FINA

OPĆA PRAVILA PRUŽANJA USLUGA CERTIFICIRANJA ZA KVALIFICIRANE CERTIFIKATE ZA ELEKTRONIČKE POTPISE I PEČATE

Verzija 1.2

Datum stupanja na snagu: 24.04.2018.

OID Dokumenta: 1.3.124.1104.5.0.3.1.1.2

Informacije o dokumentu

Ime dokumenta:	Opća pravila pružanja usluga certificiranja za kvalificirane certifikate za elektroničke potpise i pečate
OID dokumenta:	1.3.124.1104.5.0.3.1.1.2
Tip dokumenta:	Opća pravila pružanja usluga certificiranja (*Certificate Policy*, CP)
Oznaka distribucije	Javno
Vlasnik dokumenta	Financijska agencija, Fina
Kontakt	pma@fina.hr

Povijest izmjena

Verzija	Datum	Razlog izmjene
1.0	29.03.2017.	Inicijalna verzija
1.1	22.05.2017.	Promjene sukladno komentarima ocjenitelja
1.2	24.04.2018.	Ažuriranje referente liste zakonske regulative, proširenje primjerene uporabe certifikata u točkama 1.4.1.2. i 1.4.1.4., 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.

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 zaštiti osobnih podataka (NN 106/2012 - pročišćeni tekst)

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 319 411-2 V2.1.1. (2016-02) – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates

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

[12] 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

[13] 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

[14] ETSI EN 319 412-5 V2.1.1. (2016-02) – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements

[15] 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

[16] HRS CEN/TS 419 241:2014 – Sigurnosni zahtjevi za pouzdane sustave za izradu elektroničkog potpisa na strani servera (CEN/TS 419241:2014); Security Requirements for Trustworthy Systems Supporting Server Signing (CEN/TS 419241:2014)

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

[18] HR 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)

[19] HR 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)

[20] HR 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)

[21] HR 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)

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

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

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

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

[26] 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)

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

Finini dokumenti

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

[29] Pravilnik o postupcima certificiranja za kvalificirane certifikate za elektroničke potpise i pečate, $CPS_{QC\text{-}eIDAS}$

1. UVOD

Fina PKI inicijalno je osmišljen i uspostavljen u Financijskoj agenciji (Fina) kao treća strana od povjerenja (*Trusted Third Party*) s ciljem pružanja usluga certificiranja za građane, poslovne subjekte i tijela javne vlasti. Fina kao kvalificirani pružatelj usluga povjerenja omogućuje stvaranje odnosa povjerenja potrebnog za korištenje i razvitak elektroničkog poslovanja (e-poslovanje) i elektroničke javne uprave (e-uprava). Promoviranjem ovih usluga povjerenja i njihova korištenja Fina želi poticati i olakšati razvitak e-poslovanja i e-uprave.

Fina, kao hrvatska tvrtka u državnom vlasništvu, s polustoljetnom tradicijom na području financijskih usluga, partner je državi te surađuje s Hrvatskom narodnom bankom i uspješno posluje s bankama, brojnim poslovnim sustavima i drugim poslovnim subjektima u Republici Hrvatskoj. Informatički sustav Fine prokušan je najzahtjevnijim poslovima od nacionalne važnosti, a visoka profesionalna razina stručnih timova omogućuje pripremu i provedbu različitih projekata.

Tradicija, pružanje pouzdanih usluga i orijentiranost prema pružanju elektroničkih usluga građane, poslovne subjekte i tijela javne vlasti glavni su razlozi zbog kojih je Fina prepoznata kao treća strana od povjerenja u e-poslovanju i e-upravi.

Finina poslovna mreža ima nacionalnu pokrivenost podružnicama i poslovnicama, a njihova informatička povezanost jamči brzinu i pouzdanost izvršenja zahtjeva koju koristi i registracijska služba Fine (Fina RA mreža).

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 se 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 [28].

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

Fina ima uspostavljen servis udaljenog elektroničkog potpisivanja i pečatiranja u kojem generiranje ili upravljanje privatnim ključevima u ime Potpisnika i Autora pečata provodi Fina kao kvalificirani pružatelj usluga povjerenja. Kvalificirane certifikate povezane s ključevima generiranim u ovom servisu za Potpisnike i Autore pečata izdaju Fina CA-ovi. Servis udaljenog elektroničkog potpisivanja i pečatiranja izrađuje napredne elektroničke potpise i pečate koji su zasnovani na kvalificiranim certifikatima.

1.1.1. Opseg i namjena ovih Općih pravila pružanja usluge certificiranja

Ova Opća pravila pružanja usluga certificiranja za kvalificirane certifikate (engl. *Certificate Policy for Qualified Certificates* – $CP_{QC\text{-}eIDAS}$, u daljnjem tekstu: Opća pravila) sadrže temeljna pravila i skup načela pružanja usluga certificiranja kojim Fina kao kvalificirani pružatelj usluga povjerenja pruža usluge izdavanja kvalificiranih certifikata za elektroničke potpise te izdavanja kvalificiranih certifikata za elektroničke pečate (u daljnjem tekstu: kvalificirani certifikat ili certifikat).

Opseg ovih Općih pravila su kvalificirane usluge povjerenja koje pruža Fina, a koje se odnose na izdavanje i upravljanje životnom ciklusom produkcijskih kvalificiranih certifikata koji se izdaju na sigurnim kriptografskim, odnosno QSCD uređajima ili se izdaju kao softverski certifikati čiji je privatni ključ zaštićen softverskim tokenom. Također, opseg ovih Općih pravila uključuje i izdavanje i upravljanje životnom ciklusom produkcijskih kvalificiranih certifikata koji se koriste u sklopu servisa udaljenog elektroničkog potpisivanja.

Produkcijski certifikati iz opsega ovih Općih pravila sastavni su dio Registra digitalnih certifikata (Fina RDC), a koje izdaju dva certifikacijska tijela (CA) iz opsega ovih Općih pravila: 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.

Namjena ovog dokumenta je definiranje pravila iz područja određenog opsegom ovog dokumenta, a prema kojima postupaju sudionici Fina PKI navedeni u točki 1.3. ovih Općih pravila.

1.1.2. Tipovi certifikata

Ovim Općim pravilima definirana su pravila certificiranja za kvalificirane certifikate koje izdaju Fina CA-ovi, a koji su usklađeni sa zahtjevima 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 [1] (u daljem tekstu: Uredba (EU) br. 910/2014).

Ovim Općim pravilima definirane su grupe certifikata, tipovi certifikata i pripadajuće razine sigurnosti. Grupe certifikata određene su vrstom Subjekta certificiranja. Jedna grupa certifikata može imati jedan ili više tipova certifikata. Svaki tip certifikata ima dodijeljen Finin i ETSI OID općih pravila certificiranja (CP OID). Pomoću CP OID-a Potpisnici, Autori pečata i Pouzdajuće strane određuju prikladnost certifikata za određenu primjenu. Svaki tip certifikata ima dodijeljenu razinu sigurnosti kojom je određen stupanj pouzdanja u certifikat.

U sljedećim tablicama prikazane su grupe i tipovi kvalificiranih certifikata iz opsega ovih Općih pravila s nazivima certifikata i pripadajućim Fininim i ETSI OID-ovima općih pravila certificiranja (u daljnjem tekstu: CP OID). Tablica 1.1. prikazuje grupe i tipove kvalificiranih certifikata koje izdaje Fina RDC 2015, a Tablica 1.2. prikazuje grupe i tipove kvalificiranih certifikata koje izdaje Fina RDC-TDU 2015.

Kvalificirani 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 EU kvalificirani certifikat za e-potpis (QCP-n-qscd)	Fina CP OID: 1.3.124.1104.5.12.11.8.2 ETSI CP OID: 0.4.0.194112.1.2	Srednja
	Osobni EU kvalificirani certifikat za e-potpis (QCP-n)	Fina CP OID: 1.3.124.1104.5.12.11.2.2 ETSI CP OID: 0.4.0.194112.1.0	Srednja
	Osobni EU kvalificirani certifikat za udaljeni e-potpis (QCP-n)	Fina CP OID: 1.3.124.1104.5.12.11.6.2 ETSI CP OID: 0.4.0.194112.1.0	Srednja
Fina RDC 2015 poslovni certifikati	Poslovni EU kvalificirani certifikat za e-potpis (QCP-n-qscd)	Fina CP OID: 1.3.124.1104.5.12.12.8.2 ETSI CP OID: 0.4.0.194112.1.2	Srednja
	Poslovni EU kvalificirani certifikat za e-potpis (QCP-n)	Fina CP OID: 1.3.124.1104.5.12.12.2.2 ETSI CP OID: 0.4.0.194112.1.0	Srednja
	Poslovni EU kvalificirani certifikat za udaljeni e-potpis (QCP-n)	Fina CP OID: 1.3.124.1104.5.12.12.6.2 ETSI CP OID: 0.4.0.194112.1.0	Srednja
Fina RDC 2015 certifikati za e-pečat	EU kvalificirani certifikat za e-pečat (QCP-l-qscd)	Fina CP OID: 1.3.124.1104.5.12.13.8.2 ETSI CP OID: 0.4.0.194112.1.3	Srednja
	EU kvalificirani soft certifikat za e-pečat (QCP-l)	Fina CP OID: 1.3.124.1104.5.12.13.1.1 ETSI CP OID: 0.4.0.194112.1.1	Standardna
	EU kvalificirani certifikat za udaljeni e-pečat (QCP-l)	Fina CP OID: 1.3.124.1104.5.12.13.6.2 ETSI CP OID: 0.4.0.194112.1.1	Srednja

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

Kvalificirani 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 EU kvalificirani certifikat za e-potpis (QCP-n-qscd)	Fina CP OID: 1.3.124.1104.5.22.12.8.2 ETSI CP OID: 0.4.0.194112.1.2	Srednja
	TDU EU kvalificirani certifikat za e-potpis (QCP-n)	Fina CP OID: 1.3.124.1104.5.22.12.2.2 ETSI CP OID: 0.4.0.194112.1.0	Srednja
	TDU EU kvalificirani certifikat za udaljeni e-potpis (QCP-n)	Fina CP OID: 1.3.124.1104.5.22.12.6.2 ETSI CP OID: 0.4.0.194112.1.0	Srednja
Fina RDC-TDU 2015 certifikati za e-pečat	TDU EU kvalificirani certifikat za e-pečat (QCP-l-qscd)	Fina CP OID: 1.3.124.1104.5.22.13.8.2 ETSI CP OID: 0.4.0.194112.1.3	Srednja
	TDU EU kvalificirani soft certifikat za e-pečat (QCP-l)	Fina CP OID: 1.3.124.1104.5.22.13.1.1 ETSI CP OID: 0.4.0.194112.1.1	Standardna
	TDU EU kvalificirani certifikat za udaljeni e-pečat (QCP-l)	Fina CP OID: 1.3.124.1104.5.22.13.6.2 ETSI CP OID: 0.4.0.194112.1.1	Srednja

Tablica 1.2. Grupe i tipovi kvalificiranih 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 za elektroničko potpisivanje. Ovim općim pravilima određeni su sljedeći tipovi osobnih kvalificiranih certifikata:

- **Osobni EU kvalificirani certifikat za e-potpis (QCP-n-qscd)** – Osobni kvalificirani certifikat za e-potpis, srednje razine sigurnosti, koji se izdaje fizičkim osobama – građanima, a čiji se pripadajući privatni ključ čuva u QSCD uređaju, sukladno točki 6.2.1. ovih Općih pravila. Ovaj tip certifikata sukladan je s „QCP-n-qscd“ EU općim pravilima za kvalificirane certifikate iz norme ETSI EN 319 411-2.
- **Osobni EU kvalificirani certifikat za e-potpis (QCP-n)** – Osobni kvalificirani certifikat za e-potpis, srednje razine sigurnosti, koji se izdaje fizičkim osobama – građanima, a čiji se pripadajući privatni ključ čuva u sigurnom kriptografskom uređaju, sukladno točki 6.2.1. ovih Općih pravila. Ovaj tip certifikata sukladan je s „QCP-n“ EU općim pravilima za kvalificirane certifikate iz norme ETSI EN 319 411-2.
- **Osobni EU kvalificirani certifikat za udaljeni e-potpis (QCP-n)** – Osobni kvalificirani certifikat za e-potpis, srednje razine sigurnosti, koji se izdaje fizičkim osobama – građanima, a čiji se pripadajući privatni ključ čuva u servisu udaljenog elektroničkog potpisivanja i pečatiranja sukladno točki 6.2.1. ovih Općih pravila. Ovaj tip certifikata sukladan je s „QCP-n“ EU općim pravilima za kvalificirane certifikate iz norme ETSI EN 319 411-2.

1.1.2.2. Fina RDC 2015 poslovni certifikati

Fina RDC 2015 poslovni certifikati namijenjeni su za elektroničko potpisivanje 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 izdaja na zaseban Fina RDC-TDU 2015 CA sukladno točki 1.1.2.4. ovih Općih pravila.

Ovim općim pravilima određeni su sljedeći tipovi poslovnih certifikata:

- **Poslovni EU kvalificirani certifikat za e-potpis (QCP-n-qscd)** – Poslovni kvalificirani certifikat za e-potpis, srednje razine sigurnosti, koji se izdaje Pripadajućim osobama, a čiji se pripadajući privatni ključ čuva u QSCD uređaju, sukladno točki 6.2.1. ovih Općih pravila. Ovaj tip certifikata sukladan je s „QCP-n-qscd“ EU općim pravilima za kvalificirane certifikate iz norme ETSI EN 319 411-2.
- **Poslovni EU kvalificirani certifikat za e-potpis (QCP-n)** – Poslovni kvalificirani certifikat za e-potpis, srednje razine sigurnosti, koji se izdaje Pripadajućim osobama, a čiji se pripadajući privatni ključ čuva u sigurnom kriptografskom uređaju, sukladno točki 6.2.1. ovih Općih pravila. Ovaj tip certifikata sukladan je s „QCP-n“ EU općim pravilima za kvalificirane certifikate iz norme ETSI EN 319 411-2.
- **Poslovni EU kvalificirani certifikat za udaljeni e-potpis (QCP-n)** – Poslovni kvalificirani certifikat za e-potpis, srednje razine sigurnosti, koji se izdaje Pripadajućim osobama, a čiji se pripadajući privatni ključ čuva u servisu udaljenog elektroničkog potpisivanja i pečatiranja sukladno točki 6.2.1. ovih Općih pravila. Ovaj tip certifikata sukladan je s „QCP-n“ EU općim pravilima za kvalificirane certifikate iz norme ETSI EN 319 411-2.

1.1.2.3. Fina RDC 2015 certifikati za e-pečat

Fina RDC 2015 certifikati za e-pečat namijenjeni su za elektroničko pečatiranje, a izdaju se pravnim osobama. Ovim općim pravilima određeni su sljedeći tipovi certifikata za e-pečat:

- **EU kvalificirani certifikat za e-pečat (QCP-l-qscd)** – Kvalificirani certifikat za e-pečat, srednje razine sigurnosti, koji se izdaje pravnoj osobi, a čiji se pripadajući privatni ključ čuva u QSCD uređaju, sukladno točki 6.2.1. ovih Općih pravila. Ovaj tip certifikata sukladan je s „QCP-l-qscd“ EU općim pravilima za kvalificirane certifikate iz norme ETSI EN 319 411-2.
- **EU kvalificirani soft certifikat za e-pečat (QCP-l)** – Kvalificirani certifikat za e-pečat, standardne razine sigurnosti, koji se izdaje pravnoj osobi, a čiji se pripadajući privatni ključ čuva u softverskom zaštićenom tokenu, sukladno točki 6.2.1. ovih Općih pravila. Ovaj tip certifikata sukladan je s „QCP-l“ EU općim pravilima za kvalificirane certifikate iz norme ETSI EN 319 411-2.
- **EU kvalificirani certifikat za udaljeni e-pečat (QCP-l)** – Kvalificirani certifikat za e-pečat, srednje razine sigurnosti, koji se izdaje pravnoj osobi, a čiji se pripadajući privatni ključ čuva u servisu udaljenog elektroničkog potpisivanja i pečatiranja sukladno točki 6.2.1. ovih Općih pravila. Ovaj tip certifikata sukladan je s „QCP-l“ EU općim pravilima za kvalificirane certifikate iz norme ETSI EN 319 411-2.

1.1.2.4. Fina RDC-TDU 2015 certifikati

Fina RDC-TDU 2015 certifikati namijenjeni su za su za elektroničko potpisivanje, a izdaju se državnim dužnosnicima i zaposlenicima u tijelima državne uprave (u daljnjem tekstu: TDU). Ovim općim pravilima određena su sljedeći tipovi certifikata za državne dužnosnike i zaposlenike u TDU:

- **TDU EU kvalificirani certifikat za e-potpis (QCP-n-qscd)** – Kvalificirani certifikat za e-potpis, srednje razine sigurnosti, koji se izdaje državnim dužnosnicima i zaposlenicima u TDU, a čiji se pripadajući privatni ključ čuva u QSCD uređaju, sukladno točki 6.2.1. ovih Općih pravila. Ovaj tip certifikata sukladan je s „QCP-n-qscd“ EU općim pravilima za kvalificirane certifikate iz norme ETSI EN 319 411-2.
- **TDU EU kvalificirani certifikat za e-potpis (QCP-n)** – Kvalificirani certifikat za e-potpis, srednje razine sigurnosti, koji se izdaje državnim dužnosnicima i zaposlenicima u TDU, a čiji se pripadajući privatni ključ čuva u sigurnom kriptografskom uređaju, sukladno točki 6.2.1. ovih Općih pravila. Ovaj tip certifikata sukladan je s „QCP-n“ EU općim pravilima za kvalificirane certifikate iz norme ETSI EN 319 411-2.
- **TDU EU kvalificirani certifikat za udaljeni e-potpis (QCP-n)** – Kvalificirani certifikat za e-potpis, srednje razine sigurnosti, koji se izdaje državnim dužnosnicima i zaposlenicima u TDU, a čiji se pripadajući privatni ključ čuva u servisu udaljenog elektroničkog potpisivanja i pečatiranja sukladno točki 6.2.1. ovih Općih pravila. Ovaj tip certifikata sukladan je s „QCP-n“ EU općim pravilima za kvalificirane certifikate iz norme ETSI EN 319 411-2.

1.1.2.5. Fina RDC-TDU 2015 certifikati za e-pečat

Fina RDC-TDU 2015 certifikati za e-pečat namijenjeni su za elektroničko pečatiranje, a izdaju se tijelima državne uprave. Ovim općim pravilima određeni su sljedeći tipovi certifikata za e-pečat:

- **TDU EU kvalificirani certifikat za e-pečat (QCP-l-qscd)** – Kvalificirani certifikat za e-pečat, srednje razine sigurnosti, koji se izdaje TDU, a čiji se pripadajući privatni ključ čuva u QSCD uređaju, sukladno točki 6.2.1. ovih Općih pravila. Ovaj tip certifikata sukladan je s „QCP-l-qscd“ EU općim pravilima za kvalificirane certifikate iz norme ETSI EN 319 411-2.
- **TDU EU kvalificirani soft certifikat za e-pečat (QCP-l)** – Kvalificirani certifikat za e-pečat, standardne razine sigurnosti, koji se izdaje TDU, a čiji se pripadajući privatni ključ čuva u softverskom zaštićenom tokenu, sukladno točki 6.2.1. ovih Općih pravila. Ovaj tip certifikata sukladan je s „QCP-l“ EU općim pravilima za kvalificirane certifikate iz norme ETSI EN 319 411-2.
- **TDU EU kvalificirani certifikat za udaljeni e-pečat (QCP-l)** – Kvalificirani certifikat za e-pečat, srednje razine sigurnosti, koji se izdaje TDU, a čiji se pripadajući privatni ključ čuva u servisu udaljenog elektroničkog potpisivanja i pečatiranja sukladno točki

6.2.1. ovih Općih pravila. Ovaj tip certifikata sukladan je s „QCP-l“ EU općim pravilima za kvalificirane certifikate iz norme ETSI EN 319 411-2.

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: Opća pravila pružanja usluga certificiranja za kvalificirane certifikate za elektroničke potpise i pečate
- Verzija: 1.2
- Datum stupanja na snagu: 24.04.2018.
- OID: 1.3.124.1104.5.0.3.1.1.2
- Internetske adrese na kojima je dokument objavljen su:
  - http://rdc.fina.hr/RDC2015/FinaRDC2015-CPQC1-2-hr.pdf i
  - http://rdc.fina.hr/RDC-TDU2015/FinaRDC-TDU2015-CPQC1-2-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 ovih Općih pravila su Fina RDC 2015 i Fina RDC-TDU 2015 (Fina CA-ovi). Fina kao kvalificirani pružatelj usluga povjerenja preko svojih Fina CA-ova obavlja usluge izdavanja i upravljanja životnim ciklusom kvalificiranih certifikata sukladno ovim Općim pravilima.

Obveze i odgovornosti Fine koja preko svojih Fina CA-ova izdaje Korisničke certifikate navedene su u točki 9.6.1. ovih Općih pravila, a postupci certificiranja koje Fina provodi u cilju ispunjenja zahtjeva iz ovih Općih pravila opisani su u $CPS_{QC\text{-}eIDAS}$ [29] dokumentu.

1.3.1.1. Fina RDC 2015 CA

Fina RDC 2015 izdaje kvalificirane certifikate za javnost koji su navedeni u Tablici 1.1 u točki 1.1.2. ovih Općih pravila.

Fina RDC 2015 izdaje kvalificirane 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 1.3.

Polje	Atribut	Vrijednost
Issuer	commonName	Fina Root CA
	organizationName	Financijska agencija
	countryName	HR
Validity	notBefore	*Vrijeme izdavanja certifikata*
	notAfter	*Vrijeme izdavanja certifikata + 10 godina*
Subject	commonName	Fina RDC 2015
	organizationName	Financijska agencija
	countryName	HR

Tablica 1.3. 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 kvalificirane certifikate državnim dužnosnicima i zaposlenicima u TDU. Kvalificirani certifikati koje izdaje Fina RDC-TDU 2015 navedeni su u Tablici 1.2. u točki 1.1.2. ovih Općih pravila.

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

Polje	Atribut	Vrijednost
Issuer	commonName	Fina Root CA
	organizationName	Financijska agencija
	countryName	HR
Validity	notBefore	*Vrijeme izdavanja certifikata*
	notAfter	*Vrijeme izdavanja certifikata + 10 godina*
Subject	commonName	Fina RDC-TDU 2015
	organizationName	Financijska agencija
	countryName	HR

Tablica 1.4. 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 svakog 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.

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 Općim pravilima.

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.

Obveze i odgovornosti Fina RA mreže i vanjskih ugovorenih RA navedene su u točki 9.6.2. ovih Općih pravila.

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.

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. ovih Općih pravila. 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 kvalificiranim certifikatima za e-potpis je fizička osoba – građanin;
- u poslovnim kvalificiranim certifikatima za e-potpis je Pripadajuća osoba Poslovnog subjekta;
- u kvalificiranim certifikatima za e-pečat je pravna osoba.

Subjekt certificiranja u certifikatima koje izdaje Fina RDC-TDU 2015:

- u kvalificiranim certifikatima za e-potpis je Pripadajuća osoba;
- u kvalificiranim certifikatima za e-pečat je TDU.

1.3.4. Pouzdajuće strane

Pouzdajuće strane su fizičke osobe ili Poslovni subjekti koji se oslanjaju na uslugu povjerenja. Pouzdajuća strana temeljem certifikata provodi validaciju elektroničkog potpisa ili elektroničkog pečata te djeluje na osnovu razumnog pouzdanja u certifikat.

Obaveze i odgovornosti Pouzdajuće strane navedene su u točki 9.6.4. ovih Općih pravila.

1.3.5. Ostali sudionici

Nema odredbi.

1.4. Uporaba certifikata

Pouzdajuća strana odgovorna je za prihvaćanje i ostvarivanje razumnog pouzdanja u certifikat koji ima određenu razinu sigurnosti.

U Tablici 1.5. opisane su razine sigurnosti za kvalificirane 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 prikladna je 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 prikladna je 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

Tablica 1.5. Razine sigurnosti za kvalificirane certifikate

1.4.1. Primjerena uporaba certifikata

1.4.1.1. Primjerena uporaba osobnih EU kvalificiranih certifikata za e-potpis

Osobni EU kvalificirani certifikati za e-potpis navedeni u Tablici 1.1. ovih Općih pravila upotrebljavaju se samo za podršku u elektroničkim potpisima, a pripadajuće privatne ključeve ovih certifikata upotrebljavaju Fizičke osobe – građani samo za izradu elektroničkih potpisa.

U nastavku su navedena dodatne odredbe za primjerenu uporabu osobnih EU kvalificiranih certifikata za e-potpis.

- Osobni EU kvalificirani certifikat za e-potpis (QCP-n-qscd) prikladan je za podršku kvalificiranom elektroničkom potpisu, a pripadajući privatni ključ može se koristiti za izradu kvalificiranog elektroničkog potpisa.
- Osobni EU kvalificirani certifikat za e-potpis (QCP-n) i Osobni EU kvalificirani certifikat za udaljeni e-potpis (QCP-n) prikladni su za podršku naprednom elektroničkom potpisu zasnovanom na kvalificiranom certifikatu, a pripadajući privatni ključevi mogu se koristiti za izradu naprednog elektroničkog potpisa koji je zasnovan na kvalificiranom certifikatu.

1.4.1.2. Primjerena uporaba poslovnih EU kvalificiranih certifikata za e-potpis

Poslovni EU kvalificirani certifikati za e-potpis navedeni u Tablici 1.1. ovih Općih pravila upotrebljavaju se samo za podršku u elektroničkim potpisima, a pripadajuće privatne ključeve ovih certifikata upotrebljavaju Pripadajuće osobe samo za izradu elektroničkih potpisa. Poslovni certifikati koriste se u poslovne svrhe, a Potpisnici ih mogu koristiti i u osobne svrhe ukoliko to ne priječe interni akti poslovnog subjekta.

U nastavku su navedena dodatne odredbe za primjerenu uporabu poslovnih EU kvalificiranih certifikata za e-potpis.

- Poslovni EU kvalificirani certifikat za e-potpis (QCP-n-qscd) prikladan je za podršku kvalificiranom elektroničkom potpisu, a pripadajući privatni ključ može se koristiti za izradu kvalificiranog elektroničkog potpisa.
- Poslovni EU kvalificirani certifikat za e-potpis (QCP-n) i Poslovni EU kvalificirani certifikat za udaljeni e-potpis (QCP-n) prikladni su za podršku naprednom elektroničkom potpisu zasnovanom na kvalificiranom certifikatu, a pripadajući privatni ključevi mogu se koristiti za izradu naprednog elektroničkog potpisa koji je zasnovan na kvalificiranom certifikatu.

1.4.1.3. Primjerena uporaba EU kvalificiranih certifikata za e-pečat

EU kvalificirani certifikati za e-pečat navedeni u Tablici 1.1. ovih Općih pravila upotrebljavaju Autori pečata samo za podršku u elektroničkim pečatima, a pripadajuće privatne ključeve ovih certifikata upotrebljavaju Autori pečata samo za izradu elektroničkih pečata.

U nastavku su navedena dodatne odredbe za primjerenu uporabu EU kvalificiranih certifikata za e-pečat.

- EU kvalificirani certifikat za e-pečat (QCP-l-qscd) prikladan je za podršku kvalificiranom elektroničkom pečatu, a pripadajući privatni ključ može se koristiti za izradu kvalificiranog elektroničkog pečata.
- EU kvalificirani soft certifikat za e-pečat (QCP-l) i EU kvalificirani certifikat za udaljeni e-pečat (QCP-l) prikladni su za podršku naprednom elektroničkom pečatu zasnovanom na kvalificiranom certifikatu, a pripadajući privatni ključevi mogu se koristiti za izradu naprednog elektroničkog pečata koji je zasnovan na kvalificiranom certifikatu.

1.4.1.4. Primjerena uporaba TDU EU kvalificiranih certifikata za e-potpis

TDU EU kvalificirani certifikati za e-potpis navedeni u Tablici 1.2. ovih Općih pravila upotrebljavaju se samo za podršku u elektroničkim potpisima, a pripadajuće privatne ključeve ovih certifikata upotrebljavaju pripadajuće osobe u TDU samo za izradu elektroničkih potpisa. TDU certifikati za e-potpis koriste se za potrebe tijela državne uprave. TDU certifikate Potpisnici mogu koristiti i u osobne svrhe ukoliko to ne priječe interni akti tijela državne uprave.

U nastavku su navedena dodatne odredbe za primjerenu uporabu TDU EU kvalificiranih certifikata za e-potpis.

- TDU EU kvalificirani certifikat za e-potpis (QCP-n-qscd) prikladan je za podršku kvalificiranom elektroničkom potpisu, a pripadajući privatni ključ može se koristiti za izradu kvalificiranog elektroničkog potpisa.
- TDU EU kvalificirani certifikat za e-potpis (QCP-n) i TDU EU kvalificirani certifikat za udaljeni e-potpis (QCP-n) prikladni su za podršku naprednom elektroničkom potpisu zasnovanom na kvalificiranom certifikatu, a pripadajući privatni ključevi mogu se koristiti za izradu naprednog elektroničkog potpisa koji je zasnovan na kvalificiranom certifikatu.

1.4.1.5. Primjerena uporaba TDU EU kvalificiranih certifikata za e-pečat

TDU EU kvalificirani certifikati za e-pečat navedeni u Tablici 1.2. ovih Općih pravila upotrebljavaju se samo za podršku u elektroničkim pečatima, a pripadajuće privatne ključeve ovih certifikata upotrebljavaju TDU samo za izradu elektroničkih pečata. TDU certifikati za e-pečat koriste se za potrebe tijela državne uprave.

U nastavku su navedena dodatne odredbe za primjerenu uporabu TDU EU kvalificiranih certifikata za e-pečat.

- TDU EU kvalificirani certifikat za e-pečat (QCP-l-qscd) prikladan je za podršku kvalificiranom elektroničkom pečatu, a pripadajući privatni ključ može se koristiti za izradu kvalificiranog elektroničkog pečata.
- TDU EU kvalificirani soft certifikat za e-pečat (QCP-l) i TDU EU kvalificirani certifikat za udaljeni e-pečat (QCP-l) prikladni su za podršku naprednom elektroničkom pečatu zasnovanom na kvalificiranom certifikatu, a pripadajući privatni ključevi mogu se koristiti za izradu naprednog elektroničkog pečata koji je zasnovan na kvalificiranom certifikatu.

1.4.2. Zabrane uporabe certifikata

Osim uporaba u elektroničkim potpisima i elektroničkim pečatima, navedenih u točki 1.4.1. ovog dokumenta, sve ostale uporabe kvalificiranih certifikata izdanih sukladno ovim Općim pravilima su zabranjene.

1.5. Administracija dokumenta

1.5.1. Organizacija odgovorna za održavanje dokumenta

Za izradu i održavanje ovog dokumenta Općih pravila 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 ovog dokumenta Općih pravila 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 ovih Općih pravila 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 $CPS_{QC\text{-}eIDAS}$ [29] s ovim Općim pravilima utvrđuje Fina PMA.

1.5.4. Procedure odobravanja CPS-a

Procedura odobravanja $CPS_{QC\text{-}eIDAS}$ [29] dokumenta opisana je u $CPS_{QC\text{-}eIDAS}$ [29] dokumentu.

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.

POJAM	ZNAČENJE
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.
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.
EU kvalificirani certifikat	Kvalificirani certifikat kako je specificirano u Uredbi (EU) br. 910/2014
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.

POJAM	ZNAČENJE
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).
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 ocjenitelj	Fizička ili pravna osoba koja zadovoljava zahtjeve navedene u dokumentu Baseline Requirements [27] kojeg objavljuje CA/Browser Forum.
Kvalificirani certifikat za elektronički pečat	Certifikat za elektronički pečat koji izdaje kvalificirani pružatelj usluge povjerenja i koji ispunjava zahtjeve određene u Prilogu III. Uredbe (EU) br. 910/2014 [1].
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 pečat	Napredan elektronički pečat koji je izrađen pomoću sredstava za izradu kvalificiranog elektroničkog pečata i temelji se na kvalificiranom certifikatu za elektronički pečat.

POJAM	ZNAČENJE
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 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].
Lista opozvanih certifikata (CRL)	Potpisana lista u kojoj su naznačeni certifikati koje izdavatelj certifikata više ne smatra valjanim.
Napredan elektronički pečat	Elektronički pečat koji ispunjava sljedeće zahtjeve: (a) na nedvojben način je povezan s Autorom pečata; (b) omogućava identificiranje Autora pečata; (c) izrađen je korištenjem podacima za izradu elektroničkog pečata koje Autor pečata može, uz visoku razinu pouzdanja i pod svojom kontrolom, koristiti za izradu elektroničkog pečata; i (d) povezan je s podacima na koje se odnosi na takav način da se može otkriti bilo koja naknadna izmjena podataka.
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.
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.

POJAM	ZNAČENJE
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.
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.

POJAM	ZNAČENJE
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.
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	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.

POJAM	ZNAČENJE
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.
Servis udaljenog elektroničkog potpisivanja i pečatiranja	Servis koji koordinira i upravlja procesom kojim krajnji Korisnik uporabom osobnog uređaja može udaljeno potpisati ili pečatirati dokument ili drugu informaciju, uporabom potpisnog ključa koji se čuva u ovom servisu, udaljeno od Korisnika.
Siguran kriptografski uređaj	Uređaj koji čuva privatni Korisnički ključ, štiti ga protiv kompromitiranja i obavlja potpisne ili dekripcijske funkcije u ime Korisnika.
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.
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.
Sredstvo za izradu kvalificiranog elektroničkog pečata	Sredstvo za izradu elektroničkog pečata koje *mutatis mutandis* ispunjava zahtjeve određene u Prilogu II. Uredbe (EU) br. 910/2014 [1].
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.

POJAM	ZNAČENJE
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*)
TSA sustav	Sustav IT proizvoda i komponenti organiziranih za pružanje usluga izdavanja vremenskih žigova.
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 1.6. Definicije

1.6.2. Kratice

KRATICA	PUNI NAZIV	ZNAČENJE
CA	*Certification Authority*	Certifikacijsko tijelo
CP	*Certificate Policy*	Opća pravila pružanja usluga certificiranja
$CP_{QC\text{-}eIDAS}$	*Certificate Policy for Qualified Certificates for Electronic Signatures and Seals*	Opća pravila pružanja usluga certificiranja za kvalificirane certifikate za elektroničke potpise i pečate
CPS	*Certification Practice Statement*	Pravilnik o postupcima certificiranja
$CPS_{QC\text{-}eIDAS}$	*Certification Practice Statement for Qualified Certificates for Electronic Signatures and Seals*	Pravilnik o postupcima certificiranja za kvalificirane certifikate za elektroničke potpise i pečate
CRL	*Certificate Revocation List*	Lista opozvanih certifikata
DN	*Distinguished Name*	Razlikovno ime

KRATICA	PUNI NAZIV	ZNAČENJE
LDAP	*Lightweight Directory Access Protocol*	Protokol za pristup informacijskim direktorijima
LRA	*Local Registration Authority*	Lokalni registracijski ured
OCSP	*Online Certificate Status Protocol*	*Protokol online* 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
QC	*Qualified Certificate*	Kvalificirani certifikat
QCP	*Qualified Certificate Policy*	Opća pravila certificiranja za kvalificirane certifikate
QCP-l	*Certificate policy for EU qualified certificate issued to a legal person*	Opća pravila certificiranja za EU kvalificirane certifikate izdane pravnim osobama
QCP-l-qscd	*Certificate policy for EU qualified certificate issued to a legal person where the private key and the related certificate reside on a QSCD*	Opća pravila certificiranja za EU kvalificirane certifikate izdane pravnim osobama s privatnim ključem i pripadajućim certifikatom na QSCD uređaju
QCP-n	*Certificate policy for EU qualified certificate issued to a natural person*	Opća pravila certificiranja za EU kvalificirane certifikate izdane fizičkim osobama
QCP-n-qscd	*Certificate policy for EU qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD*	Opća pravila certificiranja za EU kvalificirane certifikate izdane fizičkim osobama s privatnim ključem i pripadajućim certifikatom na QSCD uređaju
QSCD	*Qualified electronic Signature/Seal Creation Device*	Kvalificirano sredstvo za izradu elektroničkog potpisa/pečata
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.

Na internetskim stranicama Fina PKI repozitorija objavljuju se:

- dokumenti općih pravila pružanja usluga certificiranja;
- pravilnici o postupcima certificiranja;
- uvjeti i izjave o pružanju usluga izdavanja certifikata (engl. *Terms and conditions* i *PKI disclosure statement*);
- cjenik usluga certificiranja;
- obrasci za Korisnike;
- Fina Root CA certifikat i certifikati subordiniranih Fina CA-ova;
- CRL Fina Root CA i CRL-ovi subordiniranih Fina CA-ova;
- certifikati namijenjeni za provjeru i testiranje;
- obavijesti Korisnicima i Pouzdajućim stranama vezane uz pružanje usluga certificiranja;
- ostale informacije vezane uz rad Fina CA-ova.

Na internetskim stranicama Fina PKI repozitorija omogućen je dohvat pojedinog izdanog certifikata.

Internetske stranice Fina PKI repozitorija dostupne su s internetske adrese http://www.fina.hr/finadigicert na hrvatskom i engleskom jeziku.

U dijelu Fina PKI repozitorija dostupnog preko javnog LDAP imenika dostupni su certifikati subordiniranih Fina CA-ova te CRL-ovi koje izdaju subordinirani Fina CA-ovi.

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.

U Fina PKI repozitoriju ne objavljuju se povjerljivi podaci.

2.3. Vrijeme ili učestalost objavljivanja

Fina na godišnjoj razini i prema potrebi održava i ažurira opća pravila i pravilnik o postupcima certificiranja te ih odobrava i objavljuje. Drugi Fina PKI dokumenti i ostale relevantne informacije objavljuju se prema potrebi, nakon odobrenja.

Certifikati su na internetskim stranicama Fina PKI repozitorija dostupni odmah po izdavanju.

Učestalost objave CRL za certifikate koje izdaju Fina CA-ovi definirana je u točki 4.9.7. ovih Općih pravila.

Online informacije o statusu izdanih certifikata dostupne su putem Fina OCSP servisa koji je opisan u točki 4.9.9. ovih Općih pravila.

2.4. Kontrole pristupa repozitoriju

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

Fina na repozitoriju ima uspostavljene kontrole pristupa u cilju sprječavanja neautoriziranog dodavanja, promjene ili brisanja informacija te zaštite njihove cjelovitosti i autentičnosti.

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

3. IDENTIFIKACIJA I POTVRĐIVANJE IDENTITETA SUBJEKTA

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 [24].

Polje *Subject* u certifikatima koji se izdaju za fizičke osobe sadrži ime i prezime osobe. U poslovnim certifikatima i certifikatima za elektronički pečat polje *Subject* dodatno sadrži i puni registrirani naziv Poslovnog subjekta i njegov identifikator.

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.

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:

- Serial Number

  Vrijednost atributa *Serial Number* u polju *Subject* jamči jedinstvenost pojedinog Subjekta. Vrijednost ovog atributa jamči i jedinstvenost polja *Subject* u certifikatima unutar Fina PKI produkcijske hijerarhije zasnovane na Fina Root CA.

U certifikatima za elektroničke potpise atribut *Serial Number* sastoji se od dvoslovčanog ISO koda države prebivališta Potpisnika, jedanaesteroznamenkastog jedinstvenog identifikatora fizičke osobe te dva broja W i Z koji predstavljaju oznake koje imaju interno značenje za FINA PKI. 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.

U certifikatima za elektroničke pečate atribut *Serial Number* sastoji se od dvije komponente: W i Z odijeljene točkom. W i Z komponente imaju interno značenje za Fina PKI.

- Common Name

  U certifikatima za elektroničke potpise ovaj atribut sadrži ime i prezime fizičke osobe kako je navedeno u identifikacijskoj ispravi.

  U certifikatima za elektroničke pečate ovaj atribut sadrži naziv pravne osobe ili TDU kako ga pravna osobe ili TDU koristi u poslovnoj primjeni. Ovaj naziv ne mora biti jednak punom registriranom nazivu Poslovnog subjekta iz službenog nadležnog nacionalnog registra.

- Given Name

  Atribut *Given Name* sadrži ime fizičke osobe kako je navedeno u identifikacijskoj ispravi.

- Surname

  Atribut *Surname* sadrži prezime fizičke osobe kako je navedeno u identifikacijskoj ispravi.

- Organizational Unit Name

  U certifikatima za elektroničke pečate i certifikatima za elektroničke potpise za TDU ovaj atribut sadrži naziv organizacijske jedinice povezane s Poslovnim subjektom imenovanim u atributu *Organization Name*.

- Organization Name

  U certifikatima izdanim fizičkim osobama koje nisu povezane s Poslovnim subjektom atribut *Organization Name* sadrži vrijednost „OSOBNI“.

  U certifikatima za elektroničke pečate i certifikatima za elektroničke potpise izdanim fizičkim osobama koje su povezane s Poslovnim subjektom atribut *Organization Name* sadrži puni registrirani naziv Poslovnog subjekta.

- Organization Identifier

  U certifikatima za elektroničke potpise izdanim fizičkim osobama koje su povezane s Poslovnim subjektom atribut *Organization Identifier* sadrži dvoslovčani ISO kod države sjedišta Poslovnog subjekta te jedanaesteroznamenkasti jedinstveni identifikator Poslovnog subjekta. Jedanaesteroznamenkasti identifikator Poslovnog subjekta je OIB ako Poslovni subjekt ima dodijeljen OIB u Republici Hrvatskoj. Ako Poslovni subjekt nema dodijeljen OIB, tada jedanaesteroznamenkasti jedinstveni identifikator Poslovnog subjekta generira Fina.

  U certifikatima za elektroničke pečate atribut *Organization Identifier* sadrži oznaku „VAT“, dvoslovčani ISO kod države koja je izdala porezni identifikacijski broj te porezni identifikacijski broj Poslovnog subjekta. Za Poslovne subjekte čije je sjedište u Republici Hrvatskoj porezni identifikacijski broj je OIB.

- Locality Name

  Za poslovne certifikate za elektroničke potpise i certifikate za elektroničke pečate atribut *Locality Name* sadrži naziv mjesta u kojem je sjedište Poslovnog subjekta.

  Za osobne certifikate za elektroničke potpise atribut *Locality Name* sadrži mjesto prebivališta Potpisnika

- Country Name

  Atribut *Country Name* sadrži oznaku dvoslovčanog ISO koda Republike Hrvatske.

- Subject Alternative Name

  Subject Alternative Name je opcionalna ekstenzija certifikata koja može sadržavati e-mail adresu Potpisnika odnosno Autora pečata u obliku koji je sukladan preporuci IETF RFC 822 i/ili interni identifikator Subjekta.

3.1.5. Jedinstvenost imena

Razlikovno ime Subjekta jedinstveno je unutar Fina PKI produkcijske hijerarhije zasnovane na Fina Root CA. Jedinstvenost razlikovnog imena osigurana je vrijednošću atributa *Serial Number* u polju *Subject* certifikata

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

Fina prikuplja osobne podatke fizičkih osoba i podatke Poslovnih subjekata isključivo za potrebe registracije u cilju izdavanja certifikata.

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 iz opsega ovih Općih pravila Fina provjerava i potvrđuje identitet fizičke osobe temeljem neposredne fizičke identifikacije ili korištenjem metoda koje pružaju jednaku razinu sigurnosti utvrđivanja identiteta.

3.2.1. Metoda dokazivanja posjeda privatnog ključa

Privatni ključ koji odgovara javnom ključu koji se dostavlja za izradu certifikata za elektronički potpis ili elektronički pečat generira Potpisnik, odnosno Autor pečata, ili ga generira Fina.

U slučaju kad Fina generira par Korisničkih ključeva tehnološkim procesima i metodama provjere osigurava se povezanost Potpisnika, odnosno Autora pečata s privatnim ključem, koji odgovara javnom ključu za koji Fina izdaje certifikat, kao i kontrola Potpisnika, odnosno Ovlaštenog predstavnika nad privatnim ključem.

U slučaju kad Potpisnik, odnosno Autor pečata generira par ključeva Fina tehnološkim procesom i metodom zahtijevanja certifikata obuhvaća provjeru posjeduje li i kontrolira li Potpisnik, odnosno Ovlašteni predstavnik privatni ključ koji je povezan s javnim ključem koji se na zaštićeni način dostavlja u Finu za izradu certifikata.

U slučaju kada opća pravila pružanja usluga certificiranja propisuju da se za određeni tip kvalificiranog certifikata generiranje i zaštita privatnog ključa provodi QSCD uređajem Fina ili vanjski ugovoreni RA tehnološkim procesima i metodama provjere osigurava da je javni ključ koji se dostavlja na certificiranje iz para ključeva generiranog u QSCD uređaju te da je povezan s privatnim ključem Potpisnika, odnosno Autora pečata.

3.2.2. Potvrda identiteta poslovnog subjekta

Provjera i potvrda identiteta Poslovnog subjekta provodi se provjerom:

- registriranog naziva Poslovnog subjekta;
- pravnog postojanja Poslovnog subjekta;
- upisa u nadležni registar;
- matičnog broja iz nadležnog registra;
- OIB-a Poslovnog subjekta, ako mu je dodijeljen;
- adrese sjedišta Poslovnog subjekta.

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.

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. ovih Općih pravila;
- poštansku adresu;
- e-mail adresu;
- broj telefona.

Za izdavanje certifikata za elektroničke potpise 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 elektronički pečat.

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. ovih Općih pravila.

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 pomoću certifikata kvalificiranog elektroničkog potpisa izdanog temeljem neposredne identifikacije fizičke osobe.

Postupak posredne identifikacije fizičke osobe Fina može provoditi i pomoću sredstava elektroničke identifikacije, za koja je prije izdavanja kvalificiranog certifikata osigurana fizička prisutnost fizičke osobe i koja ispunjavaju zahtjeve u pogledu sigurnosnih razina „značajna" ili „visoka" sukladno odredbama članka 8. Uredbe (EU) br. 910/2014 [1].

3.2.3.3. Prihvatljive vrste identifikacijskih isprava

Fizičke osobe dokazuju svoj identitet valjanom osobnom iskaznicom ili putovnicom.

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

3.2.4. Informacije o korisniku koje se ne provjeravaju

Informacije o Korisniku koje se ne provjeravaju su:

- naziv organizacijske jedinice TDU;
- telefonski brojevi za kontakt;
- adresa e-pošte za kontakt.

3.2.5. Provjera identiteta ovlaštenih osoba

Prije izdavanja poslovnih i TDU certifikata za elektroničke potpise 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., i usporedbom s podacima iz preslike važeće identifikacijske isprave osobe ovlaštene za zastupanje.

Prije izdavanja certifikata za elektroničke pečate provodi se provjera i potvrda identiteta Ovlaštenog predstavnika postupcima neposredne ili posredne identifikacije sukladno točkama 3.2.3.1. i 3.2.3.2. ovih Općih pravila.

Utvrđivanje identiteta opunomoćenika 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 ovih Općih pravila, aktualni se uvjeti pružanja usluga certificiranja komuniciraju Potpisniku, 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).

Certifikat se obnavlja redovnom obnovom ako su zadovoljeni uvjeti iz točke 4.7.1. ovih Općih pravila.

3.3.1.1. Identifikacija pri podnošenju zahtjeva u RA mreži

Identifikacija i potvrđivanje identiteta podnositelja zahtjeva provodi se podnošenjem vlastoručno potpisanog zahtjeva u papirnatom obliku uz neposrednu identifikaciju podnositelja zahtjeva u RA mreži i usporedbom podataka iz zahtjeva s podacima u Fininoj bazi registriranih Korisnika te ukoliko je primjenjivo korištenjem komunikacijskih kanala sukladno važećoj zakonskoj regulativi.

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. ovih Općih pravila, 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, odnosno pečatom uz korištenje certifikata čija se obnova traži.

U suprotnom provodi se postupak sukladno točki 3.3.1.1. ovih Općih pravila.

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. ovih Općih pravila.

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. ovih Općih pravila.

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. ovih Općih pravila.

Identifikacija i potvrđivanje identiteta podnositelja zahtjeva za oporavak certifikata provodi se sukladno proceduri inicijalnog utvrđivanja identiteta iz točke 3.2. ovih Općih pravila.

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 postupkom neposredne identifikacije podnositelja zahtjeva temeljem identifikacijske isprave podnositelja zahtjeva.

- Podnošenje zahtjeva za opoziv ili suspenziju poštanskom dostavom ili preko dostavljača

  Identifikacija i potvrđivanje identiteta podnositelja zahtjeva provodi se u registracijskom uredu RA mreže na temelju preslike identifikacijske isprave podnositelja zahtjeva iz točke 3.2.3.3. ovih Općih pravila.

- Elektronička dostava zahtjeva za opoziv ili suspenziju na e-mail adresu zaštićenim komunikacijskim kanalom

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

- Podnošenje zahtjeva za opoziv ili suspenziju telefonskim putem

  Telefonski zahtjev za opoziv ili suspenziju certifikata provodi se pozivom Fini na telefonski broj koji je objavljen na internetskim stranicama repozitorija iz točke 2.2. ovih Općih pravila, od 0 do 24 sata, 7 dana u tjednu.

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, sukladno točki 3.2.3.3. ovih Općih pravila.

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 za elektronički potpis mogu podnijeti fizičke osobe – građani.

Zahtjev za izdavanje Poslovnih certifikata za elektronički potpis mogu podnijeti Pripadajuće osobe.

Zahtjev za izdavanje certifikata za elektronički pečat mogu podnijeti Ovlašteni predstavnici.

Zahtjev za izdavanje TDU certifikata za elektronički potpis mogu podnijeti Pripadajuće osobe TDU.

Zahtjev za izdavanje TDU certifikata za elektronički pečat mogu podnijeti Ovlašteni predstavnici TDU.

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 certifikata za elektronički pečat ugovor potpisuje Ovlašteni predstavnik.

Zahtjev za izdavanje 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 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 za elektroničke potpise podnosi Pripadajuća osoba.

Zahtjev za izdavanje certifikata za elektroničke pečate podnosi Ovlašteni predstavnik.

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

Identifikacija i potvrđivanje identiteta podnositelja zahtjeva provodi se na način opisan u točki 3.2. ovih Općih pravila.

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 ova 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. ovih Općih pravila.

Prije početka pružanja usluga certificiranja iz opsega ovih Općih pravila 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 i ovjeren 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. ovih Općih pravila.

Obaveze i odgovornosti RA mreže navedene su u Poglavlju 9.6.2. ovih Općih pravila.

Obaveze i odgovornosti Fine, kao pružatelja usluga povjerenja, navedene su u Poglavlju 9.6.1. ovih Općih pravila.

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. ovih Općih pravila.

4.2.2. Odobravanje ili odbijanje zahtjeva za izdavanje certifikata

RA mreža provjerava podatke iz dokumenata koje prilaže podnositelj zahtjeva i potvrđuje točnost i cjelovitost informacija u zahtjevu za izdavanje certifikata.

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

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.

4.3. Izdavanje certifikata

Fina CA izdaje certifikat nakon provedenih svih procesa provjere podataka i nakon odobrenja zahtjeva za izdavanje certifikata. 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.

4.3.1. Postupci CA tijekom izdavanja certifikata

Fina CA tijekom procesa izdavanja certifikata:

- provjerava valjanost elektroničkog potpisa Službenika za registraciju u dostavljenom odobrenom zahtjevu;
- generira par Korisničkih ključeva za certifikate sukladno točkama 6.1.1.5. i 6.1.1.6. ovih Općih pravila;
- izrađuje zahtijevani certifikat za javni ključ Subjekta dostavljen sukladno točki 6.1.3. ovih Općih pravila;
- čini certifikat dostupnim Potpisniku, odnosno Ovlaštenom predstavniku u svrhu njegova preuzimanja;
- čini certifikat dostupnim na Fina PKI repozitoriju.

4.3.2. Obavještavanje korisnika od strane CA o izdavanju certifikata

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

4.4. Prihvaćanje certifikata

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

Prihvaćajući certifikat Potpisnik, odnosno Ovlašteni predstavnik prihvaća da su svi podaci upisani u certifikat točni i istiniti u trenutku njegova prihvaćanja te da podaci ne navode na pogrešne zaključke.

4.4.1. Provedba prihvaćanja certifikata

Potpisnik, odnosno Ovlašteni predstavnik tijekom ili neposredno po obavljenom preuzimanju certifikata provodi provjeru njegovog sadržaja. Ukoliko ne prihvaća bilo koji dio sadržaja certifikata, Potpisnik, odnosno Ovlašteni predstavnik odmah o tome obavještava Finu i pritom navodi razloge neprihvaćanja istog.

Smatra se da je Potpisnik, odnosno Ovlašteni predstavnik prihvatio certifikat u trenutku prvog korištenja certifikata.

Ukoliko Potpisnik, odnosno Ovlašteni predstavnik u roku od petnaest dana od preuzimanja certifikata ni jednom nije koristio izdani certifikat niti je u tom roku odbio prihvatiti certifikat, smatra se da je certifikat prihvatio.

4.4.2. Objava certifikata od strane CA

Ukoliko je Potpisnik, odnosno Ovlašteni predstavnik te osoba ovlaštena za zastupanje Poslovnog subjekta odobrio 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.

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 koristiti algoritme propisane normizacijskim dokumentom ETSI TS 119 312 [17] te duljine ključeva sukladno točke 6.1.5. ovih Općih pravila;
- koristiti certifikat i pripadajući privatni ključ samo u svrhe i na način propisan ovim Općim pravilima i uvjetima pružanja usluga certificiranja;
- propisno koristiti i čuvati privatni ključ za elektronički potpis, odnosno elektronički pečat;
- koristiti Subjektov par ključeva sukladno pravilima određenim u točki 1.4.1. ovih Općih pravila;
- štititi 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 kvalificiranog pružatelja usluga povjerenja i zahtijevanje suspenzije ili opoziva certifikata;
- nakon kompromitiranja privatnog ključa odmah i trajno prestati s njegovom uporabom.

Korisničkim parom ključeva iz točke 6.1.1.6. ovih Općih pravila u ime Potpisnika, odnosno Autora pečata upravlja Fina kao kvalificirani pružatelj usluga povjerenja te se Fina za ove ključeve obvezuje osigurati:

- korištenje privatnog ključa za elektronički potpis isključivo pod kontrolom Potpisnika;
- korištenje privatnog ključa za elektronički pečat pod kontrolom Autora pečata;
- izradu elektroničkog potpisa, odnosno elektroničkog pečata sukladno ovim Općom pravilima;
- korištenje Subjektovog para ključeva sukladno pravilima određenim u točki 1.4.1. ovih Općih pravila.

4.5.2. Korištenje javnog ključa i certifikata od strane pouzdajuće strane

Pouzdajuća strana koja namjerava ostvariti pouzdanje u certifikat izdan prema ovim Općim pravilima treba:

- voditi računa o primjerenoj uporabi i ograničenjima uporabe certifikata;
- upotrebljavati certifikat za elektronički potpis i pripadajući javni ključ isključivo za validaciju elektroničkog potpisa, sukladno točki 1.4.1. ovih Općih pravila;
- upotrebljavati certifikat za elektronički pečat i pripadajući javni ključ isključivo za validaciju elektroničkog pečata, sukladno točki 1.4.1. ovih Općih pravila;
- obaviti provjeru roka važenja svih certifikata u certifikacijskom lancu;
- obaviti provjeru statusa opozvanosti i suspendiranosti certifikata.

4.6. Obnova certifikata

Svaka obnova certifikata u Fina PKI podrazumijeva izdavanje certifikata s novim parom ključeva istom Subjektu certificiranja (engl. *re-key*). Postupak takve obnove certifikata opisan je u točki 4.7. ovih Općih pravila.

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 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 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 ili QSCD uređaju, 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.

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.

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. ovih Općih pravila 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. ovih Općih pravila.

U slučaju *online* podnesenog zahtjeva identifikacija i potvrđivanje identiteta podnositelja zahtjeva provodi se sukladno točki 3.3.1.2. ovih Općih pravila.

Nakon provjere autentičnosti i valjanosti zahtjeva Fina CA izdaje certifikat sukladno točki 4.3.1. ovih Općih pravila.

4.7.4. Obavještavanje korisnika o obnovi certifikata uz generiranje novog para ključeva

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

Obavještavanje Potpisnika, odnosno Ovlaštenog predstavnika o obnovi certifikata provodi se sukladno točki 4.3.2. ovih Općih pravila.

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. ovih Općih pravila.

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. ovih Općih pravila.

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. ovih Općih pravila.

4.8. Izmjene u certifikatu

Potpisnici i Autori pečata 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 certifikata za elektronički potpis mogu biti promjene podataka koje se odnose na Subjekt:

- imena ili prezimena Potpisnika;
- naziva Poslovnog subjekta;
- naziva podorganizacijske jedinice u TDU;
- naziv mjesta 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 certifikata za elektronički pečat 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 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. ovih Općih pravila 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. Identifikacija i potvrđivanje identiteta podnositelja zahtjeva provodi se sukladno proceduri inicijalnog utvrđivanja identiteta iz točke 3.2. ovih Općih pravila. Obrada zahtjeva i izdavanje certifikata provodi se sukladno točki 4.2., 4.3. i 4.4. ovih Općih pravila.

Zahtjev za izmjene *e-mail* adrese, identifikatora Subjekta u *Subject alternative name* ekstenziji certifikata te za izmjenu podataka koji se ne odnose na Subjekt može se podnijeti

online uz korištenje naprednog elektroničkog potpisa. Nakon provjere autentičnosti i valjanosti zahtjeva Fina CA izdaje certifikat sukladno točki 4.3.1. ovih Općih pravila.

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. ovih Općih pravila.

4.8.5. Provedba prihvaćanja izmijenjenog certifikata

Provedba prihvaćanja izmijenjenog certifikata provodi se sukladno točki 4.4.1. ovih Općih pravila.

4.8.6. Objavljivanje izmijenjenog certifikata od strane CA

Objavljivanje izmijenjenog certifikata provodi se na način opisan u točki 4.4.2. Općih pravila.

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. Općih pravila.

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 Autora pečata;
- 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 ovim Općim pravilima;
- 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 Općim pravilima i potpisanim ugovorima.

4.9.2. Tko može tražiti opoziv

Zahtjev za opoziv pripadajućeg osobnog certifikata za elektronički potpis podnosi Potpisnik.

Zahtjev za opoziv poslovnih ili TDU certifikata za elektronički potpis podnosi Potpisnik ili osoba ovlaštena za zastupanje Poslovnog subjekta.

Zahtjev za opoziv certifikata za elektronički pečat podnosi Ovlašteni predstavnik. Zahtjev se dodatno ovjerava pečatom Autora pečata.

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. ovih Općih pravila, 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 zaštićenim komunikacijskim kanalom.

Zahtjev za opoziv se može predati i telefonskim putem, od 0 do 24 sata, 7 dana u tjednu, pozivom Fini na telefonski broj koji je objavljen na internetskim stranicama repozitorija iz točke 2.2. ovih Općih pravila , ili na telefonski broj vanjskog ugovorenog RA, sukladno točki 3.4.1. ovih Općih pravila..

U slučaju da je zahtjev za opoziv certifikata temeljen na dojavi treće strane Fina će prije opoziva certifikata provjeriti utemeljenost zahtjeva.

Fina na osnovu točnog i cjelovito ispunjenog i potpisanog zahtjeva za opoziv, opoziva certifikat i o tome obavještava Potpisnika, odnosno Ovlaštenog predstavnika te, ukoliko je to primjenjivo, Poslovni subjekt s kojim je Potpisnik povezan.

Ako je zahtjev za opozivom zaprimljen telefonskim putem, Fina provodi autentikaciju podnositelja zahtjeva, koji se autenticira znanjem zaporke navedene na Zahtjevu za izdavanje certifikata te opoziva certifikat i o tome 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. ovih Općih pravila 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

Fina u najkraćem razumnom roku, a najkasnije u roku od 24 sata od primitka odgovarajućeg zahtjeva donosi odluku o opozivu certifikata te ovisno o donesenoj odluci opoziva 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. ovih Općih pravila. 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. Ove liste objavljuju se odmah po opozivu, suspenziji ili reaktivaciji certifikata te svakih šest sati od 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 [25].

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

Adresa Fina OCSPservisa je http://ocsp.fina.hr, a upisuje se 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. ovih Općih pravila. 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. ovih Općih pravila.

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 iz točke 4.10.1. ovih Općih pravila.

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, 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 RA mreža 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 za elektronički potpis podnosi Potpisnik.

Zahtjev za suspenziju poslovnih i TDU certifikata za elektronički potpis podnosi Potpisnik ili osoba ovlaštena za zastupanje Poslovnog subjekta.

Zahtjev za suspenziju certifikata za elektronički pečat podnosi Ovlašteni predstavnik.

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 za elektronički potpis podnosi Potpisnik.

Zahtjev za reaktivaciju poslovnih i TDU certifikata za elektronički potpis podnosi Potpisnik.

Zahtjev za reaktivaciju certifikata za elektronički pečat podnosi Ovlašteni predstavnik.

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. ovih Općih pravila 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 se može predati i telefonskim putem, od 0 do 24 sata, 7 dana u tjednu, pozivom Fini na telefonski broj koji je objavljen na internetskim stranicama repozitorija iz točke 2.2. ovih Općih pravila, ili na telefonski broj vanjskog ugovorenog RA, sukladno točki 3.4.1. ovih Općih pravila..

U slučaju da je zahtjev za suspenziju certifikata temeljen na dojavi treće strane Fina će prije suspenzije certifikata provjeriti utemeljenost zahtjeva.

Fina na osnovu točnog i cjelovito ispunjenog i potpisanog zahtjeva za suspenziju, odnosno provjerom znanja zaporke navedene na zahtjevu za izdavanje certifikata kojom se autenticira podnositelj zahtjeva u slučaju podnošenja zahtjeva putem telefona, suspendira certifikat i o tome 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.

4.9.15.2. Procedura za zahtjev za reaktivaciju

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

Fina na osnovu točnog i cjelovito ispunjenog i potpisanog zahtjeva za reaktivaciju reaktivira certifikat i o tome 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 Fina CA opoziva certifikat i objavljuje CRL.

4.10. Usluge statusa certifikata

4.10.1. Operativna svojstva

Fina daje informacije o statusu opozvanosti ili suspendiranosti certifikata kroz pružanje OCSP servisa ili objave CRL. Informacije o statusu pojedinog certifikata dostupne su za vrijeme važenja certifikata, kao i nakon isteka 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.

4.10.2. Dostupnost usluga

Dostupnost CRL 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 Fina PKI.

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 kvalificiranih 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 izdavanja kvalificiranih certifikata 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 u zgradi Fine, u posebnom štićenom prostoru izdvojenom za tu namjenu uz primjenu više razina fizičke i tehničke zaštite koje onemogućuju neovlašten fizički pristup sustavu i podacima i time sprječavaju kompromitiranje sustava i usluga. Fizička zaštita temeljena je na konceptu uporabe sigurnosnih zona te se razina zaštite povećava svakim prolaskom u sljedeću zonu. Fizička zaštita od upada ostvarena je sigurnosnim perimetrima koji razdvajaju zone postavljene oko sustava certificiranja u kojem se provode operacije izrade i opoziva kvalificiranih certifikata.

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

Sigurni prostori i podprostori u kojima se nalaze komponente Fininog sustava 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 podprostorima 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 ovlaštenih osoba i sukladno Fininim internim procedurama.

O svakom pristupu sustavima certificiranja vodi se evidencija.

Fizički pristup podacima registriranih Korisnika koje prikuplja RA mreža imaju samo ovlašteni zaposlenici Fina PKI i ovlašteni zaposlenici Fina RA mreže, odnosno ovlašteni zaposlenici vanjskog ugovorenog RA koji osobne podatke o fizičkim osobama prikupljaju, pohranjuju, koriste i brišu u skladu s odgovarajućim propisima o zaštiti osobnih podataka.

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.

5.1.4. Opasnost od poplave

Lokacija na kojem se nalaze Fina CA-ovi, Fina RA sustavi i repozitorij zaštićena je od poplave.

5.1.5. Protupožarna zaštita

Fina CA-ovi, Fina RA sustav i repozitorij zaštićeni su sustavom za detekciju požara i sustavom za automatski gašenje požara sukladno važećoj zakonskoj regulativi.

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 s uspostavljenom protupožarnom zaštitom i koje su osigurane od poplave. Ovi mediji zaštićeni su od oštećenja, krađe i neovlaštenog pristupa.

5.1.7. Zbrinjavanje otpada

Uređaji i mediji koji sadrže povjerljive informacije u elektroničkom obliku, a koji više nisu potrebni, sigurnosno se uništavaju tako da povjerljive informacije ne mogu više biti čitljive niti obnovljene. Uništavanje ovih uređaja i medija odvija se pod nadzorom ovlaštenih osoba u Fina PKI.

Papirnati dokumenti i materijali koji sadrže povjerljive informacije sigurnosno se uništavaju prije odlaganja u otpad.

5.1.8. Sigurnosne kopije na drugoj lokaciji

Sigurnosne kopije Fina CA i RA sustava, arhivske ili sigurnosne kopije podataka, kopije sadržaja repozitorija te sigurnosne kopije programske opreme pohranjuju se na lokaciji sekundarnog sustava certificiranja koji je izdvojen od primarnog produkcijskog sustava certificiranja. Ove su sigurnosne kopije u odnosu na njihove originale zaštićene jednakom ili višom razinom mjera fizičke zaštite.

5.2. Organizacijske mjere zaštite

5.2.1. Povjerljive uloge

Poslovi upravljanja informacijskim i komunikacijskim sustavom, poslovi upravljanja životnim ciklusom certifikata, administriranje i implementacije sigurnosnih postupaka te poslovi nadzora djelovanja Fina PKI obavljaju se unutar odvojenih organizacijskih jedinica Fine.

Poslovi, obaveze i odgovornosti zaposlenika podijeljene su prema odgovarajućim povjerljivim ulogama. Povjerljive uloge čine temelj povjerenja u Fina PKI i dodjeljuju se ovlaštenim zaposlenicima iz nadležnih organizacijskih jedinica Fine. Svaka povjerljiva uloga je dokumentirana s jasno definiranim opisom poslova i odgovornostima.

Povjerljive uloge uključuju uloge Službenika za sigurnost, Administratora sustava, Operatera sustava, Službenik za registraciju, Službenika za opoziv certifikata i Službenika za nadzor sustava

5.2.2. Broj osoba potrebnih za obavljanje aktivnosti

Poslove u Fina PKI obavljaju isključivo ovlaštene osobe. Fina ima stalno zaposlen dovoljan broj stručnih osoba sa znanjem, iskustvom i kvalifikacijama koji je potreban u Fina PKI za pružanje usluga iz opsega ovih Općih pravila.

Pristup i poslovi u štićenom Fina PKI prostoru provode se isključivo uz istovremenu prisutnost najmanje dvije osobe s povjerljivim ulogama koje imaju dozvole pristupa tom sustavu.

Za obavljanje pojedinih sigurnosno osjetljivih zadataka u Fina PKI štićenom prostoru zahtjeva se sudjelovanje propisanog broja osoba s određenim povjerljivim ulogama.

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

5.2.4. Uloge koje zahtijevaju odvajanje dužnosti

Zbog sigurnosnih zahtjeva izdavanja kvalificiranih certifikata provodi se odvajanje sljedećih dužnosti:

- osobi kojoj je dodijeljena povjerljiva uloga Službenik za sigurnost ili Službenik za registraciju ne dodjeljuje se povjerljiva uloga Službenik za nadzor sustava;
- osobi kojoj je dodijeljena povjerljiva uloga Administrator sustava ne dodjeljuje se povjerljiva uloga Službenik za sigurnost ili Službenik za nadzor sustava.

5.3. Osoblje

5.3.1. Kvalifikacije, radno iskustvo i zahtjevi za provjerom osoblja

Prije početka rada na poslovima 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.

Zaposlenici koji rade na poslovima Fina PKI ne smiju biti u radnom, odnosno poslovnom odnosu s drugim pružateljima usluga povjerenja.

5.3.2. Procedure provjere prikladnosti osoblja

Prije početka rada na poslovima Fina PKI, Fina provodi odgovarajuće provjere kandidata u cilju procijene njihove stručnosti, sposobnosti i pouzdanosti u skladu s potrebama poslova Fina PKI.

5.3.3. Zahtjevi za školovanjem

Zaposlenicima koji obavljaju poslove unutar Fina PKI osigurava se školovanje i usavršavanje sukladno s njihovim povjerljivim ulogama.

5.3.4. Periodičko obavljanje znanja i osvješćivanje

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

Zaposlenici Fina PKI s povjerljivim ulogama u Fina PKI imaju obavezu stjecati i usavršavati svoje znanje.

Obnova znanja zaposlenika Fina RA mreže, a obzirom na poslove koje obavljaju, provodi se redovito, najmanje jednom u dvije godine.

5.3.5. Učestalost i slijed izmjene zaposlenika

Nema odredbi.

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 kvalificiranih 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 sukladno dodijeljenoj povjerljivoj ulozi i pripadnim ovlaštenjima.

5.4. Postupci upravljanja revizijskim zapisima

5.4.1. Tipovi događaja koji se zapisuju

Fina zapisuje revizijske zapise događaja u Fina PKI vezanih uz:

- upravljanje životnim ciklusom CA ključeva Fina CA-ova;
- registraciju fizičke osobe i Poslovnog subjekta;
- pripremu i izdavanje sigurnih kriptografskih, odnosno QSCD uređaja na kojima se izdaju kvalificirani certifikati;
- životni ciklus ključeva i upravljanje ključevima;
- životni ciklus certifikata koje izdaju Fina CA-ovi;
- zahtjeve za opoziv, suspenziju i reaktivaciju certifikata te pripadajuće provedene radnje.

Revizijski zapisi uključuju i sigurnosne događaje u Fina PKI vezane uz promjene sigurnosnih politika, fizičku i tehničku zaštitu Fina PKI prostora, pokretanje i zaustavljanje rada sustava, sistemske greške i kvarove hardvera, aktivnosti vatrozida i usmjerivača te pokušaja pristupa sustavu.

5.4.2. Učestalost obrade revizijskih zapisa

Revizijski zapisi u Fina PKI redovito se pregledavaju na dnevnoj razini. Revizijski zapisi pregledavaju se i u svrhu praćenja i utvrđivanja zlonamjernih aktivnosti na sustavu. Fina koristi automatske mehanizme za upozorenja i dojavu o mogućim kritičnim sigurnosnim događajima. Takve obavijesti dostavljaju se ovlaštenim osobama U Fina PKI. Radnje poduzete na osnovu prikupljanja revizijskih zapisa se dokumentiraju.

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 zaštićeni su tijekom cijelog vremena čuvanja. Zaštita revizijskih zapisa obuhvaća zaštitu zapisa od njihovog neovlaštenog čitanja i otkrivanja te očuvanje cjelovitosti zapisa.

Tako zaštićeni revizijski zapisi su na zahtjev raspoloživi samo ovlaštenim osobama, posebice u svrhu pružanja dokaza o certifikatu za potrebe sudskih postupaka.

5.4.5. Postupci izrade sigurnosnih kopija revizijskih zapisa

Revizijski zapisi Fina PKI sustava arhiviraju se u dvije kopije na fizički odvojenim lokacijama.

Kopije revizijskih zapisa na sekundarnoj lokaciji zaštićuju se jednakom ili višom razinom zaštite u odnosu na revizijske zapise na primarnoj lokaciji (vidi točku 5.4.4.).

5.4.6. Sustav prikupljanja revizijskih zapisa (unutarnji ili vanjski)

Ovisno o vrsti podataka, revizijski zapisi se prikupljaju automatski ili ih prikuplja ovlaštena osoba.

Revizijski zapisi nastali u Fina PKI i Fina RA mreži prikupljaju se interno.

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.

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 i pripadajuća dokumentacija prikupljena postupkom registracije fizičkih osoba i Poslovnih subjekata;
- podaci i dokumentacija vezana uz sigurne kriptografske, odnosno QSCD uređaje;
- certifikati i podaci vezani uz životni ciklus pojedinog certifikata;
- evidencija opozvanih i suspendiranih certifikata, podaci o opozivu, suspenziji i reaktivaciji certifikata te pripadajuća dokumentacija;
- revizijski zapisi iz točke 5.4.1. ovih Općih pravila;
- drugi Finini interni dokumenti.

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

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

Arhivirani podaci i dokumentacija zaštićuju se mehanizmima i postupcima propisane razine sigurnosti koje osiguravaju povjerljivost i cjelovitost arhive. Arhiva se štiti od neovlaštenog pregleda, modificiranja i brisanja podataka.

Jednaka razina zaštite provodi se i za arhiviranje podataka i dokumentacije koja se prikuplja u vanjskim ugovorenim RA-ovima.

Tako zaštićeni arhivirani zapisi su na zahtjev raspoloživi samo ovlaštenim osobama, posebice u svrhu pružanja dokaza o izdanom certifikatu za potrebe sudskih postupaka.

5.5.4. Postupci izrade sigurnosnih kopija arhive

Sigurnosna kopija arhiviranih podataka u elektroničkom obliku izrađuje se u Fina PKI štićenom prostoru te se čuva na siguran način na drugoj lokaciji izdvojeno od primarnog produkcijskog sustava certificiranja, sukladno točki 5.1.8. ovih Općih pravila.

5.5.5. Zahtjevi na zaštitu zapisa vremenskim žigom

Nema odredbi.

5.5.6. Sustav prikupljanja arhivskih zapisa (unutarnji ili vanjski)

Zapisi za arhiviranje prikupljaju se na način koji ovisi o vrsti zapisa.

Zapisi za arhiviranje nastali u Fina PKI i Fina RA mreži prikupljaju se i arhiviraju interno.

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

5.5.7. Postupci dobivanja i provjere arhiviranih zapisa

Pristup zapisima iz arhive imaju samo osobe ovlaštene za pristup tim podacima.

Verifikacija podataka iz arhive obavlja se provjerom njihove cjelovitosti.

5.6. Promjena CA ključa

Fina osigurava da Fina CA kontinuirano pruža kvalificiranu uslugu povjerenja sa svojim validnim parom ključeva i pripadajućim CA certifikatom. Iz tog razloga Fina CA će dovoljno vremena prije isteka CA certifikata, generirati novi par CA ključeva. 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. U oba slučaja za novi javni CA ključ Fina Root CA izdati će CA certifikat.

Fina CA će o promjeni svojeg javnog ključa i o svojem novom CA certifikatu pravodobno obavijestiti sudionike Fina PKI.

Novi pripadajući javni ključ biti će dostupan sudionicima Fina PKI na način na koji je to bio i prethodni Fina CA javni ključ, a sukladno opisu u točki 2.2. ovih Općih pravila.

5.7. Oporavak od kompromitiranja ili nepogode

5.7.1. Postupci u slučaju incidenta ili kompromitiranja

Planom kontinuiteta poslovanja Fina PKI regulirani su postupci u slučaju izbijanja incidenta ili kompromitiranja sustava, a koji obuhvaćaju postupke za oporavak sustava i uspostavu sigurnosnih uvjeta za pružanje usluga izdavanja certifikata.

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.

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.

5.7.3. Postupci u slučaju kompromitiranja privatnog ključa

U slučaju kompromitiranja ili sumnje u kompromitiranost privatnog ključa Fina CA Fina će odmah prekinuti s uporabom tog kompromitiranog privatnog ključa.

Nakon potvrde kompromitiranosti privatnog ključa Fina donosi odluku o opozivu te će pripadajući Fina CA certifikat biti će opozvan od strane Fina Root CA.

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. Fina CA čiji je certifikat opozvan generirati će novi par CA ključeva. 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. ovih Općih pravila.

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.

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 izdavanja kvalificiranih certifikata nastaviti na svojem primarnom produkcijskom sustav certificiranja ili će pružanje usluge nastaviti na svojem sekundarni sustavu certificiranja iz točke 5.1.1. ovih Općih pravila do oporavka svojeg primarnog produkcijskog sustava.

5.8. Prestanak rada CA ili RA

U slučaju prestanka rada vanjskog ugovorenog RA njegove poslove može preuzeti Fina RA mreža. Detaljnije odredbe vezane uz prekid rada vanjskog ugovorenog RA određuju se ugovorom.

O planiranom prestanku pružanja usluga izdavanja kvalificiranih certifikata 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 izdavanja kvalificiranih certifikata;
- 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;
- opozvati sve izdane kvalificirane certifikate i uništiti privatne ključeve Korisnika u slučajevima kad Fina čuva i upravlja Korisničkim ključevima,
- 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. ovih Opći pravila 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.

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 [18].

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.

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 HRN ETSI EN 319 411-1 i sa zahtjevima CA/Browser Forum BRG [27].

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. ovih Općih pravila.

FINA CA nalazi se tijekom i nakon ceremonije generiranja parova ključeva u Fina PKI štićenom prostoru iz točke 5.1.1. ovih Općih pravila, 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 ocjenitelj.

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

Fina posjeduje izvješće Kvalificiranog ocjenitelja 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. ovih Općih pravila. Parove ključeva generiraju Službenici za registraciju u svojim LRA uredima, a mogu ih generirati i Službenici za registraciju u Središnjem RA Fine.

6.1.1.3. Generiranje para korisničkih ključeva u QSCD uređaju

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

- *Osobni EU kvalificirani certifikat za e-potpis (QCP-n-qscd)*;
- *Poslovni EU kvalificirani certifikat za e-potpis (QCP-n-qscd)*;
- *EU kvalificirani certifikat za e-pečat (QCP-l-qscd)*;

Na QSCD uređajima generiraju se parovi ključeva za sljedeći tipove kvalificiranih certifikata koje izdaje Fina RDC-TDU 2015 CA:

- *TDU EU kvalificirani certifikat za e-potpis (QCP-n-qscd)*;
- *TDU EU kvalificirani certifikat za e-pečat (QCP-l-qscd)*.

QSCD uređaj na kojem se generiraju ključevi zadovoljava zahtjeve iz točke 6.2.1. ovih Općih pravila.

Za provođenje generiranja Korisničkog para ključeva za kvalificirane certifikate koji se izdaju na QSCD uređajima ovlašteni su pripadajući Potpisnici, 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.

Postupkom generiranja para ključeva u QSCD uređaju upravlja Fina.

Postupkom generiranja para ključeva može upravljati i vanjski ugovoreni pružatelj usluga povjerenja koji ujedno obavlja usluge registracije za Finu.

Upravljanje postupkom generiranje ključeva uključuje i provjeru provodi li se generiranje para ključeva u QSCD uređaju.

6.1.1.4. Generiranje para korisničkih ključeva u sigurnom kriptografskom uređaju

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

- *Osobni EU kvalificirani certifikat za e-potpis (QCP-n)*;
- *Poslovni EU kvalificirani certifikat za e-potpis (QCP-n)*.

Na sigurnim kriptografskim uređajima generiraju se parovi ključeva za tip certifikata *TDU EU kvalificirani certifikat za e-potpis (QCP-n)* koje izdaje Fina RDC-TDU 2015 CA.

Sigurni kriptografski uređaj na kojem se generiraju ključevi zadovoljava zahtjeve iz točke 6.2.1. ovih Općih pravila.

Za provođenje generiranja Korisničkog para ključeva za kvalificirane certifikate koji se izdaju na sigurnim kriptografskim uređajima ovlašteni su pripadajući Potpisnici, odnosno Ovlašteni predstavnici, te Službenici za registraciju u Fina LRA i službenici u Središnjeg RA Fine. Ove ovlaštene osobe generiranje Korisničkog para ključeva provode na svojim lokacijama.

Postupkom generiranja para ključeva u sigurnom kriptografskom uređaju upravlja Fina.

Postupkom generiranja para ključeva može upravljati i vanjski ugovoreni pružatelj usluga povjerenja koji ujedno obavlja usluge registracije za Finu.

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

6.1.1.5. Generiranje para korisničkih ključeva za kvalificirane soft certifikate

Parovi ključeva za sljedeće tipove kvalificiranih certifikata generiraju se softverskim modulima:

- *EU kvalificirani soft certifikat za e-pečat (QCP-l)*, kojeg izdaje Fina RDC 2015*;*
- *TDU EU kvalificirani soft certifikat za e-pečat (QCP-l)*, kojeg izdaje Fina RDC-TDU 2015.

Generiranje para Korisničkih ključeva za ove certifikate provodi Fina u svojem PKI štićenom prostoru iz točke 5.1.1. ovih Općih pravila. Također, za generiranje para Korisničkih ključeva ovlašten je i Ovlašteni predstavnik. U slučaju da generiranje para ključeva provodi Ovlašteni predstavnik, generiranje se provodi na lokaciji Autora pečata. Privatni ključevi štite su u softverskom zaštićenom tokenu.

6.1.1.6. Generiranje para korisničkih ključeva koji se koriste u servisu udaljenog elektroničkog potpisivanja i pečatiranja

U servisu udaljenog elektroničkog potpisivanja i pečatiranja koriste se sljedeći tipovi kvalificiranih certifikata koje izdaje Fina RDC 2015 CA:

- *Osobni EU kvalificirani certifikat za udaljeni e-potpis (QCP-n)*;
- *Poslovni EU kvalificirani certifikat za udaljeni e-potpis (QCP-n)*;
- *EU kvalificirani certifikat za udaljeni e-pečat (QCP-l)*.

te sljedeći tipovi kvalificiranih certifikata koje izdaje Fina RDC-TDU 2015 CA:

- *TDU EU kvalificirani certifikat za udaljeni e-potpis (QCP-n)*;
- *TDU EU kvalificirani certifikat za udaljeni e-pečat (QCP-l)*.

Generiranje para Korisničkih ključeva za ove certifikate provodi Fina u svojem PKI štićenom prostoru iz točke 5.1.1. na sigurnom HSM modulu koji zadovoljava zahtjeve iz točke 6.2.1. ovih Općih pravila.

6.1.2. Dostava privatnog ključa korisniku

Ako Službenik za registraciju generira svoj par ključeva smatra se da već posjeduje privatni ključ.

Ako Potpisnik ili Ovlašteni predstavnik na svojoj lokaciji generira privatni ključ na QSCD uređaju, sigurnom kriptografskom uređaju ili softverskom modulu, smatra se da Potpisnik, 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 ili Autora pečata na sigurnom kriptografskom, odnosno QSCD uređaju, tada Fina osigurava sigurnu dostavu privatnog ključa u sigurnom kriptografskom, odnosno QSCD uređaju Potpisniku odnosno Ovlaštenom predstavniku.

Ako Fina generira privatni ključ u softverskom modulu, tada Fina osigurava sigurnu *online* dostavu privatnog ključa i pripadajućeg certifikata u softverskom zaštićenom tokenu Ovlaštenom predstavniku.

Korisničkim privatnim ključem, koji generira Fina, a koji se koristi u sklopu servisa udaljenog elektroničkog potpisivanja i pečatiranja, u ime Potpisnika, odnosno Autora pečata upravlja Fina kao kvalificirani pružatelj usluga povjerenja. Ovaj privatni ključ Fina čuva na siguran način, zaštićeno od otkrivanja, kopiranja, izmjene, oštećivanja i uporabe od neautoriziranih osoba. Fina u sklopu servisa udaljenog elektroničkog potpisivanja i pečatiranja osigurava da Potpisnik svoj pripadajući privatni ključ ima pod svojom isključivom kontrolom, odnosno da Autor pečata ima pripadajući privatni ključ pod svojom kontrolom.

6.1.3. Dostava javnog ključa CA-u

Korisnički javni ključ dostavlja se na certificiranje u Fina CA na način koji osigurava provjeru cjelovitosti i izvornosti javnog ključa te na način koji sigurno povezuje potvrđeni identitet Subjekta i pripadajući javni ključ koji se dostavlja.

Dostava javnog ključa obavlja se sigurnim elektroničkim komunikacijskim kanalom nakon uspješno provedene autentikacije osobe ovlaštene za provedbu generiranja Korisničkog para ključeva. Osobe ovlaštene za generiranje Korisničkog para ključeva za pojedine tipove Korisničkih certifikata navedene su u točki 6.1.1. ovih Općih pravila.

Ako par Korisničkih ključeva ne generira Fina proces zahtijevanja certifikata obuhvaća provjeru posjeduje li ili kontrolira li Potpisnik, odnosno Autor pečata privatni ključ koji je povezan s javnim ključem koji se dostavlja za izradu certifikata.

Za kvalificirane certifikate navedene u točki 6.1.1.3. ovih Općih pravila za proces zahtijevanja certifikata osigurava se da je javni ključ koji se dostavlja na certificiranje iz para ključeva generiranog u QSCD uređaju.

Za kvalificirane certifikate navedene u točki 6.1.1.4. ovih Općih pravila za proces zahtijevanja certifikata osigurava se da je javni ključ koji se dostavlja na certificiranje iz para ključeva generiranog u 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. Vrijednost sažetka Fina Root CA certifikata se na zahtjev dostavlja pouzdanim kanalom.

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 [18].

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. ovih Općih pravila te strogim pridržavanjem zahtjeva navedenih u certifikacijskoj dokumentaciji tih uređaja.

Ako Ovlašteni predstavnik generira par ključeva sukladno točki 6.1.1.5. ovih Općih pravila, generiranje ključeva se provodi korištenjem parametara za generiranje koji su sukladni s normizacijskim dokumentom ETSI TS 119 312 [18].

6.1.7. Namjene ključeva

U nastavku su opisane namjene ključeva certifikata iz opsega ovih Općih pravila.

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 certifikata za servis izdavanja kvalificiranih vremenskih žigova;
- potpisivanje pripadajuće CRL.

Certifikat za kvalificirani vremenski žig u ekstenziji *Key Usage* ima postavljene vrijednosti *digitalSignature* i *nonRepudiation*. Servis vremenskog žiga pripadajući privatni ključ upotrebljava samo za potpis kvalificiranog vremenskog žiga.

Kvalificirani certifikat namijenjen za službenika u Fina RA mreži u ekstenziji *Key Usage* ima postavljenu vrijednosti *nonRepudiation*. Službenik u FINA RA mreži pripadajući privatni ključ upotrebljava samo za izradu elektroničkih potpisa.

Kvalificirani certifikat za elektroničke potpise u ekstenziji *Key Usage* ima postavljenu vrijednost *nonRepudiation*. Potpisnik pripadajući privatni ključ upotrebljava samo za izradu elektroničkih potpisa.

Kvalificirani certifikat za elektroničke pečate u ekstenziji *Key Usage* ima postavljenu vrijednost *digitalSignature*. Autor pečata pripadajući privatni ključ upotrebljava samo za izradu elektroničkih pečata.

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 [22] razina 3.

Za tipove kvalificiranih certifikata navedene u točki 6.1.1.3. ovih Općih pravila zaštita privatnih ključeva provodi se QSCD uređajima koji zadovoljavaju zahtjeve norme HR EN 419 211 [18] - [21].

Za tipove kvalificiranih certifikata navedene u točki 6.1.1.4. ovih Općih pravila zaštita privatnih ključeva provodi se sigurnim kriptografskim uređajima koji zadovoljava zahtjeve norme FIPS 140-2 [22] razina 2 ili 3.

Za tipove kvalificiranih soft certifikata za e-pečate navedene u točki 6.1.1.5. ovih Općih pravila zaštita privatnih ključeva provodi se u softverskom zaštićenom tokenu. Za način zaštite ovih privatnih ključeva na lokaciji Autora pečata zadužen je Autor pečata.

Zaštita privatnih ključeva za kvalificirane certifikate navedene u točki 6.1.1.6. koji se koriste u sklopu servisa udaljenog elektroničkog potpisivanja i pečatiranja provodi se HSM modulom koji zadovoljava zahtjeve norme FIPS 140-2 [22] razina 3.

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

Upravljanje privatnim ključem od strane više osoba je sigurnosna mjera koja za upravljanje privatnim ključem zahtijeva autorizaciju više osoba.

HSM moduli kojima se štite privatni ključevi Fina CA-ova i HSM moduli kojima se štite Korisnički privatni ključevi servisa udaljenog elektroničkog potpisivanja i pečatiranja 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 privatnim ključevima Fina CA-ova i Korisničkim privatnim ključevima servisa udaljenog elektroničkog potpisivanja i pečatiranja provodi se fizičkim pristupom HSM modulu, uz autorizaciju dvije ovlaštene osobe s povjerljivim ulogama u Fina PKI.

6.2.3. Sigurno skladištenje privatnog ključa

Sigurno skladištenje privatnih ključeva Fina CA-ova se ne primjenjuje.

Sigurno skladištenje privatnih Korisničkih ključeva povezanih s kvalificiranim certifikatima se ne primjenjuje.

Fina CA-ovi uništavaju sve kopije korisničkih privatnih ključeva nakon dostave privatnog ključa korisniku.

6.2.4. Sigurnosno kopiranje privatnog ključa

Sigurnosno kopiranje privatnih ključeva Fina CA-ova provodi se u prostoru najviše razine sigurnosti unutar Fina PKI štićenog prostora uz dualnu kontrolu ovlaštenih osoba s povjerljivim ulogama u Fina PKI. 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 generiranih na QSCD uređajima, sigurnim kriptografskim uređajima ili softverskim modulima povezanih s kvalificiranim certifikatima.

Autor pečata odgovoran je za zaštitu kopija privatnih ključeva za tipove certifikata iz točke 6.1.1.5. ovih Općih pravila te je odgovoran u slučaju njihovog neovlaštenog, a sukladno točki 9.6.3. ovih Općih pravila.

Korisnički privatni ključevi povezani s kvalificiranim certifikatima koji se koriste u sklopu servisa udaljenog elektroničkog potpisivanja i pečatiranja dohvaćaju se iz HSM modula isključivo u enkriptiranom obliku te se pohranjuju u Fina PKI štićenom prostoru. Izrada sigurnosne kopije ovih enkriptiranih ključeva provodi se u štićenom Fina PKI prostoru, a pokreće je ovlaštena osoba, uz dualnu kontrolu. Sigurnosne kopije ovih privatnih ključeva u enkriptiranom obliku čuvaju u Fina PKI štićenom prostoru na odvojenim lokacijama. Broj sigurnosnih kopija privatnih ključeva kvalificiranih certifikata ne prelazi broj neophodan za osiguravanje kontinuiteta usluge.

6.2.5. Arhiviranje privatnog ključa

Fina ne arhivira privatne ključeve Fina PKI i ne arhivira privatna ključeve Korisnika.

6.2.6. Prijenos privatnog ključa

Za vrijeme dok je izvan HSM modula privatni ključ je zaštićen enkriptiranjem na način koji osigurava jednaku razinu sigurnosti kao i kad se ključ nalazi u HSM modulu. Prijenos privatnog ključa iz HSM modula autoriziraju ovlaštene osobe s povjerljivim ulogama u Fina PKI, uz dualnu kontrolu unutar PKI štićenog prostora iz točke 5.1.1. ovih Općih pravila.

Kad se Korisnički privatni ključ kvalificiranog certifikata koji se koriste u sklopu servisa udaljenog elektroničkog potpisivanja i pečatiranja prenosi iz ili u HSM modul, za vrijeme dok je izvan HSM modula privatni ključ je zaštićen enkriptiranjem na način koji osigurava jednaku razinu sigurnosti kao i kad se ključ nalazi u HSM modulu.

Kod prijenosa privatnih ključeva iz jednog HSM modula u drugi HSM privatni ključ se prenosi 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 6.1.1.5. ovih Općih pravila u drugi spremnik privatnog ključa provodi Autor pečata na način da se privatni ključ prenosi 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 povezani s kvalificiranim certifikatima navedenim u točki 6.1.1.6. koji se koriste u sklopu servisa udaljenog elektroničkog potpisivanja i pečatiranja 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

Aktivacija privatnih ključeva Fina CA-ova provodi se prema postupcima i uz zadovoljenje zahtjeva određenih u certifikacijskom dokumentu upotrijebljenog HSM modula kojim je Fina CA ključ zaštićen, uz dualnu kontrolu ovlaštenih osoba s povjerljivim ulogama u Fina PKI.

Aktivaciju privatnog ključa kvalificiranog certifikata za elektroničke potpise, odnosno elektroničke pečate provodi samo pripadajući Potpisnik ili Autor pečata korištenjem odgovarajućih aktivacijskih podataka. Aktivacija privatnog ključa obavlja se na siguran način.

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.

Aktivirani Korisnički sigurni kriptografski i QSCD uređaji te softverski moduli ne smiju biti ostavljeni bez nadzora.

Privatni ključevi Potpisnika odnosno Autora pečata pohranjeni u sigurnim kriptografskim odnosno QSCD uređajima deaktiviraju se prestankom napajanja uređaja, zaustavljanjem Korisničke aplikacije za potpisivanje ili pečatiranje te naredbom iz Korisničke aplikacije za deaktivaciju uređaja.

Privatni ključevi kvalificiranih certifikata koji se koriste u sklopu servisa udaljenog elektroničkog potpisivanja i pečatiranja deaktiviraju se završetkom postupka potpisivanja ili pečatiranja, ili zaustavljanjem aplikacije za potpisivanje ili pečatiranje od strane Potpisnika ili Autora pečata.

Privatni ključevi zaštićeni softverskim tokenom deaktiviraju se zaustavljanjem Korisničke aplikacije za potpisivanje ili pečatiranje te naredbom iz Korisničke aplikacije za deaktivaciju softverskim tokenom.

Deaktivirani privatni ključevi kvalificiranih certifikata mogu se ponovno koristiti za izradu elektroničkog potpisa, odnosno pečata 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 izvodi se od strane ovlaštenih osoba s povjerljivim ulogama u Fina PKI uz minimalno dualnu kontrolu. Postupak uništavanja privatnog Fina CA ključa uključuje i uništavanje svih sigurnosnih kopija tog privatnog ključa.

Uništavanje privatnog Fina CA ključa provodi se na način određen internim Fininim dokumentima, a koji osigurava da se nakon uništenja privatni ključ ni na koji način ne može oporaviti ili ponovno koristiti.

O uništenju privatnog Fina CA ključa vodi se zapisnik.

Uništenje privatnih ključeva Potpisnika odnosno Autora pečata pohranjenih u oblaku provodi se sigurnom metodom uništenja ključeva kojom se osigurava da se nakon uništenja privatni ključ ni na koji način ne može oporaviti ili ponovno koristiti.

Uništenje privatnih ključeva Potpisnika odnosno Autora pečata pohranjenih u sigurnim kriptografskim odnosno QSCD uređajima moguće je fizičkim uništenjem kriptografskih odnosno QSCD uređaja.

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

Uništenje privatnih ključeva Potpisnika i Autora pečata odgovornost je Potpisnika 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. ovih Općih pravila.

6.3. Ostali vidovi upravljanja parom ključeva

6.3.1. Arhiviranje javnog ključa

Javni ključevi Fina CA-ova sastavni su dio pripadajućih CA certifikata koji se arhiviraju sukladno točkama 5.5.3. i 5.5.4. ovih Općih pravila, a u arhivi se čuvaju na rok iz točke 5.5.2. ovih Općih pravila.

Javni ključevi Potpisnika odnosno Autora pečata sastavni su dio pripadajućih kvalificiranih certifikata te se arhiviraju sukladno točkama 5.5.3. i 5.5.4. ovih Općih pravila, a u arhivi se čuvaju na rok iz točke 5.5.2. ovih Općih pravila.

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
Kvalificirani certifikati za elektroničke potpise srednje razine sigurnosti	2 godine
Kvalificirani certifikati za elektroničke pečate srednje razine sigurnosti	2 godine
Kvalificirani certifikati za elektroničke pečate standardne razine sigurnosti	5 godina

Tablica 6.1. Periodi važenja certifikata

Period važenja Fina CA certifikata ne smije biti izvan perioda važenja Fina Root CA certifikata.

Vremenski period važenja privatnog ključa jednak je vremenskom periodu važenja pripadajućeg certifikata. Privatni ključevi ne smiju se upotrebljavati 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.

Aktivacijske podatke za Fina RA mrežu generiraju Službenici za registraciju uporabom prikladnog generatora slučajnih brojeva. Inicijalne aktivacijske podatke za sigurne kriptografske, odnosno QSCD uređaje generira Središnji RA, odnosno vanjski ugovoreni RA te se aktivacijski podaci čuvaju na siguran način do njihove isporuke Potpisnicima, odnosno Ovlaštenim predstavnicima.

Za privatne ključeve povezane s certifikatima iz točke 6.1.1.5. ovih Općih pravila aktivacijske podatke generira Ovlašteni predstavnik.

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

Aktivacijske podatke za privatne ključeve koji se koriste u sklopu servisa udaljenog elektroničkog potpisivanja i pečatiranja generira Potpisnik odnosno Autor. U postupku aktiviranja privatnih ključeva Potpisnika odnosno Autora pečata koji su registrirani u vanjskom ugovorenom RA može sudjelovati sustav vanjskog ugovorenog RA s kojim je povezan pametni telefon Potpisnika odnosno Autora pečata. Samo su Potpisniku odnosno Autoru pečata poznati aktivacijski podaci kojima mogu aktivirati pripadajući privatni ključ u servisu udaljenog elektroničkog potpisivanja i pečatiranja.

6.4.2. Zaštita aktivacijskih podataka

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

Aktivacijski podaci sigurnih kriptografskih, odnosno QSCD uređaja distribuiraju se Potpisnicima, odnosno Ovlaštenim predstavnicima odvojenim kanalom u odnosu na uručivanje kriptografskih, odnosno QSCD uređaja.

Ako aktivacijske podatke za certifikate iz točke 6.1.1.5. ovih Općih pravila generira Fina tada ih Fina Ovlaštenom predstavniku dostavlja na siguran način.

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

Ako sustav vanjskog ugovorenog RA sudjeluje u postupku aktiviranja privatnih ključeva Potpisnika odnosno Autora pečata koji se koriste u sklopu servisa udaljenog elektroničkog potpisivanja i pečatiranja tada vanjski ugovoreni RA osigurava zaštitu podataka koji sudjeluju u postupku aktivacije privatnih ključeva.

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

6.4.3. Ostale odredbe o aktivacijskim podacima

Aktivacijski podaci za privatne ključeve kvalificiranih certifikata se mogu mijenjati periodički kako bi se smanjila mogućnost njihova otkrivanja.

Ova Opća pravila ne postavljaju dodatne zahtjeve na životni ciklus aktivacijskih podataka kvalificiranih 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.

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.

6.5.2. Ocjena računalne sigurnosti

U cilju sigurnosti i kvalitete pružanja kvalificiranih usluga povjerenja Fina ima uspostavljen sustav upravljanja informacijskom sigurnošću sukladan normi ISO/IEC 27001 [6].

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 kvalificiranih 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.

6.6.2. Kontrole upravljanja sigurnošću

Fina provodi provjeru svih dijelova 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. ovih Općih pravila.

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 kvalificiranih 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.

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 sustavi kritični za pružanje usluga povjerenja smješteni su u Fina PKI štićenom prostoru.

CA sustavi posebno su sigurnosno podešeni i očvršćeni.

Mrežna 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 ovih Općih pravila.

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

Profili certifikata iz opsega ovih Općih pravila koje izdaju subordinirani Fina CA-ovi usklađeni su s normama HRN EN 319 411-2 [10] i HRN EN 319 412 [11] - [14].

Subordinirani Fina CA-ovi izdaju certifikate prema profilima koji su određeni ovim Općim pravilima. Ovisno o namjeni certifikata, pravilima prema kojima je certifikat izdan, razini sigurnosti i načinu čuvanja pripadajućih privatnih ključeva, svaki tip certifikata ima definiran jedinstveni OID općih pravila certificiranja (CP OID).

U tablicama 1.1. i 1.2. točke 1.1.2. ovih Općih pravila naveden je popis tipova kvalificiranih certifikata s pripadajućim CP OID-ova certifikata koje izdaju subordinirani Fina CA-ovi.

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 repozitorija iz točke 2.2. ovih Općih pravila.

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 Fina Root CA i njemu subordinirane Fina CA-ove opisani su u točki 1.3.2. ovih Općih pravila.

Oblici naziva za certifikate koje izdaju subordinirani Fina CA-ovi opisani su u točkama 3.1.1. i 3.1.4. ovih Općih pravila.

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 CP OID-ove općih pravila certificiranja naveden u tablicama 1.1. i 1.2 u točki 1.1.2. ovih Općih pravila.

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 Pravilnika o postupcima certificiranja za kvalificirane certifikate [29] 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 [24].

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 [25].

7.3.1. Broj(evi) verzije

Profil odgovora Fina OCSP servisa sukladan je verziji 1 prema IETF RFC 6960 [25].

7.3.2. OCSP ekstenzije

U odgovor Fina OCSP servisa uključene su slijedeće ekstenzije:

1. *Nonce*
2. *Extended Revoked Definition*

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 kvalificiranog 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 kvalificirani pružatelj usluga povjerenja i usluge izdavanja kvalificiranih certifikata koje Fina pruža ispunjavaju zahtjeve utvrđene Uredbom (EU) br. 910/2014 [1], Zakonom o provedbi Uredbe (EU) br. 910/2014 [2] te normom HRN ETSI/EN 319 411-2 [10].

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 svaka 24 mjeseca, sukladno zahtjevima Uredbe (EU) br. 910/2014 [1] i norme ETSI EN 319 403 [15].

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.

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 [15].

Internu provjeru sukladnosti provode interni ocjenitelji sukladnosti koji zajedno raspolažu znanjima i razumijevanjem:

- odredbi norme HRN ETSI/EN 319 411-2 [10];
- PKI područja te područja informacijske sigurnosti;
- zakonske regulative iz područja pružanja usluga povjerenja.

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 kvalificiranih usluga povjerenja:

- cjelovitost i točnost dokumentacije;
- implementiranost zahtjeva za kvalificirane 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.

8.5. Mjere u slučaju nesukladnosti

Ako je u pružanju kvalificirane usluge povjerenja utvrđena nesukladnost Fina će poduzeti potrebne korake kako bi otklonila nesukladnost, i ako je primjenjivo u roku koji je odredilo nadzorno tijelo.

Za vrijeme prekida izdavanja kvalificiranih 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.

U slučaju vanjske provjere sukladnosti Fina će dostaviti izvještaj vanjskog ocjenitelja o provjeri sukladnosti nadzornom tijelu unutar tri radna dana od primitka.

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. ovih Općih pravila.

Fina zadržava pravo izmjene cjenika. Izmjene cjenika objavljuju se na internetskim stranicama repozitorija iz točke 2.2. ovih Općih pravila.

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 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 ovim Općim pravilima i $CPS_{QC\text{-}eIDAS}$ dokumentu 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 Općim pravilima.

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. ovih Općih pravila, 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 zaštiti osobnih 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. ovih Općih pravila 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 dokument Općih pravila kao i druga Finina dokumentacija objavljena na internetskim stranicama repozitorija iz točke 2.2. 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 Autor pečata, bez obzira generira li par ključeva Potpisnik, odnosno Autor pečata, ili ga generira Fina kao kvalificirani 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 ovih Općih pravila sa zakonskom regulativom te za provođenje odredbi propisanih ovim Općim pravilima, $CPS_{QC\text{-}eIDAS}$ 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. ovih Općih pravila objavljuje uvjete pružanja usluga certificiranja, ova Opća pravila, $CPS_{QC\text{-}eIDAS}$ dokument te sve obavijesti i informacije o promjenama u radu koje na bilo koji način mogu utjecati na sudionike Fina PKI.

Fina je kao kvalificirani 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. ovih Općih pravila;
- 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. ovih Općih pravila, 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 ovim Općim pravilima;
- za parove Korisničkih ključeva koje na sigurnom kriptografskom, odnosno QSCD uređaju generira Potpisnik, odnosno 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 ovim Općim pravilima;
- osigurava provjeru da Potpisnik, odnosno Autor pečata 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, odnosno Ovlaštenom predstavniku u slučajevima kada se par ključeva generira na lokaciji Fine;
- privatnim Korisničkim ključevima koji se koriste u servisu udaljenog elektroničkog potpisivanja i pečatiranja, upravlja u ime Potpisnika, odnosno Autora pečata na način da Potpisnik svoj pripadajući privatni ključ ima pod svojom isključivom kontrolom, odnosno da Autor pečata ima pripadajući privatni ključ pod svojom kontrolom;
- osigurava odgovarajući sigurni kriptografski, odnosno QSCD uređaj i njegovu zaštićenu dostavu Potpisniku, odnosno Ovlaštenom predstavniku;
- izdani certifikat čini dostupnim sukladno točki 4.4.2. ovih Općih pravila;
- 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 ovim Općim pravilima;
- sukladno Planu kontinuiteta poslovanja Fina PKI 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. ovih Općih pravila smatraju povjerljivima štiti i te podatke koristiti isključivo za potrebe usluga certificiranja iz opsega ovih Općih pravila;
- osigurava da se interne i vanjske provjere sukladnosti Fine kao kvalificiranog pružatelja usluga povjerenja provode sukladno točki 8.1. ovih Općih pravila.

Obveze Fine u slučajevima kada Korisničkim parom ključeva u ime Potpisnika, odnosno Autora pečata upravlja Fina, opisane su u točki 4.5.1. ovih Općih pravila.

U slučaju prekida poslovanja Fina će postupiti sukladno točki 5.8. ovih Općih pravila.

Ograničenja odgovornosti Fine kao davatelja usluga certificiranja opisana su u točki 9.8. ovih Općih pravila.

9.6.2. Obveze i odgovornosti RA

Obveze i odgovornosti Fina RA mreže i vanjskih ugovorenih RA su:

- provođenje postupka registracije i identifikacije fizičkih osoba i Poslovnih subjekata na način propisan ovim Općim pravilima;
- prosljeđivanje cjelovitih, točnih i provjerenih podataka o Subjektima na daljnju obradu 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 Korisnika, na način propisan ovim Općim pravilima;
- obavještavanje podnositelja zahtjeva za izdavanje certifikata o javno objavljenim i dostupnim uvjetima pružanja usluga certificiranja i ovim Općim pravilima.

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. ovih Općih pravila;
- pažljivo koristiti i čuvati sredstvo za izradu elektroničkog potpisa, odnosno elektroničkog pečata, privatne ključeve i aktivacijske podatke sukladno ovim Općim pravilima;
- 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. ovih Općih pravila;
- 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. ovih Općih pravila;
- 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. ovih Općih pravila;
- 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. ovih Općih pravila;
- u slučajevima kad je Korisnik u posjedu para ključeva i njima upravlja, koristiti certifikat i pripadajući privatni ključ u skladu s odredbama iz točke 4.5.1. ovih Općih pravila;
- djelovati u skladu sa svim ostalim odredbama iz ovih Općih pravila koje se odnose na obveze Korisnika.

Obveze i odgovornosti Korisnika vezane uz korištenje privatnog ključa i certifikata u slučajevima kad je Korisnik u posjedu para ključeva i njima upravlja opisane su u točki 4.5.1. ovih Općih pravila.

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. ovih Općih pravila.

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 Općim pravilima, 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 u ovim Općim pravilima;
- provjerila da je elektronički potpis, odnosno elektronički pečat izrađen privatnim ključem koji 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. ovih Općih pravila.

Pouzdajuća strana koja nije poštovala propise i ova Opća pravila 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 Općim pravilima;
- 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 ovih Općih pravila.

9.8. Ograničenja odgovornosti

Finina ukupna financijska odgovornost za certifikate izdane prema ovim Općim pravilima i za transakcije obavljene na temelju pouzdavanja u tako izdane certifikate iznosi najviše 2.000.000,00 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 1.5. Finina maksimalna financijska odgovornost za kvalificirane certifikate prikazana je Tablici 9.1.

Kategorija certifikata	Maksimalna Finina financijska odgovornost	
	Po transakciji	Ukupno
Kvalificirani certifikati za elektronički potpis i pečat srednje razine sigurnosti	do 80.000 kn	2.000.000 kn

Tablica 9.1. Maksimalna Finina financijska odgovornost

9.9. Naknada štete

Svaki sudionik odgovara oštećenom za štetu koju je počinio zbog nepoštivanja odredbi ovih Općih pravila 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 odgovara oštećenom, odnosno svakom drugom sudioniku ako se pouzda u izdani certifikat bez provjere njegove valjanosti opisane u točki 9.6.4. Općih pravila ili ga koristi protivno svrhama određenim ovim Općim pravilima.

9.10. Trajanje i prestanak važenja

9.10.1. Trajanje

Ovaj dokument Općih pravila važi do stupanja na snagu novog dokumenta Općih pravila ili do objave prestanka njegovog važenja. Nova verzija dokumenta ili objava prestanka važenja biti će objavljena na internetskim stranicama repozitorija iz točke 2.2. ovih Općih pravila s naznačenim danom stupanja na snagu. Novom 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 dokumenta Općih pravila za sve certifikate izdane prema ovom dokumentu ostaju važiti one odredbe iz ovog dokumenta koje se ne mogu smisleno zamijeniti odredbama nove verzije dokumenta Općih pravila.

Prestanak važenja ovog dokumenta Općih pravila nije vezan i ne utječe na važenje certifikata izdanih primjenom ovog dokumenta.

Fina može za pojedine odredbe važećeg dokumenta Općih pravila izraditi izmjene i dopune kao što je to navedeno u točki 9.12. ovih Općih pravila.

9.10.3. Posljedice prestanka važenja i nastavak djelovanja

Stupanjem na snagu nove verzije dokumenta Općih pravila na sve se certifikate izdane od tog dana primjenjuju odredbe iz tog dokumenta.

Certifikati izdani primjenom prethodnih Općih pravila važe do njihova isteka pri čemu se mogu obnoviti primjenom Općih pravila iz novog 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

Ova Opća pravila revidiraju 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. ovih Općih pravila poslati dopis s prijedlogom za ispravke pogrešaka, prijedlog nadopuna ili izmjenu ovog 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.

9.12.2. Mehanizmi obavještavanja i vremenski periodi

Sve izmjene i dopune dokumenta Općih pravila objavljuju se u elektroničkom obliku na internetskim stranicama repozitorija iz točke 2.2. ovih Općih pravila.

Nove verzije Općih pravila s izmijenjenim OID-om dokumenta Općih pravila objavljuju se u elektroničkom obliku na internetskim stranicama repozitorija iz točke 2.2. ovih Općih pravila.

Datum stupanja na snagu izmjena i dopuna ili novoobjavljenog dokumenta Općih pravila naznačen je 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 dokumentu Općih pravila koje mogu utjecati na sudionike zahtijevaju i izmjenu OID-a dokumenta Općih pravila. Novi OID za novu verziju 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 Općim pravilima, 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 da postoji odstupanje sadržaja usluge u odnosu na objavljene uvjete pružanja usluga. Fina će povodom prigovora odgovoriti podnositelju prigovora. Prigovor se upućuje pisano u papirnatom ili elektroničkom obliku na adrese navedene u točki 9.11. ovih Općih pravila.

9.14. Važeći propisi

Kvalificirane usluge povjerenja iz opsega ovih Općih pravila Fina pruža sukladno odredbama Uredbe (EU) br. 910/2014 [1], provedbenih akata donesenih temeljem Uredbe (EU) br. 910/2014 [1], Zakona o provedbi Uredbe (EU) br. 910/2014 [2] te normizacijskih dokumenata ETSI EN 319 401 [8], ETSI EN 319 411-1 [9] i ETSI EN 319 411-2 [10].

9.15. Usklađenost s primjenjivim propisima

Ova Opća pravila i pružanje usluga certificiranja koje su obuhvaćene ovim Općim pravilima usklađeni su s propisima iz točke 9.14. ovih Općih pravila.

Svi sudionici suglasni su s primjenom hrvatskog prava u tumačenju primijenjenih odredbi.

9.16. Razne odredbe

Fina javno objavljuje ova Opća pravila, $CPS_{QC\text{-}eIDAS}$ dokument 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, odnosno Autora pečata o eventualnim izmjenama uvjeta o pružanju usluga certificiranja.