

Zahtjev za izdavanje poslovnih certifikata podnosi Pripadajuća osoba.

Zahtjev za izdavanje TDU certifikata podnosi Pripadajuća osoba TDU.

Zahtjev za izdavanje aplikacijskih certifikata podnosi Skrbnik.

Zahtjev za izdavanje certifikata za elektronički pečat *Trusted* liste može podnijeti isključivo Ovlašteni predstavnik središnjeg tijela državne uprave nadležnog za poslove gospodarstva.

Administrativni certifikati iz opsega ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta pravila izdaju se isključivo ovlaštenim zaposlenicima Fine.

4.1.2 Postupak prijave korisnika s podnošenjem zahtjeva za izdavanje certifikata i odgovornosti

Za svako izdavanje novog certifikata obvezno je podnošenje zahtjeva za izdavanje certifikata.

Prije inicijalnog izdavanja svakog certifikata Korisnik sklapa s Finom ugovor o obavljanju usluga certificiranja.

U slučaju poslovnih i TDU certifikata ugovor se sastoji od dva dijela:

- dio koji potpisuje osoba ovlaštena za zastupanje poslovnog subjekta,
- dio koji potpisuje fizička osoba, kao Pripadajuća osoba poslovnog subjekta.

U slučaju aplikacijskih certifikata Ugovor potpisuje osoba ovlaštena za zastupanje poslovnog subjekta.

U slučaju certifikata za elektronički pečat *Trusted* liste ugovor potpisuje osoba ovlaštena za zastupanje središnjeg tijela državne uprave nadležnog za poslove gospodarstva.

Zahtjev za izdavanje certifikata, ovisno o tipu certifikata, može se podnijeti u registracijskim uredima Fina RA mreže ili u registracijskim uredima vanjskih RA-ova s kojima je Fina sklopila ugovor o pružanju dijela usluga registracije korisnika.

Zahtjev za izdavanje certifikata može se podnijeti i u elektroničkom obliku ukoliko je to od strane Fine podržano za pojedini tip certifikata.

4.1.2.1 Proces podnošenja zahtjeva za izdavanje certifikata

Zahtjev za izdavanje osobnih certifikata podnosi Fizička osoba – građanin.

Zahtjev za izdavanje poslovnih i TDU certifikata podnosi Pripadajuća osoba.

Zahtjev za izdavanje aplikacijskih certifikata podnosi Skrbnik.

Zahtjev za izdavanje certifikata za elektroničke pečate podnosi Ovlašteni predstavnik.

Zahtjev za izdavanje administrativnih certifikata podnosi zaposlenik Fine.

U slučaju predaje zahtjeva u elektroničkom obliku zahtjev se potpisuje naprednim elektroničkim potpisom.

Zahtjev za izdavanje poslovnih i TDU certifikata te aplikacijskih certifikata dodatno potpisuje osoba ovlaštena za zastupanje poslovnog subjekta.

Ako je rješenjem o upisu poslovnog subjekta u nadležni registar, odnosno drugog akta ako upis u registar nije propisan, više osoba određeno za samostalno i pojedinačno zastupanje, zahtjev potpisuje bilo koja od osoba ovlaštenih za takvo zastupanje.

Pravila za potpisivanje zahtjeva za izdavanje certifikata od strane osobe ovlaštene za zastupanje jednaka su za potpisivanje zahtjeva u papirnatom obliku kao i za potpisivanje zahtjeva u elektroničkom obliku. Ova pravila su navedena u točki 3.2.5. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

Po zaprimanju i provjeri podataka iz zahtjeva, zahtjev potpisuje i Službenik za registraciju u RA mreži te na zahtjev upisuje datum njegova zaprimanja. Time potvrđuje da je podneseni zahtjev ispravno ispunjen i potpisan te da je prihvaćen od strane Službenika za registraciju u RA mreži.

U slučaju da je zahtjev za izdavanje certifikata predan u elektroničkom obliku, Finin servis za zaprimanje elektroničkih obrazaca zahtjeva provjerava zahtjev i dodaje vremenski žig s vremenom zaprimanja zahtjeva. Službenik za registraciju u RA mreži provjerava podatke iz zahtjeva, te provodi validaciju svih naprednih elektroničkih potpisa na zahtjevu. Po pozitivnoj provjeri elektroničkog zahtjeva, isti se upisuje u RA aplikaciju.

Identifikacija i potvrđivanje identiteta podnositelja zahtjeva provodi se na način opisan u točki 3.2. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

4.1.2.2 Odgovornosti i obveze u procesu podnošenja zahtjeva za izdavanje certifikata

Korisnici s Finom sklapaju ugovor o obavljanju usluga certificiranja kojim prihvaćaju Opća pravila i uvjete pružanja usluga certificiranja.

Potpisivanje ugovora na strani Korisnika obavlja se na isti način kao i potpisivanje zahtjeva za izdavanje certifikata, a koje je opisano u točki 4.1.2.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

Prije početka pružanja usluga certificiranja iz ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta pojedinom tijelu državne uprave Fina ugovara poslovni odnos s TDU zaključivanjem posebnog ugovora o obavljanju usluga certificiranja.

U procesu podnošenja zahtjeva za izdavanje certifikata podnositelji trebaju podnijeti točno i cjelovito ispunjen te pravilno potpisan zahtjev za izdavanje certifikata, a dokumentacija koju prilažu ili dostavljaju treba biti točna i cjelovita te valjana u trenutku podnošenja zahtjeva.

Obaveze i odgovornosti Korisnika navedene su u Poglavlju 9.6.3. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

Obaveze i odgovornosti RA mreže navedene su u Poglavlju 9.6.2. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

Obaveze i odgovornosti Fine, kao pružatelja usluga povjerenja, navedene su u Poglavlju 9.6.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

4.2 Obrada zahtjeva za izdavanje certifikata

4.2.1 Provedba identifikacije i potvrđivanje identiteta

Identifikacija i potvrđivanje identiteta fizičkih osoba i poslovnog subjekta iz zahtjeva provodi se sukladno Poglavlju 3. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

Pri preuzimanju zahtjeva za izdavanje certifikata Službenik za registraciju u RA mreži provodi sljedeći postupak:

- Nakon zaprimanja zahtjeva za izdavanje certifikata na kojem je označeno izdavanje nekvalificiranog certifikata, Službenik za registraciju pregledava zaprimljeni zahtjev zbog kontrole, sukladno postupcima opisanim u točkama 3.2.2., 3.2.3. i 3.2.5. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.
- Ako zahtjev nije točno i u cijelosti popunjen te pravilno potpisan Službenik za registraciju mora odbiti takav zahtjev sukladno točki 4.2.2. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta i podnositelju zahtjeva pojasniti način ispravnog i točnog popunjavanja i potpisivanja zahtjeva.
- Ako je zaprimljen zahtjev za izdavanje poslovnog certifikata ili certifikata za TDU, Službenik za registraciju provjerava je li poslovni subjekt podnositelja već registriran. Ako zapis o registraciji poslovnog subjekta ne postoji u Fina RA sustavu, upisom podataka iz zahtjeva i dostavljene dokumentacije uporabom Fina RA aplikacije i provjerom podataka upitom na nacionalni OIB sustav (ukoliko je primjenjivo), izrađuju se zapisi o registraciji poslovnog subjekta,
- Službenik za registraciju provjerava je li Potpisnik, odnosno Skrbnik ili Ovlašteni predstavnik naveden u zahtjevu već registriran. Ako zapis o registraciji Potpisnika,

odnosno Skrbnika ili Ovlaštenog predstavnika ne postoji u RA sustavu, upisom podataka iz zahtjeva i dostavljene dokumentacije uporabom Fina RA aplikacije i provjerom podataka upitom na nacionalni OIB sustav (ukoliko je primjenjivo), izrađuju se zapisi o registraciji Potpisnika, odnosno Skrbnika ili Ovlaštenog predstavnika.

- Službenik u Fina RA mreži postavlja status zahtjeva na „pripremljeno“ čime se u Fina RA aplikaciji naznačuje odobrenje zahtjeva. Tom prilikom generira se i razlikovno ime (*Distinguished Name*, DN) subjekta.
- Službenik za registraciju putem Fina RA aplikacije svojim certifikatom elektronički potpisuje narudžbu koja sadrži provjerene podatke iz zahtjeva te narudžbu prosljeđuje na daljnju obradu u Fina CA.

4.2.2 Odobravanje ili odbijanje zahtjeva za izdavanje certifikata

Službenik za registraciju u RA mreži provjerava podatke iz dokumenata koje prilaže podnositelj zahtjeva i potvrđuje točnost i cjelovitost informacija u zahtjevu za izdavanje certifikata. Službenik za registraciju u Fina LRA potpisom ovjerava uspješnu i pravilnu identifikaciju podnositelja zahtjeva te zaštićenim putem dostavlja podatke u Fina CA.

Odobravanje ili odbijanje zahtjeva za uslugu izdavanja certifikata provodi Službenik za registraciju u registracijskom uredu RA mreže u kojem je Korisnik podnio zahtjev.

Ukoliko Službenik za registraciju odbije zahtjev za izdavanje certifikata, pismenim ili usmenim putem obavještava podnositelja o odbijanju zahtjeva i razlozima odbijanja istog. Ukoliko je podnositelj zahtjeva fizički prisutan u uredu RA mreže, podnositelj se obavještava usmenim putem. Ukoliko podnositelj nije fizički prisutan u uredu RA mreže, obavještava se telefonskim pozivom ili porukom na e-mail adresu iz zahtjeva.

Zahtjev za izdavanje certifikata može se odbiti zbog:

- netočnih ili nepotpunih podataka,
- nepravilno potpisanog zahtjeva, odnosno ugovora,
- nepotpune ili neispravne priložene dokumentacije,
- prethodnih neodgovarajućih postupaka i nepoštivanja ugovornih obveza korisnika,
- zakonske zabrane.

4.2.3 Vrijeme obrade zahtjeva za izdavanje certifikata

U redovnim okolnostima vrijeme obrade zahtjeva za izdavanje certifikata je do pet radnih dana od primitka zahtjeva u RA mreži.

Ako podnositelj zahtjeva ne kompletira dokumentaciju za izdavanje certifikata u roku od 60 dana od dana podnošenja zahtjeva tada se smatra da je odustao od zahtjeva za izdavanje certifikata.

4.3 Izdavanje certifikata

Fina CA izdaje certifikat nakon provedenih svih procesa provjere podataka, odobrenja zahtjeva za izdavanje certifikata od strane Službenika za registraciju te prihvaćanja certifikata od strane Potpisnika, Skrbnika,odnosno Ovlaštenog predstavnika. Izdavanje certifikata provodi se na siguran način kako bi se osigurala autentičnost certifikata. Iz tog razloga Fina ima implementirane mjere kojima se sprječava krivotvorenje certifikata.

Mjere protiv krivotvorenja certifikata uključuju:

- korištenje propisanih algoritama i parametara te mjera zaštite privatnih ključeva,
- korištenje propisanih metoda dokazivanja posjeda privatnih korisničkih ključeva,
- sprječavanje fizičkog i logičkog (online) pristupa sustavu za izdavanje certifikata od strane neovlaštenih osoba,
- provjeru cjelovitosti kritičnih komponenti sustava,
- zaštitu računalne mreže,
- implementaciju i odvajanjem povjerljivih uloga.

4.3.1 Postupci CA tijekom izdavanja certifikata

4.3.1.1 Izdavanje NCP+ tipova certifikata navedenih u točki 6.1.1.3.a)

Službenik za registraciju u Središnjem Fina RA uporabom Fina CMS-a registrira sve QSCD uređaje.

Za tipove osobnih i poslovnih nekvalificiranih certifikata iz točke 6.1.1.3. a) koji se izdaju na sigurnom kriptografskom, odnosno QSCD uređaju provode se postupci opisani niže u stavkama a) i b). Za *Certifikat za potpis Trusted liste (NCP+)* i *Administrativni N2 certifikat (NCP+)* provodi se samo postupak naveden niže u stavci a).

a) Par ključeva generira Fina RA mreža na svojoj lokaciji

Izdavanje nekvalificiranih certifikata navedenih u točki 6.1.1.3.a) ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta kada par ključeva generira Fina RA mreža provodi se sljedećim postupkom:

- po primitku narudžbe za izdavanje certifikata iz RA aplikacije, Službenik za registraciju povezuje registrirani QSCD uređaj, odnosno sigurni kriptografski uređaj u Fina CMS sustavu s Potpisnikom, Skrbnikom, odnosno Ovlaštenim predstavnikom navedenim u narudžbi, a koji je registriran u bazi registriranih korisnika.
- Službenik za registraciju u Fina CMS sustavu generira PIN za aktivaciju privatnog ključa povezanog s nekvalificiranim certifikatom te pripadajući PUK.
- Službenik za registraciju kroz Fina CMS pokreće generiranje para ključeva u registriranom QSCD uređaju, odnosno u sigurnom kriptografskom uređaju. U slučaju korištenja QSCD uređaja Fina CMS pri tom koristi mehanizme identifikacije registriranog QSCD uređaja.
- javni ključ se u sklopu PKCS#10 zahtjeva prosljeđuje u određeni Fina CA na certificiranje te se osigurava da je javni ključ koji se dostavlja na certificiranje iz para

ključeva generiranog u registriranom uređaju. U slučaju korištenja QSCD uređaja koriste se mehanizmi svojstveni QSCD uređaju koji osigurava da je javni ključ koji se dostavlja na certificiranje iz para ključeva generiranog u registriranom QSCD uređaju.

- Fina CA certificira javni ključ izdajući korisniku certifikat prema odgovarajućem profilu,
- Fina CMS upisuje nekvalificirani certifikat u odgovarajući QSCD uređaj, odnosno sigurni kriptografski uređaj.
- QSCD uređaj, odnosno sigurni kriptografski uređaj s pripadajućim parom ključeva i certifikatom Službenik za registraciju uručuje Potpisniku, Skrbniku, odnosno Ovlaštenom predstavniku uz njegovu neposrednu identifikaciju,
- enkriptirani PIN i PUK povezani s privatnim ključem nekvalificiranog certifikata na QSCD uređaju, odnosno sigurnog kriptografskog uređaju dostavljaju se Potpisniku, Skrbniku, odnosno Ovlaštenom predstavniku putem e-mail poruke ili ga Službenik za registraciju uručuje Potpisniku, Skrbniku , odnosno Ovlaštenom predstavniku pri neposrednoj identifikaciji u Fina RA mreži ili se Potpisniku, Skrbniku, odnosno Ovlaštenom predstavniku dostavljaju preporučenom poštanskom pošiljkom.

b) Par ključeva generira Potpisnik ili Skrbnik na korisničkoj lokaciji

Izdavanje nekvalificiranih certifikata navedenih u točki 6.1.1.3.a) ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta kada par ključeva generira Potpisnik ili Skrbnik na korisničkoj lokaciji provodi se niže opisanom postupkom. Iznimno, ukoliko vanjski ugovoreni RA koristi vlastiti CMS sustav u niže opisanom postupku se umjesto CMS-a Fine koristi CMS vanjskog ugovorenog RA.

- po primitku narudžbe za izdavanje certifikata iz RA aplikacije, Službenik za registraciju povezuje registrirani QSCD uređaj, odnosno sigurni kriptografski uređaj u Fina CMS sustavu s Potpisnikom, odnosno Skrbnikom navedenim u narudžbi, a koji je registriran u bazi registriranih korisnika.
- Službenik za registraciju u Fina CMS sustavu generira PIN za aktivaciju privatnog ključa povezanog s certifikatom te pripadajući PUK.
- Službenik za registraciju QSCD uređaj, odnosno sigurni kriptografski uređaj bez generiranih ključeva i certifikata u uručuje Potpisniku, odnosno Skrbniku uz njegovu neposrednu identifikaciju.
- enkriptirani podaci za autentikaciju Potpisnika, odnosno Skrbnika te enkriptirani PIN i PUK povezani s privatnim ključem nekvalificiranog certifikata na QSCD uređaju, odnosno sigurnom kriptografskom uređaju dostavljaju se Potpisniku, odnosno Skrbniku putem e-mail poruke ili ih Službenik za registraciju uručuje Potpisniku, odnosno Skrbniku pri neposrednoj identifikaciji u Fina RA mreži ili se Potpisniku, odnosno Skrbniku dostavljaju preporučenom poštanskom pošiljkom.
- po udaljenom pristupu Fina CMS-u s korisničke lokacije, autentikaciji Potpisnika, odnosno Skrbnika te iniciranju postupka uporabom Fina CMS sustava, Fina CMS sustav inicira postupak generiranja korisničkih ključeva u potpisnikovom QSCD uređaju, odnosno sigurnom kriptografskom uređaju te pri tom Fina CMS koristi mehanizme identifikacije uređaja. U slučaju korištenja QSCD uređaja koriste se mehanizmi identifikacije registriranog QSCD uređaja.

- javni ključ se u sklopu PKCS#10 zahtjeva prosljeđuje u određeni Fina CA na certificiranje korištenjem mehanizmima koji osigurava da je javni ključ koji se dostavlja na certificiranje iz para ključeva generiranog u uređaju. U slučaju korištenja QSCD uređaja koriste se mehanizmi svojstveni QSCD uređaju koji osigurava da je javni ključ koji se dostavlja na certificiranje iz para ključeva generiranog u registriranom QSCD uređaju.
- Fina CA certificira javni ključ izdajući korisniku certifikat prema odgovarajućem profilu,
- Fina CMS upisuje nekvalificirani certifikat u odgovarajući QSCD uređaj, odnosno sigurni kriptografski uređaj.

Ako su Potpisnik ili Skrbnik registrirani putem vanjskog ugovorenog RA, Službenik za registraciju provodi postupak na lokaciji vanjskog ugovorenog RA.

Iznimno, ukoliko vanjski ugovoreni RA koristi vlastiti CMS sustav, vanjski ugovoreni RA je u slučaju korištenja QSCD uređaja obavezan provoditi kontrole svojstvene QSCD uređaju da je par ključeva generiran na identificiranom i registriranom QSCD uređaju te da je javni ključ koji se dostavlja na certificiranje iz para ključeva generiranog na tom QSCD uređaju.

4.3.1.2 Izdavanje NCP+ tipa certifikata navedenog u točki 6.1.1.3.b)

Izdavanje certifikata tipa *Aplikacijski certifikat razine 3 (NCP+)* provodi se sljedećim postupkom:

- nakon potvrde narudžbe za izdavanje certifikata iz RA aplikacije od strane Službenika za registraciju Fina CMS sustav generira i dostavlja autentikacijske podatke za prijavu Skrbnika na Fina CMS,
- autentikacijski podaci za prijavu Skrbnika dostavljaju se elektronički korištenjem dva odvojena kanala ili ove podatke Skrbniku Službenik za registraciju uručuje osobno, uz prethodnu neposrednu identifikaciju,
- Skrbnik na korisničkoj lokaciji provodi generiranje para ključeva unutar HSM modula, sukladno točki 6.1.1.3.b) ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta,
- Skrbnik na korisničkoj lokaciji izrađuje PKCS#10 zahtjev u kojem se nalazi javni ključ iz generiranog para ključeva, a zahtjev potpisuje privatnim ključem u HSM modulu iz istog generiranog para ključeva,
- Skrbnik uporabom Fina CMS-a i sigurnog TLS kanala u određeni Fina CA šalje PKCS#10 zahtjev za izdavanje certifikata,
- Fina CA certificira javni ključ izdajući korisniku certifikat,
- Skrbnik preuzima izdani certifikat putem Fina CMS sustava.

4.3.1.3 Izdavanje NCP i LCP tipova certifikata navedenih u točki 6.1.1.4.

Za tipove nekvalificiranih certifikata iz točke 6.1.1.4. provodi se samo postupak opisan niže u stavci a). Za Aplikacijski certifikat razine 1 (NCP) i Aplikacijski certifikat razine 2 (NCP) provode se postupci navedeni niže u stavkama a) i b).

a) Par ključeva generira Fina

Izdavanje nekvalificiranih certifikata navedenih u točki 6.1.1.4. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta kada par ključeva generira Fina provodi se sljedećim postupkom:

- nakon potvrde narudžbe za izdavanje certifikata iz RA aplikacije od strane Službenika za registraciju Fina CMS sustav generira i dostavlja autentikacijske podatke za prijavu Potpisnika, odnosno Skrbnika na Fina CMS,
- autentikacijski podaci za prijavu Potpisniku, odnosno Skrbniku dostavljaju se elektronički korištenjem dva odvojena kanala ili ove podatke Potpisniku, odnosno Skrbniku Službenik za registraciju uručuje osobno, uz prethodnu neposrednu identifikaciju,
- po udaljenom pristupu Fina CMS-u s korisničke lokacije, autentikaciji Potpisnika, odnosno Skrbnika te iniciranju postupka uporabom Fina CMS sustava, Fina CMS sustav generira par korisničkih ključeva te se zahtjev za izdavanje certifikata dostavlja u odgovarajući Fina CA,
- Fina CA certificira javni ključ izdajući Potpisniku, odnosno Skrbniku certifikat prema odgovarajućem profilu,
- Potpisnik, odnosno Skrbnik uporabom Fina CMS-a upisuje aktivacijski podatak za zaštitu privatnog ključa,
- Fina CMS Potpisniku, odnosno Skrbniku dostavlja privatni ključ i certifikat u PKCS#12 datoteci zaštićenoj aktivacijskim podatkom.

b) Par ključeva generira Skrbnik na korisničkoj lokaciji

Izdavanje tipova certifikata Aplikacijski certifikat razine 1 (NCP) i Aplikacijski certifikat razine 2 (NCP) kada par ključeva generira Skrbnik na korisničkoj lokaciji provodi se sljedećim postupkom:

- nakon potvrde narudžbe za izdavanje certifikata iz RA aplikacije od strane Službenika za registraciju Fina CMS sustav generira i dostavlja autentikacijske podatke za prijavu Skrbnika na Fina CMS,
- autentikacijski podaci za prijavu Skrbnika dostavljaju se elektronički korištenjem dva odvojena kanala ili ove podatke Skrbniku Službenik za registraciju uručuje osobno, uz prethodnu neposrednu identifikaciju,
- Skrbnik na korisničkoj lokaciji provodi generiranje para ključeva sukladno točki 6.1.1.4. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta,
- Skrbnik na korisničkoj lokaciji izrađuje PKCS#10 zahtjev u kojem se nalazi javni ključ iz generiranog para ključeva, a zahtjev potpisuje privatnim ključem iz istog generiranog para ključeva,
- Skrbnik uporabom Fina CMS-a i sigurnog TLS kanala u određeni Fina CA šalje PKCS#10 zahtjev za izdavanje certifikata,
- Fina CA certificira javni ključ izdajući korisniku certifikat prema odgovarajućem profilu,
- Skrbnik preuzima izdani certifikat putem Fina CMS sustava.

4.3.2 Obavještavanje korisnika od strane CA o izdavanju certifikata

Potpisnik, Skrbnik, odnosno Ovlašteni predstavnik obavještava se o mogućnosti preuzimanja certifikata telefonom, putem e-maila ili poštom.

Potpisnika, Skrbnika, odnosno Ovlaštenog predstavnika o mogućnosti preuzimanja certifikata, Službenik za registraciju obavještava telefonski. U slučaju da Službenik za registraciju nije uspio telefonski obavijestiti Potpisnika, Skrbnika, odnosno Ovlaštenog predstavnika Službenik za registraciju im obavijest šalje e-mailom. Ukoliko Potpisnik, Skrbnik, odnosno Ovlašteni predstavnik nije u zahtjevu za izdavanje certifikata naveo e-mail adresu, obavijest za preuzimanje certifikata dostavlja se poštom.

Ako Potpisnik, odnosno Skrbnik preuzima certifikat *online*, tada je isti obaviješten o izdavanju certifikata tijekom samog *online* postupka preuzimanja certifikata.

Ako Potpisnik, Skrbnik, odnosno Ovlašteni predstavnik osobno u RA mreži preuzima ključeve i certifikat na sigurnom kriptografskom, odnosno QSCD uređaju, tada je isti obaviješten o izdavanju certifikata od strane Službenika za registraciju u RA mreži.

4.4 Prihvaćanje certifikata

Prihvaćanje certifikata od strane Potpisnika, Skrbnika, odnosno Ovlaštenog predstavnika preduvjet je za izdavanje i korištenje certifikata.

Prihvaćajući certifikat Potpisnik, Skrbnik, odnosno Ovlašteni predstavnika prihvaćaju da su sve informacije koje će biti sadržane u certifikatu točne u trenutku njegova prihvaćanja.

4.4.1 Provedba prihvaćanja certifikata

Potpisnik, Skrbnik, odnosno Ovlašteni predstavnik neposredno prije izdavanja certifikata provodi provjeru sadržaja certifikata. Provjera sadržaja certifikata obavlja se uvidom u sadržaje polja *Subject* i *Issuer*, uvidom u sadržaj ekstenzije *Subject Alternative Name* te uvidom u detaljan opis profila tipa certifikata čije se izdavanje traži. Ukoliko Potpisnik, Skrbnik, odnosno Ovlašteni predstavnik prihvaća prikazani sadržaj certifikata, svoje prihvaćanje potvrđuje potpisom izjave o prihvaćanju certifikata ili označavanjem prihvaćanja certifikata na ekranu CMS sučelja, uz prethodnu autentikaciju na CMS sustav.

Nakon prihvaćanja certifikata odgovarajući Fina CA Potpisniku, Skrbniku, odnosno Ovlaštenom predstavniku izdaje traženi certifikat.

Fina osigurava da izdani certifikat sadrži iste informacije koje je Potpisnik, Skrbnik, odnosno Ovlašteni predstavnik, prije izdavanja tog certifikata, prihvatio primjenom sljedećih mjera:

- ispisivanjem, odnosno prikazivanjem podataka certifikata izravnim dohvatom prethodno provjerenih podataka korisnika iz Finine baze registriranih korisnika,
- korištenjem sigurnih komunikacijskih kanala za dohvat korisničkih podataka za njihov ispis i prikaz Potpisniku, Skrbniku, odnosno Ovlaštenom predstavniku te za dohvat javno objavljenog dokumenta s detaljnim opisom odobrenih profila certifikata,

- izdavanjem certifikata isključivo prema odobrenom profilu certifikata koji je naveden u izjavi o prihvaćanju, a koji je kao odobreni profil certifikata definiran i podešen u sustavu odgovarajućeg Fina CA,
- primjenom mjera protiv krivotvorenja certifikata iz točke 4.3.

Ukoliko Potpisnik, odnosno Ovlašteni predstavnik ne prihvaća certifikat, razloge svog neprihvaćanja može obrazložiti u registracijskom uredu RA mreže ili ih pismeno navesti i poslati u Finu na e-mail adresu info.rdc@fina.hr. RA mreža pri tome prosljeđuje obavijest o neprihvaćanju i eventualnim razlozima neprihvaćanja u Središnji RA. Neprihvaćanjem certifikata Potpisnik, Skrbnik, odnosno Ovlašteni predstavnik odustaje od zahtjeva za izdavanjem certifikata, a Fina CA ne izdaje certifikat koji se odnosi na taj zahtjev.

Fina Potpisniku, Škrbniku, odnosno Ovlaštenom predstavniku omogućuje podnošenja novog zahtjeva za izdavanje certifikata u kojem su, po potrebi, uneseni korigirani podaci u odnosu na prethodni zahtjev.

4.4.2 Objava certifikata od strane CA

Ukoliko su Potpisnik, Skrbnik, odnosno Ovlašteni predstavnik te osoba ovlaštena za zastupanje poslovnog subjekta odobrili javnu objavu certifikata Fina CA čini certifikat dostupnim na Fina PKI repozitoriju.

Suglasnost za javnu objavu certifikata u Fina PKI repozitoriju daje se prilikom sklapanja ugovora o pružanju usluga certificiranja.

Certifikat je pouzdajućim stranama dostupan preko sučelja na internetskoj stranici repozitorija iz točke 2.2.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

4.4.3 Obavještavanje drugih strana od strane CA o izdavanju certifikata

Podrazumijeva se da su druge strane obaviještene o izdavanju certifikata njegovom dostupnošću za preuzimanje u Fina PKI repozitoriju.

4.5 Par ključeva i korištenje certifikata

4.5.1 Korištenje privatnog ključa i certifikata od strane korisnika

U slučajevima kada je Korisnik u posjedu para ključeva i njima upravlja tada se Korisnik obvezuje:

- pri generiranju parova ključeva iz točke 6.1.1.3 i 6.1.1.4., u slučaju da ih generira Korisnik, koristiti algoritme propisane normizacijskim dokumentom ETSI TS 119 312 [14] te duljine ključeva sukladno točke 6.1.5. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta,
- koristiti certifikat i pripadajući privatni ključ samo u svrhe propisane ovim $CPS_{NQC\text{-}eIDAS}$ dokumentom i uvjetima pružanja usluga certificiranja,

- koristiti i čuvati privatni ključ na način koji onemogućuje njegovo neovlašteno korištenje,
- kod korištenja tipova certifikata iz točke 6.1.1.3. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta pripadajući privatni ključ koristiti uporabom QSCD uređaja, sigurnog kriptografskog uređaja, odnosno HSM modula,
- kod korištenja tipova certifikata iz točke 6.1.1.4. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta pravila pripadajući privatni ključ koristiti uz aktiviranje privatnog ključa prikladnim aktivacijskim podacima,
- koristiti Subjektov par ključeva sukladno pravilima određenim u točki 1.4.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta,
- da od trenutka kad je privatni ključ u jedinstvenom posjedu Potpisnika, odnosno poslovnog subjekta štiti privatni ključ od krađe, gubitka, izmjena, kompromitiranja i neovlaštene uporabe,
- na čuvanje aktivacijskih podatka privatnog ključa na zaštićenom mjestu odvojenom od privatnog ključa,
- na obavještavanje Fine kao pružatelja usluga povjerenja i zahtijevanje suspenzije ili opoziva certifikata u slučajevima:
  - da je privatni ključ Potpisnika, odnosno poslovnog subjekta izgubljen, ukraden ili postoji sumnja u bilo kakvo kompromitiranje privatnog ključa,
  - kada Potpisnik, odnosno poslovni subjekt više nije u jedinstvenom posjedu privatnog ključa, tj. kada se sumnja u kompromitiranost aktivacijskih podataka,
  - da su podaci sadržani u certifikatu netočni,
- nakon kompromitiranja privatnog ključa odmah i trajno prestati s njegovom uporabom.

4.5.2 Korištenje javnog ključa i certifikata od strane pouzdajuće strane

Pouzdajuća strana koja namjerava ostvariti pouzdanje u certifikat izdan prema ovom $CPS_{NQC\text{-}eIDAS}$ dokumentu treba:

- voditi računa o primjerenoj uporabi i ograničenjima uporabe certifikata koja su naznačena u certifikatu ili na njih upućuju reference u certifikatu,
- voditi računa o primjerenoj uporabi i zabrani uporabe javnog ključa i certifikata opisanim u točki 1.4. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta,
- provjeriti da su svi podaci o identitetu subjekta u certifikatu ispravno prikazani aplikacijom u koju se može pouzdati,
- u slučaju validacije elektroničkog potpisa, odnosno elektroničkog pečata provjeriti da je elektronički potpis, odnosno elektronički pečat izrađen privatnim ključem koji odgovara javnom ključu u certifikatu,
- obaviti provjeru roka važenja svih certifikata u certifikacijskom lancu te provesti provjeru certifikata prema postupcima za validaciju certifikacijske staze, sukladno dokumentu IETF RFC 5280 [21],
- obaviti provjeru statusa opozvanosti i suspendiranosti certifikata uporabom aktualnih informacija o tim statusima na način opisan u točki 4.10.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

Pouzdanjem u tako istekli, opozvani ili suspendirani certifikat pouzdajuća strana gubi jamstva dobivena od Fine kao davatelja usluge certificiranja.

4.6 Obnova certifikata

Svaka obnova certifikata u Fina PKI podrazumijeva izdavanje certifikata s novim parom ključeva istom Subjektu certificiranja.

Fina provodi obnovu certifikata na način da za postojećeg Potpisnika, odnosno poslovni subjekt čiji je certifikat pred istekom, na zahtjev Potpisnika, odnosno poslovnog subjekta generira novi par ključeva i izdaje novi certifikat. Razlikovno ime (DN) subjekta novog certifikata jednako je razlikovnom imenu (DN-u) subjekta certifikata koji je pred istekom.

Postupak obnove certifikata opisan je u točki 4.7. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

4.6.1 Razlozi za obnovu certifikata

Vidi točku 4.7.1.

4.6.2 Tko može tražiti obnovu certifikata

Vidi točku 4.7.2.

4.6.3 Obrada zahtjeva za obnovu certifikata

Vidi točku 4.7.3.

4.6.4 Obavještavanje korisnika o obnovi certifikata

Vidi točku 4.7.4.

4.6.5 Provedba prihvaćanja obnovljenog certifikata

Vidi točku 4.7.5.

4.6.6 Objava obnovljenog certifikata od strane CA

Vidi točku 4.7.6.

4.6.7 Obavještavanje drugih strana o obnovi certifikata

Vidi točku 4.7.7.

4.7 Obnova certifikata uz generiranje novog para ključeva

Nakon provedene identifikacije i potvrde identiteta podnositelja zahtjeva za:

- redovnu obnovu certifikata uz generiranje novog para ključeva,
- izdavanje certifikata nakon isteka,
- ponovno izdavanje certifikata nakon opoziva i
- oporavak certifikata

Fina izdaje certifikat čiji je razlikovno ime (DN) i drugi parametri jednaki kao i parametri certifikata na koji se zahtjev odnosi, ali s novim javnim ključem, novim serijskim brojem certifikata, novim vremenskim periodom valjanosti i novim potpisom istog Fina CA.

4.7.1 Razlozi za obnovu certifikata uz generiranje novog para ključeva

Redovna obnova certifikata uz generiranje novog para ključeva provodi se ukoliko Korisniku uskoro ističe certifikat, a Korisnik ima namjeru i dalje koristiti uslugu. Certifikat se obnavlja na ovaj način ako su zadovoljeni svi sljedeći uvjeti:

- certifikatu nije istekao period važenja i certifikat ističe kroz period kraći od 45 dana,
- certifikat nije opozvan ili suspendiran,
- podaci o Subjektu i drugi atributi sadržani u certifikatu su točni i cjeloviti u trenutku podnošenja zahtjeva za redovnu obnovu certifikata.

Oporavak certifikata provodi se u slučaju kvara na sigurnom kriptografskom uređaju, QSCD uređaju, korisničkom HSM modulu, u slučaju brisanja ili uništenja privatnog ključa Korisnika ili kada Korisnik iz nekog drugog razloga više ne može koristiti privatni ključ koji je povezan s javnim ključem u certifikatu, a provodi se prije nastupanja rokova za obnovu certifikata.

Uvjet za podnošenje zahtjeva za oporavak certifikata je da je certifikat važeći, tj. da nije istekao, nije opozvan ni suspendiran te da ne postoji potreba za promjenom korisničkih podataka u certifikatu.

Ukoliko je nastupio period u kojem je moguće zatražiti redovnu obnovu certifikata (45 dana prije datuma isteka valjanosti certifikata), nije moguće zatražiti oporavak certifikata, već korisnik treba zatražiti obnovu certifikata kroz zahtjev za izdavanje certifikata.

U postupku oporavka Fina CA će opozvati certifikat čiji se oporavak traži te će izdati novi certifikat.

Izdavanje certifikata nakon isteka provodi se ukoliko je Korisniku istekao certifikat, a Korisnik ima namjeru i dalje koristiti uslugu. Izdavanje certifikata nakon isteka ne smatra se obnovom postojećeg isteklog certifikata.

Uvjet za takvo izdavanje certifikata je da se podaci Korisnika sadržani u certifikatu nisu u međuvremenu promijenili.

Izdavanje certifikata nakon isteka ne smatra se obnovom postojećeg isteklog certifikata.

U postupku izdavanja certifikata nakon isteka perioda valjanosti podnositelj zahtjeva obvezno dostavlja svu dokumentaciju kao za inicijalno izdavanje certifikata.

4.7.2 Tko može zatražiti certificiranje novog javnog ključa

Zahtjev za obnovu, oporavak, odnosno izdavanje certifikata nakon isteka mogu podnijeti isti subjekti koji sukladno točki 4.1.1. ovog $CPS_{NQC\text{-}eIDAS}$ mogu podnijeti zahtjev za izdavanje certifikata.

4.7.3 Obrada zahtjeva za obnovu certifikata uz generiranje novog para ključeva

Fina podržava sljedeće načine obrade zahtjeva za obnovu certifikata s novim parom ključeva:

- obrada zahtjeva podnesenog u RA mreži,
- obrada *online* podnesenog zahtjeva.

U slučaju zahtjeva podnesenog u RA mreži identifikacija i potvrđivanje identiteta fizičkih osoba i poslovnog subjekta iz zahtjeva provodi se sukladno točki 3.3.1.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta. Službenik za registraciju u RA mreži provjerava podatke iz zahtjeva i potvrđuje točnost i cjelovitost informacija u zahtjevu. Odobravanje ili odbijanje zahtjeva provodi registracijski ured RA mreže u kojem je zahtjev podnesen.

U slučaju *online* podnesenog zahtjeva identifikacija i potvrđivanje identiteta podnositelja zahtjeva provodi se sukladno točki 3.3.1.2. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta. Provjerava se točnost i cjelovitost informacija u zahtjevu.

Provjera podataka iz zahtjeva provodi se usporedbom podataka iz zahtjeva s podacima u Fininoj bazi registriranih korisnika ili korištenjem komunikacijskih kanala sukladno važećoj zakonskoj regulativi.

Nakon provjere autentičnosti i valjanosti zahtjeva Fina CA izdaje certifikat sukladno točki 4.3.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

4.7.4 Obavještavanje korisnika o obnovi certifikata uz generiranje novog para ključeva

Fina obavještava Potpisnika, Skrbnika, odnosno Ovlaštenog predstavnika o skorom isteku certifikata te ga poziva na redovnu obnovu certifikata uz generiranje novog para ključeva.

Potpisnicima, Skrbnicima, odnosno Ovlaštenim predstavnicima koji su u zahtjevu za izdavanje certifikata dostavili e-mail adresu, obavijest se šalje e-mailom, a ostalim potpisnicima obavijest se šalje poštom.

Obavještavanje Potpisnika, odnosno Ovlaštenog predstavnika o obavljenoj obnovi certifikata provodi se sukladno točki 4.3.2. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

4.7.5 Provedba prihvaćanja obnovljenog certifikata s generiranim novim parom ključeva

Provedba prihvaćanja certifikata s generiranim novim parom ključeva izdanog sukladno točki 4.7.1. provodi se sukladno točki 4.4.1 ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

4.7.6 Objavljivanje certifikata po obnovi s generiranjem novog para ključeva

Objavljivanje certifikata s generiranim novim parom ključeva izdanog sukladno točki 4.7.1. provodi se sukladno točki 4.4.2. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

4.7.7 Obavještavanje drugih strana o obnovi certifikata s generiranim parom ključeva

Obavještavanje drugih strana o certifikatu s generiranim novim parom ključeva izdanog sukladno točki 4.7.1. provodi se sukladno točki 4.4.3. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

4.8 Izmjene u certifikatu

Potpisnici, odnosno poslovni subjekti imaju obvezu informiranja Fine o potrebi promjene podataka koji ulaze u sadržaj certifikata u roku od sedam dana, te zatražiti izmjene podataka u certifikatu.

Fina provodi izmjenu podataka u certifikatu samo u periodu njegovog važenja i ako nije opozvan ili suspendiran.

4.8.1 Razlozi za izmjene u certifikatu

- Razlozi za izmjene unutar osobnih, poslovnih i Administrativnih certifikata te certifikata za TDU mogu biti promjene podataka koje se odnose na Subjekt:imena ili prezimena Potpisnika,
- naziva poslovnog subjekta,
- naziva podorganizacijske jedinice u TDU,
- podataka o mjestu prebivališta fizičke osobe ili sjedišta poslovnog subjekta,
- *e-mail* adrese i/ili identifikator Subjekta za certifikate koji ove podatke sadrže u *Subject alternative name* ekstenziji certifikata,

Razlozi za izmjene unutar aplikacijskog certifikata mogu biti promjene koje se odnose na Subjekt:

- naziva aplikacije,
- naziva ili mjesta sjedišta poslovnog subjekta,
- *e-mail* adrese.

Razlozi za izmjene unutar certifikata za elektronički pečat *Trusted liste* mogu biti promjene podataka koje se odnose na Subjekt:

- naziva kojeg Subjekt obično koristi za svoje predstavljanje,
- naziva pravne osobe,
- naziva podorganizacijske jedinice u TDU,
- podataka o mjestu sjedišta pravne osobe,
- *e-mail* adrese, za certifikate koji *e-mail* adresu sadrže u *Subject Alternative Name* ekstenziji certifikata.

Razlog za izmjenu unutar certifikata mogu biti i promjene u profilu certifikata kao i promjene u sustavu certificiranja koje utječu na sadržaj polja u certifikatu.

4.8.2 Tko može zatražiti izmjene u certifikatu

Zahtjev za izmjene unutar certifikata isteka mogu podnijeti isti subjekti koji sukladno točki 4.1.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta mogu podnijeti zahtjev za izdavanje certifikata.

4.8.3 Obrada zahtjeva za izmjenama u certifikatu

Zahtjev za izmjene podataka podnosi se u registracijski ured RA mreže. Uz zahtjev podnosi se i dokumentacija kojom se dokazuje novonastala izmjena.

Identifikacija i potvrđivanje identiteta podnositelja zahtjeva provodi se sukladno proceduri inicijalnog utvrđivanja identiteta iz točke 3.2. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta. Obrada zahtjeva i izdavanje certifikata provodi se sukladno točki 4.2., 4.3. i 4.4. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

Zahtjev za izmjenu *e-mail* adrese u *Subject alternative name* ekstenziji certifikata može se podnijeti i *online* uz korištenje naprednog elektroničkog potpisa. Nakon provjere autentičnosti i valjanosti zahtjeva Fina CA izdaje certifikat sukladno točki 4.3.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

Izmjene unutar certifikata provode se opozivanjem postojećeg certifikata i izdavanjem novog certifikata s novim parom ključeva te izmijenjenim podacima u certifikatu i novim periodom valjanosti certifikata.

4.8.4 Obavještavanje korisnika o izdavanju izmijenjenog certifikata

Pri izdavanju certifikata u procesu izmjene certifikata obavještavanje korisnika provodi se sukladno točki 4.3.2. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

4.8.5 Provedba prihvaćanja izmijenjenog certifikata

Provedba prihvaćanja izmijenjenog certifikata provodi se sukladno točki 4.4.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

4.8.6 Objavljivanje izmijenjenog certifikata od strane CA

Objavljivanje izmijenjenog certifikata provodi se na način opisan u točki 4.4.2. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

4.8.7 Obavještavanje drugih strana o izdavanju izmijenjenog certifikata

Obavještavanje drugih strana o izdavanju izmijenjenog certifikata provodi se na način opisan u točki 4.4.3. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

4.9 Opoziv i suspenzija certifikata

4.9.1 Razlozi za opoziv

Fina opoziva certifikat:

- ako neka od informacija sadržanih u certifikatu postane netočna,
- u slučaju kompromitiranja privatnog ključa ili ako se pojavi osnovana sumnja da je privatni ključ kompromitiran,
- ako privatni ključ ili aktivacijski podaci nisu više u jedinstvenom posjedu Potpisnika, odnosno poslovnog subjekta,
- u slučaju gubitka ili trajne nedostupnosti privatnog ključa,
- ako prestane odnos između Potpisnika i poslovnog subjekta temeljem kojeg je izdan certifikat,
- ako je Fina primila službenu obavijest o smrti Potpisnika,
- ako je Fina primila službenu obavijest o gubitku poslovne sposobnosti Potpisnika,
- ako certifikat nije izdan sukladno zahtjevu,
- ako certifikat nije izdan sukladno Općim pravilima [26] ili $CPS_{NQC\text{-}eIDAS}$ dokumentu,
- u slučaju otkaza ugovora o obavljanju usluge certificiranja, od strane Korisnika,
- u slučaju službene obavijesti o korištenju certifikata u nezakonite svrhe,
- ako Fina procjeni da certifikat svojim tehničkim karakteristikama, profilom ili sadržajem ne pruža prikladnu razinu povjerenja Pouzdajućim stranama,
- u slučajevima kada to nalaže zakon ili drugi propis.

Fina može opozvati certifikat ako Korisnik, Potpisnik ili Ovlašteni predstavnik ne izvršava svoje obveze u skladu s ovim $CPS_{NQC\text{-}eIDAS}$ dokumentom i potpisanim ugovorima.

4.9.2 Tko može tražiti opoziv

Zahtjev za opoziv pripadajućeg osobnog certifikata podnosi Potpisnik.

Zahtjev za opoziv poslovnih i TDU certifikata podnosi Potpisnik ili osoba ovlaštena za zastupanje poslovnog subjekta.

Zahtjev za opoziv aplikacijskih certifikata podnosi Skrbnik ili osoba ovlaštena za zastupanje poslovnog subjekta.

Zahtjev za opoziv certifikata za elektronički pečat *Trusted* liste podnosi Ovlašteni predstavnik središnjeg tijela državne uprave nadležnog za poslove gospodarstva.

Zahtjev za opoziv administrativnog certifikata podnosi Potpisnik ili ovlaštena osoba u Fini.

Zahtjev za opoziv certifikata može uputiti RA mreža.

Fina može opozvati certifikat i temeljem autenticirane obavijesti treće strane ili temeljem autenticirane službene obavijesti nadležnog tijela.

4.9.3 Procedura za zahtjev za opozivom

Pisani zahtjev za opoziv certifikata treba odmah po nastupanju razloga za opoziv, koji su navedeni u točki 4.9.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta, točno i cjelovito ispuniti, potpisati i u najkraćem roku dostaviti na jedan od sljedećih načina:

- osobnom dostavom u registracijski ured RA mreže u uredovno vrijeme,
- poštanskom dostavom ili preko dostavljača na adresu registracijskog ureda u RA mreži,
- elektroničkom dostavom zahtjeva za opoziv potpisanog naprednim elektroničkim potpisom na e-mail adresu navedenu u točki 9.11. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta ili elektroničkom dostavom zahtjeva uz uporabu jake autentikacije.

Zahtjev za opoziv certifikata može se podnijeti i telefonskim putem pozivom Fini na telefonski broj koji je objavljen na internetskim stranicama repozitorija iz točke 2.2.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta. Ovaj Finin telefonski broj dostupan je od 0 do 24 sata, 7 dana u tjednu. Također, zahtjev za opoziv certifikata koji je izdan temeljem registracije u vanjskom ugovorenom RA može se predati i pozivom na telefonski broj službe za korisnike tog vanjskog RA u uredovno vrijeme službe, ukoliko vanjski RA podržava takvu mogućnost predaje zahtjeva.

Ako se zahtjev za opoziv podnosi telefonskim putem, nakon pozitivne potvrde identiteta podnositelja zahtjeva prema točki 3.4.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta ovlašteni službenik od podnositelja dobiva informacije o certifikatu za kojeg se podnosi zahtjev za opoziv, poput serijskog broja certifikata, ili ukoliko ta informacija podnositelju nije dostupna, koriste se i druge informacije poput tipa certifikata i približnog datuma njegovog izdavanja. Nakon identificiranja certifikata podnositelj potvrđuje svoj zahtjev za opozivanje identificiranog certifikata.

U slučaju da je zahtjev za opoziv certifikata temeljen na dojavi treće strane Službenik za registraciju će prije opoziva certifikata provjeriti utemeljenost zahtjeva i po potrebi zatražiti suglasnost Korisnika.

Nakon postupka identifikacije i potvrđivanja identiteta podnositelja zahtjeva iz točke 3.4.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta, Službenik za registraciju provjerava sukladno točki 4.9.2 ima li podnositelj zahtjeva pravo zatražiti opoziv predmetnog certifikata te u slučaju zadovoljenja navedenih uvjeta odobrava opoziv certifikata.

Ovlaštena osoba s povjerljivom ulogom Službenik za opoziv certifikata na osnovu odobrenja Službenika za registraciju donosi odluku o opozivu predmetnog certifikata. Nakon provedbe opoziva certifikata o opozivu obavještava Potpisnika, odnosno Ovlaštenog predstavnika te, ukoliko je to primjenjivo, poslovni subjekt s kojim je Potpisnik povezan.

Nakon opoziva certifikata Fina CA koji je izdao opozvani certifikat izdaje i objavljuje CRL, a informacija o statusu opozvanosti certifikata postaje dostupna i preko OCSP servisa.

4.9.4 Poček zahtjeva za opozivom

Podnositelji zahtjeva za opoziv certifikata iz točke 4.9.2. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta trebaju u najkraćem razumnom roku od nastanka razloga za opoziv navedenih u točki 4.9.1. podnijeti zahtjev za opoziv certifikata.

4.9.5 Vremenski period u kojem CA mora obraditi zahtjev za opozivom

Službenik za opoziv certifikata i Službenik za registraciju mogu, ako je potrebno zatražiti i prikupiti dodatne podatke koji mogu utjecati na odluku o opozivu certifikata, te po potrebi u cilju donošenja odluke mogu kontaktirati PMA.

Službenik za opoziv certifikata u najkraćem razumnom roku, a najkasnije u roku od 24 sata od primitka odgovarajućeg zahtjeva donosi odluku o opozivu certifikata. Ako Službenik za opoziv certifikata na osnovu prikupljenih podataka ne može donijeti odluku o opozivu certifikata dužan je o tome obavijestiti PMA koji u tom slučaju donosi odluku o opozivu certifikata.

Ovisno o donesenoj odluci Službenik za opoziv opoziva predmetni certifikat ili provodi druge potrebne korake.

Neposredno nakon opoziva certifikata, Fina CA promptno ažurira podatkovnu osnovicu certifikata i izdaje novu CRL.

4.9.6 Zahtjevi pouzdajućim stranama za provjeru opoziva

Pouzdanje u opozvan ili suspendiran certifikat može imati osobnu ili poslovnu štetu za Pouzdajuću stranu. Zbog toga, prije ostvarenja pouzdavanja u certifikat, Pouzdajuća strana provodi provjeru statusa certifikata u cilju utvrđivanja njegove opozvanosti ili suspenzije, a sukladno točkama 4.5.2., 4.9.9. i 4.9.10. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta. Ako Pouzdajućoj strani u danom trenutku nije moguće dobiti informacije o statusu certifikata, ona se ne smije pouzdati u takav certifikat.

4.9.7 Učestalost izdavanja CRL

Fina RDC 2015 izdaje i potpisuje Fina RDC 2015 CRL, a Fina RDC-TDU 2015 izdaje i potpisuje Fina RDC-TDU 2015 CRL. CRL liste koje izdaju Fina CA-ovi sadrže informacije o statusima opozvanosti certifikata minimalno do njihova isteka perioda važenja.

Ove CRL objavljuju se odmah po opozivu, suspenziji ili reaktivaciji certifikata te svakih šest sati od prethodnog izdavanja CRL. Vrijeme u kojem najkasnije mora biti izdana sljedeća CRL (vrijednost polja *Next Update*) je 24 sata od zadnjeg prethodnog izdavanja CRL.

4.9.8 Maksimalno kašnjenje za CRL

Neposredno nakon opoziva certifikata, Fina CA promptno ažurira podatkovnu osnovicu certifikata i izdaje novu CRL. Maksimalno kašnjenje CRL od trenutka njenog izdavanja do trenutka objave u redovitim uvjetima iznosi dvije minute.

4.9.9 Raspoloživost *online* provjere statusa opozvanosti certifikata

Fina CA-ovi podržavaju *online* provjeru statusa opozvanosti izdanih certifikata putem Fina OCSP servisa čiji je rad usklađen s preporukom IETF RFC 6960 [22].

Informacija o statusu opozvanosti certifikata korištenjem Fina OCSP servisa dostupna je u realnom vremenu.

Adresa Fina OCSP servisa je http://ocsp.fina.hr, a sadržana je u ekstenziji *Authority Information Access* svakog certifikata koje izdaju Fina CA-ovi.

CRL je primarno dostupna preko HTTP internetske adrese poslužitelja odgovarajućeg repozitorija, te sekundarno preko LDAP imenika, kao što je to opisano u točki 4.10.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta. Podaci o pristupnim točkama za dohvat CRL sadržani su u svakom izdanom certifikatu.

4.9.10 Zahtjevi na *online* provjeru statusa opozvanosti certifikata

Za korištenje Fina OCSP servisa pouzdajuća strana treba imati aplikacijsko rješenje koje može koristiti OCSP servis iz točke 4.10.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta uporabom GET i POST metode.

Za *online* preuzimanje CRL, Pouzdajuće strane moraju imati pristup internetu te koristiti aplikacije ili rješenja koja su u mogućnosti preuzeti CRL s internetskih adresa i protokolima navedenim u točki 4.10.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

4.9.11 Ostali načini objave statusa opozvanosti certifikata

Nema odredbi.

4.9.12 Posebni zahtjevi vezani uz kompromitiranje privatnog ključa

Nema odredbi.

4.9.13 Razlozi za suspenziju

Fina provodi suspenziju certifikata:

- ako Potpisnik, Skrbnik, Ovlašteni predstavnik ili osoba ovlaštena za zastupanje, zbog sumnji navedenih u točki 4.9.1. podnese zahtjev za suspenziju certifikata,
- privremeno do opoziva koji je zatražen iz razloga navedenih u točki 4.9.1., a za vrijeme dok Službenik za registraciju provodi sve potrebne provjere nužne za opoziv

certifikata, odnosno do dostave potrebne dokumentacije za opoziv u registracijski ured RA mreže,
- u slučaju neizvršenja ugovornih obveza od strane Korisnika, a koje se odnose na plaćanje pruženih usluga.

4.9.14 Tko može tražiti suspenziju

Zahtjev za suspenziju pripadajućeg osobnog certifikata podnosi Potpisnik.

Zahtjev za suspenziju poslovnih ili TDU certifikata podnosi Potpisnik ili osoba ovlaštena za zastupanje poslovnog subjekta.

Zahtjev za suspenziju aplikacijskih certifikata podnosi Skrbnik ili osoba ovlaštena za zastupanje poslovnog subjekta.

Zahtjev za suspenziju certifikata za elektronički pečat *Trusted* liste podnosi Ovlašteni predstavnik središnjeg tijela državne uprave nadležnog za poslove gospodarstva.

Zahtjev za suspenziju certifikata može uputiti RA mreža.

Fina može suspendirati certifikat i temeljem autenticirane obavijesti treće strane ili temeljem autenticirane službene obavijesti nadležnog tijela.

Zahtjev za reaktivaciju pripadajućeg osobnog certifikata podnosi Potpisnik.

Zahtjev za reaktivaciju poslovnih ili TDU certifikata podnosi Potpisnik ili osoba ovlaštena za zastupanje poslovnog subjekta.

Zahtjev za reaktivaciju aplikacijskih certifikata podnosi Skrbnik ili osoba ovlaštena za zastupanje poslovnog subjekta.

Zahtjev za reaktivaciju certifikata za elektronički pečat *Trusted* liste podnosi Ovlašteni predstavnik središnjeg tijela državne uprave nadležnog za poslove gospodarstva

4.9.15 Procedura za zahtjev za suspenziju i reaktivaciju

4.9.15.1 Procedura za zahtjev za suspenziju

Pisani zahtjev za suspenziju certifikata treba odmah po nastupanju razloga za suspenziju koji su navedeni u točki 4.9.13. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta točno i cjelovito ispuniti, potpisati i u najkraćem roku dostaviti na jedan od sljedećih načina:

- osobnom dostavom u registracijski ured RA mreže u uredovno vrijeme,
- poštanskom dostavom ili preko dostavljača na adresu registracijskog ureda u RA mreži,
- elektroničkom dostavom zahtjeva za suspenziju zaštićenim komunikacijskim kanalom.

Zahtjev za suspenziju certifikata može se podnijeti i telefonskim putem pozivom Fini na telefonski broj koji je objavljen na internetskim stranicama repozitorija iz točke 2.2.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta. Ovaj Finin telefonski broj dostupan je od 0 do 24 sata, 7 dana u tjednu. Također, zahtjev za suspenziju certifikata koji je izdan temeljem registracije u vanjskom ugovorenom RA može se predati i pozivom na telefonski broj službe za korisnike tog vanjskog RA u uredovno vrijeme službe, ukoliko vanjski RA podržava takvu mogućnost predaje zahtjeva.

Ako se zahtjev za suspenziju podnosi telefonskim putem, nakon pozitivne potvrde identiteta podnositelja zahtjeva prema točki 3.4.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta ovlašteni službenik od podnositelja dobiva informacije o certifikatu za kojeg se podnosi zahtjev za suspenziju, poput serijskog broja certifikata, ili ukoliko ta informacija podnositelju nije dostupna, koriste se i druge informacije poput tipa certifikata i približnog datuma njegovog izdavanja. Nakon identificiranja certifikata podnositelj potvrđuje svoj zahtjev za suspenziju identificiranog certifikata.

U slučaju da je zahtjev za suspenziju certifikata temeljen na dojavi treće strane Službenik za registraciju će prije suspenzije certifikata provjeriti utemeljenost zahtjeva i po potrebi zatražiti suglasnost Korisnika.

Nakon postupka identifikacije i potvrđivanja identiteta podnositelja zahtjeva iz točke 3.4.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta, Službenik za registraciju provjerava sukladno točki 4.9.14. ima li podnositelj zahtjeva pravo zatražiti suspenziju predmetnog certifikata te u slučaju zadovoljenja navedenih uvjeta odobrava suspenziju certifikata.

Ovlaštena osoba s povjerljivom ulogom Službenik za opoziv certifikata na osnovu odobrenja Službenika za registraciju donosi odluku o suspenziji predmetnog certifikata. Nakon provedbe suspenzije certifikata o suspenziji obavještava Potpisnika, odnosno Ovlaštenog predstavnika te, ukoliko je to primjenjivo, poslovni subjekt s kojim je Potpisnik povezan.

Nakon suspenzije certifikata Fina CA koji je izdao suspendirani certifikat izdaje i objavljuje CRL, a informacija o statusu suspendiranosti certifikata postaje dostupna i preko OCSP servisa.

Službenik za opoziv certifikata i Službenik za registraciju mogu, ako je potrebno zatražiti i prikupiti dodatne podatke koji mogu utjecati na odluku o provođenju suspenzije certifikata, te po potrebi u cilju donošenja odluke mogu kontaktirati PMA.

Službenik za opoziv certifikata u najkraćem razumnom roku, a najkasnije u roku od 24 sata od primitka odgovarajućeg zahtjeva donosi odluku o suspenziji certifikata. Ako Službenik za opoziv certifikata na osnovu prikupljenih podataka ne može donijeti odluku o suspenziji certifikata dužan je o tome obavijestiti PMA koji u tom slučaju donosi odluku o suspenziji certifikata.

Ovisno o donesenoj odluci Službenik za opoziv suspendira predmetni certifikat ili provodi druge potrebne korake.

Neposredno nakon suspenzije certifikata, Fina CA promptno ažurira podatkovnu osnovicu certifikata i izdaje novu CRL.

4.9.15.2 Procedura za zahtjev za reaktivaciju

Zahtjev za reaktivaciju može podnijeti osoba koja može podnijeti zahtjev za izdavanje predmetnog certifikata, a sukladno točki 4.1.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

Zahtjev za reaktivaciju certifikata treba točno i cjelovito ispuniti, potpisati i dostaviti osobnom dostavom u registracijski ured RA mreže u uredovno vrijeme.

Nakon postupka identifikacije i potvrđivanja identiteta podnositelja zahtjeva iz točke 3.4.2. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta, Službenik za registraciju provjerava ima li podnositelj zahtjeva pravo zatražiti reaktivaciju predmetnog certifikata te u slučaju zadovoljenja navedenih uvjeta odobrava reaktivaciju certifikata.

Službenik za opoziv certifikata na osnovu odobrenja Službenika za registraciju donosi odluku o reaktivaciji predmetnog certifikata te provodi reaktivaciju certifikata. O provedbi reaktivacije obavještava Potpisnika, odnosno Ovlaštenog predstavnika te, ukoliko je to primjenjivo, poslovni subjekt s kojim je Potpisnik povezan.

Nakon reaktivacije certifikata Fina CA koji je izdao reaktivirani certifikat izdaje i objavljuje CRL, a aktualna informacija o statusu certifikata postaje dostupna i preko OCSP servisa.

4.9.16 Ograničenje na trajanje suspenzije

Maksimalno vrijeme u kojem certifikat može biti u stanju suspendiranosti je 60 dana. Nakon isteka toga vremena Službenik certifikata opoziva certifikat, a Fina CA koji je izdao predmetni certifikat objavljuje CRL. Aktualna informacija o statusu certifikata postaje dostupna i preko OCSP servisa.

4.10 Usluge statusa certifikata

4.10.1 Operativna svojstva

Fina daje informacije o statusu opozvanosti ili suspendiranosti certifikata kroz pružanje OCSP servisa i objave CRL. Informacije o statusu pojedinog certifikata dostupne su minimalno tijekom vremenskog perioda važenja certifikata.

Preporuka je Pouzdajućim stranama da za provjeru statusa certifikata koriste Fina OCSP servis te da se provjera statusa dohvatom CRL koristiti kao alternativna metoda provjere u slučaju nedostupnosti OCSP servisa ili u slučaju da aplikacija Pouzdajuće strane podržava provjeru statusa certifikata samo putem CRL.

Adresa Fina OCSP servisa je http://ocsp.fina.hr, a upisuje se u ekstenziji *Authority Information Access* svih certifikata koje izdaju Fina CA-ovi.

CRL za certifikate koje izdaju Fina CA-ovi objavljuju se na internetskom poslužitelju i na javnom imeniku repozitorija određenog Fina CA. Na internetskom poslužitelju objavljuje se objedinjena CRL, a na javnom imeniku objavljuju se objedinjena i segmentirana CRL.

Adrese objave CRL sadržane su u ekstenziji *CRLDistributionPoints* u svakom izdanom certifikatu.

Ako aplikacija Pouzdajuće strane podržava rad sa segmentiranom CRL aplikacija s javnog imenika dohvaća određeni segment segmentirane CRL.

Ako aplikacija Pouzdajuće strane ne podržava rad sa segmentiranom CRL, redoslijed kojim se CRL dohvaća je sljedeći:

1. aplikacija s internetskog poslužitelja dohvaća objedinjenu CRL,
2. ako internetski poslužitelj nije dostupan, objedinjenu CRL aplikacija dohvaća s javnog LDAP imenika.

4.10.1.1 Adrese za dohvat CRL Fina RDC 2015 certifikata

Adresa objedinjene CRL za Fina RDC 2015 certifikate na internetskom poslužitelju je:

http://rdc.fina.hr/RDC2015/FinaRDCCA2015.crl.

Adresa objedinjene CRL za Fina RDC 2015 certifikate na javnom imeniku je:

ldap://rdc-ldap2.fina.hr/CN=Fina RDC 2015, O=Financijska agencija, C=HR?certificateRevocationList;binary

Adresa segmentirane CRL za Fina RDC 2015 certifikate na javnom imeniku je:

ldap://rdc-ldap2.fina.hr/cn=CRLx,ou=RDC,o=FINA,c=HR?certificateRevocationList%3Bbinary.

Oznaka x u cn=CRLx označava segment CRL.

4.10.1.2 Adrese za dohvat CRL za Fina RDC-TDU 2015 certifikate

Adresa objedinjene CRL za Fina RDC-TDU 2015 certifikate na internetskom poslužitelju je:

http://rdc.fina.hr/RDC-TDU2015/FinaRDC-TDUCA2015.crl.

Adresa objedinjene CRL za Fina RDC-TDU 2015 certifikate na javnom imeniku je:

ldap://rdc-tdu-ldap2.fina.hr/CN=Fina RDC-TDU 2015, O=Financijska agencija, C=HR?certificateRevocationList;binary

Adresa segmentirane CRL za Fina RDC-TDU 2015 certifikate na javnom imeniku je:

ldap://rdc-tdu-ldap2.fina.hr/cn=CRLx,ou=RDC-TDU,o=FINA,c=HR?certificateRevocationList%3Bbinary.

Oznaka x u cn=CRLx označava segment CRL.

4.10.2 Dostupnost usluga

Dostupnost CRL i OCSP servisa je 24 sata na dan, 7 dana u tjednu. U slučaju ispada sustava, nastanka okolnosti koje su izvan kontrole Fine ili uslijed utjecaja više sile, usluga će biti dostupna u skladu s Planom kontinuiteta poslovanja.

Adrese pristupnih točaka za uslugu provjere valjanosti certifikata dane su u točki 4.10.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

4.10.3 Opcionalna svojstva

Nema odredbi.

4.11 Kraj korištenja

Ako Korisnik otkaže ugovor prije isteka certifikata, Fina CA će opozvati sve certifikate na koje se odnosi taj ugovor.

4.12 Sigurno skladištenje i oporavak privatnog ključa

Sigurno skladištenje privatnih korisničkih ključeva nekvalificiranih certifikata nije dozvoljeno.

5 PROVJERA SUSTAVA, UPRAVLJANJA I RADNIH POSTUPAKA

Fina osigurava primjerenu zaštitu imovine koja se upotrebljava za pružanje usluga izdavanja kvalificiranih certifikata te u tu svrhu vodi cjelokupni popis te imovine s pripadajućom klasifikacijom koja je sukladna procjeni rizika.

Mjere fizičke zaštite, postupci koje Fina primjenjuje u zaštiti sustava za izdavanje certifikata (u daljnjem tekstu: sustav certificiranja), kao i postupci provjere tog sustava, upravljanja i radnih postupaka u Fina PKI interne su prirode te se njihovi detalji ne objavljuju javno.

5.1 Mjere fizičke zaštite

Fina kao pružatelj usluga povjerenja primjenjuje mjere fizičke zaštite sustava certificiranja s ciljem minimiziranja rizika vezanih uz fizički zaštitu i u skladu s poslovnom politikom Fine i važećom zakonskom regulativom.

5.1.1 Lokacija objekta i konstrukcija

Primarni produkcijski sustav certificiranja Fine smješten je na primarnoj produkcijskoj lokaciji, u zgradi Fine, u posebnom štićenom prostoru izdvojenom za tu namjenu uz primjenu više razina fizičke i tehničke zaštite.

Finin sustav certificiranja na sekundarnoj lokaciji namijenjen je za preuzimanje funkcija primarnog produkcijskog sustava certificiranja u slučaju prestanka rada primarnog produkcijskog sustava do njegovog oporavka te ponovnog uspostavljanja njegovih servisa. Sustav certificiranja na sekundarnoj lokaciji smješten je na udaljenoj pričuvnoj lokaciji Fine i u odnosu na primarni sustav udovoljava jednakim ili višim sigurnosnim zahtjevima.

Upravljanje Fina Root CA-om, njemu subordiniranim Fina CA-ovima, središnjim Fina RA sustavom, javnim imenikom i elektroničkom arhivom provodi se iz Fina PKI štićenog prostora.

Fina PKI štićeni prostor interno je podijeljen na sigurnosne zone.

Sigurni prostori u kojima se nalaze Finini sustavi certificiranja na primarnoj i sekundarnoj lokaciji u daljnjem tekstu nazivaju se zajedničkim nazivom Fina PKI štićeni prostor.

5.1.2 Fizički pristup

Fizički pristup sustavu certificiranja u Fina PKI štićenom prostoru i pripadnim sigurnosnim zonama unutar tog prostora ostvaruje se uz dualnu kontrolu prolaza ovlaštenih osoba Fina PKI, a u skladu s njihovim ulogama i ovlastima.

Osobama koje nemaju ovlaštenje fizičkog pristupa sustavu certificiranja pristup je dozvoljen samo u pratnji i uz cjelovremeni nadzor ovlaštenih osoba Fina PKI uz njihovu dualnu kontrolu, a u skladu s Fininim internim procedurama. Za vrijeme boravka osoba koje nemaju

ovlaštenje fizičkog pristupa sustavima u Fina PKI štićenom prostoru ne provode se postupci koji bi tim osobama mogli otkriti povjerljive informacije.

O svakom pristupu sustavima certificiranja vodi se evidencija.

Oprema, informacije, mediji i softver iz Fina PKI štićenog prostora iznosi se isključivo uz sudjelovanje i minimalno dualnu kontrolu ovlaštenih osoba u Fina PKI kojima su dodijeljene odgovarajuće povjerljive uloge, i uz prethodno ovlaštenje. Pri tome se vodi računa o propisnoj zaštiti ili uništavanju podataka prije njihova iznošenja, a sukladno internim procedurama.

Fizički pristup sustavu certificiranja u Fina PKI štićenom prostoru (Fina CA sustavu, središnjem Fina RA sustavu, primarnom javnom imeniku i elektroničkoj arhivi) može se ostvariti jedino prolaskom kroz pristupne zone.

Fizički pristup papirnatoj dokumentaciji koju Fina RA mreža prikuplja u postupku registracije fizičkih osoba i poslovnih subjekata kontrolira se dopuštenjem pristupa uredskim ormarima s bravom u kojima se nalazi dokumentacija. Papirnatim dokumentima koje Fina RA mreža prikuplja tijekom postupka registracije fizički mogu pristupiti samo Službenici za registraciju i ovlaštene osobe Fina RA mreže.

Pristup arhivskom prostoru u kojem se arhivira papirnata dokumentacija Fina PKI imaju samo ovlaštene osobe Fine. Arhivski prostor Fine opremljen je sustavom video nadzora i pod nadzorom je zaštitarske tvrtke.

5.1.3 Sustavi za napajanje i klimatizaciju

Uređaji i prostor u kojem se nalaze Fina CA-ovi, Fina RA sustav i repozitorij te sustavi tehničke zaštite opskrbljeni su neprekidnim napajanjem električnom energijom i klimatizacijom koja je dimenzionirana na način koji osigurava odgovarajuće radne uvjete i u slučaju prekida vanjskog napajanja.

Rezervno napajanje električnom energijom osigurano je uređajem za neprekidno napajanje u kombinaciji s dizel agregatom koje omogućuje neprekidan i pouzdani rad sustava certificiranja do ponovne uspostave primarnog napajanja.

U svim prostorijama u kojima se nalazi oprema sustava certificiranja postavljeni su klimatizacijski uređaji za održavanje propisanog radnog okruženja.

5.1.4 Opasnost od poplave

Oprema Fininog sustava certificiranja nalazi se u prostoru koji je osiguran od poplave i smještena je na povišenim podovima.

Papirnata arhiva Fina PKI pohranjena je u prostoru koji fizičkom konstrukcijom objekta štiti arhivirani materijal od poplave te puknuća vodovodnih i odvodnih cijevi.

5.1.5 Protupožarna zaštita

Automatski sustav za detekciju i zaštitu od požara unutar Fina PKI štićenog prostora instaliran je u skladu s pravilima protupožarne zaštite. Automatski sustav koristi sredstva za gašenje koja su primjenjiva za gašenje požara na električnim instalacijama i IT opremi. Fina PKI štićeni prostor ima stabilni sustav za dojavu požara i detektore požara.

Prostori u Fina RA mreži štite se u skladu s odredbama Fininog internog pravilnika o zaštiti od požara.

Arhivski prostor Fine u kojem se čuva papirnata arhiva Fina PKI opremljen je vatrodojavnim sustavom i štiti se u skladu s odredbama Fininog internog pravilnika o zaštiti od požara.

5.1.6 Pohrana medija

Mediji na kojima se nalaze arhivske i sigurnosne kopije Fina PKI podataka u elektroničkom obliku, kopije sadržaja repozitorija te sigurnosne kopije programske opreme pohranjuju se na dvije odvojene štićene lokacije na siguran način kako bi se zaštitili od oštećenja, otuđenja ili neovlaštenog pristupa. Mediji s podacima se pohranjuju u Fina PKI štićenom prostoru primarnog produkcijskog sustava te na pričuvnoj lokaciji.

Za rad sa sigurnosnim kopijama podataka ovlaštene su osobe s povjerljivim ulogama Operater sustava.

5.1.7 Zbrinjavanje otpada

Dokumenti i podaci u papirnatom i elektroničkom obliku koji se nalaze u Fina PKI štićenom prostoru ili sadržavaju povjerljive informacije, a za koje ne postoji potreba arhiviranja na siguran način se odstranjuju i uništavaju.

Zbrinjavanje otpada iz Fina PKI štićenog prostora odvija se pod nadzorom ovlaštenih osoba Fina PKI.

Svi se povjerljivi dokumenti i podaci prije odlaganja u otpad na mjestu nastanka fizički uništavaju na način da se ovako uništene informacije ne mogu rekonstruirati.

Iz sustava arhive se na siguran način izlučuju dokumenti i podaci u papirnatom i elektroničkom obliku za koje je istekla potreba za daljnjim arhiviranjem te se odstranjuju i uništavaju na siguran način.

Uništavanje medija na kojima se nalaze povjerljivi podaci te uništavanje podataka i ključeva povezanih s HSM modulima provodi se sukladno Fininim internim procedurama. Takvo brisanje i uništavanje podataka HSM modula provodi se i prije njihovog eventualnog slanja na servis ili popravak.

Fina zbrinjava sve vrste otpada koji nastaje unutar prostorija i poslovnih prostora Fine u skladu s internim radnim uputama i procedurama za ekološko zbrinjavanje otpada.

5.1.8 Sigurnosne kopije na drugoj lokaciji

Sigurnosne kopije Fina CA-ova, središnjeg Fina RA sustava, sadržaja repozitorija i arhive u elektroničkom obliku, sigurnosne kopije programske opreme pohranjuju se u Fina PKI štićenom prostoru na pričuvnoj lokaciji.

Sigurnosne kopije koje se pohranjuju u štićenom prostoru na pričuvnoj lokaciji se, u odnosu na njihove izvornike, čuvaju uz primjenu jednake ili više razine sigurnosti primijenjenih mjera fizičke zaštite.

5.2 Organizacijske mjere zaštite

5.2.1 Povjerljive uloge

Upravljanje informacijskim i komunikacijskim sustavom, sustavom upravljanja certifikatima i nadzora djelovanja Fina PKI obavlja se u unutar odvojenih organizacijskih dijelova Fine.

Fina osigurava da sve ovlaštene osobe koje obavljaju poslove vezane uz Fina CA-ove imaju dodijeljene odgovarajuće povjerljive uloge.

Povjerljive uloge dodjeljuju se ovlaštenim zaposlenicima iz nadležnih organizacijskih dijelova Fine te čine temelj povjerenja u Fina PKI. Svaka povjerljiva uloga je dokumentirana s jasno definiranim opisom poslova i odgovornostima.

Opis povjerljivih uloga te pripadni opis poslova, ovlasti i odgovornosti koje obavlja pojedina uloga opisani su u internim dokumentima Fine. U pripadajućim popisima za svaku ulogu navedeni su djelatnici Fine kojima je ta uloga dodijeljena.

5.2.2 Broj osoba potrebnih za obavljanje aktivnosti

Fina ima stalno zaposlen dovoljan broj stručnih osoba sa znanjem, iskustvom i kvalifikacijama koji je potreban u Fina PKI za davanja usluga iz opsega ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

Pristup i rad u štićenom Fina PKI prostoru provodi se isključivo uz istovremenu prisutnost najmanje dvije ovlaštene osobe Fina PKI koje imaju dozvole pristupa sustavu smještenom u štićenom Fina PKI prostoru.

Broj djelatnika s pripadnim povjerljivim ulogama za obavljanje pojedinih zadataka u subordiniranim Fina CA-ovima opisan je u Fininim internim dokumentima.

5.2.3 Identifikacija i potvrđivanje identiteta za svaku ulogu

Prilikom prijave na kritične aplikacije i servise unutar Fina PKI provodi se identifikacija i potvrda identiteta osobe koja pristupa aplikaciji ili servisu. Identifikacija i potvrda identiteta osobe provodi se odgovarajućom metodom autentikacije. Pristup i korištenje aplikacija i servisa unutar Fina PKI omogućen je samo ovlaštenim osobama sukladno povjerljivoj ulozi koju obnašaju.

Identifikacija ovlaštenih osoba Fina PKI i određivanje prava pristupa za obavljanje pojedinih zadataka u Fina PKI provodi se kroz sigurnosne procedure i postupke provjere.

Ovlaštene osobe s povjerljivim ulogama u Fina PKI moraju se autenticirati prije bilo kojeg pristupa Fina CA, odnosno Fina RA sustavu. U tu svrhu ovlaštene osobe Fina PKI dobivaju odgovarajuća sredstva za autentikaciju. Prije dobivanja sredstva za autentikaciju navedeno osoblje mora zadovoljiti zahtjeve navedene u točki 5.3. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

Sredstva za autentikaciju su:

- kartice kontrole s prolaza za ulazak u Fina PKI štićene sigurnosne zone, a dozvolu pristupa smiju dobiti samo ovlaštene osobe s povjerljivim ulogama u Fina PKI,
- certifikati na sigurnim kriptografskim uređajima koje smiju dobiti samo ovlaštene osobe u Fini s povjerljivim ulogama u Fina PKI,
- korisničko ime i zaporka ili certifikat na sigurnom kriptografskom uređaju koje smiju dobiti samo ovlaštene osobe u Fini s povjerljivim ulogama u Fina PKI,
- upravljačke kartice kriptografskog modula koje smiju dobiti samo ovlaštene osobe u Fini s povjerljivim ulogama u Fina PKI, sukladno ulogama iz točke 5.2.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

Uporaba navedenih sredstava za autentikaciju je ograničena na zadatke i sustav za koje je autorizirana određena povjerljiva uloga.

Službenik za sigurnost odgovoran je za utvrđivanje valjanosti identiteta djelatnika s povjerljivom ulogom u Fina PKI.

Tijekom korištenja kritičnih aplikacija i servisa aktivnosti prijavljene osobe propisno se bilježe, spremaju i čuvaju.

5.2.4 Uloge koje zahtijevaju odvajanje dužnosti

Za poslove povezane uz Fina Root CA provodi se sljedeće odvajanje dužnosti:

- Službenik za sigurnost ne smije obavljati poslove Službenika za nadzor sustava,
- Administrator sustava ne smije obavljati poslove Službenika za sigurnost ili poslove Službenika za nadzor sustava.

5.3 Osoblje

5.3.1 Kvalifikacije, radno iskustvo i zahtjevi za provjerom osoblja

Pri zapošljavanju osoblja na poslovima u Fina PKI uzimaju se u obzir zahtjevi za odgovarajućom stručnom spremom za svaku povjerljivu ulogu.

Prije početka rada u Fina PKI kandidati moraju posjedovati odgovarajuća stručna znanja, iskustvo, kvalifikacije i edukacije u radu s kriptografskim tehnologijama, zaštitom računalnih

sustava, informacijskom sigurnošću te zaštitom osobnih podataka u domeni vlastitog djelokruga rada u okviru poslova Fina PKI.

Prilikom zapošljavanja novih djelatnika, Fina provodi testiranje u cilju procjene njihove kvalitete i kompetencija za obavljanje povjerljivih uloga u Fina PKI sustavu.

Fina PKI osoblje s povjerljivim ulogama ne smije biti ni u kakvom sukobu interesa koji bi ugrozio rad Fina PKI sustava.

5.3.2 Procedure provjere prikladnosti osoblja

Prije zapošljavanja kandidata na poslovima Fina PKI, Fina provodi psihološko testiranje osoblja kako bi se ocijenila njihova primjerenost u skladu s potrebama poslova koje će obavljati.

Fina PKI osoblje prije zaposlenja u Fina PKI dostavlja uvjerenje o nekažnjavanju izdano od nadležnog Općinskog suda kojim se potvrđuje da se protiv fizičke osobe ne vodi kazneni postupak, da nije doneseno rješenje o istrazi, nije podignuta optužnica koja je stala na pravnu snagu, nije donesena nepravomoćna presuda po optužnom prijedlogu i nije izdan kazneni nalog.

Svaki zaposlenik Fine potpisivanjem ugovora o radu obvezuje se na čuvanje poslove tajne.

5.3.3 Zahtjevi za školovanjem

Osoblje u Fina PKI i Službenici za registraciju u RA mreži prije početka obavljanja poslova u Fina PKI, prolaze edukaciju sukladno poslovima koje će obavljati.

Fina PKI osoblju s povjerljivim ulogama u radu na Fina CA sustavima osigurava se edukacija i usavršavanje sukladno njihovim povjerljivim ulogama.

Edukacija i usavršavanje osoblja s povjerljivim ulogama u radu na Fina CA sustavima obuhvaća:

- Fina CA i Fina RA sigurnosni principi i mehanizmi,
- svjesnost o sigurnosti,
- CA softver koji je u uporabi u Fina CA sustavu,
- zadaci povezani s povjerljivim ulogama koje će obavljati na Fina CA sustavima,
- postupci oporavka od nezgode i nastavka poslovanja.

Edukacija Službenika za registraciju u Središnjem Fina RA i Službenika za registraciju u Fina LRA uključuje:

- osnovno o certifikatima,
- tipovi certifikata koje izdaju Fina CA-ovi i područja njihove uporabe,
- načini registracije korisnika te rad u Fina RA i Fina CMS aplikacijama,
- svjesnost o sigurnosti,
- informacije s kojima je potrebno upoznati korisnike.

5.3.4 Periodičko obavljanje znanja i osvješćivanje

Osvješćivanje o informacijskoj sigurnosti provodi se jednom godišnje za sve zaposlenike Fina PKI.

Osobe s povjerljivim ulogama u Fina PKI su zadužene usavršavati svoje vještine i stjecati nova znanja iz svog područja rada samostalnom edukacijom ili organiziranim internim i vanjskim edukacijama, a o čemu se vodi evidencija.

Obnova znanja osoblja Fina RA mreže, a obzirom na poslove koje obavljaju, provodi se jednom godišnje.

5.3.5 Učestalost i slijed izmjene zaposlenika

Ne primjenjuje se

5.3.6 Kazne za neovlaštene radnje

Nepridržavanje propisanih mjera za ovlaštene osobe pri radu u Fina PKI podliježe povredi radne obveze, a eventualne kaznene mjere određuju se disciplinskim postupkom.

U slučaju neovlaštenih radnji od strane ugovornih partnera primijenit će se odredbe definirane ugovorom s ugovornim partnerom.

5.3.7 Zahtjevi na vanjske suradnike

Za ugovorene vanjske suradnike koji za Finu obavljaju dio usluga iz opsega usluga izdavanja nekvalificiranih certifikata vrijede isti zahtjevi pri radu u Fina PKI kao i za interne zaposlenike.

Zahtjevi za dobavljače roba i usluga za Fina PKI regulirani su internim dokumentima o radu s dobavljačima. Pristup vanjskih suradnika informacijskoj imovini u Fina PKI odobrava se isključivo temeljem ugovora za samo onu informacijsku imovinu koja je predmet ugovora i samo za aktivnosti navedene u ugovoru.

5.3.8 Dokumentacija koja je dostupna osoblju

Svakom zaposleniku dostupna je dokumentacija potrebna za obavljanje njegovih radnih zadataka, koja uključuje interne i vanjske materijale za edukaciju, te radne upute i procedure za obavljanje pojedinih poslova u Fina PKI, sukladno dodijeljenoj povjerljivoj ili korisničkoj ulozi i pripadnim ovlaštenjima

5.4 Postupci upravljanja revizijskim zapisima

5.4.1 Tipovi događaja koji se zapisuju

Svi važni događaji u Fina PKI koji se odnose na izdavanje certifikata zapisuju se kao revizijski zapisi. Revizijski zapisi sadrže:

- datum i vrijeme događaja,
- vrstu događaja,
- identitet osobe ili jedinice sustava koja je odgovorna za radnju,
- uspješnost ili neuspješnost događaja kojeg se prati.

Datum i vrijeme koji se koriste za revizijske zapise događaja u elektroničkom obliku poslužitelji u Fina PKI svakog sata usklađuju s NTP poslužiteljem koji je sinkroniziran s izvorom točnog vremena te ima odstupanje manje od +/- 1 s u odnosu na UTC vrijeme.

Fina prikuplja revizijske zapise u elektroničkom ili papirnatom obliku o događajima u Fina PKI vezanim uz:

- upravljanje životnim ciklusom CA ključeva Fina CA-ova,
- upravljanje životnim ciklusom HSM modula kojim su zaštićeni privatni ključevi Fina CA-ova,
- upravljanje životnim ciklusom korisničkih ključeva koje generira Fina,
- pripremu i izdavanje sigurnih kriptografskih, odnosno QSCD uređaja na kojima se izdaju i nekvalificirani certifikati,
- upravljanje životnim ciklusom certifikata koje izdaju Fina CA-ovi,
- registraciju fizičke osobe i poslovnog subjekta,
- sigurnosne događaje, uključujući događaje podizanja i spuštanja sustava, ispada sustava i kvara hardvera, aktivnosti vatrozidova i usmjernika te izmjene sigurnosnih postavki sustava.

Podaci i događaji koji se zapisuju u revizijskim zapisima Fina PKI sustava opisani su u Fininim internim dokumentima.

5.4.2 Učestalost obrade revizijskih zapisa

Postupak pregleda revizijskih zapisa obuhvaća:

- pregled stavki revizijskih zapisa koje su stvorene nakon posljednje revizije,
- po potrebi, pripremu sažetog izvještaja koji sadrži objašnjenja važnih događaja.

Ovi pregledi uključuju provjeru oštećenosti revizijskih zapisa i kratku kontrolu svih zapisa, s podrobnijim istraživanjem neregularnih događaja evidentiranih u revizijskim zapisima.

Preglede revizijskih zapisa Fina CA-ova i pripadajućih HSM modula obavlja Službenik za nadzor sustava. Pregledi revizijskih zapisa Fina CA-ova i pripadajućih HSM modula obavljaju se redovito, jednom dnevno radnim danima, te u slučaju izvanrednih situacija. O obavljenom pregledu ovih revizijski zapisa vodi se evidencija u papirnatom ili elektroničkom obliku, a vodi je osoba s povjerljivom ulogom Službenik za nadzor sustava.

Analiza ostalih revizijskih zapisa obavlja se po potrebi, a provodi je ovlašteno osoblje Fina PKI.

U slučaju detektiranja nepravilnosti ili pogreške koja se odnose na sigurnost, ovlaštena osoba za pregled revizijskih zapisa izrađuje izvještaj o analizi revizijskih zapisa i daljnjim potrebnim aktivnostima. U slučaju otkrivanja neautorizirane aktivnosti, postupa se u skladu s Fininim internim procedurama.

Sve radnje poduzete na osnovi analize revizijskih zapisa moraju se dokumentirati.

5.4.3 Vremenski period pohrane revizijskih zapisa

Revizijski zapisi sa zapisima iz točke 5.4.1. čuvaju se najmanje 10 godina od isteka certifikata na kojeg se zapisi odnose.

5.4.4 Zaštita revizijskih zapisa

Revizijski zapisi u Fina PKI štite se mehanizmima i postupcima koji osiguravaju povjerljivost i cjelovitost revizijskih zapisa te ne dozvoljavaju izmjenu revizijskih zapisa, kao ni jednostavno brisanje ili uništenje revizijskih zapisa.

Zaštita cjelovitosti kritičnih revizijskih zapisa Fina CA sustava za izdavanje certifikata osigurana je pri generiranju revizijskih zapisa.

Povjerljivost revizijskih zapisa osigurava se kontrolom pristupa sustavu i pravom za čitanje revizijskih zapisa.

Pristup revizijskim zapisima ograničen je na ovlašteno Fina PKI osoblje, odnosno na osobe s povjerljivim ulogama Službenik za nadzor sustava, Službenik za sigurnost i Administrator sustava, s kombinacijom kontrola fizičkog pristupa Fina PKI štićenom prostoru i sigurnosnih kontrola pristupa podacima sustava.

Revizijski zapisi svih sustava u Fina PKI koji sadrže podatke navedene u točki 5.4.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta se, nakon perioda čuvanja na sustavima gdje su nastali, arhiviraju i štite sukladno postupcima opisanim u točki 5.5.3. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

Revizijski zapisi koji se vode u papirnatom obliku, kao što je Evidencija za praćenje ulazaka i izlazaka iz Fina PKI štićenog prostora, štite se od neovlaštenog pregleda, brisanja, izmjene ili uništenja korištenjem uobičajenim metoda za zaštitu papirnate dokumentacije.

5.4.5 Postupci izrade sigurnosnih kopija revizijskih zapisa

Novonastali revizijski zapisi u Fina PKI kopiraju se na dnevnoj razini te se njihove kopije pohranjuju i čuvaju unutar primarnog produkcijskog Fina PKI štićenog prostora. Dodatno, kopije datoteka revizijskih zapisa u Fina PKI se na medijima za pohranu podataka pohranjuju u sekundarni štićeni prostor na pričuvnoj lokaciji, sukladno točki 5.1.8. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

Postupci izrade sigurnosnih kopija revizijskih zapisa u Fini detaljnije su opisani u internim dokumentima.

5.4.6 Sustav prikupljanja revizijskih zapisa (unutarnji ili vanjski)

Sustav prikupljanja revizijskih zapisa svih sustava u Fina PKI je interni sustav na kojem se revizijski zapisi prikupljaju kombinacijom automatskih i manualnih procesa koji se izvode na Fina PKI poslužiteljima i koje pokreće, odnosno nadgleda Fina PKI osoblje s povjerljivim ulogama.

Manualni procesi prikupljanja revizijskih zapisa odnose se na ažurno vođenje Evidencije za praćenje ulazaka i izlazaka iz Fina PKI štićenog prostora.

Prikupljanje revizijskih zapisa nastalih u vanjskim ugovorenim RA-ovima regulira se ugovorom.

5.4.7 Obavještavanje subjekta uzročnika događaja

U slučaju uočavanja zapisa o značajnom događaju u radu Fina PKI koji je povezan s određenim sudionikom Fina zadržava pravo odlučiti o obavještavanju sudionika koji je taj događaj uzrokovao.

5.4.8 Procjena ranjivosti

Fina obavlja redovitu procjenu rizika informacijske imovine, procjenu ranjivosti za prepoznate javne i privatne adrese te penetracijsko testiranje.

Procjena rizika informacijske imovine provodi se jednom godišnje. Procjena ranjivosti sustava za prepoznate javne i privatne adrese Fina PKI provodi se kvartalno. Penetracijski test provodi se jednom godišnje. Procjene rizika i ranjivosti te penetracijski test provode se i nakon značajnih promjena.

Svaku novu kritičnu ranjivost Fina će razmotriti i za svaku takvu ranjivost, za koju se utvrdi potencijalni utjecaj, Fina će u roku od 48 sati od njezina saznanja postupiti na jedan od sljedećih načina:

- ukloniti ranjivost, ili
- ako uklanjanje ranjivosti u roku od 48 sati od njezina saznanja nije moguće, izraditi i provesti plan uklanjanja ranjivosti, ili
- dokumentirati činjeničnu osnovu na temelju koje je utvrđeno da ranjivost ne zahtijeva uvođenje dodatnih mjera za njeno uklanjanje.

5.5 Arhiviranje zapisa

5.5.1 Tipovi arhiviranih zapisa

Fina PKI arhivira niže navedene podatke koji, ovisno o tipu, mogu biti u elektroničkom i/ili papirnatom obliku:

- opća pravila pružanja usluga certificiranja,
- pravilnici o postupcima certificiranja,
- uvjeti pružanja usluga certificiranja,
- ugovori povezani s pružanjem usluga certificiranja,
- podaci vezani uz generiranje parova ključeva Fina CA-ova i izdavanju pripadajućih Fina CA certifikata,
- podaci i pripadajuća dokumentacija prikupljena postupkom registracije fizičkih osoba i poslovnih subjekata,
- podaci iz zahtjeva za izdavanje certifikata dostavljeni od strane korisnika,
- podaci i dokumentacija vezana uz sigurne kriptografske, odnosno QSCD uređaje,
- certifikati i podaci vezani uz životni ciklus pojedinog certifikata, uključujući sve zahtjeve i obavijesti za opoziv, suspenziju i reaktivaciju certifikata te pripadajuće provedene radnje,
- evidencija opozvanih i suspendiranih certifikata, podaci o opozivu, suspenziji i reaktivaciji certifikata te pripadajuća dokumentacija,
- revizijski zapisi iz točke 5.4.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta,
- drugi Fininі interni dokumenti.

Svaki zapis koji se arhivira sadržava podatak o vremenu koji se odnosi na taj zapis.

Detaljnije odredbe koje se odnose na tipove arhiviranih zapisa i lokacije Fina PKI arhiva nalaze se u Fininim internim dokumentima.

5.5.2 Vremenski period arhiviranja

Sve arhivirane podatke i dokumentaciju Fina čuva najmanje 10 godina od isteka certifikata na kojeg se odnosi.

5.5.3 Zaštita arhive

Arhivirana dokumentacija Fina CA sustava u papirnatom obliku čuva se u Fina PKI štićenom prostoru koji je opisan u točki 5.1.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta. Arhivirani zapisi su na zahtjev raspoloživi ovlaštenim osobama Fina PKI, uz dualnu kontrolu.

Arhivirana dokumentacija u papirnatom obliku koja je prikupljena u postupku registracije fizičkih osoba i poslovnih subjekata čuva se u štićenom arhivskom prostoru Fine koji je pod stalnim nadzorom službe tjelesne zaštite, a pristup arhiviranoj dokumentaciji omogućen je ovlaštenim osobama Fina PKI i djelatnicima zaduženim za arhivu FINE. Na ovaj način arhiva se štiti od neovlaštenog pregleda, izmjene i brisanja.

Arhivirani zapisi u elektroničkom obliku iz točke 5.5.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta čuvaju se na odgovarajućim medijima za arhiviranje podataka u Fina PKI štićenom prostoru koji je opisan u točki 5.1.1. Arhivirani zapisi štite se mehanizmima i postupcima koji osiguravaju povjerljivost i cjelovitost zapisa te ne dozvoljavaju izmjenu zapisa, kao ni jednostavno brisanje ili uništenje zapisa. Povjerljivost arhiviranih zapisa u elektroničkom obliku štiti se enkripcijom, a cjelovitost zapisa digitalnim potpisom. Arhivirani zapisi su na zahtjev

raspoloživi ovlaštenim osobama Fina PKI, uz dualnu kontrolu. Minimalno jednom godišnje Fina PKI osoblje provjerava integritet arhive, te ako je arhiva oštećena, ona se obnavlja pomoću sigurnosne kopije.

Arhivirani Fina PKI dokumenti i podaci o radu sustava su na zahtjev dostupni za potrebe pravnih postupaka u svrhu pružanja dokaza o ispravnom pružanju usluga.

5.5.4 Postupci izrade sigurnosnih kopija arhive

Sigurnosne kopije arhiviranih zapisa u elektroničkom obliku iz točke 5.5.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta čuvaju se u sekundarnom štićenom prostoru na pričuvnoj lokaciji iz točke 5.1.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta koji ima jednaku ili višu razinu zaštite u odnosu na Fina PKI štićeni prostor na primarnoj lokaciji.

Pristup sigurnosnim kopijama arhiviranih zapisa u elektroničkom obliku ima samo ovlašteno osoblje Fina PKI, uz dualnu kontrolu.

5.5.5 Zahtjevi na zaštitu zapisa vremenskim žigom

Nema odredbi.

5.5.6 Sustav prikupljanja arhivskih zapisa (unutarnji ili vanjski)

Arhivirani zapisi prikupljaju se na način koji ovisi o vrsti podataka i dokumenata.

Dokumentacija Fina CA sustava u papirnatom obliku prikuplja se manualno i arhivira se interno u Fina PKI štićenom prostoru koji je opisan u točki 5.1.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

Dokumentacija o registriranim fizičkim osobama i poslovnim subjekata u papirnatom obliku, prikupljena ili nastala u Fina RA mreži, prikuplja se manualno i arhivira se interno.

Dokumentacija o registriranim fizičkim osobama i poslovnim subjekata u papirnatom obliku, prikupljena ili nastala u vanjskim ugovorenim RA-ovima, prikuplja se manualno te se arhivira sukladno odredbama ugovora sklopljenog između Fine i vanjskog ugovorenog RA.

Zapisi u elektroničkom obliku iz točke 5.5.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta prikupljaju se automatski te se arhiviraju interno u Fina PKI štićenom prostoru na primarnoj lokaciji te u sekundarnom štićenom prostoru na pričuvnoj lokaciji iz točke 5.1.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

5.5.7 Postupci dobivanja i provjere arhiviranih zapisa

Pristup zapisima iz arhive imaju samo osobe ovlaštene za pristup podacima iz arhive. Pristup podacima arhiviranim u štićenim prostorima iz točke 5.1.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta imaju samo ovlaštene osobe Fina PKI, uz dualnu kontrolu.

Verifikacija podataka iz arhive obavlja se provjerom njihove cjelovitosti, npr. verifikacijom digitalnog potpisa kojim su arhivirani podaci potpisani.

Arhivirani podaci u elektroničkom obliku se po potrebi uspoređuju s pripadnom kopijom.

5.6 Promjena CA ključa

Radi potrebe osiguranja kontinuiteta pružanja usluge certificiranja Fina će dovoljno vremena prije isteka CA certifikata, generirati novi par ključeva za Fina CA. Također, Fina CA će dovoljno vremena ranije generirati novi par CA ključeva i u slučaju kada tu promjenu zahtjeva razina sigurnosti kriptografskog algoritma privatnog CA ključa u uporabi.

Fina CA par potpisnih ključeva generira se na način opisan u točki 6.1 ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta. Novi certifikat Fina CA s novo generiranim javnim ključem potpisuje se privatnim ključem Fina Root CA.

O planiranoj promjeni ključa Fina CA, Fina će pravovremeno obavijestiti sudionike Fina PKI objavom informacija na stranicama Fina PKI repozitorija iz točke 2.2.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta. Novi certifikat Fina CA dostupan je sudionicima Fina PKI putem javnog imenika i internetskih stranica repozitorija.

Novi certifikat Fina CA dostavit će se Potpisnicima, Autorima pečata i Pouzdajućim stranama na način na koji se dostavlja postojeći Fina CA certifikat, sukladno točki 6.1.4. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

5.7 Oporavak od kompromitiranja ili nepogode

5.7.1 Postupci u slučaju incidenta ili kompromitiranja

Fina provodi kontinuirani nadzor rada Fina PKI sustava te se u slučaju pojave greške ili incidenta na sustavu provodi pravodobno i koordinirano reagiranje na dojavljeni događaj sukladno Fininim internim procedurama.

Fina ima plan kontinuiteta poslovanja Fina PKI, a kojim su regulirani postupci u slučajevima:

- prirodnih katastrofa,
- napada, pljački ili blokade zgrade,
- uništenja IT infrastrukture na primarnoj produkcijskoj lokaciji,
- nedostupnost IT infrastrukture na primarnoj produkcijskoj lokaciji uslijed kvara hardvera ili softvera većih razmjera,
- nedostupnosti radnika,
- prekida usluga dobavljača,
- za događaje gubitka ili kompromitiranja ili sumnje u kompromitiranost privatnog ključa Fina CA.

Internim planovima obuhvaćeni su i postupci koje treba poduzeti u cilju oporavka i uspostave prvotnih sigurnosnih prilika RA sustava, arhive i repozitorija.

Nakon pojave neke od navedenih nepogoda Planom kontinuiteta poslovanja propisano je i provođenje mjera za sprečavanje ponavljanja takve nepogode, u slučajevima kada su takve mjere izvedive. Odabir mjera za sprečavanje ponavljanja nepogode donijet će se nakon analize uzroka i posljedica nepogode.

Obavještavanje u slučaju gore navedenih nepogoda opisano je u odgovarajućim postupcima za slučajeve nepogoda.

Obavještavanje u slučaju kompromitiranja ili sumnje u kompromitiranost privatnog ključa Fina CA opisano je u točki 5.7.3. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

Plan kontinuiteta poslovanja Fina PKI revidira se jednom godišnje.

5.7.2 Postupci u slučaju oštećenja u računalnim resursima, programima i/ili podacima

Finin sustav certificiranja zasnovan je na pouzdanim hardverskim i softverskim komponentama, a kritične operacije sustava podržane su redundantnim komponentama.

Za osiguranje raspoloživosti vanjskog pristupa Fina PKI servisima Fina raspolaže redundantnim mrežnim konekcijama.

Funkcionalnost, ispravnost rada i pravovremeno otklanjanje oštećenja komponenti sustava certificiranja osigurano je kroz ugovore o podršci i održavanju s dobavljačima opreme.

Plan kontinuiteta poslovanja Fina PKI regulira postupke oporavka sustava certificiranja u slučaju kvarova ili oštećenja opreme i mrežnih resursa te povrat podataka.

Sigurnosne kopije elektroničkih zapisa nastalih u radu Fina PKI sustava izrađuju se na dnevnoj razini te se periodički dostavljaju u štićeni prostor na pričuvnoj lokaciji.

5.7.3 Postupci u slučaju kompromitiranja privatnog ključa

U slučaju kompromitiranja privatnog ključa Fina CA Fina će odmah po saznanju prekinuti s uporabom kompromitiranog privatnog ključa Fina CA te će ispitati okolnosti kompromitiranja ključa. Ako se potvrdi kompromitiranje ključa Fina donosi odluku o opozivu CA certifikata povezanog s kompromitiranim ključem te Fina Root CA opoziva taj Fina CA certifikat.

O opozivu Fina CA certifikata Fina će obavijestiti sljedeće sudionike Fina PKI:

- Fina RA mrežu i vanjske ugovorene RA,
- Korisnike,
- Pouzdajuće strane.

Nakon ustanovljavanja i otklanjanja uzroka koji su prouzročili kompromitiranje CA ključa, Fina će, ako je primjenjivo, poduzeti mjere za sprječavanje ponavljanja takvog događaja.

Ovisno o utvrđenim uzrocima kompromitiranja ključa Fina može donijeti odluku o privremenom prelasku na produkciju sa sekundarne lokacije.

Fina će za Fina CA čiji je certifikat opozvan organizirati ceremoniju generiranja novog para CA ključeva te će Fina Root CA će za novi javni CA ključ izdati novi CA certifikat.

Fina CA će uporabom novog privatnog CA ključa izdati certifikate postojećim registriranim Subjektima te će sve naredne informacije o opozvanosti certifikata potpisivati uporabom novog ključa. Novi CA certifikat biti će dostupan sudionicima Fina PKI na način na koji je bio dostupan i prethodni CA certifikat, a sukladno opisu u točki 2.2.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

U slučaju da korišteni kriptografski algoritmi i parametri prestanu pružati zahtijevanu sigurnost i zaštitu Fina će, ukoliko je to moguće, pravodobno o tome obavijestiti:

- Fina RA mrežu i vanjske ugovorene RA,
- Korisnike,
- Pouzdajuće strane.

Fina će razmotriti mogućnost korištenja drugih odgovarajućih preporučenih sigurnijih kriptografskih algoritama te će, ukoliko to bude moguće, donijeti odluku o korištenju drugog algoritma. Fina će izraditi konkretne planove i postupke koji će obavezno uključivati i provedbu opoziva svih certifikata na koje utječu kriptografski algoritmi i parametri čija je sigurnost narušena. O planovima i rokovima provedbe Fina će obavijestiti Korisnike i Pouzdajuće strane te će provest planirane aktivnosti u cilju nastavka pružanja usluge Korisnicima.

5.7.4 Mogućnost nastavka poslovanja nakon nepogode

U planu kontinuiteta poslovanja Fina PKI određeni su postupci za nastavak poslovanja nakon nepogode. Ovisno o vrsti nepogode Fina će pružanje usluge certificiranja nastaviti na svojem primarnom produkcijskom sustav certificiranja ili će pružanje usluge nastaviti na svojem sekundarnom sustavu certificiranja do oporavka svojeg primarnog produkcijskog sustava.

Strategijom kontinuiteta poslovanja regulirani su uvjeti i prijelaz pružanja usluga povjerenja na sekundarni sustav certificiranja.

5.8 Prestanak rada CA ili RA

U slučaju prestanka rada vanjskog ugovorenog RA raskida se ugovor između Fine i vanjskog RA te se ukidaju sva ovlaštenja vanjskog RA, uključujući ovlaštenja Službenika za registraciju, Službenika za opoziv certifikata u vanjskom RA te sva ovlaštenja vanjskog RA za dostavu zahtjeva za izdavanje, opoziv suspenziju i reaktivaciju certifikata u Fina PKI sustav. Poslove ugovorenog RA koji prestaje s radom može preuzeti Fina RA mreža. Detaljnije odredbe vezane uz prekid rada vanjskog ugovorenog RA određuju se ugovorom.

O planiranom prestanku pružanja usluga certificiranja Fina će:

- obavijestiti sve Korisnike usluge, Pouzdajuće strane i središnje tijelo državne uprave nadležno za poslove gospodarstva najmanje tri mjeseca prije planiranog prestanka pružanja usluga certificiranja,
- za svaki vanjski RA raskinuti ugovor između Fine i vanjskog RA te time ukinuti sva ovlaštenja vanjskog RA sukladno opisu navedenom prethodno u ovoj točki,
- uložiti sav napor da kod drugog kvalificiranog pružatelja usluga povjerenja osigura nastavak pružanja usluga izdavanja kvalificiranih certifikata te će tom pružatelju usluga dostaviti svu dokumentaciju prikupljenu u postupku registracije Korisnika kao i svu dokumentaciju o izdanim certifikatima,
- na tog pružatelja usluga prenijeti svoju obavezu da pouzdajućim stranama tijekom razumnog vremena omogući raspoloživost Fina CA certifikata u kojima su javni ključevi Fina CA-ova, kao i raspoloživost drugih certifikata s javnim ključevima Fininih usluga povjerenja,
- na tog pružatelja usluga prenijeti svoju obavezu omogućavanja raspoloživosti CRL za sve opozvane Korisničke certifikate i certifikate Fina CA-ova koji prestaju s radom,
- na tog pružatelja usluga prenijeti svoju obavezu pružanja informacija putem OCSP servisa o opozvanim Korisničkim i Fina CA certifikatima,
- opozvati sve izdane nekvalificirane certifikate,
- opozvati certifikate Fina CA-ova koji prestaju s radom te uništiti pripadajuće privatne ključeva tih CA-ova.

U slučaju prestanka pružanja usluga izdavanja kvalificiranih certifikata Fina će arhivirati, zaštititi i čuvati zapise prema odredbama iz točke 5.5. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta kako bi ti zapisi bili raspoloživi za pružanje dokaza u sudskim, upravnim i drugim postupcima u skladu s važećim odredbama zakonske regulative, ili će Fina s drugim poslovnim subjektom ugovoriti takvo arhiviranje, zaštitu i čuvanje zapisa.

6 TEHNIČKE MJERE ZAŠTITE

Ovo poglavlje opisuje mjere zaštite koje se poduzimaju u cilju postizanja zahtijevane razine sigurnosti kriptografskih ključeva, aktivacijskih podataka, kritičnih sigurnosnih parametara, upravljanja ključevima i drugih mjera tehničke sigurnosti za Fina CA-ove i za izdavanje korisničkih certifikata.

Konkretni postupci i mjere zaštite koje se poduzimaju u cilju postizanja zahtijevane razine sigurnosti interne su prirode i ne objavljuju se javno.

6.1 Generiranje i instalacija para ključeva

6.1.1 Generiranje para ključeva

Fina provodi generiranje para ključeva Fina CA-ova koristeći algoritme za generiranje ključeva koji su sukladni s normizacijskim dokumentom ETSI TS 119 312 [14].

6.1.1.1 Generiranje para Fina CA ključeva

Postupak generiranja para Fina CA ključeva provodi se formalnom ceremonijom generiranja para ključeva za subordinirane Fina CA-ove kojoj prisustvuju ovlaštene osobe Fina PKI.

Ceremonija generiranja para ključeva za Fina CA provodi se prema protokolu za generiranje ključeva u kojem su dokumentirani koraci koji se izvode za vrijeme ceremonije. Protokol za generiranje ključeva sukladan je s mjerama tehničke sigurnosti prema normi ETSI EN 319 411-1 i sa zahtjevima CA/Browser Forum BRG [24].

Kriptografski algoritmi koji se koristi za generiranje ključeva kao i duljina ključeva za Fina CA odabrani su sukladno normizacijskom dokumentu ETSI TS 119 312 [14] tako da budu prikladni za cijelo vrijeme važenja CA certifikata.

Par ključeva za FINA CA generira se, uz minimalno dualnu kontrolu ovlaštenih osoba s povjerljivim ulogama u Fina PKI, u HSM modulu koji zadovoljava zahtjeve iz točke 6.2.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

FINA CA nalazi se tijekom i nakon ceremonije generiranja parova ključeva u Fina PKI štićenom prostoru iz točke 5.1.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta, a pristup Fina CA dopušten je ovlaštenim osobama Fina PKI s povjerljivim ulogama, uz minimalno dualnu kontrolu.

Provođenje postupka ceremonije generiranja para ključeva za Fina CA snima se video kamerom ili provođenju postupka svjedoči Kvalificirani auditor.

O provedenom generiranju CA ključeva vodi se zapisnik s priloženim revizijskim zapisima.

Fina posjeduje izvješće Kvalificiranog auditora koji svjedoči da je postupak generiranja parova ključeva za Fina CA proveden sukladno protokolu i zahtjevima za generiranje ključeva.

6.1.1.2 Generiranje para RA ključeva

Parovi ključeva za ovlaštene osobe Fina RA mreže generiraju se u sigurnim kriptografskim uređajima koji zadovoljavaju zahtjeve iz točke 6.2.1. $CPS_{NQC\text{-}eIDAS}$ dokumenta. Parove ključeva generiraju Službenici za registraciju u svojim LRA uredima, a po potrebi generiraju ih i Službenici za registraciju u Središnjem RA Fine.

6.1.1.3 Generiranje para korisničkih ključeva NCP+ certifikata

a) Generiranje para korisničkih ključeva na QSCD ili sigurnom kriptografskom uređaju

Na QSCD ili sigurnim kriptografskim uređajima generiraju se parovi ključeva za sljedeće tipove certifikata koje izdaje Fina RDC 2015 CA:

- *Osobni autentikacijski certifikat (NCP+),*
- *Poslovni autentikacijski certifikat (NCP+),*
- *Aplikacijski certifikat razine 2 (NCP+),*
- *Certifikat za e-pečat Trusted liste (NCP+),*
- *Administrativni certifikat (NCP+).*

Na QSCD ili sigurnim kriptografskim uređajima generiraju se parovi ključeva za *TDU autentikacijski certifikat (NCP+)* kojeg izdaje Fina RDC-TDU 2015 CA.

QSCD uređaj i sigurni kriptografski uređaj na kojem se generiraju ključevi zadovoljava zahtjeve iz točke 6.2.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

Za provođenje generiranja korisničkog para ključeva za ove certifikate koji se izdaju na QSCD ili sigurnim kriptografskim uređajima ovlašteni su pripadajući Potpisnici, Skrbnici, odnosno Ovlašteni predstavnici, te Službenici za registraciju u Fina LRA i Službenici za registraciju u Središnjem RA Fine. Ove ovlaštene osobe generiranje korisničkog para ključeva provode na svojim lokacijama.

Ukoliko par ključeva generira Službenik za registraciju u Fina LRA ili Službenik za registraciju u Središnjem RA Fine ključevi se generiraju na QSCD odnosno sigurnom kriptografskom uređaju, pod udaljenim *online* nadzorom i upravljanjem Fina CMS sustava uz prethodnu autentikaciju Službenika za registraciju i uz sigurnu TLS komunikaciju.

Ukoliko par ključeva generira Potpisnik, odnosno Skrbnik tada se ključevi na QSCD odnosno sigurnom kriptografskom uređaju generiraju na korisničkoj lokaciji, po preuzimanju QSCD odnosno sigurnog kriptografskog uređaja u RA mreži, te po primitku aktivacijskih podataka. Potpisnik, odnosno Skrbnik par ključeva generira na jedan od sljedeća dva načina:

- Ukoliko je Potpisnik, odnosno Skrbnik registriran u Fina RA mreži ili je Potpisnik registriran u RA mreži vanjskog ugovorenog RA koji u postupku ne koristi vlastiti CMS, Potpisnik, odnosno Skrbnik se autenticira na udaljeni Fina CMS sustav sigurnom TLS komunikacijom, koristeći dobivene aktivacijske podatke i pripadajući QSCD odnosno sigurni kriptografski uređaj. U tom postupku, pod udaljenim *online*

nadzorom i upravljanjem Fina CMS sustava Potpisnik, odnosno Skrbnik na QSCD odnosno sigurnom kriptografskom uređaju generira par ključeva.

- Ukoliko je Potpisnik registriran u RA mreži vanjskog ugovorenog RA koji ima uspostavljen vlastiti CMS sustav, Potpisnik generira svoj par ključeva korištenjem tog CMS sustava. Potpisnik se autenticira na udaljeni CMS sustav vanjskog ugovorenog RA sigurnom TLS komunikacijom, koristeći dobivene aktivacijske podatke i pripadajući QSCD odnosno sigurni kriptografski uređaj. U tom postupku, pod udaljenim *online* nadzorom i upravljanjem CMS sustava vanjskog ugovorenog RA potpisnik na QSCD odnosno sigurnom kriptografskom uređaju generira svoj par ključeva.

Pri upravljanju postupkom generiranje ključeva CMS sustav provjerava provodi li se generiranje para ključeva u prethodno registriranom QSCD odnosno sigurnom kriptografskom uređaju.

Generiranje korisničkog para ključeva za *Certifikat za e-pečat Trusted liste (NCP+)* provode Službenici za registraciju u Fina LRA ili Službenici za registraciju u Središnjem RA Fine na QSCD odnosno sigurnom kriptografskom uređaju, pod udaljenim *online* nadzorom i upravljanjem Fina CMS sustava uz prethodnu autentikaciju Službenika za registraciju i uz sigurnu TLS komunikaciju.

Upravljanje postupkom generiranja ključeva uključuje i provjeru provodi li se generiranje para ključeva u QSCD ili sigurnom kriptografskom uređaju.

b) Generiranje para korisničkih ključeva u HSM modulu

U HSM modulu generiraju se parovi ključeva za *Aplikacijski certifikat razine 3 (NCP+)* tip certifikata kojeg izdaje Fina RDC 2015 CA:

HSM modul u kojem se generiraju ključevi zadovoljavaj zahtjeve iz točke 6.2.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

Za provođenje generiranja korisničkog para ključeva za ove certifikate ovlašteni su pripadajući Skrbnici koji generiranje korisničkog para ključeva provode na lokaciji poslovnog subjekta.

Fina će odbiti zahtjev za izdavanje certifikata ako dostavljeni korisnički javni ključ ne zadovoljava zahtjeve navedene u točkama 6.1.5 i 6.1.6. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

6.1.1.4 Generiranje para korisničkih ključeva za NCP i LCP certifikate

Parovi ključeva za sljedeće tipove certifikata koje izdaje Fina RDC 2015 CA generiraju se softverskim modulima:

- *Osobni soft certifikat (NCP),*
- *Poslovni soft certifikat (NCP),*
- *Poslovni soft certifikat (LCP),*

- *Aplikacijski certifikat razine 1 (NCP),*
- *Aplikacijski certifikat razine 2 (NCP).*

Generiranje para korisničkih ključeva za ove certifikate provodi Fina u svojem PKI štićenom prostoru iz točke 5.1.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta. Za generiranje para korisničkih ključeva tipova certifikata *Aplikacijski certifikat razine 1 (NCP) i Aplikacijski certifikat razine 2 (NCP)* ovlašten je i Skrbnik.

Ako generiranje para ključeva aplikacijskih certifikata provodi Skrbnik generiranje se provodi na lokaciji poslovnog subjekta. Generiranje para ključeva za *Aplikacijski certifikat razine 2 (NCP)* Skrbnik je obavezan provoditi u kontroliranoj okolini. Privatni ključevi štite se u softverskom zaštićenom tokenu na način opisan u točki 6.2.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

Fina će odbiti zahtjev za izdavanje certifikata ako dostavljeni korisnički javni ključ ne zadovoljava zahtjeve navedene u točkama 6.1.5 i 6.1.6. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

6.1.2 Dostava privatnog ključa korisniku

Ako Službenik za registraciju generira svoj par ključeva smatra se da već posjeduje privatni ključ. Ako privatni ključ za Službenika za registraciju u Fina LRA generira Službenik za registraciju Središnjeg RA Fine ili drugi Službenik za registraciju, tada se privatni ključ u sigurnom kriptografskom uređaju osobno uručuje Službeniku za registraciju, uz njegovu neposrednu identifikaciju.

Ako Potpisnik, Skrbnik ili Ovlašteni predstavnik na svojoj lokaciji generira privatni ključ na QSCD uređaju, sigurnom kriptografskom uređaju ili softverskom modulu, smatra se da Potpisnik, Skrbnik, odnosno Ovlašteni predstavnik već posjeduje privatni ključ.

Ako Službenik za registraciju u Fina LRA ili Službenik za registraciju Središnjeg RA Fine na svojoj lokaciji generira privatni ključ za Potpisnika, Skrbnika ili Ovlaštenog predstavnika na QSCD ili sigurnom kriptografskom uređaju, tada Službenik za registraciju u Fina RA mreži osobno, uz neposrednu fizičku identifikaciju, uručuje privatni ključ u sigurnom kriptografskom, odnosno QSCD uređaju identificiranom Potpisniku, Skrbniku, odnosno Ovlaštenom predstavniku.

Ako Fina generira privatni ključ u softverskom modulu, tada se privatni ključa i pripadajući certifikat dostavljaju registriranom Potpisniku odnosno Skrbniku u obliku zaštićene PKCS#12 datoteke. Dostava PKCS#12 datoteke obavlja se TLS kanalom korištenjem Fina CMS sustava, uz prethodnu uspješnu autentikaciju Potpisnika, odnosno Skrbnika.

6.1.3 Dostava javnog ključa CA-u

Dostava javnog ključa obavlja se elektroničkim putem korištenjem Fina CMS sustava koji nakon uspješno provedene autentikacije osobe ovlaštene za generiranje korisničkog para ključeva ostvaruje TLS komunikacijski kanal. Ovim kanalom javni ključ se dostavlja u PKCS#10 formatu zahtjeva koji je potpisan generiranom privatnim ključem Korisnika. Osobe

ovlaštene za generiranje korisničkog para ključeva navedene su u točki 6.1.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

Ako par korisničkih ključeva ne generira Fina proces zahtijevanja certifikata obuhvaća provjeru posjeduje li ili kontrolira li Potpisnik ili Skrbnik privatni ključ koji je povezan s javnim ključem koji se dostavlja za izradu certifikata, na način koji sigurno povezuje potvrđeni identitet Potpisnika, odnosno Skrbnika i pripadajući javni ključ koji se dostavlja na certificiranje. Javni ključ se dostavlja u PKCS#10 formatu zahtjeva korištenjem Fina CMS sustava uz uspostavu TLS komunikacijskog kanala nakon uspješno provedene autentikacije Potpisnika, odnosno Skrbnika ili Ovlaštenog predstavnika.

Za certifikate navedene u točki 6.1.1.3.a) ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta proces zahtijevanja certifikata osigurava se da je javni ključ koji se dostavlja na certificiranje iz para ključeva koji je generiran u QSCD ili sigurnom kriptografskom uređaju.

6.1.4 Dostava javnog ključa CA pouzdajućim stranama

Javni ključevi Fina CA-ova dostupni su Pouzdajućim stranama u Fina CA certifikatima koje je izdao Fina Root CA te je tako osigurana cjelovitost i omogućena provjera izvornosti javnih ključeva Fina CA-ova.

Provjera izvornosti javnih ključeva Fina CA-ova osigurava se:

- objavom Fina Root CA certifikata i certifikata Fina CA-ova na internetskim stranicama Fina PKI repozitorija iz točke 2.2. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta, te dostavom sažetka Fina Root CA certifikata pouzdanim kanalom na zahtjev.
- objavom certifikata Fina CA-ova na nacionalnom pouzdanom popisu kvalificiranih pružatelja usluga povjerenja (*Trusted* lista) koje na svojim internetskim stranicama objavljuje središnje tijelo državne uprave nadležno za poslove gospodarstva kao tijelo odgovorno za pouzdani popis kvalificiranih pružatelja usluga povjerenja u Republici Hrvatskoj,

6.1.5 Duljine ključeva

Duljine ključeva u Fina PKI su sljedeće:

- Fina Root CA upotrebljava *sha256WithRSA* algoritam s ključem duljine 4096 bita,
- Subordinirani Fina CA-ovi (Fina RDC 2015 i Fina RDC-TDU 2015) upotrebljavaju *sha256WithRSA* algoritam s ključem duljine 4096 bita,
- Fina OCSP servis upotrebljava RSA ključeve duljine 2048 bita,
- RA mreža upotrebljava RSA ključeve duljine 2048 bita,
- Korisnici upotrebljavaju RSA par ključeva duljine 2048 bita.

6.1.6 Generiranje i provjera kvalitete parametara javnog ključa

Fina CA provodi generiranje para ključeva koristeći parametre za generiranje koji su sukladni s normizacijskim dokumentom ETSI TS 119 312 [14].

Zadovoljenje zahtjeva za generiranje i provjeru kvalitete parametara ključeva osigurava se korištenjem certificiranih HSM modula, sigurnih kriptografskih uređaja i QSCD uređaja prema odgovarajućim normama navedenim u točki 6.2.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta te strogim pridržavanjem zahtjeva navedenih u certifikacijskoj dokumentaciji tih uređaja.

Kad Skrbnik generira par ključeva sukladno točkama 6.1.1.3.b) i 6.1.1.4. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta, Skrbnik je dužan generiranje para ključeva provesti na način koji osigurava korištenjem parametara sukladno normizacijskom dokumentu ETSI TS 119 312 [14]. Pri zaprimanju javnog ključa generiranog od strane Skrbnika Fina provjerava da li javni ključ zadovoljava kvalitetu određenu ETSI TS 119 312 dokumentom te odbacuje javni ključ koji ne zadovoljava ove zahtjeve kvalitete i za njega ne izdaje certifikat.

6.1.7 Namjene ključeva

Certifikat Fina CA u ekstenziji *Key Usage* ima postavljene vrijednosti *keyCertSign* i *cRLSign*. Fina CA pripadajući privatni ključ koristi samo za:

- potpisivanje korisničkih certifikata i certifikata za LRA,
- potpisivanje certifikata za potpis odgovora OCSP servisa,
- potpisivanje pripadajuće CRL.

Svi certifikati iz tablica 1.1. i 1.2. iz točke 1.1.2. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta, osim *Certifikata za e-pečat Trusted liste (NCP+)* namijenjeni su za podršku elektroničkim potpisima, za jaku autentikaciju i enkripciju ključa. Ekstenzija *Key Usage* ovih certifikata označena je kritičnom (*critical*) i ima postavljene vrijednosti *digitalSignature* i *keyEncipherment*.

Certifikat za e-pečat Trusted liste (NCP+) namijenjen je isključivo za podršku elektroničkom pečatu *Trusted* liste. Ekstenzija *Key Usage* ovog certifikata označena je kritičnom (*critical*) i ima postavljene vrijednosti *digitalSignature* i *keyEncipherment*, a ekstenzija *extKeyUsage* sadrži OID koji označava da je privatni ključ certifikata namijenjen za potpis *Trusted* liste.

6.2 Zaštita privatnog ključa i tehnike upravljanja kriptografskim modulom

6.2.1 Norme i tehničke mjere zaštite kriptografskog modula

Privatni ključevi za subordinirane Fina CA-ove generiraju se i štite HSM modulima koji zadovoljavaju zahtjeve norme FIPS 140-2 [19] razina 3.

Privatni ključevi za Fina OCSP servise generiraju se i štite HSM modulima koji zadovoljavaju zahtjeve norme FIPS 140-2 [19] razina 3.

Za tipove certifikata navedene u točkama 6.1.1.2 i 6.1.1.3.a) ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta zaštita privatnih ključeva provodi se QSCD uređajima koji zadovoljavaju zahtjeve norme HRN EN 419 211 [15], [16], [17] i [18] ili sigurnim kriptografskim uređajima koji zadovoljava

zahtjeve norme FIPS 140-2 [19] razina 2 ili 3. Fina prati status certificiranosti ovih QSCD uređaja.

Za *Aplikacijski certifikat razine 3 (NCP+)* zaštita privatnih ključeva provodi se HSM modulom koji zadovoljava zahtjeve norme FIPS 140-2 [19] razina 3.

Zaštita privatnog ključa certifikata iz točke 6.1.1.4. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta provodi se u softverskom zaštićenom tokenu. Za tip certifikata *Aplikacijski certifikat razine 2 (NCP)* zaštita privatnog ključa dodatno se provodi kontroliranom okolinom na lokaciji poslovnog subjekta. Za način zaštite ovih privatnih ključeva na lokaciji fizičke osobe - građanina ili poslovnog subjekta zadužen je Potpisnik, odnosno poslovni subjekt.

6.2.2 Upravljanje privatnim ključem od strane više osoba (n od m)

HSM moduli kojim se štite privatni ključevi Fina CA-ova, OCSP servisa smješteni su u prostoru najviše razine sigurnosti unutar Fina PKI štićenog prostora. Fizički pristup ovim HSM modulima provodi se uz dualnu kontrolu ovlaštenih osoba s povjerljivim ulogama u Fina PKI.

Upravljanje Fina CA privatnim potpisnim ključevima provodi se uz najmanje dualnu kontrolu osoba s povjerljivim ulogama u Fina PKI. Pri upravljanju privatnim ključevima Fina CA osobe s povjerljivim ulogama koriste pripadajuće upravljačke kartice kriptografskog modula na principu n od m.

6.2.3 Sigurno skladištenje privatnog ključa

Nije dozvoljeno skladištenje privatnih ključeva Fina CA-ova.

Nije dozvoljeno skladištenje privatnih korisničkih ključeva povezanih s nekvalificiranim certifikatima.

6.2.4 Sigurnosno kopiranje privatnog ključa

Sigurnosno kopiranje privatnih ključeva Fina CA-ova provodi se uz dualnu kontrolu ovlaštenih osoba s povjerljivim ulogama u Fina PKI, u prostoru najviše razine sigurnosti unutar Fina PKI štićenog prostora. Privatni Fina CA ključ se izvan HSM modula nalazi isključivo u enkriptiranom obliku te se u tom obliku kopira i čuva u sigurnom prostoru najviše razine sigurnosti unutar Fina PKI štićenih prostora na odvojenim lokacijama.

Fizički pristup sigurnosnim kopijama privatnih ključeva Fina CA-ova imaju isključivo ovlaštene osobe s povjerljivim ulogama u Fina PKI uz dualnu kontrolu.

Fina nikada ne provodi sigurnosno kopiranje korisničkih privatnih ključeva povezanih s nekvalificiranim certifikatima.

Korisnik je odgovoran za zaštitu kopija privatnih ključeva za tipove certifikata iz točke 6.1.1.4. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta te je odgovoran u slučaju njihovog neovlaštenog korištenja na isti način kao i originala, a sukladno točki 9.6.3. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

6.2.5 Arhiviranje privatnog ključa

Nije dozvoljeno arhiviranje privatnih ključeva Fina CA-ova te se on uništava sukladno točki 6.2.10. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

Korisnički privatni ključevi se ne arhiviraju.

6.2.6 Prijenos privatnog ključa

Za vrijeme dok je izvan HSM modula privatni ključ je zaštićen enkriptiranjem. Enkriptiranje privatnog ključa provodi se strogim pridržavanjem zahtjeva navedenih u certifikacijskoj dokumentaciji HSM modula te se time osigurava jednaka razina sigurnosti privatnog ključa kao i kad se ključ nalazi u HSM modulu.

Prijenos privatnog ključa Fina CA iz HSM modula autoriziraju ovlaštene osobe s povjerljivim ulogama u Fina PKI, uz dualnu kontrolu unutar CA prostora Fina PKI štićenog prostora iz točke 5.1.1 ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

Kod prijenosa privatnih ključeva iz jednog HSM modula u drugi HSM privatni ključ se smije prenositi samo u HSM jednake ili više razine sigurnosti u odnosu na HSM iz kojega se privatni ključ prenosi.

Prijenos privatnih ključeva za tipove certifikata iz točke 6.1.1.4. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta u drugi spremnik privatnog ključa smije provoditi Potpisnik, odnosno Skrbnik na način da se privatni ključ prenositi samo u kriptografski modul jednake ili više razine sigurnosti u odnosu na kriptografski modul iz kojega se privatni ključ prenosi. Privatni ključ se prije prijenosa enkriptira kako bi tijekom prijenosa bio adekvatno zaštićen.

6.2.7 Spremanje privatnog ključa u kriptografskom modulu

Privatni ključevi Fina CA-ova zaštićeni su HSM modulima i mogu se koristiti jedino ako su propisno aktivirani.

Privatni ključevi *Aplikacijskog certifikata razine 3 (NCP+)* zaštićeni su HSM modulima i mogu se koristiti jedino ako su propisno aktivirani.

Nema ograničenja obzirom na format u kojem su privatni ključevi spremljeni u HSM modulima.

6.2.8 Metoda aktivacije privatnog ključa

Pokretanje CA servisa za izradu certifikata te aktivacija privatnog Fina CA ključa u hardverskom kriptografskom modulu provodi se pod dualnom kontrolom ovlaštenih osoba Fina CA.

Jednom aktiviran, privatni ključ ostaje aktiviran bez vremenskog ograničenja.

Aktivaciju privatnih ključeva korisničkih nekvalificiranih certifikata iz tablica 1.1 i 1.2. iz točke 1.1.2. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta smije provoditi pripadajući Potpisnik odnosno Skrbnik ili

Autor pečata korištenjem svojeg PIN-a ili odgovarajućih aktivacijskih podataka. Aktivacija privatnog ključa obavlja se na siguran način.

Samo Potpisnik, odnosno Skrbnik ili Autor pečata smije znati PIN ili odgovarajući aktivacijski podatak za aktivaciju svojeg privatnog ključa. Potpisnik obavlja aktivaciju privatnog ključa na način u kojem PIN ili odgovarajući aktivacijski podatak i dalje ostaje tajan.

6.2.9 Metoda deaktivacije privatnog ključa

Deaktivacija privatnog ključa Fina CA-ova provodi se prema postupcima i uz zadovoljenje zahtjeva određenih u certifikacijskom dokumentu upotrijebljenog HSM modula, uz dualnu kontrolu ovlaštenih osoba s povjerljivim ulogama u Fina PKI.

Deaktivacija privatnih ključeva subordiniranih Fina CA-ova, provodi se kada postoji neposredan zahtjev za privremenim obustavljanjem aktivnosti sustava, u slučajevima isteka perioda valjanosti privatnog ključa te u slučaju opoziva pripadajućeg certifikata.

Privatni ključevi subordiniranih Fina CA-ova deaktiviraju se:

- zaustavljanjem CA serverskog procesa,
- isključenjem HSM-a,
- isključenjem servera povezanim s HSM-om.

Privatni ključevi certifikata navedenih u točki 6.1.1.3. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta deaktiviraju se prestankom napajanja uređaja, zaustavljanjem korisničke aplikacije za potpisivanje ili pečatiranje te naredbom iz korisničke aplikacije za deaktivaciju uređaja.

Privatni ključevi certifikata navedenih u točki 6.1.1.4. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta zaštićeni softverskim tokenom deaktiviraju se zaustavljanjem korisničke aplikacije za potpisivanje ili pečatiranje te naredbom iz korisničke aplikacije za deaktivaciju softverskog tokena.

Deaktivirani privatni ključevi mogu se ponovno koristiti tek nakon ponovne aktivacije pripadajućim aktivacijskim podacima.

6.2.10 Metoda uništavanja privatnog ključa

Postupak uništavanja privatnog Fina CA ključa provodi se nakon isteka perioda valjanosti privatnog ključa, zbog kompromitiranja ili sumnje u kompromitiranost privatnog ključa, ili zbog prestanka njegova korištenja, a provode ga ovlaštene osobe s povjerljivim ulogama u Fina PKI. Postupkom uništavanja privatnog Fina CA ključa trajno su onesposobljene sve sigurnosne kopije tog privatnog ključa te ih više nije moguće upotrijebiti.

Prilikom povlačenja HSM-a Fina CA iz uporabe ili prije prijenosa HSM-a na drugu lokaciju obavlja se uništavanje privatnog potpisnog ključa Fina CA smještenog u HSM-u prema uputama proizvođača. Uništavanje privatnog ključa u HSM-u provodi se prije nego HSM napusti Fina PKI štićeni prostor.

Uništavanje privatnog Fina CA ključa provodi se uz prisutnost osoba s povjerljivim ulogama u Fina PKI.

Uništenje korisničkih privatnih ključeva pohranjenih u HSM modulu provodi Skrbnik na način koji osigurava da se nakon uništenja privatni ključ ni na koji način ne može oporaviti ili ponovno koristiti.

Uništenje korisničkih privatnih ključeva pohranjenih u QSCD ili sigurnim kriptografskim uređajima moguće je fizičkim uništenjem kriptografskih odnosno QSCD uređaja ili korištenjem odgovarajućih softverskih alata sukladno uputama proizvođača kriptografskih odnosno QSCD uređaja.

Uništenje privatnih ključeva pohranjenih u softverskim zaštićenim tokenima moguće je prikladnim aplikacijama ili softverskim alatima za uništavanje podataka.

Uništenje privatnih ključeva odgovornost je Potpisnika, Skrbnika, odnosno Autora pečata.

6.2.11 Ocjena kriptografskog modula

Ocjena HSM modula, sigurnih kriptografskih i QSCD uređaja provodi se certificiranjem prema odgovarajućim normama za kriptografske module navedenim u točki 6.2.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

6.3 Ostali vidovi upravljanja parom ključeva

6.3.1 Arhiviranje javnog ključa

Javni ključevi Fina CA i korisnički javni ključevi arhiviraju se u svrhu pružanja dokaza o certifikatima u sudskim, upravnim i drugim postupcima.

Javni ključevi Fina CA-ova sastavni su dio pripadajućih CA certifikata koji se arhiviraju sukladno točkama 5.5.3. i 5.5.4. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta, a u arhivi se čuvaju na rok iz točke 5.5.2. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

Javni ključevi Potpisnika i poslovnog subjekta sastavni su dio pripadajućih korisničkih certifikata. Fina provodi arhiviranje svih certifikata koje izdaju Fina CA-ovi te ih arhivira sukladno točkama 5.5.3. i 5.5.4. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta, a u arhivi se čuvaju na rok iz točke 5.5.2. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

6.3.2 Vremenski period važenja certifikata i korištenja para ključeva

Rok važenja certifikata po vrstama je definiran u Tablici 6.1.

Certifikat	Rok
Fina CA certifikat	10 godina
Certifikati standardne razine sigurnosti	Ne dulje od 5 godina
Certifikati srednje razine sigurnosti	2 godine
Certifikati visoke razine sigurnosti	1 godina

Tablica 6.1. Periodi važenja certifikata

Fina CA certifikat se izdaje s vremenom važenja koje ne prelazi perioda važenja Fina Root CA certifikata.

Vremenski period važenja privatnog ključa jednak je vremenskom periodu važenja pripadajućeg certifikata. Nije dozvoljena uporaba privatnih ključeva nakon isteka perioda važenja pripadajućih certifikata, nakon opoziva certifikata ili za vrijeme dok je certifikat suspendiran.

6.4 Aktivacijski podaci

6.4.1 Generiranje i instalacija aktivacijskih podataka

Aktivacijski podaci povezani s privatnim ključevima za Fina CA-ove generiraju se i instaliraju prilikom provođenja formalne ceremonije generiranja para ključeva za subordinirane Fina CA-ove. Aktivacijski podaci instaliraju se na pripadajuće upravljačke kartice kriptografskih modula koje se koriste za aktivaciju privatnog ključa subordiniranog Fina CA na principu n od m za pojedini Fina PKI štićeni prostor.

Aktivacijske podatke za Fina RA mrežu generiraju Službenici za registraciju u Središnjem RA Fine uporabom prikladnog generatora slučajnih brojeva, a na jednak način ih mogu generirati i Službenici za registraciju u Fina LRA.

Inicijalne aktivacijske podatke za sigurne kriptografske, odnosno QSCD uređaje generiraju Službenici za registraciju u Središnjem RA, odnosno u vanjskom ugovorenom RA uporabom prikladnog generatora slučajnih brojeva te se aktivacijski podaci čuvaju na siguran način do njihove isporuke Potpisnicima, Skrbnicima, odnosno Ovlaštenim predstavnicima.

Ako privatne ključeve za certifikate iz točke 6.1.1.4. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta generira Fina tada Fina prethodno generira i pripadajuće autentikacijske podatke kojima se Potpisnik, odnosno Skrbnik prijavljuje na Fina CMS. Aktivacijske podatke kojima se štiti privatni ključ u PKCS#12 datoteci generira i upisuje autenticirani Potpisnik, odnosno Skrbnik koristeći Fina CMS i TLS komunikacijski kanal.

Aktivacijske podatke za Aplikacijski certifikat razine 3 (NCP+) certifikate generira Skrbnik.

Ako aktivacijske podatke generira Potpisnik isti je odgovoran za sigurnost i zadovoljenje propisane kvalitete aktivacijskih podataka.

Ako aktivacijske podatke generira Skrbnik ili Ovlašteni predstavnik, za sigurnost i zadovoljenje propisane kvalitete aktivacijskih podataka odgovoran je pripadajući poslovni subjekt.

6.4.2 Zaštita aktivacijskih podataka

Aktivacijski podaci povezani s privatnim ključem Fina CA-ova čuvaju se na siguran način.

Aktivacijski podaci za privatne ključeve subordiniranih Fina CA-ova koji su smješteni na upravljačke kartice kriptografskih modula zaštićeni su pripadajućim zaporkama koje su generirane u Fina PKI štićenom prostoru. Upravljačke kartice kriptografskih modula dodjeljuju se ovlaštenim osobama s povjerljivim ulogama u Fina PKI sukladno točki 5.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta. Upravljačke kartice kriptografskih modula i pripadajuće zaporke čuvaju se u odvojenim sigurnosnim spremnicima pojedinog Fina PKI štićenog prostora.

Aktivacijski podaci sigurnih kriptografskih, odnosno QSCD uređaja distribuiraju se Potpisnicima, Skrbnicima odnosno Ovlaštenim predstavnicima na siguran način, odvojenim kanalom u odnosu na uručivanje kriptografskih, odnosno QSCD uređaja. Prije prve uporabe QSCD uređaja Potpisnik, Skrbnik odnosno Ovlašteni predstavnik mora na QSCD uređaju promijeniti aktivacijske podatke. Preporuka je da prije prve uporabe sigurnog kriptografskog uređaja Potpisnik, Skrbnik odnosno Ovlašteni predstavnik na uređaju promijeni aktivacijske podatke.

Ako privatne ključeve za certifikate iz točke 6.1.1.4. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta generira Fina tada Fina Potpisniku, odnosno Skrbniku dostavlja autentikacijske podatke kojima će se Ovlašteni predstavnik prijaviti na Fina CMS pomoću dva odvojena kanala ili ih Službenik za registraciju osobno uručuje Ovlaštenom predstavniku.

Potpisnici, Skrbnici, odnosno Autori pečata zaduženi su i odgovorni za zaštitu i čuvanje aktivacijskih podataka pripadajućih privatnih ključeva.

Aktivacijski podaci ne smiju se čuvati zajedno sa QSCD ili sigurnim kriptografskim uređajem na kojeg se odnose.

6.4.3 Ostale odredbe o aktivacijskim podacima

Ukoliko aktivacijske podatke generira Fina, aktivacijske podatke Potpisniku, Skrbniku odnosno Ovlaštenom predstavniku Fina dostavlja e-mailom ili preporučenom poštanskom pošiljkom. E-mailom se aktivacijski podaci dostavljaju u enkriptiranom obliku.

Potpisnik, Skrbnik odnosno Ovlašteni predstavnik može periodički mijenjati aktivacijske podatke za privatne ključeve kvalificiranih certifikata kako bi se smanjila mogućnost njihova otkrivanja.

Ne postavljaju se dodatni zahtjevi na životni ciklus aktivacijskih podataka korisničkih certifikata.

Dodatna pravila o uvjetima i životnom ciklusu aktivacijskih podataka subjekata mogu biti određena u ugovoru o obavljanju usluga certificiranja.

6.5 Upravljanje računalnom sigurnošću

6.5.1 Posebni tehnički zahtjevi na računalnu sigurnost

Pristup IT sustavu i aplikacijama u Fina PKI imaju isključivo ovlaštene osobe nakon autentikacije. Kontrola pristupa operacijskim sustavima Fina CA poslužitelja dopušta pristup samo ovlaštenom osoblju s povjerljivim ulogama u Fina PKI.

Fina provodi odvajanje dužnosti i odgovornosti za povjerljive uloge osoblja u Fina PKI, sukladno točki 5.2.4. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

Fina provodi upravljanje korisničkim računima ovlaštenih osoba s povjerljivim ulogama u Fina PKI sukladno internoj dokumentaciji. Upravljanje korisničkim računima obuhvaća pravovremenu izmjenu korisničkih prava, onemogućavanje pristupa i ukidanje korisničkog računa.

Identifikacija i potvrđivanje identiteta za svaku povjerljivu ulogu u Fina PKI provodi se korištenjem odgovarajućih sredstava za autentikaciju sukladno točki 5.2.3. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

Za sve korisničke račune koji mogu izravno pokrenuti izdavanje certifikata nužna je dvofaktorska autentikacija.

Izmjena i objava statusa opozvanosti certifikata provodi se uz dvofaktorsku autentikaciju i obveznu kontrolu pristupa.

Fina PKI sustav provodi kontinuirano praćenje i posjeduje alarmni sustav u svrhu detektiranja, bilježenja i pravovremenog reagiranja na pokušaje nedozvoljenog pristupa resursima sustava.

Implementiran je sustava zaštite od zloćudnog koda te je zabranjeno korištenja neautoriziranog softvera. Provodi se test CA softvera u cilju provjere njegove autentičnosti i cjelovitosti.

Uređaji za pohranu podataka na kojem se nalaze ili su se nalazili povjerljivi podaci se prije ponovne uporabe izvan PKI na siguran način brišu korištenjem alata propisanih u internoj Fininoj dokumentaciji, a kako bi se spriječio neovlašteni pristup podacima koji su se na njima nalazili.

Komunikacija između Fina CMS i klijentske aplikacije na strani korisnika provodi se zaštićenim kanalom.

6.5.2 Ocjena računalne sigurnosti

U cilju sigurnosti i kvalitete pružanja usluga povjerenja Fina ima uspostavljen sustav upravljanja informacijskom sigurnošću sukladan normi ISO/IEC 27001 [6]. Sukladnost se potvrđuje certifikatom izdanim od strane neovisnog certifikacijskog tijela.

6.6 Tehničke kontrole životnog ciklusa

6.6.1 Kontrole razvoja sustava

Pri nabavi razvoja softvera od vanjskog izvođača, Fina ugovorom s dobavljačem osigurava sigurnosne principe razvoja sustava.

Analiza sigurnosnih zahtjeva provodi se u fazi dizajna i specifikacije bilo kojeg projekta razvoja Fina PKI sustava kako bi se osiguralo da je sigurnost ugrađena u informacijske tehnologije u Fina PKI sustavima.

Softver koji se koristi za pružanje usluge izdavanja nekvalificiranih certifikata potječe iz pouzdanog izvora. Nove verzije softvera testiraju se u testnom okruženju. Implementacija softvera u produkciju provodi se u skladu s dokumentiranim postupcima upravljanja promjenama.

Plan za upravljanje konfiguracijom Fina PKI sustava sadrži jasan prikaz trenutnog stanja, popis dokumentacije nastale u sklopu izrade informacijskog sustava, mjere za osiguranje kvalitete, procjenu ranjivosti, softverski dizajn, sistemski test i definicije kontrolnih mehanizama.

6.6.2 Kontrole upravljanja sigurnošću

Sustav za izdavanje certifikata automatski obavlja periodičku provjeru integriteta baze podataka kojom se provjerava konzistentnosti podataka u bazi. Provodi se i automatska periodička provjera integriteta revizijskih zapisa sustava za izdavanje certifikata.

HSM-ovi za Fina CA-ove se prilikom transporta u nabavi štite mjerama od proboja i neovlaštene izmjene koje osigurava proizvođač. Prilikom isporuke HSM-ovi se provjeravaju obzirom na proboj te se provjerava njihov integritet. Transfer HSM-a kojeg obavlja Fina reguliran je posebnom internom procedurom.

Pri pokretanju HSM modula provodi se automatska provjera njihovog integriteta.

Fina provodi upravljanje primjene softverskih zakrpi kroz sustav upravljanja promjenama. Pri tome se pravovremeno instaliraju dostupne softverske zakrpe. Prije instalacije zakrpe provjerava se da li primjena zakrpe uzrokuje nestabilnost ili unosi ranjivost u rad sustava. Razlozi zbog kojih se pojedina zakrpa ne primjenjuje se dokumentiraju kroz sustav upravljanja promjenama.

Prilikom instalacije softvera i njegovih zakrpi u Fina PKI provode se mjere za provjeru autentičnosti i cjelovitosti softvera koji se instalira.

Ovlašteno osoblje u Fini provodi kontrolu i nadzor postavki Fina PKI sustava.

Fina provodi provjeru sustava certificiranja u Fina PKI produkcijskoj hijerarhiji zasnovanoj na Fina Root CA u odnosu na sigurnost, pouzdanost i kvalitetu djelovanja, a u skladu s važećim propisima iz točke 9.14. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

U slučaju povrede sigurnosti sustava certificiranja ili gubitka njegovog integriteta koji može imati značajan utjecaj na pružanje usluge povjerenja ili na zaštitu osobnih podataka Fina će u roku od 24 sata o istome obavijestiti središnje tijelo državne uprave nadležno za poslove gospodarstva kao tijelo nadležno za nadzor pružatelja usluga povjerenja te prema potrebi, druga nadležna tijela. U slučaju da gubitak integriteta može imati negativni utjecaj na korisnike Fininih usluga povjerenja Fina će o istome bez odgode obavijestiti sve fizičke osobe i poslovne subjekte na koje povreda sigurnosti može utjecati.

6.6.3 Sigurnosne kontrole životnog ciklusa

Fina provodi upravljanje promjenama u Fina PKI kako bi se promjene izvodile iz opravdanog razloga te na kontrolirani i formalizirani način.

Integritet sustava certificiranja i informacija štiti se antivirusnom zaštitom i uporabom autoriziranog softvera.

Provodi se praćenje raspoloživih kapaciteta sustava certificiranja te se procjenjuje zadovoljenje postojećih kapaciteta za buduće potrebe sustava kako bi se pravodobno planiralo njihovo proširenje.

6.7 Provjera mrežne sigurnosti

Sigurnost računalne mreže Fina PKI sustava zasnovana je na konceptu odjeljivanja mreže na mrežne zone različitih razina. Mrežne zone odjeljuju se vatrozidovima koji propuštaju samo nužan mrežni promet. Na sve sustave locirane unutar jedne mrežne zone primjenjuju se jednake sigurnosne mjere.

Mrežni segment na kojem se nalaze radne stanice za administraciju Fina CA vatrozidom je odvojen od ostalih mrežnih segmenata i računala koja se nalaze u tim mrežnim segmentima.

Oprema za zaštitu računalne mreže bilježi tok prometa i pokušaje pristupa Fina CA servisima te LDAP servisu javnog imenika. Informacije koje se bilježe definirane su u točki 5.4.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta. Samo ovlašteno osoblje u Fina PKI ima administratorske ovlasti za podešavanje i upravljanje opremom za zaštitu računalne mreže. Udaljeno podešavanje opreme za zaštitu računalne mreže nije dozvoljeno.

Nepotrebne komunikacije, računi, portovi, protokoli i servisi su eksplicitno zabranjeni ili deaktivirani.

Interna računalna mreža Fina PKI zaštićena je od neovlaštenog pristupa, uključujući pristup korisnika i trećih strana.

Svi kritični sustavi za pružanje usluga povjerenja smješteni su u Fina PKI štićenom prostoru te su raspoređeni u više različitih sigurnosnih mrežnih zona.

Kritičnim sustavima u Fina PKI štićenom prostoru onemogućen je mrežni pristup izvan tog prostora.

CA sustavi posebno su sigurnosno podešeni i očvršćeni.

Mrežne komponente Fina PKI sustava čuvaju se u fizički i logički sigurnom okruženja i usklađenost njihove konfiguracije periodički se provjerava.

6.8 Uporaba vremenskog žiga

Vremenski žig se ne upotrebljava u opsegu usluga certificiranja iz ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

Vrijeme u sustavu certificiranja Fine usklađeno je s UTC točnim vremenom. Revizijski zapisi Fina PKI sustava sadržavaju točan podatak o datumu i vremenu njihovog nastanka, uz odstupanje manje od +/- 1 s.

7 SADRŽAJ CERTIFIKATA, LISTA OPOZVANIH CERTIFIKATA I OCSP PROFILI

7.1 Profil certifikata

Ovo poglavlje sadrži opis profila certifikata, lista opozvanih certifikata (CRL) i odgovora OCSP servisa koje Fina kao pružatelj usluga certificiranja kroz Fina RDC 2015 i Fina RDC-TDU 2015 CA-ove izdaje sukladno opsegu ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

Profili certifikata iz opsega ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta koje izdaju subordinirani Fina CA-ovi usklađeni su s normama ETSI EN 319 411-1 [9] i ETSI EN 319 412 [10], [11] i [12].

Subordinirani Fina CA-ovi izdaju certifikate prema profilima koji su određeni ovim $CPS_{NQC\text{-}eIDAS}$ dokumentom. Ovisno o namjeni certifikata, pravilima prema kojima je certifikat izdan, razini sigurnosti i načinu čuvanja pripadajućih privatnih ključeva, svaki tip certifikata ima definiran jedinstveni Finin OID općih pravila certificiranja (CP OID), a pored tog OID-a sadrži i odgovarajući ETSI OID općih pravila certificiranja.

7.1.1 Broj(evi) verzije

Certifikati su sukladni verziji 3 prema X.509 specifikaciji.

7.1.2 Ekstenzije certifikata

Dokument s opisom profila certifikata dostupan je na internetskim stranicama Fina PKI repozitorija iz točke 2.2.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

7.1.3 Identifikator objekta (OID) algoritama

Algoritmi s pripadajućim OID identifikatorima za sve certifikate koje izdaju subordinirani Fina CA-ovi prikazani su u Tablici 7.1.

Algoritam	OID
sha256WithRSAEncryption	1.2.840.113549.1.1.11
rsaEncryption	1.2.840.113549.1.1.1

Tablica 7.1. Algoritmi s pripadajućim OID identifikatorima

7.1.4 Oblici naziva

Oblici naziva za subordinirane Fina CA-ove opisani su u točki 1.3.2. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

Oblici naziva za certifikate koje izdaju subordinirani Fina CA-ovi opisani su u točkama 3.1.1. i 3.1.4. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

7.1.5 Ograničenja u nazivima

Ekstenzija *Name Constraints* se ne koristi.

7.1.6 Identifikator objekta (OID) općih pravila certificiranja

Ekstenzija *Certificate Policies* certifikata sadrži odgovarajuće Finine i ETSI OID-ove. U tablicama 1.1. i 1.2. točke 1.1.2. $CPS_{NQC\text{-}eIDAS}$ dokumenta naveden je popis tipova certifikata te pripadajući Finini i ETSI OID-ovi općih pravila certificiranja u ekstenziji *Certificate Policies*.

7.1.7 Uporaba ekstenzije *Policy Constraints*

Ekstenzija *Policy Constraints* se ne koristi.

7.1.8 Sintaksa i semantika kvalifikatora općih pravila

Kvalifikator općih pravila u ekstenziji *Certificate Policies* sadrži dva pokazivača u URI formatu koji sadrže internetsku adresu ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta na hrvatskom i engleskom jeziku.

7.1.9 Procesne semantike za kritičnu ekstenziju *Certificate Policies*

Nema odredbi.

7.2 Profil CRL

Profil CRL koje izdaju subordinirani Fina CA-ovi sukladan je preporuci IETF RFC 5280 [21].

7.2.1 Broj(evi) verzije

CRL su sukladne verziji 2 prema X.509 specifikaciji.

7.2.2 CRL i ekstenzije unosa u CRL

Ekstenzije CRL koje se koriste u CRL listama i u elementima unosa CRL lista koje izdaju Fina CA-ovi definirane su u Tablici 7.2.

Ekstenzije	Kritično	Vrijednost
crlExtensions		
cRLNumber	NO	Jednolično rastući serijski broj CRL duljine do 20 okteta.
AuthorityKeyIdentifier	NO	SHA-1 hash vrijednost duljine 160 bita
crlEntryExtensions		
reasonCode	NO	Kod razloga opoziva certifikata

Tablica 7.2. Ekstenzije CRL liste i elemenata unosa CRL listi koje izdaju Fina CA-ovi

7.3 OCSP profil

Profil odgovora Fina OCSP servisa usklađen je s preporukom IETF RFC 6960 [22].

7.3.1 Broj(evi) verzije

Profil odgovora Fina OCSP servisa sukladan je verziji 1 prema IETF RFC 6960 [22].

7.3.2 OCSP ekstenzije

Ekstenzije odgovora Fina OCSP servisa prikazane su u Tablici 7.3.

Ekstenzije	Kritično	Vrijednost
Nonce	NO	Vrijednost Nonce iz zahtijeva za status certifikata.
Extended Revoked Definition	NO	Kod razloga opoziva certifikata (*Reason code*)

Tablica 7.3. Ekstenzije odgovora Fina OCSP servisa

8 PROVJERA SUKLADNOSTI

Nadzor nad radom Fine kao kvalificiranog pružatelja usluga povjerenja reguliran je Uredbom (EU) br. 910/2014 [1] i Zakonom o provedbi Uredbe (EU) br. 910/2014 [2], a provodi ga središnje tijelo državne uprave nadležno za poslove gospodarstva.

Nadzor nad radom pružatelja usluga povjerenja u području prikupljanja, uporabe i zaštite osobnih podataka potpisnika mogu provoditi i državna te druga tijela određena zakonom i drugim propisima koji uređuju zaštitu osobnih podataka.

Provjera sukladnosti obavlja se u cilju potvrđivanja da Fina kao pružatelj usluga povjerenja i usluge izdavanja certifikata koje Fina pruža ispunjavaju zahtjeve utvrđene Uredbom (EU) br. 910/2014 [1], Zakonom o provedbi Uredbe (EU) br. 910/2014 [2] te normom ETSI EN 319 411-1 [9].

Fina ima implementiran sustav upravljanja kvalitetom prema normi ISO 9001 te se nalazi u certifikacijskom ciklusu čime dokazuje da ispunjava zahtjeve te norme, da ima dokumentiran sustav, definirane ovlasti, odgovornosti te opisane procese.

Također, Fina ima uspostavljen, kontinuirano nadziran, certificiran i prema poslovnim potrebama unaprjeđivan vlastiti sustav informacijske sigurnosti u skladu sa normom ISO/IEC 27001 [6].

8.1 Učestalost ili okolnosti ocjene sukladnosti

Provjere sukladnosti u radu Fina PKI su vanjske provjere sukladnosti i interne provjere sukladnosti.

Interne i vanjske provjere sukladnosti u radu Fina PKI provode se i kod vanjskih ugovorenih RA-ova.

8.1.1 Vanjska provjera sukladnosti

Vanjska provjera sukladnosti provodi se najmanje svakih 12 mjeseci, sukladno zahtjevima normi ETSI EN 319 411-1 [9] i ETSI EN 319 403 [13].

8.1.2 Interna provjera sukladnosti

Interna provjera sukladnosti provodi se prije početka pružanja nove kvalificirane usluge povjerenja, periodično najmanje svakih 12 mjeseci te nakon značajnijih promjena u radu Fina PKI.

Internom provjerom sukladnosti provodi se provjera usklađenosti sustava sa zahtjevima norme ETSI EN 319 411-2 [11].

8.2 Identitet/kvalifikacije ocjenitelja

Vanjsku provjeru sukladnosti provodi tijelo za ocjenjivanje sukladnosti. Osposobljenost tijela za ocjenjivanje sukladnosti i osposobljenost pripadajućih ocjenitelja osigurana je akreditacijom tijela za ocjenjivanje sukladnosti prema normi ETSI EN 319 403 [13].

Internu provjeru sukladnosti provode interni ocjenitelji sukladnosti koji zajedno raspolažu znanjima i razumijevanjem:

- odredbi norme ETSI/EN 319 411-1 [9],
- PKI područja te područja informacijske sigurnosti,
- zakonske regulative iz područja pružanja usluga povjerenja.

Interni ocjenitelji sukladnosti provode interne provjere sukladnosti uz pomoć zaposlenika kojima je dodijeljena uloga Službenik za nadzor sustava.

8.3 Odnos ocjenitelja s predmetom ocjenjivanja sukladnosti

Tijelo za ocjenjivanje sukladnosti i pripadajući ocjenitelji neovisni su od Fine i Fininih sustava ocjenjivanja.

Interni ocjenitelji sukladnosti ne ocjenjuju sukladnost iz vlastitog djelokruga odgovornosti.

8.4 Predmeti ocjenjivanja sukladnosti

Predmeti ocjenjivanja sukladnosti obuhvaćaju slijedeća područja pružanja usluga povjerenja:

- cjelovitost i točnost dokumentacije,
- implementiranost zahtjeva za usluge povjerenja,
- organizacijski procesi i procedure,
- tehničke procese i procedure,
- implementirane mjere informacijske sigurnosti,
- vjerodostojne sustave,
- fizičku sigurnost predmetnih lokacija.

Opis predmetnog ocjenjivanja sukladnosti definiran je planom ocjenjivanja sukladnosti.

Fina će ocjenitelju sukladnosti na zahtjev omogućiti pristup svim prostorima Fina PKI sustava, uključivo i prostoru vanjskog RA, pristup izvješćima internih i vanjskih provjera sukladnosti te drugim izvješćima i zapisima iz djelokruga pružanja usluga povjerenja. Fina će također ocjenitelju sukladnosti omogućiti pristup zapisima i ugovorima vezanim uz treće strane, interna, vanjska i upravljačka izvješća i sl. iz djelokruga pružanja usluga povjerenja.

8.5 Mjere u slučaju nesukladnosti

U ovisnosti o značaju otkrivene nesukladnosti vanjski ocjenitelj sukladnosti može u izvješću navesti koju nesukladnost Fina mora otkloniti.

U slučaju značajne nesukladnosti Fina će što prije formirati plan otklanjanja značajne nesukladnosti i uz konzultaciju sa vanjskim ocjeniteljem sukladnosti što prije otkloniti značajne nesukladnosti.

Ako je u pružanju usluga povjerenja utvrđena značajna nesukladnost koja kroz kraći vremenski rok nije otklonjiva Fina će poduzeti potrebne korake kako bi otklonila nesukladnost i ako je moguće u roku koji je odredilo nadzorno tijelo.

Manje nesukladnosti, uz konzultaciju sa vanjskim ocjeniteljem, Fina će otkloniti do slijedeće ocjene sukladnosti.

Vanjski ocjenitelj može predložiti i savjetovati izmjenu koja utječe na pružanje usluga povjerenja u cilju podizanja efikasnosti ili poboljšanja pružanja usluge povjerenja. U tom slučaju Fina zadržava pravo prihvaćanja prijedloga.

Za vrijeme prekida izdavanja certifikata određenog tipa zbog utvrđene značajne neusklađenosti, Fina će izdavati samo one certifikate tog tipa u kojima je naznačeno da služe za interne i testne svrhe te će osigurati da ti certifikati ne budu dostupni ni jednom drugom korisniku.

8.6 Priopćavanje rezultata

Rezultati interne provjere sukladnosti povjerljive su prirode i Fina ih ne objavljuje javno.

Svi dokumenti interne provjere usklađenosti su na zahtjev dostupni vanjskim ocjeniteljima koji provode provjeru usklađenosti Fina PKI sustava.

Rezultate vanjske provjere sukladnosti Fina objavljuje javno na internetskim stranicama repozitorija iz točke 2.2 ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta. Nesukladnosti utvrđene tijekom provjere sukladnosti ne objavljuju se javno jer mogu sadržavati povjerljive informacije.

9 OSTALE POSLOVNE I PRAVNE ODREDBE

9.1 Naknade za usluge

Fina i vanjski ugovoreni RA, sukladno uvjetima iz sklopljenog ugovora, obavještavaju Korisnike i Pouzdajuće strane o svim uslugama koje se naplaćuju. Ukoliko posebnim ugovorom nije drugačije određeno, usluge se naplaćuju sukladno cjeniku Fine. Cjenik svih usluga koje se naplaćuju objavljen je na internetskim stranicama repozitorija iz točke 2.2. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

Fina zadržava pravo izmjene cjenika. Izmjene cjenika objavljuju se na internetskim stranicama repozitorija iz točke 2.2.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

9.1.1 Naknade za izdavanje ili obnovu certifikata

Fina sukladno objavljenom cjeniku naplaćuje naknadu za usluge izdavanja i obnove certifikata koje Korisnicima izdaju Fina CA-ovi.

9.1.2 Naknade za pristup certifikatu

Fina ne naplaćuje naknadu za pristup certifikatima.

9.1.3 Naknade za opoziv i pristup informacijama o statusu certifikata

Fina sukladno objavljenom cjeniku naplaćuje naknadu za uslugu opoziva certifikata te može odrediti i naplaćivati primjerenu naknadu za suspenziju i reaktivaciju certifikata.

Fina uvijek po svakom zaprimljenom zahtjevu u roku od 24 sata provodi opoziv i suspenziju certifikata, neovisno o statusu plaćanja pojedinog zahtjeva.

Fina ne naplaćuje uslugu davanja informacija o statusu opozvanosti ili suspendiranosti certifikata koju pruža u vidu OCSP servisa ili objave CRL.

9.1.4 Naknade za ostale usluge

Fina ili vanjski ugovoreni RA, sukladno uvjetima iz sklopljenog ugovora, mogu odrediti i naplaćivati primjerene naknade i za ostale usluge kao što su registracija poslovnog subjekta ili Korisnika, promjena podataka u certifikatu, isporuka certifikata i opreme na lokaciju Korisnika i sl.

Za pristup ovom $CPS_{NQC\text{-}eIDAS}$ dokumentu i Općim pravilima ne naplaćuju se naknade.

9.1.5 Povrat naknada

Povrat naknade Fina Korisnicima isplaćuje u slučaju pogrešne uplate ili preplate.

9.2 Financijska odgovornost

Fina kao pružatelj usluga povjerenja posjeduje financijsku stabilnost te raspolaže dostatnim financijskim sredstvima koja osiguravaju nesmetano pružanje usluga certificiranja u skladu s ovim $CPS_{NQC\text{-}eIDAS}$ dokumentom.

9.2.1 Pokrivenost osiguranjem

Fina kao pružatelj usluga povjerenja ima osiguran rizik od odgovornosti za štete koje nastanu obavljanjem usluga certificiranja.

Fina dodatno osigurava imovinu policom osiguranja koja pokriva osiguranje od rizika požara, vremenskih nepogoda, poplava, eksplozija, udar vozila, pad ili udar letjelice, demonstracija, osiguranje opreme, strojne opreme, elektroničkih i komunikacijskih uređaja, instalacija i sl.

Fina može od vanjskog ugovorenog RA-a zahtijevati da se osigura od šteta koje mogu nastati obavljanjem usluga ugovorenih s vanjskim RA.

9.2.2 Druga sredstva

Nema odredbi.

9.2.3 Osiguranje ili garancije krajnjim korisnicima

Vidi točku 9.2.1.

9.3 Povjerljivost poslovnih podataka

9.3.1 Opseg povjerljivih poslovnih podataka

Povjerljivi poslovni podaci su svi podaci, u bilo kojem obliku, koje na bilo koji način između sebe razmjene sudionici u svezi s uspostavom i pružanjem usluga certificiranja, a koje sudionici označe povjerljivim, ili određenom vrstom ili stupnjem tajnosti, ili koji su po prirodi povjerljivi jer bi njihovo neovlašteno otkrivanje moglo prouzročiti štetu sudioniku.

9.3.2 Podaci koji se ne smatraju povjerljivim poslovnim podacima

Podaci koji se ugrađuju u sadržaj certifikata, podaci o statusu certifikata te podaci i dokumenti javno objavljeni u Fina PKI repozitoriju ne smatraju se povjerljivim poslovnim podacima.

9.3.3 Odgovornost za zaštitu povjerljivih poslovnih podataka

Svaki sudionik obvezan je štititi povjerljive poslovne podatke iz točke 9.3.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta, koje je saznao na bilo koji način, sukladno propisima koji uređuju zaštitu podataka prema vrsti podatka, odnosno vrsti i stupnju tajnosti podataka. U protivnom odgovara za nastalu štetu.

9.4 Zaštita osobnih podataka

Sklapanjem ugovora o pružanju usluga certificiranja Potpisnici su suglasni s objavom certifikata u javnom imeniku, da Fina koristi i obrađuje njihove podatke prikupljene u postupku registracije sukladno važećoj zakonskoj regulativi te su suglasni da je Fina ovlaštena čuvati te podatke u trajanju od najmanje 10 godina od isteka certifikata na kojeg se zapisi odnose.

9.4.1 Plan zaštite osobnih podataka

Fina provodi tehničke, kadrovske i organizacijske mjere zaštite osobnih podataka sukladno Zakonu o provedbi Opće uredbe o zaštiti podataka [5] u svrhu zaštite privatnosti osoba i zaštite podataka od moguće zlouporabe te očuvanja točnosti, potpunosti i ažurnosti osobnih podataka.

Mjere zaštite osobnih podataka primjenjuju se prilikom razmjene osobnih podataka korisnika između RA mreže i sustava certificiranja te prilikom čuvanja i arhiviranja osobnih podataka korisnika do njihovog izlučivanja iz arhive i uništavanja.

Potrebne mjere zaštite osobnih podataka provode i ugovoreni RA-ovi.

9.4.2 Povjerljivi osobni podaci

U postupku registracije korisnika i nakon toga, Fina ili vanjski ugovoreni RA ovlašteni su prikupljati osobne podatke koji su potrebni za valjano utvrđivanje identiteta korisnika te druge podatke potrebne za valjano pružanje usluga certificiranja. Osobni podaci koje prikupi Fina ili vanjski ugovoreni RA i koji nisu sadržaj certifikata su povjerljivi osobni podaci koje Fina propisno štiti.

9.4.3 Osobni podaci koji nisu povjerljivi

Osobni podaci koje u postupku registracije korisnika i nakon toga prikupi Fina ili vanjski ugovoreni RA i koji su sadržaj certifikata su osobni podaci koji zbog dostupnosti svima zainteresiranima nisu povjerljivi.

9.4.4 Odgovornost za zaštitu osobnih podataka

Fina je odgovorna za zaštitu osobnih podataka prikupljenih u svrhu pružanja usluga certificiranja.

Ugovorima s vanjskim ugovorenim RA Fina regulira odgovornost za zaštitu osobnih podataka u ugovorenim RA.

9.4.5 Ovlaštenje za korištenje osobnih podataka

Fina je ovlaštena, osim za potrebe ispunjenja zakonskih obveza, odnosno ugovornih obveza po ugovoru o certificiranju, koristiti ili objavljivati osobne podatke samo temeljem pisane suglasnosti korisnika.

9.4.6 Dostupnost podataka mjerodavnim tijelima

Fina neće činiti dostupnima podatke iz točaka 9.3.1. i 9.4.2. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta osim u slučajevima propisanim zakonom ili kada to pisano zahtjeva mjerodavni sud, upravno ili neko drugo mjerodavno državno tijelo.

9.4.7 Ostale okolnosti objave podataka

Nema odredbi.

9.5 Prava intelektualnog vlasništva

Ovaj $CPS_{NQC\text{-}eIDAS}$ dokument kao i druga Finina dokumentacija objavljena na internetskim stranicama repozitorija iz točke 2.2. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta je intelektualno vlasništvo Fine.

Fina ne polaže pravo intelektualnog vlasništva na softver koji se koriste u Fina PKI, a koji je u vlasništvu trećih osoba

Vlasnik privatnog i javnog ključa je Korisnik, a za uporabu privatnog ključa ovlašten je isključivo Potpisnik, odnosno Skrbnik ili Autor pečata, bez obzira generira li par ključeva Potpisnik, odnosno Skrbnik ili Autor pečata, ili ga generira Fina kao pružatelj usluga povjerenja te bez obzira na način na koji je privatni ključ zaštićen.

Fina kao pružatelj usluga certificiranja vlasnik je certifikata koje izdaje.

9.6 Obveze i odgovornosti

9.6.1 Obveze i odgovornosti CA

Fina je odgovorna je za usklađenost ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta s Općim pravilima, njegovu usklađenost sa zakonskom regulativom te za provođenje odredbi propisanih ovim $CPS_{NQC\text{-}eIDAS}$ dokumentom, Uvjetima pružanja usluga certificiranja i sukladno obvezama u ugovoru o obavljanju usluga certificiranja sklopljenim s Korisnikom.

Fina na internetskim stranicama repozitorija iz točke 2.2.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta objavljuje uvjete pružanja usluga certificiranja, ovaj $CPS_{NQC\text{-}eIDAS}$ dokument, Opća pravila te sve obavijesti i informacije o promjenama u radu koje na bilo koji način mogu utjecati na sudionike Fina PKI.

Fina je kao pružatelj usluga povjerenja odgovorna za štetu nastalu tijekom pružanja usluge prouzročene od strane poslovnog subjekta s kojim je Fina podugovorila dio usluge certificiranja. Ova odgovornost između Fine i poslovnog subjekta uređuje se posebnim ugovorom.

Fina je odgovorna za:

- ispravnu provjeru identiteta i podataka fizičke osobe i/ili poslovnog subjekta u cilju izdavanja certifikata,
- izdavanje certifikata na siguran način radi očuvanja njegove autentičnosti i točnosti,
- usklađenost sa svojim obvezama.

Sukladno obvezama i odgovornostima Fina:

- pri pružanju usluge certificiranja primjenjuje odredbe važećih propisa iz točke 9.14. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta,
- izdaje certifikat na siguran način radi očuvanja njegove autentičnosti i točnosti, temeljeći ga na pouzdano utvrđenom identitetu fizičke osobe i/ili poslovnog subjekta,
- izdaje certifikat s profilom sukladnim poglavlju 7.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta, a prema tipu certifikata navedenom u zahtjevu za izdavanje certifikata,
- parovi korisničkih ključeva koje generira Fina generiraju se na siguran način i uz osiguranje tajnosti privatnog ključa, sukladno ovom $CPS_{NQC\text{-}eIDAS}$ dokumentu,
- za parove korisničkih ključeva koje na sigurnom kriptografskom, odnosno QSCD uređaju generira Potpisnik, odnosno Skrbnik ili Ovlašteni predstavnik, osigurava da se par ključeva generira na certificiranom sigurnom kriptografskom, odnosno QSCD uređaju i da je tajnost privatnog ključa osigurana na način opisan u ovom $CPS_{NQC\text{-}eIDAS}$ dokumentu,
- provodi provjeru da Potpisnik, odnosno poslovni subjekt posjeduje privatni ključ čiji se pripadajući javni ključ dostavlja na certificiranje,
- za certifikate koji se izdaju na sigurne kriptografske, odnosno QSCD uređaje te za certifikate koji se izdaju u softverskom zaštićenom tokenu osigurava siguran način generiranja i dostave privatnog ključa i pripadajućih aktivacijskih podataka Potpisniku, Skrbniku, odnosno Ovlaštenom predstavniku u slučajevima kada se par ključeva generira na lokaciji Fine,
- osigurava odgovarajući sigurni kriptografski, odnosno QSCD uređaj i njegovu zaštićenu dostavu Potpisniku, odnosno Skrbniku ili Ovlaštenom predstavniku,
- izdani certifikat čini dostupnim sukladno točki 4.4.2. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta,
- temeljem autenticiranog i autoriziranog zahtjeva, po provedenom propisanom postupku, opoziva, suspendira ili reaktivira certifikat, te ga objavljuje u listi opozvanih certifikata,
- pruža informaciju o statusu opozvanosti, odnosno suspendiranosti certifikata,
- provodi zahtijevane sigurnosne mjere za zaštitu prostora i opreme sustava certificiranja,
- primjenjuje organizacijske i tehničke mjere zaštite ključeva i certifikata sukladno ovom $CPS_{NQC\text{-}eIDAS}$ dokumentu,
- sukladno Planu kontinuiteta poslovanja osigurava nesmetan rad i maksimalnu raspoloživost usluga certificiranja,
- prati raspoloživost kapaciteta, planira održavanje i daljnji razvoj sustava certificiranja sukladno budućim potrebama, zahtjevima normi i razvoju tehnologije,

- podatke koji se sukladno točkama 9.3. i 9.4. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta smatraju povjerljivima štiti i te podatke koristiti isključivo za potrebe usluga certificiranja iz opsega ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta,
- osigurava da se interne i vanjske provjere sukladnosti Fine kao pružatelja usluga povjerenja provode sukladno točki 8.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

U slučaju prekida poslovanja Fina će postupiti sukladno točki 5.8. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

Ograničenja odgovornosti Fine kao davatelja usluga certificiranja opisana su u točki 9.8. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

9.6.2 Obveze i odgovornosti RA

Obveze i odgovornosti Fina RA mreže i vanjskih ugovorenih RA su:

- provođenje postupka registracije i identifikacije i provjere podataka fizičkih osoba i poslovnih subjekata na način propisan ovim $CPS_{NQC\text{-}eIDAS}$ dokumentom,
- odobravanje zahtjeva za izdavanje certifikata te zahtjeva za opoziv, suspenziju i reaktivaciju certifikata na način propisan ovim $CPS_{NQC\text{-}eIDAS}$ dokumentom,
- prosljeđivanje cjelovitih, točnih i provjerenih podataka registriranih fizičkih osoba i poslovnih subjekata u Fina CA,
- čuvanje, arhiviranje i zaštita podataka i dokumentacije na period od najmanje 10 godina od isteka certifikata na kojeg se odnose,
- osiguravanje od gubitka ili povrede povjerljivosti, cjelovitosti i dostupnosti arhiviranih podataka registriranih fizičkih osoba i poslovnih subjekata, na način propisan ovim $CPS_{NQC\text{-}eIDAS}$ dokumentom,
- obavještavanje podnositelja zahtjeva za izdavanje certifikata o javno objavljenim i dostupnim uvjetima pružanja usluga certificiranja i ovim $CPS_{NQC\text{-}eIDAS}$ dokumentom.

Vanjski ugovoreni RA uz ove obveze moraju poštovati i obveze proizašle iz ugovora o obavljanju RA usluga sklopljenog s Finom.

9.6.3 Obveze i odgovornosti korisnika

Korisnik je dužan:

- u procesu registracije predstaviti se na način propisan u poglavlju 3. i u točki 4.1.2.2. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta,
- pažljivo koristiti i čuvati sredstvo za izradu elektroničkog potpisa, privatne ključeve i aktivacijske podatke sukladno ovom $CPS_{NQC\text{-}eIDAS}$ dokumentu,
- poduzeti odgovarajuće mjere zaštite sredstva za izradu elektroničkog potpisa, odnosno elektroničkog pečata, privatnog ključa i aktivacijskih podataka od neovlaštenog pristupa i uporabe u skladu s poglavljem 6. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta,
- u najkraćem mogućem roku zatražiti opoziv, odnosno suspenziju certifikata u slučaju kompromitiranja privatnog ključa, gubitka ili oštećenja sredstva za izradu

elektroničkog potpisa, odnosno elektroničkog pečata, privatnog ključa i aktivacijskih podataka, sukladno točki 4.9. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta,
- dostaviti u registracijski ured RA mreže sve potrebne podatke i informacije o promjenama koje utječu ili mogu utjecati na točnost elektroničkog potpisa, odnosno elektroničkog pečata u roku iz točke 4.8. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta,
- koristiti certifikat i pripadajući privatni ključ u skladu sa zakonima i drugim propisima Republike Hrvatske te sukladno odredbama iz točke 1.4.1. i 1.4.2. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta,
- koristiti certifikat i pripadajući privatni ključ u skladu s odredbama iz točke 4.5.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta,
- djelovati u skladu sa svim ostalim odredbama iz ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta koje se odnose na obveze Korisnika.

Obveze i odgovornosti Korisnika vezane uz korištenje privatnog ključa i certifikata opisane su u točki 4.5.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

Potpisnik odnosno poslovni subjekt odgovorni su za točnost i ispravnost podataka dostavljenih u postupku registracije.

U slučaju promjene kontakt podataka nastale promjene Korisnik je dužan dostaviti Fini na kontakt podatke navedene u točki 9.11. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

Poslovni subjekt, odnosno osoba ovlaštena za zastupanje poslovnog subjekta, dužna je u najkraćem mogućem roku zatražiti opoziv poslovnog certifikata izdanog Pripadajućoj osobi koja više nije zaposlena u poslovnom subjektu ili više nije na drugi način povezana s poslovnim subjektom.

Autor pečata dužan je u najkraćem mogućem roku dostaviti Fini eventualnu promjenu Ovlaštenog predstavnika povezanog sa certifikatom za elektronički pečat.

Korisnik odgovara za nepravilnosti koje su nastale zbog neispunjavanja obveza utvrđenih gore navedenim odredbama iz ove točke.

Korisniku koji ne postupa u skladu s preuzetim obvezama može biti opozvan certifikat te će izgubiti sva prava proizašla iz ugovora o obavljanju usluga certificiranja.

9.6.4 Obveze i odgovornosti pouzdajuće strane

Pouzdajuća strana dužna je samostalno i svjesno donijeti odluku o razumnom pouzdanju u certifikat.

Razumnim pouzdanjem smatra se odluka Pouzdajuće strane da se pouzda u certifikat ako je u vrijeme ostvarenja pouzdanja:
- poduzela potrebne mjere opreza i koristiti certifikat u svrhe propisane ovim $CPS_{NQC\text{-}eIDAS}$ dokumentom, odnosno uvjetima pružanja usluge, pod okolnostima u kojima je pouzdanje razumno i u dobroj namjeri te pod okolnostima koje su poznate ili bi trebale biti poznate Pouzdajućoj strani prije ostvarenja pouzdanja,
- koristila aplikacijsko rješenje i IT okolinu u koju se može pouzdati,

- provjerila period važenja certifikata,
- provjerila status opozvanosti ili suspendiranosti certifikata, a što Pouzdajuća strana utvrđuje provodeći provjeru statusa certifikata putem OCSP servisa ili temeljem zadnje izdane CRL, kako je propisano ovim $CPS_{NQC\text{-}eIDAS}$ dokumentom,
- provjerila da je elektronički potpis, odnosno elektronički pečat izrađen privatnim ključem koji odgovara javnom ključu u certifikatu za vrijeme perioda važenja certifikata,
- provjerila da privatni ključ koji se koristi za autentikaciju odgovara javnom ključu u certifikatu za vrijeme perioda važenja certifikata.

Korištenje javnog ključa i certifikata od strane Pouzdajuće strane opisano je u točki 4.5.2., a zahtjevi za provjeru opoziva certifikata navedeni su u točki 4.9.6. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

Pouzdajuća strana koja nije poštovala propise i ovaj $CPS_{NQC\text{-}eIDAS}$ dokument te nije postupala sukladno obvezama i odgovornostima iz ove točke sama snosi sve rizike pouzdanja u takav certifikat.

Pouzdajuća strana snosi sve rizike pouzdanja u certifikat ako zna ili ima razloga smatrati da postoje činjenice koje mogu uzrokovati osobnu ili poslovnu štetu prouzročenu korištenjem certifikata.

9.6.5 Obveze i odgovornosti ostalih sudionika

Nema odredbi.

9.7 Odricanje od odgovornosti

Fina nije odgovorna za štete, uključujući i indirektne, štete za slučaj nezgode, štete za slučaj nepogode s posljedicama ili za bilo koji gubitak dobiti, gubitak podataka ili druge indirektne štete koje su proizašle iz veze s uslugama certificiranja.

Fina nije odgovorna za štete:

- štete pretrpljene u vremenu od opoziva certifikata do izdavanja nove CRL,
- štete zbog neautorizirane uporabe korisničkih ključeva i certifikata,
- štete nastale uporabom certifikata koja nije dopuštena ovim $CPS_{NQC\text{-}eIDAS}$ dokumentom,
- štete prouzročene prijevarnom ili nemarnom uporabom certifikata, CRL ili OCSP servisa,
- štete nastale kao rezultat neispravnosti i pogrešaka u softveru i hardveru Subjekta i Pouzdajuće strane.

Fina nije odgovorna za štete, uključujući i indirektne štete, štete za slučaj nezgode, štete za slučaj nepogode s posljedicama ili za bilo koji gubitak dobiti, gubitak podataka ili druge indirektne štete koje su nastale kao rezultat prijevarnog davanja podataka i prijevarnog

predstavljanja korisnika tijekom procesa identifikacije i potvrde identiteta ako je provjeru podataka ured RA mreže provodio u skladu sa zahtjevima iz ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

9.8 Ograničenja odgovornosti

Finina ukupna financijska odgovornost za nekvalificirane certifikate izdane prema ovom $CPS_{NQC\text{-}eIDAS}$ dokumentu i prema $CPS_{WSA\text{-}eIDAS}$ dokumentu [27] te za transakcije obavljene na temelju pouzdavanja u tako izdane certifikate iznosi najviše 1.500.000 kuna.

Ako nije posebnim ugovorom ili na drugi način određeno, Finina maksimalna financijska odgovornost prema Korisniku i Pouzdajućoj strani koja se razumno pouzdaje u certifikat ograničava se sukladno preporučenim financijskim limitima određenim u Tablici 1.6. Finina maksimalna financijska odgovornost za nekvalificirane certifikate prikazana je Tablici 9.1.

Kategorija certifikata	Maksimalna Finina financijska odgovornost		
	Po kategoriji	Po transakciji	Ukupno
Nekvalificirani certifikati standardne razine sigurnosti	do 100.000 kn	do 8.000 kn	1.500.000 kn
Nekvalificirani certifikati srednje razine sigurnosti	do 600.000 kn	do 80.000 kn	
Nekvalificirani certifikati visoke razine sigurnosti	do 800.000 kn	do 400.000 kn	

Tablica 9.1. Maksimalna Finina financijska odgovornost

9.9 Naknada štete

Svaki sudionik odgovara oštećenom za štetu koju je počinio zbog nepoštivanja odredbi ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta, Općih pravila [26] i važećih relevantnih propisa.

Potpisnik, odnosno poslovni subjekt ili fizička osoba, u čije ime Potpisnik djeluje i koju predstavlja, te Autor pečata odgovara oštećenom, odnosno svakom drugom sudioniku ako ishodi i koristi certifikat izdan od Fine temeljem prijevarno danih podataka u zahtjevu za izdavanje certifikata.

Pouzdajuća strana odgovora oštećenom, odnosno svakom drugom sudioniku ako se pouzda u izdani certifikat bez provjere njegove valjanosti opisane u točki 9.6.4. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta ili ga koristi protivno svrhama određenim ovim $CPS_{NQC\text{-}eIDAS}$ dokumentom.

9.10 Trajanje i prestanak važenja

9.10.1 Trajanje

Ovaj $CPS_{NQC\text{-}eIDAS}$ dokument važi do stupanja na snagu novog $CPS_{NQC\text{-}eIDAS}$ dokumenta ili do objave prestanka njegovog važenja.

Nova verzija dokumenta ili objava prestanka važenja biti će objavljena na internetskim stranicama repozitorija iz točke 2.2 ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta s naznačenim danom stupanja na snagu. Novom $CPS_{NQC\text{-}eIDAS}$ dokumentu biti će dodijeljena nova verzija i novi OID te će u njemu biti naznačene obavljene izmjene.

9.10.2 Prestanak važenja

Stupanjem na snagu nove verzije $CPS_{NQC\text{-}eIDAS}$ dokumenta za sve certifikate izdane prema ovom $CPS_{NQC\text{-}eIDAS}$ dokumentu ostaju važiti one odredbe iz ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta koje se ne mogu smisleno zamijeniti odredbama nove verzije $CPS_{NQC\text{-}eIDAS}$ dokumenta .

Prestanak važenja ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta nije vezan i ne utječe na važenje certifikata izdanih primjenom ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

Fina može za pojedine odredbe važećeg $CPS_{NQC\text{-}eIDAS}$ dokumenta izraditi izmjene i dopune kao što je to navedeno u točki 9.12. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

9.10.3 Posljedice prestanka važenja i nastavak djelovanja

Stupanjem na snagu nove verzije $CPS_{NQC\text{-}eIDAS}$ dokumenta na sve se certifikate izdane od tog dana primjenjuju odredbe iz tog dokumenta.

Certifikati izdani primjenom prethodnih $CPS_{NQC\text{-}eIDAS}$ dokumenata važe do njihova isteka pri čemu se mogu obnoviti primjenom pravila iz novog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

9.11 Individualne obavijesti i komunikacija sa sudionicima

Individualna komunikacija sa sudionicima primarno se provodi preko Finine službe za odnose s korisnicima:

- besplatni telefon: 0800 0080

Individualne obavijesti i druga službena komunikacija u pisanom obliku provodi se korištenjem sljedećih kontaktnih podataka:

Kontaktni podaci za dostavu dopisa prema Fini	
Poštanska adresa:	Fina Centar elektroničkog poslovanja, Ulica grada Vukovara 70 10000 Zagreb Hrvatska
E-mail:	info.rdc@fina.hr
Telefaks:	+385-1-6304-081

9.12 Izmjene i dopune

9.12.1 Procedure izmjena i dopuna

Ovaj $CPS_{NQC\text{-}eIDAS}$ dokument revidira se po potrebi.

Fina može bez obavijesti unositi tipografske ispravke, promjene kontakt podataka te druge manje ispravke koje bitno ne utječu na sudionike.

Svi sudionici mogu na kontakt adresu Fina PMA iz točke 1.5. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta poslati dopis s prijedlogom za ispravke pogrešaka, prijedlog nadopuna ili izmjenu ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta. U dopisu se navode kontakt podaci osobe koja je poslala prijedlog promjene. Fina PMA može prihvatiti, prilagoditi ili odbiti predložene promjene nakon razmatranja istih.

Izradu novog ili izmjenu i dopunu postojećeg $CPS_{NQC\text{-}eIDAS}$ dokumenta odobrava i provodi Fina PMA, a sukladno poslovnim zahtjevima Fine i zahtjevima zakonske regulative i propisa iz točke 9.14 ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

9.12.2 Mehanizmi obavještavanja i vremenski periodi

Sve izmjene i dopune $CPS_{NQC\text{-}eIDAS}$ dokumenta prikladne za javnu objavu objavljuju se u elektroničkom obliku na internetskim stranicama repozitorija iz točke 2.2. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

Nove verzije i podverzije $CPS_{NQC\text{-}eIDAS}$ dokumenta za javnu objavu s izmijenjenim OID-om $CPS_{NQC\text{-}eIDAS}$ dokumenta objavljuju se u elektroničkom obliku na internetskim stranicama repozitorija iz točke 2.2.1. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

Datum stupanja na snagu izmjena i dopuna ili novoobjavljenog $CPS_{NQC\text{-}eIDAS}$ dokumenta naznačeni su na njegovoj naslovnoj strani kao i na internetskim stranicama na kojima je objavljen.

9.12.3 Okolnosti pod kojima se mora mijenjati OID

Veće izmjene u $CPS_{NQC\text{-}eIDAS}$ dokumentu koje mogu utjecati na sudionike zahtijevaju i izmjenu OID-a $CPS_{NQC\text{-}eIDAS}$ dokumenta. Novi OID za novu verziju $CPS_{NQC\text{-}eIDAS}$ dokumenta određuje Fina PMA.

9.13 Postupak rješavanja sporova

U slučaju spora ili neslaganja između Fine i drugih sudionika povodom radnji i/ili postupaka glede pružanja usluge certificiranja uređene ovim $CPS_{NQC\text{-}eIDAS}$ dokumentom, isti će se nastojati razriješiti sporazumno. Ako sporazumno razrješenje spora nije moguće, isti će se razriješiti pred mjerodavnim sudom u Zagrebu uz primjenu hrvatskog prava.

Sudionici mogu Fini uputiti prigovor ako smatraju postoji odstupanje sadržaja usluge u odnosu na objavljene uvjete pružanja usluga. Fina će povodom prigovora odgovoriti podnositelju prigovora. Prigovori se upućuju pisano u papirnatom ili elektroničkom obliku na adrese navedene u točki 9.11. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

9.14 Važeći propisi

Usluge povjerenja iz opsega ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta Fina pruža sukladno odredbama Uredbe (EU) br. 910/2014 [1], provedbenih akata donesenih temeljem Uredbe (EU) br. 910/2014 [3] i [4], Zakona o provedbi Uredbe (EU) br. 910/2014 [2] te normizacijskih dokumenata ETSI EN 319 401 [8] i ETSI EN 319 411-1 [9].

9.15 Usklađenost s primjenjivim propisima

Ovaj $CPS_{NQC\text{-}eIDAS}$ dokument i pružanje usluga certificiranja koje su obuhvaćene ovim $CPS_{NQC\text{-}eIDAS}$ dokumentom usklađeni su s propisima iz točke 9.14. ovog $CPS_{NQC\text{-}eIDAS}$ dokumenta.

Svi sudionici suglasni su s primjenom hrvatskog prava u tumačenju primijenjenih odredbi.

9.16 Razne odredbe

Nema odredbi.

9.17 Ostale odredbe

Gdje je to moguće, Fina i vanjski ugovoreni RA omogućuju da usluge certificiranja i proizvodi za krajnjeg korisnika koji se koriste pri pružanju tih usluga budu dostupni osobama s invaliditetom.

Ako podnositelj zahtjeva ima neku vrstu invaliditeta, Fina i vanjski RA pomažu podnositelju pri predaji zahtjeva i registraciji. Pomoć podnositelju također je osigurana prilikom predaje zahtjeva za opoziv, suspenziju i reaktivaciju certifikata.

Fina javno objavljuje ovaj $CPS_{NQC\text{-}eIDAS}$ dokument u verziji za javnu objavu, Opća pravila i uvjete pružanja usluga certificiranja.

Uvjeti pružanja usluga certificiranja komuniciraju se dokumentom u papirnatom obliku ili dokumentom u elektroničkom obliku čija je cjelovitost zaštićena.

Prije sklapanja ugovora o obavljanju usluga certificiranja korisnici se informiraju o uvjetima pružanja usluga certificiranja. Prihvaćanje uvjeta pružanja usluga certificiranja preduvjet je za izdavanje certifikata.

U postupcima obnove certifikata, ponovnog izdavanja certifikata nakon isteka, opoziva ili izmjene podataka u certifikatu Fina obavještava Potpisnika, Skrbnika, odnosno Ovlaštenog predstavnika o eventualnim izmjenama uvjeta o pružanju usluga certificiranja.