FINA

OPĆA PRAVILA DAVANJA USLUGA CERTIFICIRANJA

Verzija 5.1

Datum objave: 26.08.2016.

Datum stupanja na snagu: 5.09.2016.

OID Dokumenta: 1.3.124.1104.5.0.0.1.5.1

Informacije o dokumentu

Ime dokumenta:	Fina – Opća pravila davanja usluga certificiranja
OID dokumenta:	1.3.124.1104.5.0.0.1.5.1
Tip dokumenta:	Opća pravila davanja usluga certificiranja (*Certificate Policy*, CP)
Oznaka distribucije	Javno
Vlasnik dokumenta	Financijska agencija, Fina
Kontakt	pma@fina.hr

Povijest izmjena

Verzija	Datum	Razlog izmjene
3.0	15.07.2002.	
3.1	15.09.2002.	Redefiniranje tipova certifikata
3.2	31.03.2003.	Usklađivanje pojmova
3.3	30.06.2008.	Ispravak uočenih grešaka u tekstu
4.0	31.10.2013.	Usklađivanje s pravilnicima [5] i [6], Popisom normizacijskih dokumenata [7] te s preporukom IETF RFC 3647 [22], izmjene profila certifikata i dodavanje Poslovnog soft certifikata (LCP).
4.1	1.10.2015.	Ugradnja Izmjena i dopuna Općih pravila br. 1/4.0 i br. 2/4.0, usklađivanje s poslovnim procesima Fine i ispravak uočenih grešaka u tekstu.
5.0	7.12.2015.	Prijelaz na novu, dvorazinsku arhitekturu produkcijskih CA-ova, prijelaz na SHA-256 kriptografski algoritam i veće duljine ključeva.
5.1	24.08.2016.	Usklađivanje s poslovnim procesima Fina PKI i ispravljanje tipografskih grešaka

SADRŽAJ

AUTORSKA PRAVA

REFERENTNE DOKUMENTIRANE INFORMACIJE

Temeljni zakon

[1] Zakon o elektroničkom potpisu (NN 10/2002)

[2] Zakon o izmjenama i dopunama Zakona o elektroničkom potpisu (NN 80/2008)

[3] Zakon o izmjeni Zakona o elektroničkom potpisu (NN 30/2014)

Podzakonski akti

[4] Pravilnik o evidenciji davatelja usluga certificiranja u Republici Hrvatskoj (NN 107/2010)

[5] Pravilnik o izradi elektroničkog potpisa, uporabi sredstava za izradu elektroničkog potpisa, općim i posebnim uvjetima poslovanja za davatelje usluga izdavanja vremenskog žiga i certifikata (NN 107/2010)

[6] Pravilnik o izmjenama i dopunama Pravilnika o izradi elektroničkog potpisa, uporabi sredstava za izradu elektroničkog potpisa, općim i posebnim uvjetima poslovanja za davatelje usluga izdavanja vremenskog žiga i certifikata (NN 89/2013)

[7] Popis normizacijskih dokumenata u području primjene Zakona o elektroničkom potpisu i Pravilnika o izradi elektroničkog potpisa, uporabi sredstva za izradu elektroničkog potpisa, općim i posebnim uvjetima poslovanja za davatelje usluga izdavanja vremenskog žiga i certifikata u poslovanju davatelja usluga certificiranja u Republici Hrvatskoj (NN 89/2013)

[8] Uredba o djelokrugu, sadržaju i nositelju poslova certificiranja elektroničkih potpisa za tijela državne uprave (NN 146/2004)

Ostali zakoni

[9] Zakon o zaštiti osobnih podataka (NN 106/2012)

Direktive Europskog parlamenta

[10] Direktiva 1999/93/EZ Europskog parlamenta i Vijeća od 13. prosinca 1999. o okviru Zajednice za elektroničke potpise

Normizacijski dokumenti

[11] HRN ETSI/EN 319 411-2 V1.1.1:2013 Elektronički potpisi i infrastrukture (ESI) – Opća pravila i sigurnosni zahtjevi za vjerodostojne davatelje usluga certificiranja – 2. dio: Zahtjevi za opća pravila za certifikacijska tijela koja izdaju kvalificirane certifikate (EN 319 411-2 V1.1.1:2013)

[12] HRN ETSI/EN 319 411-3 V1.1.1:2013 Elektronički potpisi i infrastrukture (ESI) – Zahtjevi za opća pravila i sigurnost za vjerodostojne davatelje usluga koji

izdaju certifikate – 3. dio: Opća pravila za certifikacijska tijela koja izdaju certifikate s javnim ključem (EN 319 411-3 V1.1.1:2013)

[13] HRN ETSI/EN 319 412-5 V1.1.1:2013 Elektronički potpisi i infrastrukture (ESI) – Profili vjerodostojnih davatelja usluga koji izdaju certifikate – 5. dio: Proširenje za profil kvalificiranoga certifikata (EN 319 412-5 V1.1.1:2013)

[14] ETSI TS 119 612 V1.2.1:2014 Electronic Signatures and Infrastructures (ESI) - Trusted Lists

[15] ETSI TS 119 312 V1.1.1:2014 - Electronic Signatures and Infrastructures (ESI); Cryptographic Suites

[16] ETSI TS 119 403 V2.2.1:2015 - Electronic Signatures and Infrastructures (ESI);Trust Service Provider Conformity Assessment

[17] CEN Workshop Agreement 14167-1:2003 – Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1: System Security Requirements

[18] CEN Workshop Agreement 14169:2004 – Secure signature-creation devices "EAL 4+"

[19] ISO/IEC 27001:2013 - Information technology — Security techniques — Information security management systems — Requirements

[20] ISO/IEC 27002:2013 - Information technology - Security techniques - Code of practice for information security controls

[21] IETF RFC 3279 – Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile

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

[23] IETF RFC 3739 – Internet X.509 Public Key Infrastructure: Qualified Certificates Profile

[24] IETF RFC 5280 – 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

[26] IETF RFC 5322 – Internet Message Format

[27] HRN ISO/IEC 15408:2013 (dijelovi 1 do 3) Informacijska tehnologija – Sigurnosne tehnike – Kriteriji za vrednovanje sigurnosti IT – 1. dio: Uvod i opći model, – 2. Dio: Funkcionalni zahtjevi za sigurnost, – 3. Dio: Jamstveni zahtjevi za sigurnost (ISO/IEC 15408-1:2009, ISO/IEC 15408-2:2008, ISO/IEC 15408-3:2008)

[28] NIST FIPS PUB 140-1:1994 – Security Requirements for Cryptographic Modules

[29] NIST FIPS PUB 140-2:2002 – Security Requirements for Cryptographic Modules

[30] NIST FIPS PUB 186-2: Digital Signature Standard (DSS)

[31] ITU-T Recommendation X.509:2000 / ISO/IEC 9594-10:2012: Information technology – Open Systems Interconnection – The Directory: Public-key attribute certificate frameworks

[32] ITU-T Recommendation X.501:10:2012 – Information technology – Open Systems Interconnection – The Directory: Models

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

Finini dokumenti

[34] Fina – Opća pravila davanja usluga certificiranja Fina Root CA, ver 1.0

[35] Fina – Pravilnik o postupcima certificiranja Fina Root CA, CPS_{ROOT}, ver 1.0

[36] Fina – Pravilnik o postupcima certificiranja za kvalificirane certifikate, CPS_{QC}, ver 5.1

[37] Fina – Pravilnik o postupcima certificiranja za nekvalificirane certifikate, CPS_{NQC}, ver 5.1

[38] Fina - Opća pravila davanja usluga izdavanja naprednih vremenskih žigova, ver 1.0

1. UVOD

Fina PKI je inicijalno osmišljen i uspostavljen u Financijskoj agenciji (Fina) kao treća strana od povjerenja (*Trusted Third Party*) s ciljem davanja usluga certificiranja za građane, pravne osobe i tijela javne vlasti. Fina kao davatelj usluga certificiranja omogućuje stvaranje odnosa povjerenja potrebnog za korištenje i razvitak elektroničkog poslovanja (e-poslovanje) i elektroničke javne uprave (e-uprava). Promoviranjem ovih usluga certificiranja 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, obavljanje pouzdanih usluga i orijentiranost prema davanju elektroničkih usluga za 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 poslovnicama i podružnicama, 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 certificiranja usklađene su sa zakonskom regulativom o elektroničkom potpisu u Republici Hrvatskoj [1] – [8] i europskom Direktivom o elektroničkim potpisima [10] te samim time i s mjerodavnim međunarodnim normama iz djelokruga davanja usluga certificiranja. Fina neprekidno prati potrebe korisnika, razvoj tehnologije i promjene u mjerodavnim normama iz područja davanja usluga certificiranja te sukladno tome unapređuje i usklađuje svoj PKI sustav pritom nastojeći svoje proizvode i usluge što više prilagoditi zahtjevima za međugraničnu interoperabilnost.

1.1. Pregled

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

Dvorazinsku arhitekturu produkcijskih certifikacijskih tijela Fine čine:

- korijensko certifikacijsko tijelo: Fina Root CA
- dva subordinirana certifikacijska tijela:
  - Fina RDC 2015;
  - Fina RDC-TDU 2015.

Fina Root CA je samom sebi izdao samopotpisani Fina Root CA certifikat te je certifikate izdao za njemu podređenim subordinirane Fina RDC 2015 i Fina RDC-TDU 2015 CA-ove.

Opća pravila koja se odnose se na Fina Root CA i na cijelu Fina PKI hijerarhiju zasnovanu na Fina Root CA opisana su u dokumentu Opća pravila davanja usluga certificiranja Fina Root CA [34].

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).

1.1.1. Opseg i namjena ovih Općih pravila davanja usluge certificiranja

Ova Fina PKI – Opća pravila davanja usluga certificiranja (engl. *Certificate Policy* – CP, u daljnjem tekstu: Opća pravila) sadrže temeljna pravila i skup načela za davanje usluga certificiranja kojim Fina kao davatelj usluga certificiranja, u smislu Zakona o elektroničkom potpisu [1], [2] i [3] i Direktive 1999/93/EC [10], pruža usluge izdavanja i upravljanja životnim ciklusom korisničkih digitalnih certifikata (u daljnjem tekstu: certifikat).

Fina PKI je PKI infrastruktura uspostavljena u Fini kojom Fina u ulozi davatelja usluga certificiranja obavlja usluge certificiranja.

Opseg ovih Općih pravila su Fina PKI usluge certificiranja koje pruža Fina, a koje se odnose na izdavanje i upravljanje životnom ciklusom produkcijskih kvalificiranih i nekvalificiranih certifikata.

Produkcijski certifikati iz opsega ovih Općih pravila čine Registar digitalnih certifikata (Fina RDC), a koji se sastoji od 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.

Finina usluga izdavanja naprednih vremenskih žigova opisana je u dokumentu Fina - Opća pravila davanja usluga izdavanja naprednih vremenskih žigova [38] objavljenom na internetskim stranicama http://www.fina.hr/finadigicert.

Namjena ovog dokumenta je definiranje i uređivanje pravila i načela prema kojima trebaju postupati svi sudionici Fina PKI navedeni u točki 1.3. ovih Općih pravila, u poslovima iz opsega ovog dokumenta.

Odredbe navedene u ovim Općim pravilima služe za:

- oblikovanje PKI usluga i pravila rada Fina PKI iz opsega ovog dokumenta, koja se moraju uzeti u obzir pri određivanju postupaka u pripadajućem Pravilniku o postupcima certificiranja za kvalificirane certifikate [36] (dalje u tekstu CPS_{QC}) i Pravilniku o postupcima certificiranja za nekvalificirane certifikate [37] (dalje u tekstu CPS_{NQC}), u drugim unutarnjim pravilnicima, pri izradi uputa, ugovora, priručnika i sl., a koji služe za određivanje načina rada certifikacijskih tijela, registracijskih tijela, repozitorija i arhive Fina PKI;

- određivanje načina korištenja Fina PKI usluga od strane korisnika, potpisnika, skrbnika i pouzdajućih strana.

1.1.2. Tipovi certifikata

Unutar ovih Općih pravila kao glavnog dokumenta, definirana su opća pravila certificiranja za tipove certifikata koji imaju različite namjene, područje uporabe i razine sigurnosti.

Fina kao davatelj usluga certificiranja preko Fina RDC 2015 i Fina RDC-TDU 2015 izdaje kvalificirane, normalizirane i *lightweight* certifikate.

Kvalificirani certifikati su kvalificirani certifikati u smislu Zakona o elektroničkom potpisu [1], [2] i [3] te su namijenjeni isključivo za podršku naprednom elektroničkom potpisu koji se izrađuje sredstvima za izradu naprednog elektroničkog potpisa. Kvalificirani certifikati usklađeni su s općim pravilima za „QCP public + SSCD“ norme HRN ETSI/EN 319 411-2 [11] te zadovoljavaju zahtjeve norme HRN ETSI/EN 319 412-5 [13] i preporuke IETF RFC 3739 [23]. Navedeni kvalificirani certifikati imaju oznaku QCP+.

Normalizirani certifikati su certifikati u smislu Zakona o elektroničkom potpisu [1], [2] i [3], te se koriste za podršku elektroničkom potpisu. Normalizirani certifikati s oznakom NCP usklađeni su s općim pravilima za NCP (*Normalized Certificate Policy*) norme HRN ETSI/EN 319 411-3 [12], a normalizirani certifikati s oznakom NCP+ usklađeni su s općim pravilima za NCP+ (*Extended Normalized Certificate Policy*) norme HRN ETSI/EN 319 411-3 [12]. Pored podrške elektroničkom potpisu, normalizirani certifikati mogu se koristiti i za druge potrebe kao što su jaka autentifikacija i enkripcija.

***Lightweight* certifikati** su certifikati u smislu Zakona o elektroničkom potpisu [1], [2] i [3] te se koriste za podršku elektroničkom potpisu. *Lightweight* certifikati usklađeni su s općim pravilima za LCP (*Lightweight Certificate Policy)* norme HRN ETSI/EN 319 411-3 [12]. Pored podrške elektroničkom potpisu, *lightweight* certifikati mogu se koristiti i za druge potrebe kao što su jaka autentifikacija i enkripcija. Navedeni *lightweight* certifikati imaju oznaku LCP.

Normalizirani i *lightweight* certifikati ne smatraju se kvalificiranim certifikatima u smislu Zakona o elektroničkom potpisu [1], [2] i [3] pa se u nastavku ovog dokumenta zajednički nazivaju **nekvalificirani certifikati**.

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 za određenu namjenu ili vid uporabe. Svaki tip certifikata u svom nazivu ima navedenu razinu sigurnosti kojom je određen stupanj pouzdanja u certifikat te OID pravila certificiranja (CP OID). Svaki izdani certifikat ima upisan CP OID kojim se određuje tip certifikata, njegova namjena, područje uporabe i razina sigurnosti. Pomoću ugrađenog CP OID-a potpisnici, skrbnici i pouzdajuće strane određuju prikladnost certifikata za određenu primjenu.

Fina kao davatelj usluga certificiranja za korisnike izdaje sljedeće grupe certifikata obuhvaćene opsegom ovih Općih pravila:

- Fina RDC 2015 osobni certifikati;
- Fina RDC 2015 poslovni certifikati;
- Fina RDC-TDU 2015 certifikati;
- Fina RDC 2015 poslovni certifikati za IT opremu;
- Fina RDC-TDU 2015 certifikati za IT opremu;
- Fina RDC 2015 administrativni certifikati (samo za ovlaštene zaposlenike Fine).

Tablica 1.1. prikazuje tipove certifikata iz opsega ovih Općih pravila s njihovim nazivima i pripadajućim CP OID-ovima, po grupama certifikata za pojedini Fina CA.

Fina Registar digitalnih certifikata (Fina RDC)		
Fina RDC 2015		
Fina RDC 2015 osobni certifikati	Osobni potpisni Q2 certifikat (QCP+)	CP OID: 1.3.124.1104.5.12.1.2.2
	Osobni autentifikacijski N2 certifikat (NCP+)	CP OID: 1.3.124.1104.5.12.1.4.2
	Osobni soft certifikat (NCP)	CP OID: 1.3.124.1104.5.12.1.3.1
Fina RDC 2015 poslovni certifikati	Poslovni potpisni Q2 certifikat (QCP+)	CP OID: 1.3.124.1104.5.12.2.2.2
	Poslovni autentifikacijski N2 certifikat (NCP+)	CP OID: 1.3.124.1104.5.12.2.4.2
	Poslovni soft certifikat (NCP)	CP OID: 1.3.124.1104.5.12.2.3.1
	Poslovni soft certifikat (LCP)	CP OID: 1.3.124.1104.5.12.2.5.1
Fina RDC 2015 poslovni certifikati za IT opremu	SSL certifikat razine 2 (NCP)	CP OID: 1.3.124.1104.5.12.3.3.2
	SSL certifikat razine 3 (NCP+)	CP OID: 1.3.124.1104.5.12.3.4.3
	Aplikacijski certifikat razine 1 (NCP)	CP OID: 1.3.124.1104.5.12.5.3.1
	Aplikacijski certifikat razine 2 (NCP)	CP OID: 1.3.124.1104.5.12.5.3.2
	Aplikacijski certifikat razine 2 (NCP+)	CP OID: 1.3.124.1104.5.12.5.4.2
	Aplikacijski certifikat razine 3 (NCP+)	CP OID: 1.3.124.1104.5.12.5.4.3
	Certifikat za potpis *Trusted* liste (NCP+)	CP OID: 1.3.124.1104.5.12.8.4.2.
	Certifikat za vremenski žig (NCP+)	CP OID: 1.3.124.1104.5.12.52.4.3
	Certifikat za potpis odgovora OCSP servisa (NCP+)	CP OID: 1.3.124.1104.5.12.9.4.3
Fina RDC 2015 administrativni certifikati	Administrativni N2 certifikat (NCP+)	CP OID: 1.3.124.1104.5.12.6.4.2

Fina Registar digitalnih certifikata (Fina RDC)		
Fina RDC-TDU 2015		
Fina RDC-TDU 2015 certifikati	TDU potpisni Q2 certifikat (QCP+)	CP OID: 1.3.124.1104.5.22.2.2.2
	TDU autentifikacijski N2 certifikat (NCP+)	CP OID: 1.3.124.1104.5.22.2.4.2
Fina RDC-TDU 2015 certifikati za IT opremu	Certifikat za potpis odgovora OCSP servisa (NCP+)	CP OID: 1.3.124.1104.5.22.9.4.3

Tablica 1.1. Tipovi certifikata

1.1.2.1. Fina RDC 2015 osobni certifikati

Fina RDC 2015 osobni certifikati namijenjeni su fizičkim osobama – građanima za osobnu uporabu. Ovim općim pravilima određena su tri tipa osobnih certifikata.

- **Osobni potpisni Q2 certifikat (QCP+)** – Osobni potpisni kvalificirani certifikat srednje razine sigurnosti koji se izdaje na Fina e-kartici za građane i na Fina e-tokenu za građane, a koristi se isključivo za izradu naprednog elektroničkog potpisa.

- **Osobni autentifikacijski N2 certifikat (NCP+)** – Osobni autentifikacijski normalizirani certifikat srednje razine sigurnosti koji se izdaje na Fina e-kartici za građane i na Fina e-tokenu za građane, a koristi se za jaku autentifikaciju, elektronički potpis i enkripciju.

- **Osobni soft certifikat (NCP)** – Osobni autentifikacijski normalizirani certifikat standardne razine sigurnosti koji se izdaje u PKCS#12 formatu, a koristi se za jaku autentifikaciju, elektronički potpis i enkripciju.

1.1.2.2. Fina RDC 2015 poslovni certifikati

Fina RDC 2015 poslovni certifikati namijenjeni su za poslovnu uporabu. Ovi certifikati izdaju se pripadajućim osobama unutar poslovnog subjekta. Ovim općim pravilima određena su četiri tipa poslovnih certifikata.

- **Poslovni potpisni Q2 certifikat (QCP+)** – Poslovni potpisni kvalificirani certifikat srednje razine sigurnosti koji se izdaje na Fina poslovnu e-karticu i Fina poslovni e-token, a koristi se isključivo za izradu naprednog elektroničkog potpisa.

- **Poslovni autentifikacijski N2 certifikat (NCP+)** – Poslovni autentifikacijski normalizirani certifikat srednje razine sigurnosti koji se izdaje na Fina poslovnu e-karticu i Fina poslovni e-token, a koristi se za jaku autentifikaciju, elektronički potpis i enkripciju.

- **Poslovni soft certifikat (NCP)** – Poslovni autentifikacijski normalizirani certifikat standardne razine sigurnosti koji se izdaje u PKCS#12 formatu, a koristi se za jaku autentifikaciju, elektronički potpis i enkripciju.

- **Poslovni soft certifikat (LCP)** – Poslovni autentifikacijski *lightweight* certifikat standardne razine sigurnosti koji se izdaje u PKCS#12 formatu, a koristi se za jaku autentifikaciju, elektronički potpis i enkripciju.

1.1.2.3. Fina RDC-TDU 2015 certifikati

Fina RDC-TDU 2015 certifikati namijenjeni su za državne dužnosnike i zaposlenike u tijelima državne uprave (u daljnjem tekstu: TDU). Ovim općim pravilima određena su dva tipa certifikata za državne dužnosnike i zaposlenike u TDU.

- **TDU potpisni Q2 certifikat (QCP+)** – Potpisni kvalificirani certifikat srednje razine sigurnosti za državne dužnosnike i zaposlenike u TDU koji se izdaje na Fina e-kartici za TDU i Fina e-tokenu za TDU, a koristi se isključivo za izradu naprednog elektroničkog potpisa.

- **TDU autentifikacijski N2 certifikat (NCP+)** – Autentifikacijski normalizirani certifikat srednje razine sigurnosti za državne dužnosnike i zaposlenike u TDU koji se izdaje na Fina e-kartici za TDU i Fina e-tokenu za TDU, a koristi se za jaku autentifikaciju, elektronički potpis i enkripciju.

1.1.2.4. Fina RDC 2015 poslovni certifikati za IT opremu

Fina RDC 2015 poslovni certifikati za IT opremu izdaju se za poslužitelje, aplikacije, potpisivanje *Trusted* liste te za potpisivanje naprednih vremenskih žigova i odgovora OCSP servisa. Ovim općim pravilima određeno je devet tipova poslovnih certifikata za IT opremu koje izdaje Fina RDC 2015.

- **SSL certifikat razine 2 (NCP)** – Normalizirani certifikat za poslužitelje srednje razine sigurnosti uz korištenje softverskog spremnika ključa.

- **SSL certifikat razine 3 (NCP+)** – Normalizirani certifikat za poslužitelje visoke razine sigurnosti uz korištenje HSM modula.

- **Aplikacijski certifikat razine 1 (NCP)** – Normalizirani certifikat za aplikacije standardne razine sigurnosti uz korištenje softverskog spremnika ključa.

- **Aplikacijski certifikat razine 2 (NCP)** – Normalizirani certifikat za aplikacije srednje razine sigurnosti uz korištenje softverskog spremnika ključa.

- **Aplikacijski certifikat razine 2 (NCP+)** – Normalizirani certifikat za aplikacije srednje razine sigurnosti uz korištenje SSCD uređaja.

- **Aplikacijski certifikat razine 3 (NCP+)** – Normalizirani certifikat za aplikacije visoke razine sigurnosti uz korištenje HSM modula.

- **Certifikat za potpis *Trusted* liste (NCP+)** – Normalizirani certifikat za potpis *Trusted* liste srednje razine sigurnosti uz korištenje SSCD uređaja.

- **Certifikat za vremenski žig (NCP+)** – Normalizirani certifikat visoke razine sigurnosti uz korištenje HSM modula, za izradu naprednih vremenskih žigova.

- **Certifikat za potpis odgovora OCSP servisa (NCP+)** – Normalizirani certifikat za potpis odgovora OCSP servisa visoke razine sigurnosti uz korištenje HSM modula.

1.1.2.5. Fina RDC-TDU 2015 certifikati za IT opremu

U grupi naziva Fina RDC-TDU 2015 certifikati za IT opremu određen je jedan tip certifikata:

- **Certifikat za potpis odgovora OCSP servisa (NCP+)** – Normalizirani certifikat za potpis odgovora OCSP servisa visoke razine sigurnosti uz korištenje HSM modula.

1.1.2.6. Fina RDC 2015 administrativni certifikati

Fina RDC 2015 administrativni certifikati namijenjeni su za korištenje unutar sustava certificiranja Fine. Ovi certifikati izdaju se ovlaštenim zaposlenicima Fine za obavljanje radnji u sustavu certificiranja. Ovim općim pravilima određen je jedan tip administrativnog certifikata.

- **Administrativni N2 certifikat (NCP+)** – Administrativni normalizirani certifikat srednje razine sigurnosti izdaje se na SSCD uređaj, a koristi se za radnje unutar sustava certificiranja.

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: Fina – Opća pravila davanja usluga certificiranja
- Verzija: 5.1
- Datum objave: 26.08.2016.
- Datum stupanja na snagu: 5.09.2016.
- OID: 1.3.124.1104.5.0.0.1.5.1
- Internet adrese na kojima je dokument objavljen su:
  - http://rdc.fina.hr/RDC2015/FinaRDC2015-CP5-1-hr.pdf i
  - http://rdc.fina.hr/RDC-TDU2015/FinaRDC-TDU2015-CP5-1-hr.pdf

1.3. Sudionici u PKI

Sudionici unutar Fina PKI su:

- tijelo za upravljanje pravilima certificiranja (*Policy Management Authority*, PMA);

- 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;
- ostali sudionici:
  - proizvođači IT opreme za PKI;
  - proizvođači sigurnih uređaja (*smart* kartice, USB tokeni i sl.);
  - ovlaštena nadzorna tijela.

1.3.1. Tijelo za upravljanje pravilima certificiranja

Tijelo za upravljanje pravilima certificiranja u Fini je Fina PMA. Fina PMA je tijelo ovlašteno i odgovorno za izradu, uvođenje i administriranje pravila davanja usluga certificiranja, pripadnu dokumentaciju i postupke te za kontrolu provođenja istih.

1.3.2. 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 preko svojih Fina CA-ova obavlja usluge izdavanja certifikata i upravljanja životnim ciklusom izdanih 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 koje Fina CA-ovi provode u cilju ispunjenja zahtjeva iz Općih pravila opisani su u CPS_{QC} [36], odnosno CPS_{NQC} [37] dokumentima.

1.3.2.1. Fina RDC 2015 CA

Fina RDC 2015 izdaje kvalificirane, normalizirane i *lightweight* certifikate za javnost koji pripadaju sljedećim grupama tipova certifikata:

- Fina RDC 2015 osobni certifikati (kvalificirani i normalizirani certifikati);
- Fina RDC 2015 poslovni certifikati (kvalificirani, normalizirani i *lightweight* certifikati);
- Fina RDC 2015 poslovni certifikati za IT opremu (normalizirani certifikati);
- Fina RDC 2015 administrativni certifikati.

Osnovni podaci o Fina RDC 2015 CA certifikatu dani su u Tablici 1.2.

Polje	Atribut	Vrijednost
Version	Version	X.509 V3
serialNumber	CertificateSerialNumber	Serijski broj certifikata s entropijom od 32 bita (duljina serijskog broja:12 ili 13 okteta)
signatureAlgorithm	AlgorithmIdentifier	sha256WithRSAEncryption OID: 1.2.840.113549.1.1.11
signatureValue		Potpis izdavatelja certifikata

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
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption OID: 1.2.840.113549.1.1.1
	subjectPublicKey	Javni ključ CA: 4096 bita

Tablica 1.2. 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.

1.3.2.2. Fina RDC-TDU 2015 CA

Fina RDC-TDU 2015 uspostavljen je temeljem:

- članka 20. Zakona o elektroničkom potpisu [1], [2] i [3], i
- članka 30. Uredba o djelokrugu, sadržaju i nositelju poslova certificiranja elektroničkih potpisa za tijela državne uprave [8].

Fina RDC-TDU 2015 izdaje kvalificirane i normalizirane certifikate državnim dužnosnicima i zaposlenicima u tijelima državne uprave.

Osnovni podaci o Fina RDC-TDU 2015 certifikatu dani su u Tablici 1.3.

Polje	Atribut	Vrijednost
Version	Version	X.509 V3
serialNumber	CertificateSerialNumber	Serijski broj certifikata s entropijom od 32 bita (duljina serijskog broja:12 ili 13 okteta)
signatureAlgorithm	AlgorithmIdentifier	sha256WithRSAEncryption OID: 1.2.840.113549.1.1.11
signatureValue		Potpis izdavatelja certifikata
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
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption OID: 1.2.840.113549.1.1.1
	subjectPublicKey	Javni ključ CA: 4096 bita

Tablica 1.3. 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.

1.3.3. 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.

Fina PKI ima organiziranu mrežu registracijskih ureda (u daljnjem tekstu: RA mreža) koja obavlja poslove registracije korisnika za Fina CA-ove. RA mrežu čine Fina RA mreža i mreža pojedinog vanjskog ugovorenog RA.

Fina RA mrežu čini mreža lokalnih registracijskih ureda (u daljnjem tekstu: Fina LRA) u poslovnoj mreži Fine te Središnji Fina RA. Registraciju korisnika u Fina RA mreži provodi Fina LRA, a iznimno i Središnji Fina RA. U Fina LRA registraciju provode zaposlenici Fine zaduženi za poslove LRA (u daljnjem tekstu LRA službenici). Poslovima registracije u Fina RA mreži koordinira Središnji Fina RA koji je središnja komunikacijska točka Fina RA mreže.

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. Registraciju korisnika u vanjskim ugovorenim RA-ovima obavljaju zaposlenici poslovnog subjekta s kojim je Fina ugovorila obavljanje usluga registracije. Poslove registracije korisnika s vanjskim ugovorenim RA koordinira Središnji Fina RA.

RA mreža obvezna je poslove registracije obavljati u skladu s ovim Općim pravilima.

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

1.3.4. Korisnici

Korisnici Fina PKI su osobe koje s Finom ugovaraju korištenje usluga certificiranja.

Korisnici Fina PKI mogu biti:

- fizičke osobe – građani;
- poslovni subjekti.

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

Za korištenje usluge certificiranja korisnici trebaju obaviti postupak registracije i predaje zahtjeva te prihvatiti obaveze i odgovornosti korisnika koje su navedene u točki 9.6.3. ovih Općih pravila. U sklopu procedure registracije korisnici s Finom sklapaju ugovor o obavljanju usluga certificiranja.

Na temelju sklopljenog ugovora, zaprimljenog zahtjeva i provedenog postupka registracije određeni Fina CA izdaje traženi certifikat.

1.3.4.1. Subjekti certificiranja

Pri izradi certifikata u certifikat se ugrađuju identifikacijski podaci subjekta certificiranja za kojeg se certifikat izdaje. Subjekt certificiranja može biti fizička osoba – građanin, pripadajuća osoba, poslovni subjekt i IT oprema (npr. poslužitelj, aplikacija i sl.). Podaci o subjektu sastavni su dio certifikata.

U slučaju kada je subjekt certificiranja IT oprema, korisnik obvezno određuje skrbnika certifikata.

1.3.5. Pouzdajuće strane

Pouzdajuće strane su fizičke osobe ili poslovni subjekti koji su primatelji certifikata i djeluju temeljem razumnog pouzdanja u certifikat. Certifikat omogućuje pouzdajućoj strani provjeru cjelovitosti i izvornosti elektronički potpisanog zapisa, odnosno provjeru identiteta subjekta.

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

1.3.6. Ostali sudionici

Ostali sudionici Fina PKI su pravne osobe koje ne pružaju i ne koriste usluge certificiranja, ali sudjeluju u dijelovima procesa vezanim uz davanje usluga certificiranja. U ovu grupu sudionika Fina PKI spadaju proizvođači i distributeri hardvera i softvera korištenih u Fina PKI, proizvođači i distributeri *smart* kartica, USB tokena, HSM-ova i drugih kriptografskih uređaja, neovisni ocjenitelji i dr.

1.4. Uporaba certifikata

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

- pravne zahtjeve za identifikaciju druge strane, npr. zaštita tajnosti informacija, pravna prihvatljivost elektroničkog potpisa kojeg se može primijeniti;
- sve podatke koji se nalaze u certifikatu ili činjenice o kojima je pouzdajuća strana obaviještena, uključujući i ova Opća pravila;
- ekonomsku vrijednost transakcije ili komunikacije, ako je to primjenjivo;
- potencijalne gubitke ili štetu koja može biti uzrokovana pogrešnom identifikacijom, gubitkom povjerenja ili tajnosti informacija u transakcijama ili komunikaciji;
- primjenjivost hrvatskih zakona;
- običaj ili naviku trgovanja, odnosno razmjene, posebno trgovanja koje se obavlja vjerodostojnim sustavima ili drugim metodama temeljenim na računalnim sustavima;
- bilo koji pokazatelj prikladnosti ili neprikladnosti ili druge činjenice koje pouzdajuća strana zna, a odnose se na subjekt, primijenjeno rješenje, komunikaciju ili transakciju;

- preporučeni financijski limit povezan s razinom sigurnosti certifikata.

U Tablici 1.4. prikazane su razine sigurnosti za certifikate koje izdaju Fina CA-ovi, a koji su obuhvaćeni opsegom ovih Općih pravila. Za svaku razinu sigurnosti u tablici je prikazan pripadajući opis područja primjene i preporučeni financijski limit.

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

Tablica 1.4. Razine sigurnosti za certifikate koje izdaju Fina CA-ovi

1.4.1. Primjerena uporaba certifikata

Fina RDC 2015 osobni certifikati koji se izdaju sukladno ovim Općim pravilima jamče elektronički identitet fizičke osobe – građanina, dok Fina RDC 2015 poslovni certifikati i Fina RDC-TDU 2015 certifikati za državne dužnosnike i zaposlenike u TDU jamče profesionalni identitet pripadajućih osoba kao i identitet te legitimitet poslovnog subjekta, odnosno TDU. Fina RDC 2015 poslovni certifikati za IT opremu izdani sukladno ovim Općim pravilima jamče elektronički identitet poslužitelja, aplikacija te identitet i legitimitet poslovnog subjekta, odnosno TDU.

Elektronički potpisi podržani normaliziranim, odnosno *lightweight* certifikatima smatraju se elektroničkim potpisima za cijelo vrijeme u kojem se takvi potpisi mogu logički povezati s potpisanim podacima na koje se odnose, na takav način da se mogu otkriti sve naknadne promjene potpisanih podataka.

1.4.1.1. Primjerena uporaba Fina RDC 2015 i Fina RDC-TDU 2015 potpisnih QCP+ kvalificiranih certifikata

Fina RDC 2015 i Fina RDC-TDU 2015 potpisni QCP+ certifikati su kvalificirani certifikati koji su usklađeni s općim pravilima za „QCP public + SSCD“ norme HRN ETSI/EN 319 411-2 [11] i njihova je uporaba ograničena isključivo na podršku naprednom elektroničkom potpisu koji se izrađuje sredstvom za izradu naprednog elektroničkog potpisa sukladno Zakonu o elektroničkom potpisu [1], [2] i [3].

Ova točka obuhvaća tri tipa certifikata.

- Osobni potpisni Q2 certifikat (QCP+), izdaje se fizičkim osobama – građanima za vlastite potrebe. Fizička osoba – građanin može ovaj certifikat koristiti i za poslovnu

uporabu ukoliko pritom nije nužno certifikatom dokazivati pripadnost poslovnom subjektu.
- Poslovni potpisni Q2 certifikat (QCP+), izdaje se pripadajućim osobama u poslovnim subjektima koji nisu TDU za poslovnu uporabu.
- TDU potpisni Q2 certifikat (QCP+), izdaje se državnim dužnosnicima i zaposlenicima u TDU za službenu uporabu.

Navedeni tipovi certifikata imaju srednju razinu sigurnosti te se potpisnicima izdaju isključivo na sredstvo za izradu naprednog elektroničkog potpisa (u daljnjem tekstu: SSCD uređaj), primjerice na adekvatnu *smart* karticu ili USB token.

Ekstenzija *keyUsage* ovih tipova certifikata označena je kritičnom te isključivo ima vrijednost postavljenu na *nonRepudation*. Ovi certifikati imaju ekstenziju *qCStatements* koja nije označena kritičnom i koja ima vrijednost *id-etsi-qcs-QcCompliance* sukladno normi HRN ETSI/EN 319 412-5 [13]. Elektronički potpisi podržani ovim kvalificiranim potpisnim certifikatima smatraju se naprednim elektroničkim potpisima za cijelo vrijeme u kojem se takvi potpisi mogu logički povezati s potpisanim podacima na koje se odnose, na takav način da se mogu otkriti sve naknadne promjene potpisanih podataka.

1.4.1.2. Primjerena uporaba Fina RDC 2015 i Fina RDC-TDU 2015 autentifikacijskih NCP+ normaliziranih certifikata

Fina RDC 2015 i Fina RDC-TDU 2015 autentifikacijski NCP+ normalizirani certifikati usklađeni su s općim pravilima za NCP+ (*Extended Normalized Certificate Policy*) norme HRN ETSI/EN 319 411-3 [12] i njihova je uporaba ograničena na podršku elektroničkom potpisu u smislu Zakona o elektroničkom potpisu [1], [2] i [3] na jaku autentifikaciju i enkripciju ključa.

Ova točka obuhvaća tri tipa certifikata.

- Osobni autentifikacijski N2 certifikat (NCP+), izdaje se fizičkim osobama – građanima za privatnu uporabu. Fizička osoba – građanin može ovaj certifikat koristiti i za poslovnu uporabu ukoliko pritom nije nužno certifikatom dokazivati pripadnost poslovnom subjektu.
- Poslovni autentifikacijski N2 certifikat (NCP+), izdaje se pripadajućim osobama u poslovnim subjektima koji nisu TDU za poslovnu uporabu.
- TDU autentifikacijski N2 certifikat (NCP+), izdaje se državnim dužnosnicima i zaposlenicima u TDU za službenu uporabu.

Navedeni tipovi certifikata imaju srednju razinu sigurnosti te se izdaju potpisnicima isključivo na SSCD uređaj, primjerice na adekvatnu *smart* karticu ili USB token.

Ekstenzija *keyUsage* označena je kritičnom te ima vrijednost postavljenu na *digitalSignature* i *keyEncription*.

1.4.1.3. Primjerena uporaba Fina RDC 2015 autentifikacijskih NCP normaliziranih certifikata

Fina RDC 2015 autentifikacijski NCP normalizirani certifikati usklađeni su s općim pravilima za NCP (*Normalized Certificate Policy*) norme HRN ETSI/EN 319 411-3 [12] i njihova je uporaba ograničena na podršku elektroničkom potpisu u smislu Zakona o elektroničkom potpisu [1], [2] i [3] na jaku autentifikaciju i enkripciju ključa.

Ova točka obuhvaća dva tipa certifikata.

- Osobni soft certifikat (NCP), izdaje se fizičkim osobama – građanima za privatnu uporabu. Fizička osoba – građanin može ovaj certifikat koristiti i za poslovnu uporabu ukoliko pritom nije nužno certifikatom dokazivati pripadnost poslovnom subjektu.
- Poslovni soft certifikat (NCP), izdaje se pripadajućim osobama u poslovnim subjektima koji nisu TDU za poslovnu uporabu.

Navedeni tipovi certifikata imaju standardnu razinu sigurnosti te se izdaju uz korištenje softverskog spremnika ključa.

Ekstenzija *keyUsage* označena je kritičnom te ima vrijednost postavljenu na *digitalSignature* i *keyEncription.*

1.4.1.4. Primjerena uporaba Fina RDC 2015 autentifikacijskih LCP lightweight certifikata

Fina RDC 2015 autentifikacijski LCP *lightweight* certifikati usklađeni su s općim pravilima za LCP (*Lightweight Certificate Policy)* norme HRN ETSI/EN 319 411-3 [12] i njihova je uporaba ograničena na podršku elektroničkom potpisu u smislu Zakona o elektroničkom potpisu [1], [2] i [3] na jaku autentifikaciju i enkripciju ključa.

Ova točka obuhvaća poslovni soft certifikat (LCP) koji se izdaje pripadajućim osobama u poslovnim subjektima koji nisu TDU za poslovnu uporabu.

Navedeni tip certifikata ima standardnu razinu sigurnosti te se izdaje uz korištenje softverskog spremnika ključa.

Ekstenzija *keyUsage* označena je kritičnom te ima vrijednost postavljenu na *digitalSignature* i *keyEncription.*

1.4.1.5. Primjerena uporaba Fina RDC 2015 SSL normaliziranih certifikata

Fina RDC 2015 SSL certifikati usklađeni su s općim pravilima za NCP odnosno NCP+ norme HRN ETSI/EN 319 411-3 [12], a sukladno podacima iz niže navedenog popisa tipova certifikata obuhvaćenih ovom točkom. U istom popisu navedene su i pripadajuće razine sigurnosti.

Ova točka obuhvaća dva tipa certifikata.

- SSL certifikat razine 2 (NCP), srednje razine sigurnosti uz korištenje softverskog spremnika ključa.

- SSL certifikat razine 3 (NCP+), visoke razine sigurnosti uz korištenje adekvatnog HSM modula.

Tipovi certifikata iz popisa koji u nazivu imaju oznaku SSL izdaju se internetskim poslužiteljima i upotrebljavaju se za uspostavu SSL/TLS sigurnog komunikacijskog kanala između klijenta i poslužitelja, gdje se enkripcija i digitalni potpis upotrebljavaju u svrhe autentifikacije subjekata u komunikaciji. Primjeri uporabe ovih certifikata su internetski servisi s jakom autentifikacijom korisnika servisa.

Ekstenzija *keyUsage* označena je kritičnom te ima vrijednost postavljenu na *digitalSignature* i *keyEncription*.

1.4.1.6. Primjerena uporaba Fina RDC 2015 aplikacijskih normaliziranih certifikata

Fina RDC 2015 aplikacijski certifikati usklađeni su s općim pravilima za NCP odnosno NCP+, norme HRN ETSI/EN 319 411-3 [12], a sukladno podacima iz niže navedenog popisa tipova certifikata obuhvaćenih ovom točkom. U istom su popisu navedene i pripadajuće razine sigurnosti.

Ova točka obuhvaća četiri tipa certifikata.

- Aplikacijski certifikat razine 1 (NCP), standardne razine sigurnosti uz korištenje softverskog spremnika ključa.
- Aplikacijski certifikat razine 2 (NCP), srednje razine sigurnosti uz korištenje softverskog spremnika ključa.
- Aplikacijski certifikat razine 2 (NCP+), srednje razine sigurnosti uz korištenje SSCD uređaja.
- Aplikacijski certifikat razine 3 (NCP+), visoke razine sigurnosti uz korištenje HSM modula.

Navedeni tipovi certifikata izdaju se za aplikacije ili elektroničke servise te je njihova uporaba ograničena na podršku elektroničkom potpisu u smislu Zakona o elektroničkom potpisu [1], [2] i [3] na jaku autentifikaciju i enkripciju ključa.

Ekstenzija *keyUsage* označena je kritičnom te ima vrijednost postavljenu na *digitalSignature* i *keyEncription*.

1.4.1.7. Primjerena uporaba Fina RDC 2015 certifikata za potpis Trusted liste

Fina RDC 2015 certifikati za potpis *Trusted* liste usklađeni su s općim pravilima za NCP+ norme HRN ETSI/EN 319 411-3 [12] i normizacijskim dokumentom ETSI TS 119 612 [14] te se izdaju ministarstvu nadležnom za gospodarstvo.

Ovaj tip certifikata jamči elektronički identitet poslovnog subjekta koji je potpisao *Trusted* listu u svrhu provjere autentičnosti i osiguranje cjelovitosti *Trusted* liste.

Ova točka odnosi se na jedan tip certifikata:

- Certifikat za potpis *Trusted* liste (NCP+).

Ovi certifikati izdaju se uz korištenje SSCD uređaja te imaju srednju razinu sigurnosti.

Ekstenzija keyUsage označena je kritičnom te ima vrijednost postavljenu na digitalSignature. Ovaj tip certifikata ima i dodatnu ekstenziju extKeyUsage koja nije označena kritično, a koja ima vrijednost postavljenu na *id-tsl-kp-tslSigning*.

Certifikat se smije koristiti samo za podršku elektroničkog potpisa *Trusted* liste.

1.4.1.8. Primjerena uporaba Fina RDC 2015 certifikata za vremenski žig

Fina RDC 2015 certifikati za vremenski žig usklađeni su s općim pravilima za NCP+ norme HRN ETSI/EN 319 411-3 [12] te se izdaju poslovnom subjektu, uključujući i TDU, isključivo za podršku potpisa servisa za izdavanje naprednih vremenskih žigova. Ovaj tip certifikata jamči elektronički identitet Fina servisa izdavanja naprednih vremenskih žigova Fina QTSA 2015.

Ova točka odnosi se na jedan tip certifikata:

- Certifikat za vremenski žig (NCP+).

Ovi certifikati izdaju se uz korištenje HSM uređaja te imaju visoku razinu sigurnosti.

Ekstenzija *keyUsage* je označena kritičnom te ima vrijednost postavljenu na *digitalSignature* i *nonRepudation*, a certifikat ima i dodatnu ekstenziju *extKeyUsage* označenu kritičnom i postavljenu na vrijednost *timeStamping*.

1.4.1.9. Primjerena uporaba Fina RDC 2015 administrativnih NCP+ normaliziranih certifikata

Fina RDC 2015 administrativni NCP+ normalizirani certifikati usklađeni su s općim pravilima za NCP+ norme HRN ETSI/EN 319 411-3 [12] i njihova je uporaba ograničena isključivo na radnje unutar sustava certificiranja FINE.

Ova točka odnosi se na jedan tip certifikata:

- Administrativni N2 certifikat (NCP+).

Ovaj tip certifikata ima srednju razinu sigurnosti te se izdaje isključivo na SSCD uređaju ovlaštenim zaposlenicima FINE za poslove administriranja sustava certificiranja Fine.

1.4.2. Zabrane uporabe certifikata

Sve uporabe certifikata izdanih sukladno ovim Općim pravilima različite od uporaba navedenih u točki 1.4.1. ovog dokumenta su zabranjene.

Preporuka je pouzdajućim stranama da provjeravaju i koriste CP OID certifikata kako bi donijele valjanu odluku o prihvaćanju ili odbacivanju uporabe određenog certifikata na način opisan u točki 9.6.4. ovih Općih pravila. Popis CP OID-ova za certifikate iz opsega ovih Općih pravila naveden je Tablici 1.1.

1.5. Administracija dokumenta Opća pravila

1.5.1. Organizacija odgovorna za održavanje dokumenta Opća pravila

Za izradu i održavanje dokumenta Općih pravila odgovorno je tijelo za upravljanje pravilima certificiranja Fina PMA (vidi točku 1.3. Općih pravila).

1.5.2. Kontakt podaci

Kontakt podaci za administraciju i sadržaj ovih Općih pravila dani su u nastavku.

Poštanska adresa:

Fina
Sektor financijskih i elektroničkih usluga
Ured za upravljanje politikom e-poslovanja
Koturaška cesta 43
10000 Zagreb
Hrvatska

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

1.5.3. Tijelo koje utvrđuje uskladivost CPS-a s Općim pravilima

Uskladivost CPS_{QC} [36], odnosno CPS_{NQC} [37] dokumenata s ovim Općim pravilima utvrđuje Fina PMA.

1.5.4. Procedure odobravanja CPS-a

Prije primjene CPS_{QC} [36], odnosno CPS_{NQC} [37] dokumenata za Fina CA, ovi dokumenti moraju biti odobreni od strane Fina PMA. Početak i prestanak važenja CPS_{QC} [36], odnosno CPS_{NQC} [37] dokumenata određuje Fina PMA u skladu sa svojim internim postupcima.

1.6. Definicije i kratice

1.6.1. Definicije

DEFINICIJA	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.
Autentifikacija	Proces provjere korisničkog identiteta, tj. provjera je li korisnik upravo taj za kojeg se predstavlja. Autentifikacija korisnika provodi se u cilju dobivanja pristupa određenim podacima odnosno računalnim resursima.
CA certifikat	Certifikat u kojem je kao subjekt certificiranja naveden (isti ili neki drugi) CA. CA certifikat sadrži naziv i javni ključ CA.
CA privatni potpisni ključ	Privatni ključ CA koji s javnim CA ključem čini par CA ključeva. CA privatni potpisni ključ koristi se za potpisivanje certifikata koje izdaje taj CA. Pripadni CA javni ključ upisan je u CA certifikat tog CA.
CA *root* certifikat	CA certifikat kojeg je samom sebi izdao i potpisao isti CA, tj. subjekt certificiranja i izdavatelj u CA root certifikatu su jednaki.
Certifikacijsko tijelo (CA)	Treća strana od povjerenja koja potvrđuje identitet subjekta certificiranja, izrađuje i potpisuje te za subjekt certificiranja izdaje traženi certifikat. CA je davatelj usluga certificiranja koji izdaje i upravlja životnom ciklusom izdanih certifikata u skladu s objavljenim CP-om, a može biti fizička osoba te pravna osoba ili njen sastavni dio.
Certifikat	Potvrda u elektroničkom obliku koja: • imenuje i identificira subjekt certificiranja naveden u certifikatu; • sadrži subjektov javni ključ; • ima upisan vremenski period valjanosti certifikata; • ima značenje u skladu s važećim propisima i normama; • identificira CA koji izdaje certifikate; • elektronički je potpisan od strane CA.
Davatelj usluga certificiranja (CSP)	Pravna ili fizička osoba koja izdaje certifikate ili daje druge usluge povezane s elektroničkim potpisima. Druge usluge povezane s elektroničkim potpisom mogu biti usluga izdavanja vremenskog žiga, usluga izrade elektroničkog potpisa, usluga verifikacije elektroničkog potpisa, usluga dugotrajnog čuvanja elektronički potpisanih zapisa i sl.
Digitalni potpis	Podaci koji se dodaju podatkovnom skupu ili kriptografska transformacija podatkovnog skupa koja omogućuje njegovom primatelju dokazivanje izvornosti i cjelovitosti podatkovnog skupa te koja podatkovni skup štiti od krivotvorenja, npr. od strane primatelja.
Dnevnik sustava	Skup zapisa o događajima u informacijskom sustavu (engl. *log, audit log*).
Elektronički potpis	Skup podataka u elektroničkom obliku koji su pridruženi ili su logički povezani s drugim podacima u elektroničkom obliku i koji služe za identifikaciju potpisnika i utvrđivanje vjerodostojnosti potpisanoga elektroničkog dokumenta.
Fina LRA	LRA (lokalni registracijski ured) u Fina poslovnoj mreži.

DEFINICIJA	ZNAČENJE
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 Fina RA i Fina LRA ureda.
Fina RDC	Registar digitalnih certifikata kojeg vodi Fina za pružanje usluga izdavanja i upravljanja životnim ciklusom digitalnih certifikata.
Identifikator objekta (OID)	Identifikator koji predstavlja specifičan objekt. OID se sastoji od brojeva odijeljenih točkama i navedenih u hijerarhijskom poretku. Svaki broj identificira poseban čvor u stablu čvorova, počevši od korijena tog stabla.
Ime (naziv) subjekta	Polje certifikata koje sadrži jedinstveni identifikator imena odnosno naziva subjekta (polje *subject*).
Infrastruktura javnog ključa (PKI)	Arhitektura, organizacija, hardver, softver, osoblje, pravila, operativni postupci i procedure koje zajednički podržavaju implementaciju i rad kriptografskog sustava javnog ključa za upravljanje životnim ciklusom digitalnih certifikata.
Izdavanje certifikata nakon isteka	Izdavanje novog certifikata čiji su parametri jednaki kao i parametri certifikata na koji se zahtjev odnosi, ali s novim ključem, novim serijskim brojem certifikata, novim vremenskim periodom valjanosti i novim potpisom istog Fina CA. Ovisno o tipu certifikata i roku u kojem se provodi izdavanje certifikata, novoizdani certifikat može imati isti ili izmijenjeni interni Finin serijski broj u razlikovnom imenu.
Izdavanje certifikata nakon opoziva	Izdavanje novog certifikata čiji su parametri jednaki kao i parametri certifikata na koji se zahtjev odnosi, ali s novim ključem, novim serijskim brojem certifikata, novim vremenskim periodom valjanosti, novim potpisom istog Fina CA te izmijenjenim internim Fininim serijskim brojem u razlikovnom imenu.
Javni imenik	Informatički sustav u nadležnosti CA koji služi za *online* objavu dokumenata i informacija vezanih uz certifikate, uključujući i informacije o valjanosti ili opozvanosti certifikata.
Javni ključ (*Public key*)	Javno dostupan kriptografski ključ koji odgovara uparenom privatnom ključu. Javni ključ može služiti za provjeru elektroničkog potpisa ili za enkripciju podataka.
Korisničke uloge	Uloge koje imaju djelatnici uključeni u poslovne procese certificiranja, a koje ne spadaju u povjerljive uloge. Odgovornosti ovih uloga opisane su u opisu posla djelatnika.
Korisnik	Fizička osoba-građanin ili poslovni subjekt kojima davatelj usluga certificiranja daje usluge, odnosno s kojim sklapa ugovor o korištenju usluga certificiranja.
Kriptografski modul	Softver ili uređaj određene razine sigurnosti koji: • generira par ključeva i/ili • štiti kriptografske informacije i/ili • obavlja kriptografske funkcije.

DEFINICIJA	ZNAČENJE
Kvalificirani certifikat	Elektronička potvrda kojom davatelj usluga izdavanja kvalificiranih certifikata potvrđuje napredni elektronički potpis. Kvalificirani certifikat izdaje davatelj usluga izdavanja kvalificiranog certifikata koji ispunjava uvjete propisane Zakonom o elektroničkom potpisu.
LCP certifikat	LCP certifikat, vidi pojam „*Lightweight* certifikat“
***Lightweight* certifikat**	Certifikat koji pruža manje zahtjevnu razinu kvalitete usluge u odnosu na certifikate izdane sukladno Općim pravilima izdavanja kvalificiranih certifikata opisanim u HRN ETSI/EN 319 411-2, LCP certifikat.
***Lightweight Directory Acess Protocol* (LDAP)**	Aplikacijski protokol koji radi iznad TCP/IP sloja, a služi za pristup i održavanje distribuiranih usluga povezivanja, pretraživanja i izmjena informacija putem mrežnog internetskog protokola.
Lista opozvanih certifikata (CRL)	Potpisana lista koja ukazuje na skup certifikata koji se od strane izdavatelja certifikata više ne smatraju važećim.
LRA službenik	Ovlašteni zaposlenik FININOG lokalnog registracijskog ureda odnosno registracijskog ureda koji prikuplja dokumentaciju, provodi identifikaciju i potvrđivanje identiteta korisnika i/ili obavlja registraciju korisnika.
Nacionalni OIB sustav	Informacijski sustav Evidencije o osobnim identifikacijskim brojevima kojeg Porezna uprava Ministarstva financija.
Napredan elektronički potpis	Elektronički potpis koji pouzdano jamči identitet potpisnika i koji: • je povezan isključivo s potpisnikom; • nedvojbeno identificira potpisnika; • nastaje korištenjem sredstava kojima potpisnik može samostalno upravljati i koja su isključivo pod nadzorom potpisnika; • sadržava izravnu povezanost s podacima na koje se odnosi i to na način koji nedvojbeno omogućava uvid u bilo koju izmjenu izvornih podataka.
Napredan vremenski žig	Elektronički potpisana potvrda izdavatelja naprednog vremenskog žiga koja potvrđuje sadržaj podataka na koji se odnosi u navedenom vremenu i koja ispunjava uvjete za napredan elektronički potpis.
Normalizirani certifikat	Certifikat koji pruža istu kvalitetu kao i certifikati izdani sukladno općim pravilima izdavanja kvalificiranih certifikata opisanim u HRN ETSI/EN 319 411-2, ali bez pravne valjanosti u smislu Direktive 1999/93/EC te bez zahtijevanja uporabe sigurnog sredstva za izradu elektroničkog potpisa (sredstva za izradu naprednog elektroničkog potpisa).
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 ključem, novim serijskim brojem certifikata, novim vremenskim periodom valjanosti i novim potpisom istog Fina CA, a provodi se u definiranom periodu prije datuma isteka valjanosti certifikata.
Opća pravila davanja usluga certificiranja - *Certificate Policy* (CP)	Imenovani skup pravila koji ukazuje na primjenjivost certifikata za određenu skupinu i/ili klasu primjena sa zajedničkim zahtjevima na sigurnost.

DEFINICIJA	ZNAČENJE
Oporavak certifikata	Izdavanje novog certifikata čiji su parametri jednaki kao i parametri certifikata na koji se zahtjev odnosi, ali s novim ključem, novim serijskim brojem certifikata, novim vremenskim periodom valjanosti i novim potpisom istog Fina CA, a provodi se prije nastupanja rokova za obnovu certifikata. Korisnički certifikat čiji se oporavak traži se opoziva, a novoizdani certifikat ima isti Finin interni serijski broj u razlikovnom imenu certifikata kao i korisnički certifikat čiji se oporavak traži.
Opoziv certifikata	Radnja koja certifikat nepovratno čini nevažećim od tog trenutka pa na nadalje. Opoziv postaje važećim objavom CRL u kojoj je naznačen i opoziv tog certifikata.
Osoba ovlaštena za zastupanje	Osoba koja vlastitim očitovanjem volje sklapa pravni posao ili poduzima neku drugu pravnu radnju za drugog (zastupnik). Ovlaštenje za zastupanje može se temeljiti na zakonu, statutu, društvenom ugovoru ili pravilima pravne osobe, aktu nadležnog državnog tijela ili na punomoći.
Par ključeva	Dva matematički povezana kriptografska ključa (privatni ključ i njegov odgovarajući javni ključ) koji imaju sljedeća svojstva: • jedan ključ iz para ključeva može biti korišten za enkripciju podataka, a koji se mogu dekriptirati samo korištenjem drugog ključa iz istog para ključeva i • u slučaju poznavanja samo jednog ključa nije moguće (u razumnom vremenu i uz poznatu tehnologiju) otkriti drugi ključ.
Period valjanosti certifikata	Vremenski period tijekom kojeg vrijedi certifikat. Ovaj vremenski period počinje vremenom označenim u polju „vrijedi od“ i završava vremenom „vrijedi do“.
Podaci za izradu elektroničkog potpisa	Jedinstveni podaci, poput kodova ili privatnih kriptografskih ključeva, koje potpisnik koristi za izradu elektroničkog potpisa.
Podaci za verificiranje elektroničkog potpisa	Podaci poput kodova ili javnih kriptografskih ključeva, koji se koriste u svrhu verificiranja (ovjere) elektroničkog 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; • javni ovršitelji i dr.

DEFINICIJA	ZNAČENJE
Potpisnik	Osoba koja posjeduje sredstvo za izradu elektroničkog potpisa kojim se potpisuje, a koja djeluje u svoje ime ili u ime fizičke ili pravne osobe koju predstavlja.
Pouzdajuća strana	Primatelj certifikata koji djeluje temeljem razumnog pouzdanja u certifikat. Certifikat omogućuje pouzdajućoj strani provjeru cjelovitost i izvornosti elektronički potpisanog zapisa odnosno provjeru identiteta subjekta.
Povjerljive uloge	Uloge koje se dodjeljuju djelatnicima i o kojima ovisi sigurnost rada davatelja usluga certificiranja. Povjerljive uloge (engl. Trusted Roles) i pripadne odgovornosti moraju biti jasno određene i opisane u opisu posla djelatnika.
Pravilnik o postupcima certificiranja (CPS)	Dokument koji sadrži operativne postupke davatelja usluga certificiranja. Operativni postupci definirani Pravilnikom o postupcima certificiranja moraju biti sukladni odredbama definiranim u dokumentu Opća pravila davanja usluga certificiranja (CP).
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	Kriptografski ključ kojeg korisnik čuva u tajnosti, a koji odgovara uparenom javnom ključu. Koristi se za izradu elektroničkog potpisa ili za dekriptiranje podataka enkriptiranih odgovarajućim javnim ključem.
Profil certifikata	Detaljan popis i opis gradivnih elemenata certifikata i njihovih vrijednosti.
RA mreža	Cjelokupna mreža registracijskih ureda, a sastoji se od središnjeg Fina RA, Fina LRA ureda te od vanjskih ugovorenih RA s kojima Fina ima sklopljen ugovor o obavljanju poslova registracije.
Razlikovno ime subjekta (DN subjekta)	Jedinstveno ime subjekta upisano u certifikat. Razlikovno ime subjekta jedinstveno identificira subjekt kojem je izdan certifikat i jedinstveno je unutar jednog CA.
Razumno pouzdanje	Razumnim pouzdanjem smatra se odluka pouzdajuće strane da se pouzda u certifikat ako je u vrijeme ostvarenja pouzdanja: • koristila certifikat u svrhe propisane CP-om 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; • provjerila da certifikat nije istekao u vrijeme ostvarenja pouzdanja te da certifikat nije opozvan ili suspendiran, a što pouzdajuća strana treba utvrditi provodeći provjeru statusa certifikata temeljem zadnje izdane CRL kako je propisano u CP-u; • provjerila da su svi podaci o identitetu subjekta certifikata ispravno prikazani aplikacijom u koju se može pouzdati; • ako je u pitanju elektronički potpis, provjerila da je elektronički potpis izrađen privatnim ključem koji odgovara javnom ključu u certifikatu za vrijeme perioda valjanosti certifikata. 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.
Reaktivacija certifikata	Postupak ponovnog aktiviranja suspendiranog certifikata nakon prestanka postojanja razloga za suspenziju.

DEFINICIJA	ZNAČENJE
Registracijski ured (RA)	Pravna ili fizička osoba ovlaštena od CA i zadužena za identifikaciju i potvrdu identiteta podnositelja zahtjeva za izdavanje, opoziv, suspenziju ili reaktivaciju certifikata, za obradu zahtjeva te za isporuku certifikata i uređaja korisnicima.
Sigurno sredstvo za izradu elektroničkog potpisa (SSCD)	Vidi pojam: „Sredstvo za izradu naprednog elektroničkog potpisa“.
Skrbnik	Fizička osoba zaposlena u poslovnom subjektu ili na drugi način povezana s poslovnim subjektom, a koja je od strane istog poslovnog subjekta autorizirana za preuzimanje, uporabu, čuvanje i brigu o privatnom ključu i pripadnom certifikatu izdanom za poslužitelj, aplikaciju i sl. Skrbnik podnosi zahtjev za izdavanje, obnovu, opoziv, suspenziju ili reaktivaciju certifikata te je kontakt osoba za taj certifikat.
Središnji RA	Središnji registracijski ured. Može registrirati korisnike, ali primarno je zadužen za koordiniranje cjelokupne RA mreže.
Sredstvo za izradu elektroničkog potpisa	Odgovarajuća računalna oprema ili računalni program kojeg potpisnik koristi pri izradi elektroničkog potpisa.
Sredstvo za izradu naprednog elektroničkog potpisa (SSCD)	Sredstvo za izradu elektroničkog potpisa koje osigurava: • da se podaci za izradu naprednoga elektroničkog potpisa mogu pojaviti samo jednom te da je ostvarena njihova sigurnost; • da se podaci za izradu naprednoga elektroničkog potpisa ne mogu ponoviti te da je potpis zaštićen od krivotvorenja pri korištenju postojeće raspoložive tehnologije; • da podatke za izradu naprednoga elektroničkog potpisa subjekt može pouzdano zaštititi protiv korištenja od strane drugih. Sredstvo za izradu naprednoga elektroničkog potpisa ne smije pri izradi naprednoga elektroničkog potpisa promijeniti podatke koji se potpisuju ili onemogućiti subjektu uvid u te podatke prije procesa izrade naprednoga elektroničkog potpisa.
Subjekt ili subjekt certificiranja	Subjekt (certificiranja) je entitet za kojeg se izdaje certifikat, tj. može biti fizička osoba – građanin, fizička osoba povezana s poslovnim subjektom (vidi pojam: „Pripadajuća osoba“), poslužitelj, aplikacija i sl. Podaci o subjektu sastavni su dio certifikata.
Suspenzija certifikata	Postupak kojim certifikat privremeno postaje nevažećim.
Tijelo (tijela) državne uprave (TDU)	Tijelo državne uprave je tijelo državne vlasti nadležno za obavljanje poslova državne uprave u upravnom području za koje je nadležno. Tijela državne uprave su ministarstva, državni uredi Vlade Republike Hrvatske, državne upravne organizacije i uredi državne uprave u županijama ili druga tijela državne uprave utvrđena mjerodavnim važećim zakonom.
Tijelo za upravljanje pravilima certificiranja (PMA)	Tijelo koje je ovlašteno i odgovorno za izradu, uvođenje i administriranje pravila davanja usluga certificiranja, pripadnu dokumentaciju i procedure te za kontrolu provođenja istih.
***Trusted* lista**	Pouzdani popis davatelja usluga certificiranja koje nadziru/akreditiraju države članice EU.
Ugovor o obavljanju usluga certificiranja	Ugovor između fizičke osobe odnosno poslovnog subjekta zastupanog po ovlaštenoj osobi za zastupanje i davatelja usluge certificiranja koji detaljno opisuje prava i obveze svake strane u odnosu na certifikat koji se izdaje subjektu.

DEFINICIJA	ZNAČENJE
Vanjski LRA	Lokalni registracijski ured pod ingerencijom vanjskog ugovorenog RA.
Vjerodostojan sustav	Informacijski sustav ili proizvod implementiran kao hardver i/ili softver koji stvara pouzdane i autentične zapise zaštićene od izmjena te dodatno osigurava tehničku i kriptografsku sigurnost podržanog procesa (engl. *Trustworthy System*).
Vremenski žig	Elektronički potpisana potvrda izdavatelja koja potvrđuje sadržaj podataka na koji se odnosi u navedenom vremenu.
Zaporka	Tajna riječ ili niz znakova kojeg unosi korisnik u cilju dobivanja pristupa podacima ili pristupa određenom sustavu.

Tablica 1.5. Definicije

1.6.2. Kratice

KRATICA	PUNI NAZIV	ZNAČENJE
CA	*Certification Authority*	Certifikacijsko tijelo
CP	*Certificate Policy*	Opća pravila davanja usluga certificiranja
CP_{ROOT}	*Certificate Policy Fina Root CA*	Opća pravila davanja usluga certificiranja za Fina Root CA
CPS	*Certification Practice Statement*	Pravilnik o postupcima certificiranja
CPS_{NQC}	*Certification Practice Statement for Non-Qualified Certificates*	Pravilnik o postupcima certificiranja za nekvalificirane certifikate
CPS_{QC}	*Certification Practice Statement for Qualified Certificates*	Pravilnik o postupcima certificiranja za kvalificirane certifikate
CPS_{ROOT}	*Certification Practice Statement Fina Root CA*	Pravilnik o postupcima certificiranja za *Fina Root CA*
CRL	*Certificate Revocation List*	Lista opozvanih certifikata
CSP	*Certification Service Provider*	Davatelj usluga certificiranja
DN	*Distinguished Name*	Razlikovno ime
DR	*Disasier Recovery*	Oporavak od katastrofe
ISO	*International Standards Organization*	Međunarodna organizacija za normizaciju
LCP	*Lightweight Certificate Policy*	Opća pravila certificiranja za *lightweight* (lagane) certifikate
LDAP	*Lightweight Directory Access Protocol*	Protokol za pristup informacijskim direktorijima
LRA	*Local Registration Authority*	Lokalni registracijski ured
NCP	*Normalized Certificate Policy*	Opća pravila certificiranja za normalizirane certifikate
OCSP	*Online Certificate Status Protocol*	*Online* provjera statusa certifikata
OID	*Object Identifier*	Identifikator objekta
PIN	*Personal Identification Number*	Osobni tajni broj za aktivaciju *smart* kartice, USB tokena ili sličnog uređaja
PKCS	*Public Key Criptography Standards*	Skup normi za područje kriptografije javnog ključa

KRATICA	PUNI NAZIV	ZNAČENJE
PKI	*Public Key Infrastructure*	Infrastruktura javnog ključa
PMA	*Policy Management Authority*	Tijelo za upravljanje pravilima certificiranja
RA	*Registration Authority*	Registracijski ured
SSCD	*Secure Signature Creation Device*	Sredstvo za izradu naprednog elektroničkog potpisa (sigurno sredstvo za izradu elektroničkog potpisa)
SSL	*Secure Sockets Layer*	Kriptografski protokol za sigurnu razmjenu podataka putem Interneta
TDU	Tijelo (ili tijela) državne uprave	Tijelo (ili tijela) državne uprave
TL	*Trusted List*	Pouzdani popis davatelja usluga certificiranja koje nadziru/akreditiraju države članice.
TSA	*Time-Stamping Authority*	Davatelj usluga izdavanja vremenskog žiga
URL	*Uniform Resource Locator*	Internetska adresa određenog resursa
UTC	*Coordinated Universal Time*	Koordinirano svjetsko vrijeme

Tablica 1.6. Kratice

2. OBJAVE I ODGOVORNOSTI ZA REPOZITORIJ

2.1. Identifikacija tijela koje vodi repozitorij

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

Repozitorij se sastoji od dijela dostupnog na internetskim stranicama i dijela dostupnog preko javnog LDAP imenika, sukladno opisu iz točke 2.2. ovih Općih pravila.

2.2. Objava informacija o certificiranju

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

Na internetskim stranicama Fina PKI repozitorija objavljuju se:

- dokumenti općih pravila davanja usluga certificiranja,
- uvjeti pružanja usluga certificiranja,
- cjenik usluga certificiranja,
- obrasci za korisnike,
- Fina Root CA certifikat i certifikati subordiniranih Fina CA-ova,
- CRL Fina Root CA i CRL subordiniranih CA-ova,
- obavijesti korisnicima vezane uz davanje usluga certificiranja,
- ostale informacije vezane uz rad Fina CA-ova.

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

Fina PKI repozitorij koji je objavljen na internetskim stranicama dostupan je s adrese http://www.fina.hr/finadigicert.

U dijelu Fina PKI repozitorija dostupnog preko javnog LDAP imenika objavljuju se certifikati i CRL koje izdaju subordinirani Fina CA-ovi te je korištenjem LDAP-a omogućen dohvat pojedinog izdanog certifikata. Adrese LDAP imenika je ldap://rdc-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.

Na Fina PKI repozitoriju nisu javno objavljeni dokumenti i informacije koje predstavljaju povjerljivi dio internih postupaka certificiranja.

2.3. Vrijeme ili učestalost objavljivanja

Opća pravila, drugi Fina PKI dokumenti i ostale relevantne informacije objavljuju se po potrebi nakon odobrenja odgovornog tijela unutar davatelja usluga certificiranja.

Certifikati se u javnom imeniku objavljuju 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 2015 servisa koji je opisan u točki 4.9.10. ovih Općih pravila.

2.4. Kontrole pristupa repozitoriju

Informacije objavljene na Fina PKI repozitoriju su javno dostupne.

Izmjene sadržaja na internetskim stranicama Fina PKI repozitorija obavljaju ovlaštene osobe Fine nakon odobrenja odgovornog tijela unutar davatelja usluga certificiranja.

Izmjene sadržaja LDAP imenika mogu obavljati samo ovlaštene osobe s povjerljivim ulogama u Fina PKI.

Fina osigurava stalnu raspoloživost repozitorija u skladu s najboljim poslovnim praksama.

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. Podaci o imenu ili nazivu koji se upisuju u certifikat trebaju se odnositi na autentično ime ili naziv subjekta. Polje „*Subject*“ u certifikatu usklađeno je s preporukom IETF RFC 5280 [24] i normom X.501 [32].

Polje „*Subject*“ u certifikatima koji se izdaju za fizičke osobe sadrži ime i prezime osobe te serijski broj kojim se osigurava jedinstvenost polja „*Subject*“. U certifikatima za pripadajuće osobe polje „*Subject*“ dodatno sadrži i skraćeni naziv poslovnog subjekta i njegov identifikator.

Nazivi poslužitelja i aplikacija koji se upisuju u polje „*Subject*“ certifikata koji se izdaju za poslužitelje i aplikacije te sadržaj polja „*Subject Alternative Name*“ certifikata u skladu su s preporukom IETF RFC 5322 [26].

Nazivi poslužitelja/aplikacije mogu biti FQDN, IP adresa poslužitelja, odnosno naziv ili URL aplikacije/servisa.

Polje „Subject“ u certifikatima koji se izdaju za potpis *Trusted* liste sadrži skraćeni naziv i identifikator ministarstva zaduženog za gospodarstvo te naziv uloge unutar nacionalnog operatera koja je ovlaštena za potpis.

3.1.2. Smislenost imena

Imena u polju „*Subject*“ koja identificiraju fizičku osobu i poslovni subjekt moraju biti smislena.

U slučajevima kada se primjenjuje preporuka IETF RFC 5322 [26], imena i nazivi ne moraju biti smisleni.

3.1.3. Anonimnost korisnika ili pseudonimi

Anonimnost i pseudonimi korisnika nisu podržani.

3.1.4. Pravila tumačenja raznih oblika imena

Tumačenje oblika imena po X.501 normi [32] u Fina PKI određeno je na način prikazan u Tablici 3.1. Tumačenje imena po X.501 normi [32].

Poslovni certifikati			
Polje po X.501	**Fina RDC 2015**	**Fina RDC-TDU 2015**	**Pojašnjenje**
Country (C)	HR	HR	Dvoslovčani ISO kod države.
Organization (O)	Skraćeni naziv i identifikator poslovnog subjekta.	Skraćeni naziv i identifikator tijela državne uprave.	Naziv poslovnog subjekta ili TDU, dvoslovčani ISO kod države sjedišta poslovnog subjekta ili TDU te OIB. Za poslovne subjekte kojima nije dodijeljen OIB i nisu registrirani u Hrvatskoj umjesto OIB-a u ovo polje upisuje se jedinstveni jedanaesteroznamenkasti broj kojeg dodjeljuje Fina CA.
Organization Unit (OU)	Ne koristi se.	Naziv podorganizacijske jedinice.	Certifikati izdani od strane RDC-TDU certifikacijskog tijela podržavaju do dvije podorganizacijske jedinice unutar TDU.
Locality (L)	Mjesto sjedišta poslovnog subjekta.	Mjesto sjedišta TDU.	Mjesto sjedišta poslovnog subjekta.
Serial Number (SN)	Identifikator pripadajuće osobe (potpisnika). Za poslovne certifikate za IT opremu ili aplikacije ovo polje se ne koristi. Za certifikate za potpis *Trusted* liste vrijednost ovog polja je identifikator poslovnog subjekta.	Identifikator pripadajuće osobe (potpisnika).	Identifikator se sastoji od dvoslovčanog ISO koda države prebivališta pripadajuće osobe, OIB-a pripadajuće osobe te dva broja W i Z koji predstavljaju oznake koje imaju interno značenje za Fina PKI. Za pripadajuće osobe kojima nije dodijeljen OIB i nemaju prebivalište u Hrvatskoj umjesto OIB-a u ovo polje upisuje se jedinstveni jedanaesteroznamenkasti broj kojeg dodjeljuje Fina CA.

Poslovni certifikati			
Polje po X.501	**Fina RDC 2015**	**Fina RDC-TDU 2015**	**Pojašnjenje**
Common Name (CN)	Poslovni certifikati za pripadajuće osobe (potpisnika): - ime i prezime pripadajuće osobe (potpisnika). Certifikati za poslužitelje i aplikacije: - može biti jedinstveni naziv poslužitelja, odnosno aplikacije/servisa. Za certifikate za potpis *Trusted* liste: - naziv uloge unutar ministarstva zaduženog za gospodarstvo koja je ovlaštena za potpis *Trusted* liste.	Ime i prezime pripadajuće osobe (potpisnika).	Ime i prezime iz identifikacijske isprave pripadajuće osobe (potpisnika).
Osobni certifikati			
Polje po X.501	**Fina RDC 2015**	**Fina RDC-TDU 2015**	**Pojašnjenje**
Country (C)	HR	Nije primjenjivo.	Dvoslovčani ISO kod države.
Organization (O)	OSOBNI	Nije primjenjivo.	Interna klasifikacija osobnog certifikata.
Locality (L)	Mjesto prebivališta fizičke osobe – građanina (potpisnika).	Nije primjenjivo.	
Serial Number (SN)	Identifikator fizičke osobe – građanina (potpisnika).	Nije primjenjivo.	Identifikator se sastoji od dvoslovčanog ISO koda države prebivališta fizičke osobe - građanina, OIB-a fizičke osobe – građanina te dva broja W i Z koji predstavljaju oznake koje imaju interno značenje za Fina PKI. Za fizičke osobe – građanina kojima nije dodijeljen OIB i nemaju prebivalište u Hrvatskoj umjesto OIB-a u ovo polje upisuje se jedinstveni jedanaesteroznamenkasti broj kojeg dodjeljuje Fina CA.
Common Name (CN)	Ime i prezime fizičke osobe – građanina (potpisnika).	Nije primjenjivo.	Ime i prezime iz identifikacijske isprave fizičke osobe – građanina (potpisnika).

Tablica 3.1. Tumačenje imena po X.501 normi [32]

Tumačenje oblika imena prema preporuci IETF RFC 5322 [26] u Fina PKI primjenjuje se:

- za nazive u atributu „*Common Name*“ (CN) u slučajevima kad je subjekt certificiranja poslužitelj ili aplikacija;
- za nazive u polju certifikata „*Subject Alternative Name*“ koja imaju oblik *e-mail* adrese.

3.1.5. Jedinstvenost imena

Razlikovno ime u polju „Subject“ certifikata jedinstveno je unutar Fina PKI produkcijske hijerarhije zasnovane na Fina Root CA.

3.1.6. Prepoznavanje, potvrđivanje identiteta i uloga zaštitnog znaka

Nema odredbi.

3.2. Inicijalno utvrđivanje identiteta

Inicijalno utvrđivanje identiteta korisnika opisano je u sljedećim točkama ovog Poglavlja.

3.2.1. Metoda dokazivanja posjeda privatnog ključa

3.2.1.1. Dokazivanje posjeda privatnog ključa za QCP+ i NCP+ certifikate

Način dokazivanja posjeda privatnog ključa za QCP+ i NCP+ certifikate provodi se na jedan o sljedećih načina:

- **Generiranje ključeva na SSCD uređaju na lokaciji Fina CA**

Dokazivanje posjeda privatnog ključa, koji pripada odgovarajućem javnom ključu, sastoji se u kombinaciji procesa generiranja ključeva u SSCD uređaju i prosljeđivanja javnog ključa sustavu za izdavanje certifikata. Fina CA odgovoran je za sigurnost ovog procesa (vidi točku 6.1.1.3. ovih Općih pravila). SSCD uređaj sa subjektovim ključevima i izdanim certifikatom uz neposrednu identifikaciju dostavlja se potpisniku, odnosno skrbniku.

- **Generiranje ključeva na SSCD uređaju na lokaciji Fina LRA ili Središnjeg Fina RA**

Generiranje ključeva na lokaciji Fina LRA ili Središnjeg Fina RA provodi se na SSCD uređaju pod udaljenim *online* nadzorom Fina CA te korištenjem potpisanog PKCS#10 formata zahtjeva (vidi točku 6.1.1.3. ovih Općih pravila).

- **Generiranje ključeva na SSCD uređaju na korisničkoj lokaciji**

Dokazivanje posjeda privatnog ključa, koji pripada odgovarajućem javnom ključu, osigurava se sigurnom dostavom SSCD uređaja potpisniku, odnosno skrbniku, sigurnim načinom slanja aktivacijskih podataka za SSCD potpisniku, odnosno skrbniku, odvojenim zaštićenim kanalom, generiranjem ključeva na SSCD uređaju pod udaljenim *online* nadzorom Fina CA te korištenjem potpisanog PKCS#10 formata zahtjeva (vidi točku 6.1.1.3. ovih Općih pravila).

Ukoliko zadovolji potrebne uvjete, udaljeni *online* nadzor, umjesto Fina CA, može osiguravati vanjski ugovoreni RA.

3.2.1.2. Dokazivanje posjeda privatnog ključa za NCP i LCP certifikate

Subjektovi ključevi za normalizirani i *lightweight* certifikat (tipovi certifikata NCP i LCP iz točke 1.1.2. ovih Općih pravila) čuvaju se u adekvatnom softverskom spremniku ključa.

Pristupni i aktivacijski podaci uručuju se osobno potpisniku, odnosno skrbniku od strane Fina LRA službenika, uz prethodnu neposrednu identifikaciju potpisnika, odnosno skrbnika ili se dostavljaju adekvatnim odvojenim elektroničkim kanalima.

- **Generiranje ključeva NCP certifikata na lokaciji Fina CA**

Dokazivanje posjeda privatnog ključa, koji pripada odgovarajućem javnom ključu, sastoji se u kombinaciji procesa generiranja ključeva i prosljeđivanja javnog ključa sustavu za izdavanje certifikata. Ovaj proces osigurava i nadgleda Fina CA unutar svoje lokacije. Subjektov par ključeva i izdani certifikat dostavljaju se potpisniku, odnosno skrbniku sigurnim autentificiranim *online* kanalom u PKCS#12 formatu (vidi točku 6.1.1.4. ovih Općih pravila).

- **Generiranje ključeva LCP certifikata na lokaciji Fina CA**

Dokazivanje posjeda privatnog ključa, koji pripada odgovarajućem javnom ključu, obavlja se na jednak način kao i za NCP certifikate kada se generiranje ključa obavlja na lokaciji Fina CA.

3.2.2. Potvrda identiteta poslovnog subjekta

Minimalna potrebna provjera i potvrda identiteta poslovnog subjekta zahtjeva provjeru:

- punog naziva poslovnog subjekta;
- pravno postojanje poslovnog subjekta;
- upisa u nadležni registar;
- točnosti i cjelovitosti podataka u zahtjevu u vremenu podnošenja zahtjeva.

Identifikaciju i potvrđivanje identiteta poslovnog subjekta u Fina PKI provodi Fina RA mreža ili vanjski ugovoreni RA u skladu s uspostavljenim postupcima identificiranja i potvrđivanja identiteta poslovnog subjekta. Identifikaciju i potvrđivanje identiteta poslovnog subjekta može provoditi i Fina CA.

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

- važeći izvadak iz nadležnog registra sukladno zakonima i propisima Republike Hrvatske u smislu dokazivanja registracije poslovne djelatnosti;
- obavijest Državnog zavoda za statistiku o razvrstavanju prema NKD-u;

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

Ako je identitet osobe ovlaštene za zastupanje prilikom ovjere punomoći kojom osoba ovlaštena za zastupanje opunomoćuje drugu osobu za potpisivanje Ugovora o obavljanju usluga certificiranja za poslovne subjekte i Zahtjeva za izdavanje poslovnih certifikata utvrdio javni bilježnik tada se, umjesto preslike identifikacijske isprave osobe ovlaštene za zastupanje poslovnog subjekta, zajedno s punomoći prilaže preslika identifikacijske isprave njenog opunomoćenika.

Za poslovne subjekte osnovane izvan Republike Hrvatske potrebno je dostaviti odgovarajuću dokumentaciju izdanu od nadležnog tijela u zemlji sjedišta pravnog subjekta.

Službenik u RA mreži provjerava sadržaj priloženih dokumenata. Provjera može uključivati i upit na nacionalni OIB sustav za one podatke koje nacionalni OIB sustav sadrži.

Ako je određeni RA ili LRA već provjerio i potvrdio identitet poslovnog subjekta te RA ili LRA i poslovni subjekt već imaju poslovni odnos u kojem postoji zakonska obveza da poslovni subjekt za cijelo vrijeme trajanja poslovnog odnosa mora osigurati ažurnost i točnost podataka u RA ili LRA, tada se RA ili LRA može pouzdati u prijašnju identifikaciju poslovnog subjekta i time zadovoljiti zahtjeve za njegovu identifikaciju i potvrđivanje identiteta.

RA ili LRA osigurava prikupljanje, kontrolu i čuvanje informacija koje se odnose na identitet poslovnog subjekta.

Poslovni subjekt kazneno i materijalno odgovara za točnost i ispravnost dostavljenih podataka.

3.2.3. Potvrda identiteta fizičke osobe

Inicijalnu identifikaciju i potvrđivanje identiteta fizičke osobe u Fina PKI provodi Fina RA mreža ili vanjski ugovoreni RA u skladu s uspostavljenim postupcima neposredne identifikacije i potvrđivanja identiteta fizičke osobe.

Postupak neposredne identifikacije i utvrđivanje identiteta fizičke osobe obvezan je za podnositelje zahtjeva za izdavanje kvalificiranih, odnosno normaliziranih certifikata u postupku podnošenja zahtjeva.

Neposredna identifikacija fizičke osobe u svojstvu potpisnika obvezna je, također, u slučajevima podnošenja zahtjeva za izdavanje certifikata nakon njegova isteka te u slučajevima podnošenja zahtjeva za izdavanje certifikata nakon opoziva.

Postupak identifikacije podnositelja zahtjeva za izdavanje kvalificiranih, odnosno normaliziranih certifikata može se, također provesti preko potpisniku već izdanog kvalificiranog certifikata od strane kvalificiranog davatelja usluga izdavanja kvalificiranih certifikata registriranog u nekoj od zemalja članica EU.

Postupak neposredne identifikacije ne provodi se za podnositelje zahtjeva za izdavanje *lightweight* certifikata, već se utvrđivanje identiteta podnositelja provodi na temelju prikupljene potrebne dokumentacije i podataka te provjerom i pozivom na službeni telefonski broj podnositelja zahtjeva.

Postupak identifikacije i potvrđivanje identiteta fizičke osobe može provoditi i Fina CA.

Podaci koje dostavlja podnositelj zahtjeva moraju sadržavati najmanje ime i prezime, OIB, broj identifikacijske isprave s datumom do kada isprava vrijedi, državljanstvo i telefonski broj za kontakt. Fizička osoba kojoj nije dodijeljen OIB u zahtjevu dostavlja drugi odgovarajući identifikator dodijeljen od ovlaštenog nacionalnog tijela.

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

Službenik u RA mreži potpisom ovjerava uspješnu i pravilnu identifikaciju podnositelja zahtjeva te zaštićenim putem dostavlja podatke u Fina CA.

3.2.3.1. Prihvatljive vrste identifikacijskih isprava

Podnositelji zahtjeva za izdavanje certifikata (potpisnici, skrbnici ili opunomoćenici) moraju dokazati svoj identitet valjanom osobnom iskaznicom ili drugom javnom ispravom s fotografijom i potpisom podnositelja.

Strani podnositelj zahtjeva dokazuje svoj identitet valjanom putnom ispravom s kojom je ušao u Republiku Hrvatsku. Za odobrenje dokazivanja identiteta stranih podnositelja zahtjeva drugim vrstama identifikacijskih isprava s fotografijom izdanim od nadležnog tijela Republike Hrvatske, potrebno je kontaktirati Fina PMA.

3.2.3.2. Postupak neposredne identifikacije

Neposredna identifikacija provodi se u fizičkoj prisutnosti podnositelja zahtjeva temeljem važeće identifikacijske isprave koja je opisana u točki 3.2.3.1. ovih Općih pravila, a kojom se potvrđuje njegov identitet. Ovaj postupak provodi se na lokaciji registracijskog ureda RA mreže ili na drugoj lokaciji u prisutnosti LRA službenika, a može se provoditi i u Fina CA-u.

3.2.3.3. Postupak posredne identifikacije

Postupak posredne identifikacije podnositelja zahtjeva može se provesti jedino na način koji pruža jednaku razinu sigurnosti utvrđivanja identiteta podnositelja zahtjeva kao i postupak neposredne fizičke identifikacije.

Kao posredni dokaz potvrde identiteta podnositelja zahtjeva prihvaća se dokaz u elektroničkom obliku o provedenom postupku provjere identiteta podnositelja zahtjeva koji je proveden neposrednom fizičkom identifikacijom podnositelja zahtjeva.

Identifikacija i potvrđivanje identiteta podnositelja zahtjeva za izdavanje *lightweight* certifikata može se provesti prikupljanjem propisane dokumentacije i provjerom podataka bez neposredne identifikacije podnositelja zahtjeva.

3.2.4. Informacije o korisniku koje se ne provjeravaju

Informacije o korisniku koje se ne provjeravaju su:

- naziv podorganizacijske jedinice TDU;
- telefonski brojevi (osim za poslovni subjekt kod podnošenja zahtjeva za izdavanje *lightweight* certifikata).

Za točnost i cjelovitost gore navedenih informacija jamči i odgovara potpisnik, odnosno skrbnik.

3.2.5. Provjera identiteta ovlaštenih osoba

Službenik u RA mreži dužan je utvrditi je li osoba koja je uz pečat potpisala zahtjev ili ugovor osoba ovlaštena za zastupanje te utvrditi identitet osobe ovlaštene za zastupanje, odnosno opunomoćenika poslovnog subjekta.

Utvrđivanje identiteta osobe ovlaštene za zastupanje provodi se provjerom podataka iz dostavljene dokumentacije za utvrđivanje pravnog subjektiviteta i identiteta navedene u točki 3.2.2. i usporedbom s podacima iz preslike prihvatljive i važeće identifikacijske isprave osobe ovlaštene za zastupanje. Vrste prihvatljivih identifikacijskih isprava navedene su u točki 3.2.3.1. ovih Općih pravila.

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

3.2.6. Kriteriji interoperabilnosti

Certifikati iz opsega ovih Općih pravila koje za subjekte izdaju Fina CA-ovi namijenjeni su za korištenje u elektroničkom poslovanju unutar i izvan Republike Hrvatske. Certifikati za potpisnike zadovoljavaju odredbe europske Direktive o elektroničkim potpisima [10].

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

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

Kod obnove certifikata provodi se postupak generiranja novog para subjektovih ključeva (vidi točke 4.6. i 4.7) te se provodi postupak izdavanja novog certifikata.

Identifikacija i potvrđivanje identiteta korisnika kod obnove certifikata uz generiranje novog para ključeva provodi se na tri moguća načina.

3.3.1.1. Identifikacija i potvrđivanje identiteta kod obnove certifikata s generiranjem para ključeva na lokaciji Fine

Postupak identifikacije i potvrđivanja identiteta kod obnove certifikata s generiranjem para ključeva može se provesti na lokaciji registracijskog ureda RA mreže ili na drugom za to određenom mjestu, pri čemu identifikaciju i potvrđivanje identiteta korisnika, odnosno skrbnika provodi službenik RA mreže sukladno odredbama točke 3.2.2. i 3.2.3. ovih Općih pravila.

3.3.1.2. Identifikacija i potvrđivanje identiteta kod obnove s generiranjem para ključeva uz udaljeni nadzor Fina CA

Postupak identifikacije i potvrđivanja identiteta kod obnove certifikata s generiranjem para ključeva zaštićenim elektroničkim putem uz udaljeni nadzor Fina CA obavlja se *online* pristupom valjanim certifikatom.

Ukoliko zadovolji potrebne uvjete, udaljeni *online* nadzor umjesto Fina CA može osiguravati vanjski ugovoreni RA.

Identifikacija i potvrđivanje identiteta korisnika, odnosno skrbnika, obavlja se autentifikacijom i provjerom elektroničkog potpisa potpisnika, odnosno skrbnika pri *online* podnošenju zahtjeva za obnovom certifikata.

3.3.1.3. Identifikacija i potvrđivanje identiteta kod obnove s korisničkim generiranjem para ključeva

Postupak identifikacije i potvrđivanja identiteta kod obnove certifikata u slučajevima kada skrbnik sam generira par ključeva za komponentu IT opreme identičan je postupku kod inicijalnog izdavanja certifikata pa se i identifikacija i potvrđivanje identiteta provodi na način opisan u točki 3.2. ovih Općih pravila.

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

U slučaju da korisnik ima opozvan ili istekao certifikat tada se za izdavanje certifikata identifikacija i potvrda identiteta korisnika provodi sukladno proceduri inicijalnog utvrđivanja identiteta iz točke 3.2. ovih Općih pravila.

Po pozitivnoj identifikaciji, potvrdi identiteta i zaprimanju točnog i cjelovitog zahtjeva za izdavanje certifikata, korisniku se izdaje certifikat čiji su parametri jednaki kao i parametri certifikata na koji se zahtjev odnosi, ali s novim ključem, novim serijskim brojem certifikata, novim vremenskim periodom valjanosti i novim potpisom istog Fina CA. Novoizdani certifikat ima izmijenjen interni Finin serijski broj u razlikovnom imenu certifikata.

Za izdavanje certifikata nakon opoziva korisnik sklapa s Finom novi ugovor o pružanju usluga certificiranja.

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

Fina CA u trenutku primitka zahtjeva za opoziv ili suspenziju certifikata mora provesti postupke potvrđivanja identiteta podnositelja zahtjeva kako bi se utvrdilo radi li se o subjektu za kojeg se podnositelj zahtjeva predstavlja.

Opoziv i suspenzija certifikata opisani su u točki 4.9. ovih Općih pravila.

3.4.1. Osobno podnošenje zahtjeva za opoziv u registracijskom uredu RA mreže

Točno i cjelovito ispunjen te pravilno ovjeren i potpisan obrazac zahtjeva podnositelj zahtjeva predaje u registracijski ured RA mreže gdje se na temelju identifikacijske isprave provodi postupak neposredne identifikacije podnositelja zahtjeva opisan u točki 3.2.3.2. ovih Općih pravila.

3.4.2. Podnošenje zahtjeva za opoziv poštanskom dostavom ili preko dostavljača

Točno i cjelovito ispunjen te pravilno ovjeren i potpisan obrazac zahtjeva zajedno s preslikom identifikacijske isprave podnositelj zahtjeva poštanskom dostavom ili preko dostavljača podnositelj zahtjeva dostavlja u registracijski ured RA mreže.

Identifikacija i potvrđivanje identiteta podnositelja zahtjeva provodi se u registracijskom uredu RA mreže na temelju preslike identifikacijske isprave podnositelja zahtjeva dostavljene zajedno sa zahtjevom za opoziv.

3.4.3. Podnošenje zahtjeva za opoziv putem telefona

Fina CA ne podržava postupak opoziva telefonskim putem.

3.4.4. Podnošenje zahtjeva za opoziv putem telefaksa

Fina CA ne podržava postupak opoziva certifikata putem telefaksa.

3.4.5. Elektronička dostava zahtjeva za opoziv na *e-mail* adresu

Točno i cjelovito ispunjen obrazac zahtjeva potpisan naprednim elektroničkim potpisom podnositelj zahtjeva dostavlja elektroničkim putem na adresu elektroničke pošte: info.rdc@fina.hr.

Identifikacija i potvrđivanje identiteta podnositelja zahtjeva provodi se verifikacijom i validacijom podataka naprednog elektroničkog potpisa podnositelja zahtjeva.

3.4.6. Osobno podnošenje zahtjeva za suspenziju u registracijskom uredu RA mreže

Točno i cjelovito ispunjen te pravilno ovjeren i potpisan obrazac zahtjeva podnositelj zahtjeva predaje u registracijski ured RA mreže gdje se na temelju identifikacijske isprave provodi

postupak neposredne identifikacije podnositelja zahtjeva opisan u točki 3.2.3.2. ovih Općih pravila.

3.4.7. Podnošenje zahtjeva za suspenziju poštanskom dostavom ili preko dostavljača

Točno i cjelovito ispunjen te pravilno ovjeren i potpisan obrazac zahtjeva za suspenziju, zajedno s preslikom identifikacijske isprave podnositelja zahtjeva, poštanskom dostavom ili preko dostavljača podnositelj zahtjeva dostavlja na adresu registracijskog ureda u RA mreži.

Identifikacija i potvrđivanje identiteta podnositelja zahtjeva provodi se u registracijskom uredu RA mreže na temelju preslike identifikacijske isprave podnositelja zahtjeva dostavljene zajedno sa zahtjevom za opoziv.

3.4.8. Podnošenje zahtjeva za suspenziju putem telefona

Telefonski zahtjev za suspenziju certifikata provodi se pozivom Fininom Centru za odnose s korisnicima u uredovno vrijeme Centra koje je objavljeno na internetskim stranicama http://www.fina.hr/finadigicert.

Ukoliko je zahtjev za inicijalno izdavanje certifikata bio podnesen u vanjskom ugovorenom RA tada se telefonski zahtjev za suspenziju certifikata provodi pozivom službe za korisnike vanjskog ugovorenog RA u uredovno vrijeme službe.

U slučaju podnošenja zahtjeva za suspenzijom certifikata telefonskim putem ovlašteni službenik provodi postupak identifikacije i potvrđivanja identiteta podnositelja zahtjeva na temelju upita i usporedbe odgovora sa zapisima pohranjenim u RA sustavu. Podaci koji se pritom provjeravaju su podaci povezani s certifikatom čija se suspenzija zahtijeva te osobni podaci potpisnika/skrbnika, odnosno osobe ovlaštene za zastupanje.

3.4.9. Podnošenje zahtjeva za suspenziju putem telefaksa

Točno i cjelovito ispunjen te pravilno ovjeren i potpisan obrazac zahtjeva za suspenziju, zajedno s preslikom identifikacijske isprave podnositelja zahtjeva, podnositelj zahtjeva može podnijeti na broj telefaksa +385-1-6304-081.

Identifikacija i potvrđivanje identiteta podnositelja zahtjeva provodi se na temelju preslike identifikacijske isprave podnositelja zahtjeva dostavljene telefaksom zajedno sa zahtjevom za suspenziju.

3.4.10. Elektronička dostava zahtjeva za suspenziju na *e-mail* adresu

Točno i cjelovito ispunjen obrazac zahtjeva podnositelj zahtjeva dostavlja elektroničkom poštom na adresu: info.rdc@fina.hr.

Identifikacija i potvrđivanje identiteta podnositelja zahtjeva provodi se usporedbom podataka u zahtjevu s podacima pohranjenim u RA sustavu. Podaci koji se pritom provjeravaju su

podaci povezani s certifikatom čija se suspenzija zahtijeva te osobni podaci potpisnika/skrbnika, odnosno osobe ovlaštene za zastupanje.

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 mogu podnijeti fizičke osobe – građani ili poslovni subjekti, osim ako im propisi, odnosno akti donijeti temeljem propisa isto priječe.

4.1.2. Proces prijave korisnika s podnošenjem zahtjeva za izdavanje certifikata i odgovornosti

Fina CA može zaprimati zahtjeve za izdavanje certifikata te provoditi identifikaciju i potvrđivanje identiteta pri registraciji korisnika. Fina CA delegira navedene poslove registracijskim uredima u Fina RA mreži i vanjskim RA-ovima s kojima je Fina sklopila odgovarajući ugovor o pružanju usluga. Odgovornost vanjskog RA za propuste u obavljanju ugovorenih usluga regulirana je ugovorom sklopljenim s Finom. Fina RA mreža ili vanjski ugovoreni RA može odrediti jednog ili više LRA službenika koji će provoditi identifikaciju i potvrđivanja identiteta u skladu s ovim Općim pravilima.

4.1.2.1. Proces podnošenja zahtjeva za izdavanje certifikata

Zahtjev za izdavanje certifikata mora biti potpun, točan i cjelovit te mora biti potpisan, čime se potvrđuje istinitost podataka u zahtjevu.

Zahtjev za izdavanje osobnih certifikata potpisuje fizička osoba – građanin.

Zahtjev za izdavanje Fina RDC 2015 poslovnih certifikata ili Fina RDC-TDU 2015 certifikata potpisuje pripadajuća osoba, odnosno skrbnik, a zahtjev dodatno uz pečat potpisuje osoba ovlaštena za zastupanje poslovnog subjekta.

Zahtjev za izdavanje Fina RDC 2015 poslovnih certifikata ili Fina RDC-TDU 2015 certifikata, uz pečat, može potpisati i fizička osoba koju poslovni subjekt ovjerenom posebnom punomoći ovlasti za potpisivanje zahtjeva, odnosno ugovora.

Zahtjev za izdavanje certifikata može se predati i u elektroničkom obliku. U slučaju predaje zahtjeva u elektroničkom obliku zahtjev se potpisuje naprednim elektroničkim potpisom.

Registracija korisnika 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 koji podnose zahtjev za izdavanje certifikata 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.

Ugovor o obavljanju usluga certificiranja može se sklopiti i u elektroničkom obliku. U slučaju sklapanja ugovora u elektroničkom obliku ugovor se potpisuje naprednim elektroničkim potpisom.

Prije davanja usluga certificiranja iz opsega ovih Općih pravila pojedino tijelo državne uprave ugovara poslovni odnos s Finom zaključivanjem posebnog ugovora o obavljanju usluga certificiranja.

Sklapanjem ugovora korisnici prihvaćaju sljedeće odgovornosti i obveze u procesu podnošenja zahtjeva za izdavanje certifikata:

- zahtjev za uslugu certificiranja treba biti ispunjen točno i cjelovito te pravilno ovjeren i potpisan;
- dostavljena dokumentacija potrebna za registraciju korisnika i izdavanje certifikata treba biti točna i cjelovita te valjana u trenutku podnošenja zahtjeva;
- potpisnik, odnosno skrbnik, kazneno i materijalno odgovara za točnost i ispravnost dostavljenih podataka o sebi;
- osoba ovlaštena za zastupanje poslovnog subjekta, odnosno poslovni subjekt kazneno i materijalno odgovara za točnost i ispravnost dostavljenih podataka o sebi, poslovnom subjektu, pripadajućoj osobi ili drugom subjektu certificiranja;
- korisnik, potpisnik, odnosno skrbnik, pristaju da Fina PKI koristi i obrađuje podatke sukladno propisima te izjavama i potvrdama iz zahtjeva za izdavanja certifikata te je suglasan da je Fina ovlaštena čuvati podatke u najmanje zakonom propisanom trajanju od 10 godina od dana isteka zadnjeg obnovljenog certifikata za isti subjekt certificiranja, a može ih čuvati i duže ako tako utvrdi u svojim pravilima, odnosno postupcima.

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

Obaveze i odgovornosti Fina CA navedene su u Poglavlju 9.6.1. ovih Općih pravila.

4.2. Obrada zahtjeva za izdavanje certifikata

4.2.1. Obavljanje identifikacije i potvrđivanje identiteta

Identifikacija i potvrđivanje identiteta korisnika provodi se sukladno Poglavlju 3. ovih Općih pravila.

4.2.2. Odobravanje ili odbijanje zahtjeva za izdavanje certifikata

Odobravanje ili odbijanje zahtjeva za uslugu izdavanja certifikata provodi registracijski ured RA mreže u kojem je korisnik podnio zahtjev. Ukoliko registracijski ured RA mreže odbije zahtjev za izdavanje certifikata, dužan je korisnika obavijestiti o odbijanju i razlozima odbijanja zahtjeva.

Svi zahtjevi za izdavanje certifikata podložni su pregledu, odobrenju i prihvatu od strane Fina CA.

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 primitka zahtjeva za izdavanje certifikata, provedenih svih procesa provjere podataka i nakon odobrenja zahtjeva.

4.3.1. Radnje CA tijekom izdavanja certifikata

Tijekom procesa izdavanja certifikata Fina CA:

- provjerava valjanost elektroničkog potpisa registracijskog ureda RA mreže u dostavljenom odobrenom zahtjevu;
- generira se par subjektovih ključeva sukladno točki 6.1.1.;
- izrađuje zahtijevani certifikat;
- objavljuje subjektov certifikat na javnom imeniku ukoliko je korisnik dozvolio objavu;
- čini certifikat dostupnim potpisniku, odnosno skrbniku u svrhu njegova prihvaćanja.

Opis postupaka Fina CA tijekom izdavanja certifikata opisan je u pripadajućem CPS_{QC} [36], odnosno CPS_{NQC} [37] dokumentu.

4.3.2. Obavještavanje korisnika od strane CA o izdavanju certifikata

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

Ukoliko potpisnik, odnosno skrbnik preuzima certifikat *online*, tada je isti obaviješten o izdavanju certifikata od strane Fina CA u tijeku samog *online* postupka preuzimanja certifikata.

Ukoliko potpisnik, odnosno skrbnik osobno u RA mreži preuzima ključeve i certifikat na SSCD uređaju, tada je isti obaviješten o izdavanju certifikata od strane službenika u RA mreži.

4.4. Prihvaćanje certifikata

Prihvaćanje certifikata od strane potpisnika preduvjet je da potpisnik može rabiti certifikat.

Prihvaćanje certifikata od strane skrbnika preduvjet je da IT oprema može rabiti poslovni certifikat za IT opremu.

Prihvaćajući certifikat potpisnik, odnosno skrbnik 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

Po obavještavanju potpisnika, odnosno skrbnika o izdavanju certifikata potpisnik, odnosno skrbnik može preuzeti certifikat, ovisno o načinu njegova izdavanja, na dva načina:

- u registracijskom uredu RA mreže zajedno s generiranim korisničkim ključevima na SSCD uređaju;
- sigurnim autentificiranim *online* kanalom.

Potpisnik, odnosno skrbnik dužan je tijekom ili neposredno po obavljenom preuzimanju certifikata provesti provjeru sadržaja certifikata sukladno uputama dobivenim od Fina CA. Ukoliko ne prihvaća bilo koji dio sadržaja certifikata, potpisnik, odnosno skrbnik treba odbiti prihvaćanje certifikata, odmah o tome obavijestiti Fina CA i pritom navesti razloge neprihvaćanja istog. Fina CA će po primitku obavijesti provesti opoziv, odnosno suspenziju navedenog certifikata sukladno točki 4.9. ovih Općih pravila. Ukoliko je provedena suspenzija certifikata, Fina će, nakon identifikacije potpisnika, odnosno skrbnika u roku iz točke 4.9.16. opozvati certifikat sukladno točki 4.9.3. te omogućiti izdavanje novog certifikata s potrebnim izmjenama, a na temelju zahtjeva za izdavanje certifikata.

Smatra se da je potpisnik, odnosno skrbnik prihvatio certifikat u trenutku prvog korištenja certifikata.

Ukoliko potpisnik, odnosno skrbnik u roku od osam dana od preuzimanja certifikata ni jednom nije koristio izdani certifikat i u tom roku nije odbio prihvatiti certifikat, smatra se da je potpisnik, odnosno skrbnik certifikat prihvatio.

4.4.2. Objava izdanog certifikata od strane CA

Ukoliko je potpisnik, odnosno skrbnik odobrio javnu objavu certifikata Fina CA objavljuje izdani korisnikov certifikat u javnom imeniku.

4.4.3. Obavještavanje drugih strana od strane CA o izdavanju certifikata

Podrazumijeva se da su druge strane obaviještene o izdavanju certifikata njegovom objavom u javnom imeniku. Fina CA ni na koji drugi način ne obavještava druge strane o izdavanju certifikata. Ukoliko potpisnik, odnosno skrbnik nije odobrio javnu objavu certifikata, on preuzima obavezu da, ukoliko je to potrebno, sam obavijesti druge strane o izdanom certifikatu (npr. dostavom certifikata drugoj strani).

4.5. Par ključeva i korištenje certifikata

4.5.1. Korištenje privatnog ključa i certifikata od strane korisnika

Potpisivanjem ugovora i u skladu s propisima iz ovih Općih pravila, poslovni subjekti, potpisnik, odnosno skrbnik obvezuju se:

- na korištenje privatnog ključa i pripadajućeg certifikata samo u svrhe propisane ovim Općim pravilima;
- na korištenje privatnog ključa i pripadajućeg certifikata samo tijekom perioda valjanosti certifikata, odnosno da ne koriste privatni ključ i certifikat nakon njegova isteka, opoziva ili tijekom suspenzije;
- da od trenutka kad je privatni ključ u jedinstvenom posjedu potpisnika, odnosno skrbnika štite privatni ključ i njegove kopije (ukoliko je njihova izrada dozvoljena i moguća) od krađe, gubitka, izmjena, kompromitiranja i neovlaštene uporabe;
- na čuvanje aktivacijskih podatka privatnog ključa na zaštićenom mjestu odvojenom od privatnog ključa;
- na obavještavanje Fina CA i zahtijevanje suspenzije ili opoziva certifikata u slučajevima:
  - da je privatni ključ potpisnika, odnosno komponente IT opreme izgubljen, ukraden ili postoji sumnja u bilo kakvo kompromitiranje privatnog ključa;
  - kada potpisnik, odnosno skrbnik više nije u jedinstvenom posjedu privatnog ključa, tj. kada se sumnja u kompromitiranost aktivacijskih podataka;
  - da su podaci sadržani u certifikatu netočni.

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:

- koristiti certifikat isključivo u svrhe propisane u točki 1.4. ovih Općih pravila;
- obaviti provjeru isteka certifikata;
- obaviti provjeru statusa certifikata u kojeg namjerava ostvariti pouzdanje;
- provesti provjeru certifikata prema postupcima za validaciju certifikacijske staze;
- provjeriti da su svi podaci o identitetu subjekta u certifikatu ispravno prikazani aplikacijom u koju se može pouzdati;
- u slučaju verificiranja elektroničkog potpisa, provjeriti da je elektronički potpis izrađen privatnim ključem koji odgovara javnom ključu u certifikatu za vrijeme perioda valjanosti certifikata.

Pouzdajuća strana ne smije ostvariti pouzdanje u istekli, odnosno opozvani ili suspendirani certifikat. Pouzdanjem u istekli, opozvani ili suspendirani certifikat pouzdajuća strana gubi sva jamstva dobivena od Fine kao davatelja usluge certificiranja.

4.6. Obnova certifikata

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

Postupak 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

4.7.1. Razlozi za obnovu certifikata uz generiranje novog para ključeva

Obnova certifikata uz generiranje novog para ključeva provodi se ukoliko korisniku uskoro ističe certifikat, a korisnik ima namjeru i dalje koristiti uslugu. Certifikat se na ovaj način može obnoviti ako su zadovoljeni svi sljedeći uvjeti:

- certifikatu nije istekla valjanost;
- certifikat nije opozvan ili suspendiran;
- certifikat ističe kroz period kraći od 45 dana;
- podaci o subjektu i drugi atributi sadržani u certifikatu su točni i cjeloviti u trenutku traženja obnove certifikata.

Oporavak certifikata predstavlja izdavanje novog certifikata čiji su parametri jednaki kao i parametri certifikata na koji se zahtjev odnosi, ali s novim ključem, novim serijskim brojem certifikata, novim vremenskim periodom valjanosti i novim potpisom istog Fina CA, a provodi se prije nastupanja rokova za obnovu certifikata. Provodi se u slučaju kvara na kriptografskom uređaju, brisanja ili uništenja privatnog ključa korisnika ili kada korisnik iz nekog drugog razloga ne može koristiti privatni ključ koji je povezan s javnim ključem u certifikatu.

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

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

Ukoliko je zahtjev za oporavak certifikata opravdan Fina CA će opozvati certifikat čiji se oporavak traži te će izdati novi certifikat s istim razlikovnim imenom (i istim internim Fininim serijskim brojem u razlikovnom imenu).

Izdavanje certifikata nakon isteka predstavlja izdavanje novog certifikata čiji su parametri jednaki kao i parametri certifikata na koji se zahtjev odnosi, ali s novim ključem, novim serijskim brojem certifikata, novim vremenskim periodom valjanosti i novim potpisom istog Fina CA. Izdavanje certifikata nakon isteka ne smatra se obnovom postojećeg isteklog certifikata.

Ovisno roku u kojem se provodi izdavanje certifikata na kriptografskim uređajima, novoizdani certifikat može imati isti ili izmijenjeni interni Finin serijski broj u razlikovnom imenu kao i korisnički certifikat kojem je istekao period valjanosti.

Ako se izdavanje certifikata provodi u roku do 30 dana nakon isteka certifikata interni Finin serijski broj u razlikovnom imenu certifikata ostaje isti ukoliko se izdavanje certifikata provodi na istom kriptografskom uređaju na kojem se nalazio istekao certifikat. U tu svrhu korisnik mora u Fina LRA registracijskli ured osobno dostaviti kriptografski uređaj na kojem se nalazi istekao certifikat.

Ako se izdavanje certifikata provodi nakon 30 dana od datuma isteka certifikata tada se mijenja serijski broj u razlikovnom imenu certifikata.

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

U postupku izdavanja certifikata nakon isteka perioda valjanosti osobnog ili poslovnog certifikata koji se izdaje na SSCD (Fina e-kartica ili USB token) podnositelj zahtjeva obvezno dostavlja dokumentaciju kao za inicijalno izdavanje certifikata.

4.7.2. Tko može zatražiti certificiranje novog javnog ključa

Potpisnik, odnosno skrbnik, je ovlašten za podnošenje zahtjeva za obnovu, odnosno oporavak pripadajućih certifikata.

4.7.3. Obrada zahtjeva za obnovu certifikata uz generiranje novog para ključeva

Fina PKI podržava sljedeće načine obrade zahtjeva za obnovu certifikata s novim parom ključeva ovisno o tome provodi li se generiranje novog para ključeva na lokaciji Fina CA, lokaciji Središnjeg Fina RA, na lokaciji Fina LRA registracijskog ureda, na korisničkoj lokaciji pod udaljenim nadzorom Fina CA, odnosno vanjskog ugovorenog RA ili generiranje novog para ključeva na korisničkoj lokaciji provodi skrbnik za certifikat za komponentu IT opreme.

U slučaju da se obnova certifikata s generiranjem novog para ključeva provodi na lokaciji Fina CA, Središnjeg RA ili na lokaciji Fina LRA, nužno je provesti sljedeće:

- Potpisnik, odnosno skrbnik u RA mreži ili na drugom za to određenom mjestu predaje zahtjev za obnovu certifikata uz pravilnu identifikaciju sukladno točki 3.3.1.1.;
- Službenik u RA mreži provodi odobravanje ili odbijanje zahtjeva sukladno točki 4.2.2. ovih Općih pravila;
- Fina CA obavlja izdavanje certifikata sukladno točki 4.3.1. ovih Općih pravila.

U slučaju da se obnova certifikata s generiranjem novog para ključeva provodi pod udaljenim nadzorom Fina CA, odnosno vanjskog ugovorenog RA nužno je provesti sljedeće:

- Potpisnik, odnosno skrbnik se s valjanim certifikatom i aktivacijskim podacima spaja na zaštićeni *online* servis Fine, odnosno vanjskog ugovorenog RA;
- Potpisnik, odnosno skrbnik preko *online* servisa provjerava podatke o važećem certifikatu, a koji će biti sadržani i u novom certifikatu;
- ukoliko su podaci o važećem certifikatu točni i cjeloviti u trenutku obnove certifikata potpisnik, odnosno skrbnik može zahtijevati njegovu obnovu na način da preko *online* servisa kreira zahtjev za obnovu certifikata, elektronički ga potpiše trenutno važećim certifikatom te ga proslijedi u Fina CA na daljnju provjeru i obradu;
- uz udaljeni nadzor potpisnik, odnosno skrbnik inicira generiranje novog para ključeva te novi javni ključ prosljeđuje na certificiranje u Fina CA;
- potpisnik *online* servisom preuzima novi certifikat.

U slučaju da obnovu certifikata s generiranjem novog para ključeva provodi skrbnik za komponentu IT opreme na korisničkoj lokaciji potrebno je slijediti pravila za inicijalno izdavanje certifikata za komponentu IT opreme opisana u točkama 3.2., 4.1., 4.2., 4.3. i 4.4. ovih Općih pravila.

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

Fina CA ili središnji Fina RA tijekom mjeseca koji prethodi mjesecu u kojem ističe certifikat obavještava potpisnika, odnosno skrbnika o skorom isteku certifikata te ga poziva na obnovu certifikata uz generiranje novog para ključeva.

Pri izdavanju certifikata u procesu obnove certifikata uz generiranje novog para ključeva provode se isti postupci za obavještavanje navedeni u točki 4.3.2. ovih Općih pravila.

4.7.5. Provedba prihvaćanja obnovljenog certifikata s generiranim novim parom ključeva

Provedba prihvaćanja obnovljenog certifikata s generiranim novim parom ključeva provodi se sukladno točki 4.4.1. ovih Općih pravila.

4.7.6. Objavljivanje certifikata po obnovi s generiranjem novog para ključeva

Objavljivanje certifikata po obnovi s generiranjem novog para ključeva provodi se na način opisan u točki 4.4.2. ovih Općih pravila.

4.7.7. Obavještavanje drugih strana o obnovi certifikata s generiranim parom ključeva

Obavještavanje drugih strana o obnovi certifikata s generiranim novim parom ključeva provodi se na način opisan u točki 4.4.3. ovih Općih pravila.

4.8. Izmjene unutar certifikata

Potpisnici i skrbnici imaju obvezu informiranja Fina PKI o promjeni podataka koji ulaze u sadržaj certifikata u roku od dva dana kako je propisano Zakonom o elektroničkom potpisu [1], [2] i [3] te zatražiti izmjene podataka u certifikatu.

Fina CA može omogućiti izmjenu podataka u certifikatu samo za certifikat koji nije opozvan, suspendiran ili nije istekao.

4.8.1. Razlozi za izmjene unutar certifikata

U slučaju da je certifikat izdan kao osobni ili poslovni certifikat kojima je potpisnik fizička osoba, odnosno pripadajuća osoba poslovnog subjekta razlozi za izmjene unutar certifikata mogu biti promjene:

- imena ili prezimena potpisnika;
- naziva poslovnog subjekta;
- izmjene identifikatora poslovnog subjekta;
- podataka o mjestu prebivališta fizičke osobe ili sjedišta poslovnog subjekta;
- *e-mail* adrese, za certifikate koji sadrže e-mail adresu u Subject alternative name ekstenziji certifikata.

U slučaju da je certifikat izdan kao poslovni certifikat za IT opremu, razlozi za izmjene unutar certifikata mogu biti promjene:

- naziva poslužitelja ili aplikacije/servisa;
- naziva uloge ovlaštene za potpis *Trusted liste*;
- naziva poslovnog subjekta;
- podataka o mjestu sjedišta poslovnog subjekta;
- *e-mail* adrese;
- sadržaja ekstenzije certifikata.

4.8.2. Tko može zatražiti izmjene unutar certifikata

Izmjene unutar certifikata može zatražiti potpisnik, odnosno skrbnik.

4.8.3. Obrada zahtjeva za izmjenama unutar certifikata

Potpisnik, odnosno skrbnik zahtjev za izmjene unutar certifikata podnosi u registracijski ured RA mreže i dostavlja dokumentaciju određenu u točki 3.2. ovih Općih pravila kojom dokazuje novonastale izmjene.

Izmjene unutar certifikata provode se opozivanjem postojećeg certifikata i izdavanjem novog certifikata s novim parom ključeva te izmijenjenim podacima u certifikatu i novim periodom valjanosti certifikata. Izdavanje novog certifikata obavlja se sukladno točkama 4.2., 4.3. i 4.4. ovih Općih pravila.

4.8.4. Obavještavanje korisnika o izdavanju izmijenjenog certifikata

Pri izdavanju certifikata u procesu izmjene certifikata provode se isti postupci za obavještavanje navedeni u 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

Certifikati se moraju opozvati zbog sljedećih razloga:

- ako neka od informacija sadržanih u certifikatu postane netočna;
- ako se pojavi osnovana sumnja da je privatni ključ kompromitiran ili ako dođe do kompromitiranja privatnog ključa;
- u slučaju gubitka ili trajne nedostupnosti privatnog ključa;
- ako se pojavi osnovana sumnja da privatni ključ ili aktivacijski podaci nisu više u jedinstvenom posjedu potpisnika, odnosno skrbnika ili ako dođe do otuđenja privatnog ključa ili aktivacijskih podataka;
- ako prestane odnos koji je bio razlog da se potpisniku izda certifikat kojim će kao pripadajuća osoba djelovati u ime fizičke ili pravne osobe;
- ako Fina CA smatra da certifikat nije izdan sukladno zahtjevu ili navodima iz ovih Općih pravila;
- u slučaju otkaza ugovora o obavljanju usluge certificiranja, od strane korisnika.

Fina CA može opozvati certifikat ako korisnik, potpisnik ili skrbnik, ne izvršavaju svoje obveze u skladu s ovim Općim pravilima i potpisanim ugovorima. Fina CA može opozvati certifikat i temeljem autentificirane obavijesti treće strane, uz prethodnu provjeru navoda, ili temeljem autenticirane službene obavijesti nadležnog tijela.

4.9.2. Tko može tražiti opoziv

Potpisnici su ovlašteni za podnošenje zahtjeva za opoziv pripadajućih osobnih certifikata.

Zahtjev za opoziv poslovnih certifikata izdanih fizičkim osobama, poslovnih certifikata za IT opremu te certifikata za TDU može podnijeti potpisnik, odnosno skrbnik ili osoba ovlaštena za zastupanje poslovnog subjekta, a uvijek ga potpisuje osoba ovlaštena za zastupanje poslovnog subjekta.

RA mreža može uputiti zahtjev za opoziv certifikata u svoje vlastito ime.

Fina CA može opozvati bilo koji izdani certifikat uz odobrenje ovlaštene osobe u Fina PKI.

4.9.3. Procedura za zahtjev za opozivom

Zahtjev za opoziv certifikata u obliku obrasca dostupan je na internetskim stranicama Fina PKI repozitorija iz točke 2.2. Općih pravila. 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 u Fina PKI na jedan od sljedećih navedenih 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 na e-mail adresu.

Fina CA na osnovu točnog i cjelovito ispunjenog i potpisanog zahtjeva za opoziv, opoziva certifikat, objavljuje CRL i o tome obavještava potpisnika, odnosno skrbnika te, ukoliko je to primjenjivo, poslovni subjekt s kojim je potpisnik ili skrbnik povezan.

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 CA opoziva certifikat u najkraćem razumnom roku, a najkasnije u roku od 24 sata od primitka zahtjeva za opoziv.

Fina CA ili drugi ovlašteni službenici Fina PKI mogu suspendirati certifikat prije njegova opoziva. Razlozi suspenzije su navedeni u točki 4.9.13.

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

Svi zahtjevi za opoziv i dokumentacija u vezi s postupcima koje je poduzeo Fina CA se arhiviraju.

4.9.6. Zahtjevi za provjeru opoziva za pouzdajuće strane

Pouzdanje u opozvan ili suspendiran certifikat može imati osobnu ili poslovnu štetu za pouzdajuću stranu. Zbog toga, prije ostvarenja pouzdavanja u certifikat, pouzdajuća strana mora provesti provjeru statusa certifikata u cilju utvrđivanja njegove opozvanosti ili suspenzije u skladu s metodama i postupcima koji su navedeni u točki 4.5.2. ovih Općih pravila. Ako je pouzdajućoj strani u danom trenutku nemoguće 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 također svakih šest sati.

4.9.8. Maksimalno kašnjenje za CRL

Nakon opoziva, suspenzije i reaktivacije certifikata Fina CA promptno ažurira podatkovnu osnovicu certifikata i CRL. Maksimalno kašnjenje CRL od trenutka njenog izdavanja do trenutka objave u redovitim uvjetima iznosi do dvije minute.

4.9.9. *Online* dostupnost provjere opozvanih certifikata/statusa 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 OCSP 2015 servisa 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 opozvanih certifikata

Za *online* preuzimanje CRL, pouzdajuće strane moraju imati pristup internetu te koristiti internetske preglednike ili aplikacije koje su u mogućnosti preuzeti CRL s internetskih adresa i protokolima navedenim u točki 4.10.1. ovih Općih pravila.

4.9.11. Drugi dostupni načini objave opozvanih certifikata

Nije podržano.

4.9.12. Posebni zahtjevi za obnovu certifikata uz generiranje novog para ključeva

Nema zahtjeva.

4.9.13. Razlozi za suspenziju

Certifikat može biti postavljen u status suspenzije u slučajevima:

- kada korisnik, potpisnik ili skrbnik, zbog sumnji navedenih u točki 4.9.1. traži suspenziju certifikata do potvrde ili opovrgavanja tih sumnji (posljedično: opoziv, odnosno reaktivacija certifikata);
- privremeno do opoziva koji je zatražen iz razloga navedenih u točki 4.9.1., a za vrijeme dok Fina CA ili RA mreža provode sve potrebne provjere nužne za opoziv certifikata, odnosno do dostave potrebne dokumentacije za opoziv u registracijski ured RA mreže;

- neizvršenja ugovornih obveza od strane korisnika, a koje se odnose na plaćanje pruženih usluga.

4.9.14. Tko može tražiti suspenziju

Potpisnici su ovlašteni za podnošenje zahtjeva za suspenziju pripadajućih osobnih certifikata.

Zahtjev za suspenziju poslovnih certifikata izdanih fizičkim osobama, poslovnih certifikata za IT opremu te certifikata za TDU može podnijeti potpisnik, odnosno skrbnik ili osoba ovlaštena za zastupanje poslovnog subjekta.

RA mreža može uputiti zahtjev za suspenziju certifikata u svoje vlastito ime.

Fina CA može suspendirati bilo koji izdani certifikata uz odobrenje ovlaštene osobe u Fina PKI.

Potpisnici su ovlašteni za podnošenje zahtjeva za reaktivaciju pripadajućih osobnih certifikata.

Zahtjev za reaktivaciju poslovnih certifikata izdanih fizičkim osobama, poslovnih certifikata za IT opremu te certifikata za TDU podnosi potpisnik, odnosno skrbnik, a zahtjev dodatno potpisuje osoba ovlaštena za zastupanje poslovnog subjekta.

4.9.15. Procedura za zahtjev za suspenziju i reaktivaciju

4.9.15.1. Procedura za zahtjev za suspenziju

Zahtjev za suspenziju certifikata dostupan je u obliku obrasca na internetskim stranicama Fina PKI repozitorija iz točke 2.2. ovih Općih pravila. 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 u Fina PKI na jedan od sljedećih navedenih načina:

- osobnom dostavom u registracijski ured RA mreže u uredovno vrijeme,
- poštanskom dostavom ili preko dostavljača na adresu registracijskog ureda u RA mreži,
- telefonskim pozivom službi za korisnike,
- putem telefaksa,
- elektroničkom dostavom zahtjeva za opoziv na e-mail adresu.

Na osnovu točnog i cjelovito ispunjenog i potpisanog zahtjeva za suspenziju, odnosno provjerom podataka podnositelja zahtjeva u slučaju podnošenja zahtjeva putem telefona, Fina CA suspendira certifikat i objavljuje CRL te o tome obavještava potpisnika, odnosno skrbnika i, ukoliko je to primjenjivo, poslovni subjekt s kojim je potpisnik ili skrbnik povezan.

Po suspenziji certifikata može se provesti njegov opoziv ili reaktivacija.

4.9.15.2. Procedura za zahtjev za reaktivaciju

Za reaktivaciju certifikata mora se podnijeti zahtjev za reaktivaciju certifikata.

Zahtjev za reaktivaciju certifikata treba točno i cjelovito ispuniti, potpisati i dostaviti u Fina PKI na jedan od sljedećih navedenih 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 na e-mail adresu.

Na osnovu točnog i cjelovito ispunjenog i potpisanog zahtjeva za reaktivaciju Fina CA reaktivira certifikat i objavljuje CRL te o tome obavještava potpisnika, odnosno skrbnika i, ukoliko je to primjenjivo, poslovni subjekt s kojim je potpisnik ili skrbnik povezan.

4.9.16. Ograničenje na trajanje suspenzije

Maksimalno vrijeme u kojem certifikat može biti u stanju „suspendiran“ je 60 dana. Nakon toga Fina CA opoziva certifikat i objavljuje CRL.

4.10. Usluge statusa certifikata

4.10.1. Operativna svojstva

Usluge provjere statusa certifikata osiguravaju informaciju o statusu opozvanosti certifikata čiji vremenski period valjanosti nije istekao. Provjera statusa certifikata obavlja se korištenjem OCSP servisa ili korištenjem CRL.

Preporuka je pouzdajućim stranama da za provjeru statusa certifikata koriste Fina OCSP servis, a provjera statusa dohvatom CRL može se koristiti kao alternativna metoda provjere u slučaju nedostupnosti OCSP servisa.

Adresa Fina OCSP 2015 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 dohvaća CRL je sljedeći:

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

4.10.1.1. Adrese za dohvat CRL Fina RDC 2015 certifikata

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

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

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

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

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

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

Oznaka x u cn=CRLx označava segment CRL.

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

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

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

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

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

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

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

Oznaka x u cn=CRLx označava segment CRL.

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 maksimalno moguće vrijeme u skladu s najboljim poslovnim praksama.

Točke pristupa usluzi za provjeru valjanosti certifikata dane su u točki 4.10.1. ovih Općih pravila.

4.10.3. Opcionalna svojstva

Nema odredbi.

4.11. Kraj korištenja

Ako osoba ili poslovni subjekt 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 u Fina CA dozvoljeno je samo za nekvalificirane certifikate standardne razine sigurnosti.

4.12.1. Pravila i prakse sigurnog skladištenja i povrata privatnog ključa

Sigurno skladištenje privatnih korisničkih ključeva povezanih s nekvalificiranim certifikatima standardne razine sigurnosti provodi se na način koji osigurava da je oporavak privatnog ključa moguć samo od strane pripadajućeg potpisnika, odnosno skrbnika.

Postupci sigurnog skladištenja i povrata privatnog ključa opisani su u točki 4.12.1. CPS_{NQC} [37] dokumenta.

4.12.2. Pravila i prakse enkapsulacije ključa sesije

Ne primjenjuje se.

5. PROVJERA SUSTAVA, UPRAVLJANJA I RADNIH POSTUPAKA

Mjere fizičke zaštite, postupci koje Fina primjenjuje u zaštiti Fina PKI sustava, kao i postupci provjere sustava, upravljanja i radnih postupaka u Fina PKI interne su prirode te se njihovi detalji ne objavljuju javno. Detaljnije mjere i postupci opisani su pripadajućem CPS_{QC} [36], odnosno CPS_{NQC} [37] dokumentu te u internim dokumentima Fine koji su na raspolaganju ovlaštenim tijelima iz poglavlja 8. ovih Općih pravila.

5.1. Kontrole fizičke sigurnosti

Fina kao davatelj usluga certificiranja primjenjuje mjere fizičke zaštite sustava certificiranja s ciljem smanjenja rizika na najmanju prihvatljivu mjeru i u skladu s poslovnom politikom Fine, važećom zakonskom regulativom i međunarodnim preporukama.

5.1.1. Lokacija objekta i njegova 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.

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

5.1.2. Fizički pristup

Fizički pristup Fina CA sustavu, Fina RA sustavu, repozitoriju i arhivi omogućen je isključivo ovlaštenim zaposlenicima Fine u skladu s njihovim osnovnim, povjerljivim ulogama i ovlastima.

Svi pristupi navedenim sustavima zaštićeni su sukladno važećoj zakonskoj regulativi, internim propisima te se o svakom pristupu vodi evidencija.

Fizički pristup podacima koje prikuplja RA mreža imaju samo ovlašteni zaposlenici Fina CA i ovlašteni zaposlenici Fina RA mreže, odnosno ovlašteni zaposlenici vanjskog ugovorenog RA koji osobne podatke o fizičkim osobama i poslovne podatke o poslovnim subjektima moraju prikupljati, pohranjivati, koristiti i brisati u skladu s odgovarajućim propisima o zaštiti osobnih i poslovnih podataka.

5.1.3. Sustavi za napajanje i klimatizaciju

Uređaji i prostor u kojem se nalazi Fina CA sustav opskrbljen je neprekidnim napajanjem električnom energijom i klimatizacijom koja je dimenzionirana na način da osigura odgovarajuće radne uvjete i u slučaju prekida vanjskog napajanja.

5.1.4. Opasnost od poplave

Oprema sustava certificiranja Fine smještena je na mjestu koje je osigurano od poplave.

5.1.5. Protupožarna zaštita

Sustav certificiranja Fine zaštićen je automatskim sustavom protupožarne zaštite sukladno propisanoj i važećoj zakonskoj regulativi.

5.1.6. Pohrana medija

Sigurnosne kopije Fina PKI baza podataka redovito se obnavljaju. Mediji s podacima koje koriste Fina CA i RA sustav, arhivske ili sigurnosne kopije podataka, kopije sadržaja repozitorija te sigurnosne kopije programske opreme pohranjuju se na dvije odvojene štićene lokacije na siguran način kako bi se zaštitile od oštećenja, otuđenja ili neovlaštenog pristupa.

5.1.7. Zbrinjavanje otpada

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

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

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

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. Kontrola procedura

5.2.1. Povjerljive uloge

Upravljanje informacijskim sustavom, sustavom upravljanja certifikatima, poslovima zaštite i kontrole te poslovi pravne zaštite i nadzora djelovanja Fina PKI obavljaju se u unutar odvojenih organizacijskih dijelova Fina.

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

Povjerljive uloge uključuju uloge Službenika za sigurnost, Administratora sustava, Operatera sustava i Službenika za nadzor sustava.

5.2.2. Broj osoba potrebnih za obavljanje zadataka

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 davanja usluga iz opsega ovih Općih pravila.

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

5.2.3. Identifikacija i potvrđivanje identiteta za svaku ulogu

Identifikacija ovlaštenih zaposlenika i određivanje prava pristupa za obavljanje pojedinih zadataka u skladu s organizacijom Fina PKI provodi se kroz sigurnosne procedure i postupke provjere te se ostvaruje pomoću sigurnosnih mehanizama na sustavu.

5.2.4. Uloge koje zahtijevaju odvajanje dužnosti

Zbog sigurnosnih zahtjeva izdavanja kvalificiranih certifikata potrebno je odvajanje sljedećih dužnosti:

- Službenik za sigurnost ili RA službenik ne smiju obavljati poslove službenika za nadzor sustava;
- Administrator sustava ne smije obavljati poslove Službenika za sigurnost ili poslove Službenika za nadzor sustava.

5.3. Provjere osoblja

5.3.1. Kvalifikacije, radno iskustvo i zahtjevi za provjerom osoblja

Prije početka rada u Fina CA kandidati moraju imati odgovarajuća stručna znanja u radu s kriptografskim tehnologijama te stručna znanja iz zaštite računalnih sustava i informacijskih baza. Zaposlenici koji rade na poslovima Fina PKI ne smiju biti u radnom, odnosno poslovnom odnosu s drugim davateljima usluga certificiranja.

5.3.2. Procedure provjere primjerenosti osoblja

Prije početka rada na poslovima Fina PKI, Fina provodi odgovarajuće provjere kandidata da bi procijenila njihovu sposobnost i pouzdanost 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 ili korisničkim ulogama.

5.3.4. Učestalost i uvjeti za obnovu znanja

Fina CA osoblje kontinuirano usavršava specijalistička znanja i vještine.

Obnova znanja Fina RA mreže provodi se redovito, najmanje jednom u dvije godine.

5.3.5. Učestalost i slijed izmjene zaposlenika

Ne primjenjuje se.

5.3.6. Kazne za neovlaštene radnje

U slučaju izvođenja neovlaštene radnje ili zlonamjerne radnje koju je izvela ovlaštena osoba u Fina PKI primjenjuju se odredbe važeće zakonske regulative i internih pravilnika Fine. Takvoj osobi bit će zabranjen rad na poslovima Fina PKI.

5.3.7. Zahtjevi na vanjske suradnike

Zahtjevi za vanjske suradnike opisani su u pripadajućem CPS_{QC} [36] odnosno CPS_{NQC} [37] dokumentu te u internim dokumentima Fine.

5.3.8. Dokumentacija koja je dostupna osoblju

Svakom zaposleniku dostupna je dokumentacija potrebna za obavljanje njegovih radnih zadataka sukladno dodijeljenoj korisničkoj ili povjerljivoj ulozi i pripadnim ovlaštenjima.

5.4. Postupci s dnevnicima sustava

5.4.1. Tipovi događaja koji se zapisuju

U dnevnicima vjerodostojnih sustava zapisuju se tipovi događaja vezani uz:

- registraciju fizičke osobe i poslovnog subjekta;
- izdavanje certifikata;
- pripremu i izdavanje SSCD uređaja;
- životni ciklus i upravljanje ključevima;
- opoziv, suspenziju i reaktivaciju certifikata;
- ostale bitne elemente vezane uz rad Fina PKI.

5.4.2. Učestalost obrade dnevnika sustava

Dnevnici vjerodostojnih sustava redovito se pregledavaju. Radnje poduzete na osnovu prikupljanja dnevnika sustava moraju se dokumentirati.

5.4.3. Vremenski period pohrane dnevnika sustava

Dnevnici vjerodostojnih sustava sa zapisima iz točke 5.4.1. čuvaju se najmanje 10 godina.

5.4.4. Zaštita dnevnika sustava

Dnevnici vjerodostojnih sustava zaštićuju se mehanizmima i postupcima koji osiguravaju povjerljivost i cjelovitost dnevnika. Novi zapisi dnevnika vjerodostojnih sustava ne smiju se automatski zapisivati preko postojećih zapisa.

Tako zaštićeni dnevnici sustava su na zahtjev raspoloživi samo ovlaštenim osobama, posebice u svrhu pružanja dokaza o certifikatu i vremenskom žigu za potrebe sudskih postupaka.

5.4.5. Postupci izrade sigurnosnih kopija dnevnika sustava

Novonastali dnevnici Fina PKI sustava se kopiraju te se njihove kopije pohranjuju na lokaciji sekundarnog sustava certificiranja koji je izdvojen od sustava certificiranja u upotrebi. Kopije dnevnika sustava u odnosu na dnevnike na primarnoj produkcijskoj lokaciji Fina CA sustava zaštićuju se jednakom ili višom razinom zaštite (vidi točku 5.4.4).

5.4.6. Sustav prikupljanja dnevnika sustava (unutarnji ili vanjski)

Ovisno o vrsti podataka, dnevnici sustava na internom sustavu prikupljaju se automatski ili ih prikuplja ovlaštena osoba.

Detaljnije odredbe koje se odnose na sustav prikupljanja dnevnika sustava nalaze se u pripadajućem CPS_{QC} [36], odnosno CPS_{NQC} [37] dokumentu.

5.4.7. Obavještavanje subjekta uzročnika događaja

Obavještavanje uzročnika događaja regulirano je internim pravilima Fine.

5.4.8. Procjena ranjivosti

Rezultati analize dnevnika sustava koriste se za procjenu ranjivosti sustava.

5.5. Arhiviranje zapisa

5.5.1. Tipovi arhiviranih zapisa

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

- podaci o fizičkim osobama i poslovnim subjektima iz postupaka registracije i pripadajuća dokumentacija;
- certifikati i podaci o postupcima njihova izdavanja;
- evidencija opozvanih certifikata i podaci o postupcima opoziva, suspenzije i reaktivacije certifikata te pripadajuća dokumentacija;
- podaci i dokumentacija vezana uz SSCD uređaj;
- tehnički podaci nastali bilježenjem rada sustava certificiranja;
- drugi dokumenti Fina PKI sukladno važećim propisima.

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

5.5.2. Vremenski period arhiviranja

Svi arhivirani podaci i dokumentacija čuvaju se najmanje 10 godina.

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 mora biti provedena i za arhiviranje podataka i dokumentacije koja se prikupljaju u vanjskim ugovorenim RA-ovima.

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

5.5.4. Postupci izrade sigurnosnih kopija arhive

Sigurnosna kopija arhive Fina PKI zapisa izrađuje se u Fina PKI štićenom prostoru te se čuva na siguran način na drugoj lokaciji izdvojeno od primarnog produkcijskog sustava certificiranja.

5.5.5. Zahtjevi na zaštitu zapisa vremenskim žigom

Nema odredbi.

5.5.6. Sustav prikupljanja arhiva (unutarnji ili vanjski)

Arhivirani zapisi prikupljaju se na način koji ovisi o vrsti zapisa.

Zapisi za arhiviranje nastali u Fina CA sustavu 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 pristupa i verifikacije podataka iz arhiva

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

U slučaju zamjene Fina CA potpisnog ključa novim, Fina CA će obavijestiti sudionike Fina PKI o promjeni potpisnog ključa.

Novi certifikat Fina CA s novo generiranim javnim ključem potpisuje se privatnim ključem Fina Root CA

Novi pripadajući javni ključ biti će dostupan sudionicima Fina PKI na način na koji je to bio i prethodni Fina CA javni ključ.

5.7. Oporavak od kompromitiranja ili nepogode

5.7.1. Postupci u slučaju incidenta ili kompromitiranja

Fina PKI ima planove za očuvanje i oporavak sustava certificiranja nakon katastrofe.

Internim planovima obuhvaćeni su postupci očuvanja i oporavka sustava za slučaj nepogoda kao što su kvar opreme, ljudske pogreške, otuđenje ili kompromitiranje opreme i podataka, požar, prirodne nepogode, teroristički čin i sl.

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

5.7.2. Oštećenja u računalnim resursima, programima i/ili podacima

Planovi navedeni u točki 5.7.1. obuhvaćaju i povrat podataka te izmjenu opreme u slučaju oštećenja Fina PKI računalnih i mrežnih resursa, softvera ili podataka.

5.7.3. Postupci u slučaju kompromitiranja privatnog ključa

U slučaju kompromitiranja privatnog ključa Fina CA, pripadajući certifikat bit će opozvan.

Fina će izdati novi Fina CA certifikat.

O opozivu certifikata Fina će obavijestiti sljedeće sudionike Fina PKI:

- Fina RA mrežu i vanjske ugovorene RA;
- korisnike;
- pouzdajuće strane.

Fina će pouzdajuće strane obavijestiti putem obavijesti na internetskim stranicama repozitorija iz točke 2.2. ovih Općih pravila.

Nakon ustanovljavanja i otklanjanja uzroka koji su prouzročili kompromitiranje ključa, Finin CA čiji je certifikat opozvan će generirati novi par CA ključeva, ponovno će izdati certifikate postojećim korisnicima 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 opozvani CA certifikat.

Detaljnije odredbe, koje se odnose na postupke u slučaju kompromitiranja privatnog ključa korisnika, nalaze se u pripadajućem CPS_{QC} [36], odnosno CPS_{NQC} [37] dokumentu.

5.7.4. Mogućnost nastavka poslovanja nakon nepogode

Vidi točku 5.7.1.

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 međusobnim ugovornim obvezama.

O mogućem planiranom prestanku obavljanja usluga certificiranja Fina će obavijestiti svakog korisnika usluge, pouzdajuće strane i ministarstvo nadležno za gospodarstvo najmanje tri mjeseca prije planiranog prestanka davanja usluga certificiranja.

U slučaju prestanka davanja usluga certificiranja iz bilo kojeg razloga Fina će kod drugog davatelja usluga certificiranja osigurati nastavak davanja usluga certificiranja te će drugom davatelju usluga certificiranja dostaviti svu dokumentaciju prikupljenu u postupku registracije korisnika kao i svu dokumentaciju o izdanim certifikatima.

U slučaju da Fina iz bilo kojeg razloga nije u mogućnosti osigurati nastavak obavljanja usluga certificiranja kod drugog davatelja usluga tada će Fina opozvati sve izdane certifikate.

U slučaju prestanka obavljanja usluga certificiranja Fina će nastaviti održavati podatke korisnika koji su prikupljeni u postupku registracije te podatke nastale u radu Fina CA koji su nužni za pružanje dokaza u sudskim, upravnim i drugim postupcima u skladu s važećim odredbama zakonske regulative ili će s drugim poslovnim subjektom ugovoriti održavanje istih.

6. PROVJERA TEHNIČKE SIGURNOSTI

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, za Fina OCSP 2015 servis i za izdavanje korisničkih certifikata.

Konkretni postupci i mjere zaštite koje se poduzimaju u cilju postizanja zahtijevane razine sigurnosti interne su prirode i ne objavljuju se javno. Sigurnosni koncept Fina PKI sustava na raspolaganju je ovlaštenim tijelima iz poglavlja 8. ovih Općih pravila.

6.1. Generiranje i instalacija para ključeva

6.1.1. Generiranje para ključeva

6.1.1.1. Generiranje para Fina CA ključeva

Postupak generiranja para Fina CA ključeva provodi se formalnom ceremonijom generiranja para ključeva za Fina CA kojoj prisustvuju ovlaštene osobe s povjerljivim ulogama u Fina PKI.

Ceremoniji generiranja para ključeva FINA CA prisustvuje kvalificirani auditor koji svjedoči da je ceremonija generiranja parova ključeva Fininih CA-ova provedena u skladu s Fininom dokumentacijom, u skladu sa zahtjevima CA/Browser Forum Baseline Requirements [33] i u skladu s mjerama tehničke sigurnosti prema normama HRN ETSI/EN 319 411-2 [11].

Kriptografski algoritmi koji se koristi za generiranje ključeva kao i duljina ključeva za Fina CA odabrani su sukladno normizacijskom dokumentu ETSI TS 119 312 [15] tako da budu prikladni za cijelo vrijeme važenja CA certifikata.

Par ključeva za FINA CA generira se, uz minimalno dualnu kontrolu ovlaštenih osoba s povjerljivim ulogama u Fina PKI, u HSM modulima koji zadovoljavaju 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.

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.

Provođenje postupka ceremonije generiranja para ključeva za Fina CA snima se video kamerom.

Fina posjeduje izvješće kvalificiranog auditora koje svjedoči da je postupak generiranja parova ključeva za Fina CA proveden sukladno zahtjevima protokola.

O provedenom generiranju CA ključeva vodi se zapisnik s priloženim dnevnicima sustava.

6.1.1.2. Generiranje para ključeva za Fina OCSP 2015 servis

Generiranje para ključeva za potpis odgovora Fina OCSP servisa certifikatima koje izdaju Fina RDC 2015 i Fina RDC-TDU 2015 CA-ovi provodi se uz dualnu kontrolu ovlaštenih osoba Fina PKI u HSM-u koji zadovoljava zahtjeve iz točke 6.2.1. ovih Općih pravila, a koji je smješten u Fina PKI štićenom prostoru iz točke 5.1.1. ovih Općih pravila.

6.1.1.3. Generiranje para RA ključeva

Parovi ključeva za ovlaštene osobe Fina RA mreže moraju biti generirani na SSCD uređajima. Parove ključeva generiraju ovlaštene osobe Fina CA na lokaciji Fina CA. Svoj par ključeva na SSCD uređaju može generirati i ovlaštena osoba Fina RA mreže pod udaljenim *online* nadzorom Fin CA.

Parove ključeva za IT opremu na strani Fina RA sustava generiraju ovlaštene osobe Fina CA na opremi Fina RA.

Parove ključeva vanjskih ugovorenih RA mogu generirati ovlaštene osobe Fina CA ili vanjski RA, ukoliko vanjski RA zadovoljava uvjete za generiranje para ključeva iz ovih Općih pravila i pripadajućeg internog CPS_{QC} [36], odnosno CPS_{NQC} [37] dokumenta.

6.1.1.4. Generiranje para ključeva za QCP+ i NCP+ certifikate korisnika

Generiranje subjektovog para ključeva za QCP+ tipove certifikata usklađeno je s normom HRN ETSI/EN 319 411-2 [11], a generiranje subjektovog para ključeva za NCP+ tipove certifikata usklađeno je s normom HRN ETSI/EN 319 411-3 [12], a mogu ih generirati Fina CA, Središnji Fina RA, Fina LRA ili potpisnik, odnosno skrbnik.

Ukoliko Fina CA generira subjektov par ključeva, ključevi se generiraju na SSCD uređaju na lokaciji Fina CA.

Ukoliko par ključeva generira ovlaštena osoba Fina LRA ili Središnjeg Fina RA ključevi se generiraju na SSCD uređaju pod udaljenim nadzorom Fina CA.

Ukoliko par ključeva generira potpisnik, odnosno skrbnik, ključevi se generiraju na SSCD uređaju pod udaljenim nadzorom Fina CA. Ukoliko zadovolji potrebne uvjete, udaljeni *online* nadzor može osiguravati i vanjski ugovoreni RA. Fina CA, odnosno vanjski ugovoreni RA procesom nadzora osigurava da je par ključeva generiran isključivo na identificiranom SSCD uređaju kojeg je potpisnik, odnosno skrbnik prethodno preuzeo u RA mreži uz neposrednu identifikaciju.

6.1.1.5. Generiranje para ključeva za NCP certifikate

Generiranje korisničkog para ključeva za NCP tipove certifikata usklađeno je s normom HRN ETSI/EN 319 411-3 [12] te ih mogu generirati Fina CA ili potpisnik, odnosno skrbnik.

Ukoliko Fina CA provodi generiranje ključeva NCP certifikata, generiranje se provodi u kriptografskom modulu u svom štićenom prostoru.

Ukoliko generiranje ključeva NCP certifikata provodi potpisnik, odnosno skrbnik, generiranje se provodi u propisanoj kontroliranoj okolini na korisničkoj lokaciji. U tom slučaju Fina CA za pojedini tip NCP certifikata prihvaća parove ključeva propisane duljine i korištenih algoritama navedenih u profilima certifikata u poglavlju 7. ovih Općih pravila.

Detaljnije odredbe koje se odnose na postupke generiranja parova ključeva Fina CA, RA mreže i korisnika nalaze se u pripadajućem CPS_{QC} [36], odnosno CPS_{NQC} [37] dokumentu.

6.1.1.6. Generiranje para ključeva za LCP certifikate

Generiranje korisničkog para ključeva za LCP tipove certifikata usklađeno je s normom HRN ETSI/EN 319 411-3 [12].

Generiranje korisničkog para ključeva za LCP tip certifikata provodi Fina CA na kriptografskom modulu u svom štićenom prostoru.

6.1.2. Dostava privatnog ključa korisniku

Privatni ključ za ovlaštene osobe Fina RA mreže se osobno, uz neposrednu identifikaciju, uručuje na SSCD uređajima. Ukoliko ovlaštena osoba Fina RA mreže generira svoj par ključeva smatra se da već posjeduje privatni ključ. Privatni ključevi za IT opremu na strani Fina RA sustava generiraju se na opremi Fina RA sustava i stoga se smatra da ih Fina RA sustav već posjeduje.

Ukoliko privatne ključeve generira vanjski ugovoreni RA, smatra se da ih već posjeduje. Ukoliko Fina CA generira privatne ključeve za vanjski RA, privatni se ključevi osobno, uz neposrednu identifikaciju, uručuju skrbnicima na zaštićeni način.

Kada Fina CA ili Središnji Fina RA na SSCD uređaju generira privatni ključ za potpisnika, aplikaciju ili potpis *Trusted* liste, tada se SSCD uređaj s privatnim ključem zaštićenim kanalom dostavlja u registracijski ured RA mreže te se osobno uručuje identificiranom potpisniku, odnosno skrbniku.

Kada Fina LRA na SSCD uređaju generira privatni ključ za potpisnika, tada ovlašteni službenih Fina LRA osobno uručuje SSCD uređaj s privatnim ključem identificiranom potpisniku, odnosno skrbniku.

Ako potpisnik ili skrbnik na svojoj lokaciji pod udaljenim nadzorom Fina CA, odnosno vanjskog ugovorenog RA, generira privatni ključ na SSCD uređaju, smatra se da ga potpisnik, odnosno skrbnik, već posjeduje.

Kod izdavanja normaliziranih certifikata koji se ne izdaju na SSCD uređaj, odnosno izdavanja *lightweight* certifikata, privatni ključ subjekta Fina CA dostavlja autentificiranom potpisniku ili skrbniku zaštićenim kanalom u PKCS#12 formatu.

6.1.3. Dostava javnog ključa CA-u

Ukoliko javni ključ generira Središnji Fina RA, Fina LRA ili potpisnik/skrbnik, tada javni ključ mora biti dostavljen u Fina CA na način koji osigurava cjelovitost i izvornost javnog ključa.

Javni ključ se u Fina CA dostavlja na certificiranje na način koji sigurno povezuje potvrđeni identitet subjekta i pripadajući javni ključ koji se dostavlja. Postupci dostave koriste PKCS#10 format zahtjeva koji uključuje dokaz o posjedovanju pridruženog privatnog ključa.

Dostava javnog ključa u PKCS#10 formatu obavlja se elektroničkim putem preko sigurnog komunikacijskog kanala (npr. SSL/TLS) nakon uspješno provedene autentifikacije potpisnika, odnosno skrbnika. Potpisnik, odnosno skrbnik, može javni ključ u navedenom formatu dostaviti fizički na mediju za pohranu podataka uz neposrednu identifikaciju u registracijski ured Fina RA mreže.

6.1.4. Dostava CA javnog ključa pouzdajućim stranama

Pouzdajuće strane mogu preuzeti Fina Root CA certifikat i certifikate subordiniranih Fina CA-ova s internetskih stranica Fina PKI repozitorija iz točke 2.2. ovih Općih pravila.

Izvornost Fina Root CA certifikata osigurava se dostavom njegova sažetka pouzdanim kanalom, na zahtjev.

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

Ključevi koje upotrebljavaju Fina CA-ovi generiraju se sukladno normizacijskom dokumentu ETSI TS 119 312 [15].

Ključevi koje upotrebljava Fina OCSP 2015 servis generiraju se sukladno normizacijskom dokumentu ETSI TS 119 312 [15].

Ključevi u SSCD uređajima generiraju se sukladno normizacijskom dokumentu ETSI TS 119 312 [15].

Kod generiranja parametara javnog ključa u softverskim kriptografskim modulima (za certifikate za poslužitelje ili aplikacije/servise) skrbnik mora koristiti softverske kriptografske

module kojima je generiranje parametara RSA javnog ključa usklađeno s normama FIPS 186-2 [30] (ili novija) ili ANSI X9.31.

6.1.7. Namjene ključeva (po X.509 v3 polju uporabe ključa)

Fina CA-ovi koriste svoje privatne potpisne ključeve samo za:

- potpisivanje izdanih certifikata te odgovarajuće CRL (X.509 v3 *KeyUsage Extension*: *keyCertSign, cRLSign*).

Privatni ključevi Fina OCSP servisa koriste se samo za potpise odgovora Fina OCSP servisa.

Fina RA ključevi se koriste u RA aplikacijama za:

- napredni elektronički potpis zasnovan na kvalificiranom cerifikatu (X.509 v3 *KeyUsage Extension*: *nonRepudiation*);
- autentifikacije na RA aplikacije i elektronički potpis (X.509 v3 *KeyUsage Extension*: *digitalSignature, keyEncipherment*).

Ključevi subjekta namjeni su za:

- napredni elektronički potpis zasnovan na kvalificiranom cerifikatu (X.509 v3 *KeyUsage Extension*: *nonRepudiation*);
- elektronički potpis, autentifikaciju i enkripciju (X.509 v3 *KeyUsage Extension*: *digitalSignature, keyEncipherment*).

Ključevi za poslužitelje i aplikacije namijenjeni su za:

- elektronički potpis, autentifikaciju i enkripciju (X.509 v3 *KeyUsage Extension*: *digitalSignature, keyEncipherment*).

Ključevi za potpis *Trusted* liste namijenjeni su za:

- elektronički potpis *Trusted* liste (X.509 v3 *KeyUsage Extension*: *digitalSignature*, extKeyUsage Extension: *id-tsl-kp-tslSigning*).

6.2. Zaštita privatnog ključa i tehnike upravljanja kriptografskim modulom

6.2.1. Norme i upravljačke funkcije kriptografskog modula

Privatni ključevi za subordinirane Fina CA-ove generiraju se i štite HSM-om koji zadovoljava zahtjeve prema FIPS 140-2 [29] razina 3.

Svi ključevi za certifikate visoke razine sigurnosti generiraju se u kriptografskom modulu:

- koji zadovoljava zahtjeve prema FIPS 140-1 [28] ili FIPS 140-2 [29] razina 3 ili više ili zahtjeve primjenjenih jednako vrijednih sigurnosnih kriterija.

Svi ključevi za certifikate srednje razine sigurnosti moraju se generirati u SSCD uređaju koji zadovoljava jedan od sljedećih obrazaca zaštite sredstava za izradu naprednog elektroničkog potpisa:

- FIPS 140-1 [28] ili FIPS 140-2 [29] razina 2 ili više;
- CEN/ISSS SSCD-PP definiran dokumentom CWA 14169 [18].

Iznimno, za NCP certifikate srednje razine sigurnosti za poslužitelje i aplikacije/servise ključevi se mogu generirati u kriptografskom modulu koji zadovoljava zahtjeve prema FIPS 140-1 [28] ili FIPS 140-2 [29] razina 1 ili zahtjeve primijenjenih jednako vrijednih sigurnosnih kriterija uz primjenu dodatnih mjera fizičke i ICT sigurnosti.

U slučaju kada skrbnik generira ključeve za certifikate standardne razine sigurnosti, svi ključevi moraju se generirati u kriptografskom modulu koji zadovoljava zahtjeve prema FIPS 140-1 [28] ili FIPS 140-2 [29] razina 1 ili viša ili zahtjeve primijenjenih jednako vrijednih sigurnosnih kriterija.

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 od više osoba.

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

Upravljanje privatnim ključevima subordiniranih Fina CA-ova provodi se fizičkim pristupom HSM-u, uz autorizaciju dvije ovlaštene osobe s povjerljivim ulogama u Fina PKI.

HSM kojim se štiti privatni ključevi Fina OCSP servisa smješten je u prostoru najviše razine sigurnosti unutar Fina PKI štićenog prostora. Upravljanje privatnim ključem ključevima Fina OCSP servisa provodi se fizičkim pristupom HSM-u uz dualnu kontrolu te autorizacijom dvije ovlaštene osobe s povjerljivim ulogama u Fina PKI.

6.2.3. Sigurno skladištenje privatnog ključa (*key escrow*)

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

Sigurno skladištenje privatnih korisničkih ključeva u Fina CA dozvoljeno je samo za nekvalificirane certifikate standardne razine sigurnosti i provodi se na način koji osigurava da je oporavak privatnog ključa moguć samo od strane pripadajućeg potpisnika, odnosno skrbnika.

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 pod dualnom kontrolom ovlaštenih osoba s povjerljivim ulogama u Fina PKI. Privatni Fina CA ključ kopira se i dohvaća iz kriptografskog modula isključivo u enkriptiranom obliku. Sigurnosne kopije privatnog ključa Fina Root CA i njemu subordiniranih Fina CA-ova čuvaju se u enkriptiranom obliku na magnetskim trakama u kontroliranom broju kopija privatnog ključa u sigurnim prostorima najviše razine sigurnosti unutar Fina PKI štićenih prostora na odvojenim lokacijama.

Sigurnosne kopije privatnih ključeva Fina OCSP servisa čuvaju se u enkriptiranom obliku na magnetskim trakama u kontroliranom broju kopija privatnog ključa u sigurnom prostoru najviše razine sigurnosti unutar Fina PKI štićenih prostora na odvojenim lokacijama.

Fizički pristup sigurnosnim kopijama privatnih ključeva Fina CA-ova te sigurnosnim kopijama privatnih ključeva Fina OCSP servisa imaju isključivo ovlaštene osobe s povjerljivim ulogama u Fina PKI pod dualnom kontrolom.

Fina CA-ovi nikada ne provodi sigurnosno kopiranje korisničkih privatnih ključeva generiranih na SSCD uređajima.

Fina CA-ovi obavljaju sigurno skladištenje korisničkih privatnih ključeva samo za nekvalificirane certifikate standardne razine sigurnosti na način opisan u točki 6.2.3. ovih Općih pravila.

Ako privatni ključ nije namijenjen za napredni elektronički potpis (ne izdaje se kvalificirani certifikat za pripadajući javni ključ) tada potpisnik, odnosno skrbnik smije izraditi sigurnosnu kopiju privatnog ključa na mediju za pohranu podataka ukoliko mu je to tehnički omogućeno.

Sigurnosna kopija korisničkog privatnog ključa u odnosu na original treba biti pohranjena i zaštićena istom ili većom razinom zaštite kako bi se onemogućilo neovlašteno korištenje i eventualna zlouporaba privatnog ključa.

Poslovni subjekt, potpisnik ili skrbnik odgovoran je za zaštitu kopija korisničkog privatnog ključa te je odgovoran u slučaju njihovog neovlaštenog korištenja na isti način kao i originala, a sukladno točki 4.5.1. ovih Općih pravila.

6.2.5. Arhiviranje privatnog ključa

Privatni ključevi Fina Root CA i njemu subordiniranih Fina CA-ova ne arhiviraju se.

Privatni ključevi Fina OCSP servisa ne arhiviraju se.

Privatni ključevi korisnika ne arhiviraju se.

6.2.6. Prijenos privatnog ključa u ili iz kriptografskog modula

Ako privatni ključ Fina CA treba prenijeti iz ili u HSM, za vrijeme dok je izvan HSM-a privatni ključ je zaštićen na način koji osigurava jednaku razinu sigurnosti kao i kad se nalazi u HSM-

u. Postupak prijenosa privatnog ključa provode samo ovlaštene osobe s povjerljivim ulogama u Fina PKI, uz dualnu kontrolu.

Za prijenos privatnog ključa Fina CA-ova iz jednog HSM-a u drugi mora se osigurati da se privatni ključ prenosi samo u HSM jednake ili više razine sigurnosti u odnosu na HSM iz kojega se privatni ključ prenosi.

Prijenos privatnih ključeva Fina OCSP servisa provodi se na jednak način kao i prijenos privatnih ključeva subordiniranih Fina CA-ova.

Prijenos odgovarajućeg privatnog ključa poslovnog certifikata za IT opremu u drugi kriptografski modul dozvoljen je za certifikate izdane za poslužitelje ili aplikacije/servise.

Prijenos odgovarajućeg privatnog ključa potpisnika, za osobne i poslovne soft certifikate (NCP i LCP) definirane u točki 1.1.2. ovih Općih pravila, u drugi spremnik privatnog ključa smije izvoditi isključivo potpisnik.

U svim navedenim slučajevima u kojima je dozvoljen prijenos privatnog ključa mora se osigurati 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 prije prijenosa adekvatno enkriptira kako bi bio zaštićen dok se nalazi izvan kriptografskog modula.

6.2.7. Spremanje privatnog ključa u kriptografskom modulu

Privatni ključevi Fina Root CA ili njemu subordiniranih Fina CA-ova zaštićeni su kriptografskim modulima i mogu se koristiti jedino ako su propisno aktivirani.

Privatni ključevi za potpis odgovora Fina OCSP servisa zaštićeni su kriptografskim modulima i mogu se koristiti jedino ako su propisno aktivirani.

6.2.8. Metoda aktivacije privatnog ključa

Aktivaciju privatnih ključeva Fina CA-ova provode dvije ovlaštene osobe s povjerljivim ulogama u Fina PKI. Svaka od ovih ovlaštenih osoba za aktivaciju HSM-a upotrebljava hardversko sredstvo za aktivaciju i pripadajući tajni PIN.

Aktivacija privatnih ključeva za potpis odgovora Fina OCSP servisa provodi se na isti način kao i aktivacija privatnih ključeva Fina Root CA ili njemu subordiniranih Fina CA-ova.

Aktivaciju privatnog ključa subjekta može izvesti samo pripadajući potpisnik, odnosno skrbnik korištenjem odgovarajućih aktivacijskih podataka.

6.2.9. Metoda deaktivacije privatnog ključa

Deaktivacija privatnog ključa Fina CA-ova provodi se pod dualnom kontrolom ovlaštenih osoba s povjerljivim ulogama u Fina PKI.

Privatni ključevi subordiniranih Fina CA-ova deaktiviraju se:

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

Privatni ključevi za potpis odgovora Fina OCSP servisa deaktiviraju se na isti način kao i privatni ključevi subordiniranih Fina CA-ova.

Korisnički kriptografski moduli koji su aktivirani ne smiju biti ostavljeni bez nadzora. Nakon uporabe moraju se deaktivirati na jedan od slijedećih načina:

- raskidom veze sa SSCD uređajem ili HSM modulom;
- odjavom s operativnog sustava;
- istekom vremenskog ograničenja neaktivnosti.

6.2.10. Metoda uništavanja privatnog ključa

Postupak uništavanja privatnog ključa Fina CA-ova provodi se nakon isteka perioda njihove valjanosti, a izvodi se od strane ovlaštenih osoba s povjerljivim ulogama u Fina PKI pod minimalno dualnom kontrolom.

Uništavanje privatnog ključa Fina CA-ova provodi se na siguran način, sukladno internim Fininim dokumentima. Postupak uništavanja privatnih ključeva Fina CA-ova osigurava da se nakon uništavanja privatni ključevi ni na koji način ne mogu oporaviti ili ponovno koristiti.

Uništenje privatnih ključeva za Fina OCSP servis provodi se na isti način kao i uništenje privatnih ključeva subordiniranih Fina CA-ova.

6.2.11. Ocjena kriptografskog modula

Ocjena HSM-ova i drugih kriptografskih modula provodi se prema 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 ključ Fina Root CA kao i javni ključevi njemu subordiniranih Fina CA-ova su sastavni 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.

Arhiviranje privatnih ključeva za Fina OCSP 2015 servis i Fina QTSA 2015 provodi se na isti način kao i arhiviranje javnih ključeva subordiniranih Fina CA-ova.

Ovi ključevi u arhivi čuvaju se na rok iz točke 5.5.2. ovih Općih pravila.

6.3.2. Periodi valjanosti certifikata i korištenja para ključeva

Predviđeni rok valjanosti certifikata po vrstama je definiran u Tablici 6.1.

Certifikat	Rok
Certifikat za Fina RDC 2015 i Fina RDC-TDU 2015 CA	10 godina
Certifikat za Fina QTSA 2015 servis	10 godina
Certifikati za potpis odgovora Fina OCSP servisa	12 mjeseci
Certifikat standardne razine sigurnosti	Ne dulje od 5 godina
Certifikat srednje razine sigurnosti	2 godine
Certifikat visoke razine sigurnosti	1 godina

Tablica 6.1. Rokovi uporabe certifikata

Vremenski period valjanosti privatnog ključa jednak je vremenskom periodu valjanosti pripadajućeg certifikata. Certifikati i pripadajući ključevi ne smiju se upotrebljavati nakon isteka roka valjanosti 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 upotrebljavaju se za zaštitu pristupa privatnom ključu.

Aktivacijski podaci povezani s privatnim ključevima za Fina CA-ove generiraju se i instaliraju prilikom provođenja formalne ceremonije generiranja para ključeva za subordinirane Fina CA-ove.

Aktivacijski podaci povezani s privatnim ključem za Fina OCSP servis generiraju se i instaliraju u prilikom postupka generiranja pripadajućeg privatnog ključa.

Aktivacijske podatke za Fina RA mrežu generira se u Fina CA.

Aktivacijske podatke za pristup privatnim ključevima za vanjske ugovorene RA, korisnike te za poslužitelje i aplikacije može generirati Fina CA ili aktivacijske podatke za pripadajuće privatne ključeve mogu generirati ugovoreni RA, potpisnici, odnosno skrbnici, na njihovim lokacijama.

Aktivacijske podatke za pristup privatnim ključevima za certifikate za potpis *Trusted* liste generira Fina CA.

Ukoliko aktivacijske podatke generira Fina CA, podaci se čuvaju na siguran način te se dostavljaju subjektu odvojenim distribucijskim kanalom od kanala isporuke SSCD uređaja i/ili

privatnog ključa. Preporuka je da potpisnik ili skrbnik promijeni aktivacijske podatke pri prvoj aktivaciji ključa.

Ukoliko aktivacijske podatke generira vanjski ugovoreni RA, potpisnik ili skrbnik, isti je odgovoran za sigurnost i kvalitetu aktivacijskih podataka.

Preporuka je da potpisnik, odnosno skrbnik radi očuvanja sigurnosti privatnog ključa periodički mijenja aktivacijske podatke.

6.4.2. Zaštita aktivacijskih podataka

Aktivacijski podaci povezani s privatnim ključem Fina CA-ova podijeljeni su na hardverska sredstva za aktivaciju, sukladno točki 6.2.2. ovih Općih pravila, a koja se zaštićena pripadajućim PIN-ovima na siguran način čuvaju u Fina PKI štićenom prostoru.

Zaštita aktivacijskih podataka povezanih s privatnim ključem za Fina OCSP servis provodi se na jednak način kao i zaštita aktivacijskih podataka povezanih s privatnim ključevima subordiniranih Fina CA-ova.

Ovlaštene osobe Fina RA mreže, vanjskih ugovorenih RA te potpisnici i skrbnici zaduženi su i odgovorni za zaštitu aktivacijskih podataka pripadajućih privatnih ključeva.

Preporuka je korisnicima da ne zapisuju aktivacijske podatke. Ako korisnici zapisuju aktivacijske podatke, ti podaci moraju biti pohranjeni na zaštićeni način dostupan samo osobi ovlaštenoj za korištenje certifikata.

Aktivacijski podaci ne smiju se čuvati zajedno s kriptografskim modulom ili sličnim sredstvom na kojeg se odnose.

6.4.3. Ostale odredbe o aktivacijskim podacima

Dodatni zahtjevi za aktivacijske podatke privatnih ključeva Fina Root CA i njemu subordiniranih Fina CA-ova određeni su internim dokumentima.

Ova Opća pravila ne postavljaju uvjete na životni ciklus aktivacijskih podataka subjekata. Podaci se mogu mijenjati periodički kako bi se smanjila mogućnost njihova otkrivanja.

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

Fina osigurava da su svi zahtjevi na računalnu sigurnost Fina PKI sustava usklađeni s normom HRN ETSI/EN 319 411-3 [12] te normom HRN ETSI/EN 319 411-2 [11] u slučajevima kada ova postavlja strože zahtjeve na računalnu sigurnost te sa zahtjevima iz dokumenta CA/Browser Forum Baseline Requirements [33].

Računalni resursi štite se mjerama sigurnosti prema ISO/IEC 27001 [19] i ISO/IEC 27002 [20] normi.

6.5.2. Ocjena računalne sigurnosti

Sigurnosne mjere koje se odnose na računalnu sigurnost periodički se ispituju sukladno normama iz točke 6.5.1. ovih Općih pravila.

6.6. Tehničko upravljanje životnim ciklusom

Ako Fina obavlja razvoj softvera za Fina PKI posebno se vodi računa o:

- sigurnosti razvojne okoline,
- smjernicama o sigurnosti u životnog ciklusa razvoja softvera,
- metodologiji za siguran razvoj softvera i sigurnoj izradi koda,
- posebnim i specifičnim smjernicama za korišteni programski jezik,
- sigurnošću u upravljanju verzijama,
- sposobnošću za izbjegavanje, pronalaženje i popravljanje ranjivosti na sustavima.

Kada se nabavlja razvoj informacijskog sustava i softvera od vanjskog izvođača, Fina ugovorom s dobavljačem osigurava sigurnosne principe razvoja sustava.

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

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 vatrozidima koji propuštaju samo nužan mrežni promet.

Detaljnije odredbe koje se odnose na provjeru mrežne sigurnosti Fina PKI sustava nalaze se u pripadajućem CPS_{QC} [36], odnosno CPS_{NQC} [37] dokumentu.

6.8. Uporaba vremenskog žiga

Fina PKI sustav usklađuje se s internim servisom točnog vremena koji je usklađen s vanjskim izvorom točnog vremena.

Podatak o vremenu dobiven s internog servisa točnog vremena ugrađuje se u zapise dnevnika sustava iz opisanim u točki 5.4. ovih Općih pravila.

7. SADRŽAJ CERTIFIKATA, LISTA OPOZVANIH CERTIFIKATA I OCSP PROFILI

Ovo poglavlje sadrži opis profila certifikata, lista opozvanih certifikata (CRL) i odgovora OCSP servisa koje Fina kao davatelj usluga certificiranja kroz Fina RDC 2015 i Fina RDC-TDU 2015 CA-ove izdaje sukladno ovim Općim pravilima.

Profili kvalificiranih certifikata koje izdaju Fina RDC 2015 CA i Fina RDC-TDU 2015 CA usklađeni su s normom HRN ETSI/EN 319 412-5 [13].

Profili normaliziranih certifikata koje izdaju Fina RDC 2015 CA i Fina RDC-TDU 2015 CA usklađeni su s normom HRN ETSI/EN 319 411-3 [12] u dijelu pravila za normalizirane certifikate (NCP ili NCP+) i preporukom IETF RFC 5280 [24].

Profil *lightweight* certifikata koje izdaje Fina RDC 2015 CA usklađen je s normom HRN ETSI/EN 319 411-3 [12] u dijelu pravila za lightweight certifikate (LCP) i preporukom IETF RFC 5280 [24].

Profili CRL koje izdaju subordinirani Fina CA-ovi usklađeni su s preporukom IETF RFC 5280 [24].

Profili OCSP odgovora Fina OCSP i Fina RDC servisa usklađen je s preporukom IETF RFC 6960 [25].

7.1. Profil certifikata

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 pravila certificiranja (CP OID).

U točki 1.1.2., Tablici 1.1 ovih Općih pravila naveden je popis definiranih CP OID-ova tipova certifikata koje izdaju subordinirani Fina CA-ovi.

7.1.1. Broj(evi) verzije

Koristi se X.509 verzija 3 certifikata.

7.1.2. Ekstenzije certifikata

Zajedničke ekstenzije svih certifikata koje izdaju Fina CA-ovi su navedene u Tablici 7.1.

Ekstenzija	Kritično	Atribut	Vrijednost
AuthorityKeyIdentifier	NE	keyIdentifier	160-bit SHA-1 hash vrijednost (određeno prema RFC 5280, točka 4.2.1.2 metoda (1))
SubjectKeyIdentifier	NE	keyIdentifier	160-bit SHA-1 hash vrijednost (određeno prema RFC 5280, točka 4.2.1.2 metoda (1))
BasicConstraints	NE		cA=FALSE pathLenConstraint=None

Tablica 7.1. Zajedničke ekstenzije svih certifikata izdanih od Fina CA-ova

7.1.2.1. Fina RDC 2015 certifikati

Podjela certifikata koje izdaje Fina RDC 2015 CA po grupama korisnika:

1. Fina 2015 RDC osobni certifikati;
2. Fina 2015 RDC poslovni certifikati;
3. Fina 2015 RDC poslovni certifikati za IT opremu;
4. Fina 2015 RDC administrativni certifikati.

Certifikati koje izdaje Fina RDC 2015 CA imaju zajedničke ekstenzije profila certifikata definirane u Tablici 7.2.

Ekstenzija	Kritično	Atribut	Vrijednost
CRLDistributionPoints	NE	DistributionPoint	[1]URI: http://rdc.fina.hr/RDC2015/FinaRDCCA2015.crl ldap://rdc-ldap2.fina.hr/CN=Fina RDC 2015, O=Financijska agencija, C=HR?certificateRevocationList;binary [2]DirName:/C=HR/O=Financijska agencija/CN=Fina RDC 2015/CN=CRLx
Authority Information Access	NE	id-ad-ocsp	http://ocsp.fina.hr
		id-ad-caIssuers	http://rdc.fina.hr/RDC2015/FinaRDCCA2015.cer

Tablica 7.2. Zajedničke ekstenzije svih certifikata izdanih od Fina RDC 2015 CA

1. Fina RDC 2015 osobni certifikati

Osobne certifikate izdaje Fina RDC 2015 CA. Ova grupa od tri tipa certifikata namijenjena je fizičkim osobama (građanima) za osobnu uporabu.

Fina e-kartica za građane i **Fina e-token za građane** na *smart* kartici, odnosno USB tokenu sadrži Osobni potpisni Q2 certifikat (QCP+) i/ili Osobni autentifikacijski N2 certifikat (NCP+).

- **Osobni potpisni Q2 certifikat (QCP+)** – Osobni potpisni kvalificirani certifikat srednje razine sigurnosti koji se koristi isključivo za izradu naprednog elektroničkog potpisa te ima definiran OID: **1.3.124.1104.5.12.1.2.2.** Izdaje se na SSCD uređaju u skladu s općim pravilima za „QCP public + SSCD“ norme HRN ETSI/EN 319 411-2 [11] i izdaje ga Fina RDC 2015 CA. Certifikat vrijedi dvije godine.

Ekstenzije profila certifikata specifične za Osobni potpisni Q2 certifikat (QCP+) prikazane su u Tablici 7.3.

Ekstenzija	Kritično	Atribut	Vrijednost
subjectAltName	NE	rfc822Name	Opcionalno. Sadrži e-mail adresu potpisnika u IETF RFC 822 standardiziranom obliku.
KeyUsage	DA	nonRepudiation	Uključen nonRepudiation bit
certificatePolicies	NE	policyIdentifier	OID: 1.3.124.1104.5.12.1.2.2
		cPSuri	http://rdc.fina.hr/RDC2015/FinaRDC2015-CP5-1-hr.pdf http://rdc.fina.hr/RDC2015/FinaRDC2015-CP5-1-en.pdf
		policyQualifierID	CPS
qCStatements	NE	esi4-qcStatement-1	id-etsi-qcs-QcCompliance
		esi4-qcStatement-4	id-etsi-qcs-QcSSCD
		Esi4-qcStatement-5	id-etsi-qcs-QcPDS https://rdc.fina.hr/RDC2015/FinaRDC2015-PDSp5-1-hr.pdf https://rdc.fina.hr/RDC2015/FinaRDC2015-PDSp5-1-en.pdf

Tablica 7.3. Ekstenzije profila specifične za Osobni potpisni Q2 certifikat (QCP+)

- **Osobni autentifikacijski N2 certifikat (NCP+)** – Osobni autentifikacijski normalizirani certifikat srednje razine sigurnosti koji se koristi za jaku autentifikaciju, elektronički potpis i enkripciju te ima definiran OID: **1.3.124.1104.5.12.1.4.2**. Izdaje se na SSCD uređaju u skladu s normom HRN ETSI/EN 319 411-3 (NCP+) [12] i izdaje ga Fina RDC 2015 CA. Certifikat vrijedi dvije godine.

Ekstenzije profila certifikata specifična za Osobni autentifikacijski N2 certifikat (NCP+) definirana su u Tablici 7.4.

Ekstenzija	Kritično	Atribut	Vrijednost
subjectAltName	NE	rfc822Name	Opcionalno. Sadrži e-mail adresu potpisnika u IETF RFC 822 standardiziranom obliku.
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit
		dataEncipherment	Uključen dataEncipherment bit
extKeyUsage	NE	emailProtection	OID: 1.3.6.1.5.5.7.3.4
		clientAuth	OID: 1.3.6.1.5.5.7.3.2
certificatePolicies	NE	policyIdentifier	OID: 1.3.124.1104.5.12.1.4.2
		cPSuri	http://rdc.fina.hr/RDC2015/FinaRDC2015-CP5-1-hr.pdf http://rdc.fina.hr/RDC2015/FinaRDC2015-CP5-1-en.pdf
		policyQualifierID	CPS

Tablica 7.4. Ekstenzije profila specifične za Osobni autentifikacijski N2 certifikata (NCP+)

- **Osobni soft certifikat (NCP)** – Osobni autentifikacijski normalizirani certifikat standardne razine sigurnosti koji se izdaje u PKCS#12 formatu, a koristi se za jaku autentifikaciju, elektronički potpis i enkripciju s definiranim OID-om:

1.3.124.1104.5.12.1.3.1. Izdavanje ovog certifikata je u skladu s normom HRN ETSI/EN 319 411-3 (NCP) [12] i izdaje ga Fina RDC 2015 CA. Certifikat vrijedi pet godina.

Ekstenzije profila certifikata specifične za Osobni soft certifikat (NCP) definirane su u Tablici 7.5.

Ekstenzija	Kritično	Atribut	Vrijednost
subjectAltName	NE	rfc822Name	Opcionalno. Sadrži e-mail adresu potpisnika u IETF RFC 822 standardiziranom obliku.
Key Usage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit
		dataEncipherment	Uključen dataEncipherment bit
extKeyUsage	NE	emailProtection	OID: 1.3.6.1.5.5.7.3.4
		clientAuth	OID: 1.3.6.1.5.5.7.3.2
certificatePolicies	NE	policyIdentifier	OID: 1.3.124.1104.5.12.1.3.1
		cPSuri	http://rdc.fina.hr/RDC2015/FinaRDC2015-CP5-1-hr.pdf http://rdc.fina.hr/RDC2015/FinaRDC2015-CP5-1-en.pdf
		policyQualifierID	CPS

Tablica 7.5. Ekstenzije profila specifične za Osobni soft certifikat (NCP)

2. Fina RDC 2015 poslovni certifikati

Poslovne certifikate izdaje Fina RDC 2015 CA. Ova grupa certifikata namijenjena je za poslovnu uporabu te se ovi certifikati izdaju pripadajućim osobama unutar poslovnog subjekta.

Fina poslovna e-kartica i **Fina poslovni e-token** na *smart* kartici ili USB tokenu sadrži Poslovni potpisni Q2 certifikat (QCP+) i/ili Poslovni autentifikacijski N2 certifikat (NCP+).

- **Poslovni potpisni Q2 certifikat (QCP+)** – Poslovni potpisni kvalificirani certifikat srednje razine sigurnosti koji se koristi isključivo za izradu naprednog elektroničkog potpisa te ima definiran OID: **1.3.124.1104.5.12.2.2.2.** Izdaje se na SSCD uređaju u skladu s općim pravilima za „QCP public + SSCD“ norme normom HRN ETSI/EN 319 411-2 [11] i izdaje ga Fina RDC 2015 CA. Certifikat vrijedi dvije godine.

Ekstenzije profila certifikata specifične za Poslovni potpisni Q2 certifikat (QCP+) definirane su u Tablici 7.6.

Ekstenzija	Kritično	Atribut	Vrijednost
subjectAltName	NE	rfc822Name	Opcionalno. Sadrži e-mail adresu potpisnika u IETF RFC 822 standardiziranom obliku.
KeyUsage	DA	nonRepudiation	Uključen nonRepudiation bit
certificatePolicies	NE	policyIdentifier	OID: 1.3.124.1104.5.12.2.2.2
		cPSuri	http://rdc.fina.hr/RDC2015/FinaRDC2015-CP5-1-hr.pdf http://rdc.fina.hr/RDC2015/FinaRDC2015-CP5-1-en.pdf
		policyQualifierID	CPS
qCStatements	NE	esi4-qcStatement-1	id-etsi-qcs-QcCompliance
		esi4-qcStatement-4	id-etsi-qcs-QcSSCD
		Esi4-qcStatement-5	id-etsi-qcs-QcPDS https://rdc.fina.hr/RDC2015/FinaRDC2015-PDSb5-1-hr.pdf https://rdc.fina.hr/RDC2015/FinaRDC2015-PDSb5-1-en.pdf

Tablica 7.6. Ekstenzije profila specifične za Poslovni potpisni Q2 certifikat (QCP+)

- **Poslovni autentifikacijski N2 certifikat (NCP+)** – Poslovni autentifikacijski normalizirani certifikat srednje razine sigurnosti koji se koristi za jaku autentifikaciju, elektronički potpis i enkripciju te ima definiran OID: **1.3.124.1104.5.12.2.4.2**. Izdavanje ovog certifikata je u skladu s normom HRN ETSI/EN 319 411-3 (NCP+) [12] i izdaje ga Fina RDC 2015 CA. Certifikat vrijedi dvije godine.

Ekstenzije profila certifikata specifične za Poslovni autentifikacijski N2 certifikat (NCP+) definirane su u Tablici 7.7.

Ekstenzija	Kritično	Atribut	Vrijednost
subjectAltName	NE	rfc822Name	Opcionalno. Sadrži e-mail adresu potpisnika u IETF RFC 822 standardiziranom obliku.
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit
		dataEncipherment	Uključen dataEncipherment bit
extKeyUsage	NE	emailProtection	OID: 1.3.6.1.5.5.7.3.4
		clientAuth	OID: 1.3.6.1.5.5.7.3.2
certificatePolicies	NE	policyIdentifier	OID: 1.3.124.1104.5.12.2.4.2
certificatePolicies	NE	cPSuri	http://rdc.fina.hr/RDC2015/FinaRDC2015-CP5-1-hr.pdf http://rdc.fina.hr/RDC2015/FinaRDC2015-CP5-1-en.pdf
		policyQualifierID	CPS

Tablica 7.7. Ekstenzije profila specifične za Poslovni autentifikacijski N2 certifikata (NCP+)

- **Poslovni soft certifikat (NCP)** – Poslovni autentifikacijski normalizirani certifikat standardne razine sigurnosti koji se izdaje u PKCS#12 formatu, a koristi se za jaku autentifikaciju, elektronički potpis i enkripciju te ima definiran OID: **1.3.124.1104.5.12.2.3.1**. Izdavanje ovog certifikata je u skladu s normom HRN ETSI/EN 319 411-3 (NCP) [12] i izdaje se od strane Fina RDC 2015 CA. Certifikat vrijedi pet godina.

Ekstenzije profila certifikata specifične za Poslovni soft certifikat (NCP) definirane su u Tablici 7.8.

Ekstenzija	Kritično	Atribut	Vrijednost
subjectAltName	NE	rfc822Name	Opcionalno. Sadrži e-mail adresu potpisnika u IETF RFC 822 standardiziranom obliku.
Key Usage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit
		dataEncipherment	Uključen dataEncipherment bit
extKeyUsage	NE	emailProtection	OID: 1.3.6.1.5.5.7.3.4
		clientAuth	OID: 1.3.6.1.5.5.7.3.2
certificatePolicies	NE	policyIdentifier	OID: 1.3.124.1104.5.12.2.3.1
		cPSuri	http://rdc.fina.hr/RDC2015/FinaRDC2015-CP5-1-hr.pdf http://rdc.fina.hr/RDC2015/FinaRDC2015-CP5-1-en.pdf
		policyQualifierID	CPS

Tablica 7.8. Ekstenzije profila specifične za Poslovni soft certifikata (NCP)

- **Poslovni soft certifikat (LCP)** – Poslovni autentifikacijski *lightweight* certifikat standardne razine sigurnosti koji se izdaje u PKCS#12 formatu, a koristi se za jaku autentifikaciju, elektronički potpis i enkripciju.te ima definiran OID: **1.3.124.1104.5.12.2.5.1**. Izdavanje ovog certifikata je u skladu s normom HRN ETSI/EN 319 411-3 (LCP) [12] i izdaje se od strane Fina RDC 2015 CA. Certifikat vrijedi pet godina.

Ekstenzije profila certifikata specifične za Poslovni soft certifikat (LCP) definirane su u Tablici 7.9.

Ekstenzija	Kritično	Atribut	Vrijednost
subjectAltName	NE	rfc822Name	Opcionalno. Sadrži e-mail adresu potpisnika u IETF RFC 822 standardiziranom obliku.
Key Usage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit
		dataEncipherment	Uključen dataEncipherment bit
extKeyUsage	NE	emailProtection	OID: 1.3.6.1.5.5.7.3.4
		clientAuth	OID: 1.3.6.1.5.5.7.3.2

Ekstenzija	Kritično	Atribut	Vrijednost
certificatePolicies	NE	policyIdentifier	OID: 1.3.124.1104.5.12.2.5.1
		cPSuri	http://rdc.fina.hr/RDC2015/FinaRDC2015-CP5-1-hr.pdf http://rdc.fina.hr/RDC2015/FinaRDC2015-CP5-1-en.pdf
		policyQualifierID	CPS

Tablica 7.9. Ekstenzije profila specifične za Poslovni soft certifikata (LCP)

3. Fina RDC 2015 poslovni certifikati za IT opremu

Poslovne certifikate za IT opremu izdaje Fina RDC 2015 CA. Ovi certifikati se mogu izdati kao:

- certifikati za poslužitelje;
- certifikati za aplikacije;
- certifikati za potpis *Trusted* liste;
- certifikat za izradu vremenskog žiga;
- certifikat za potpis odgovora OCSP servisa.

U nastavku su opisane ekstenzije certifikata za poslužitelje.

- **SSL certifikat razine 2 (NCP)** – Normalizirani certifikat za poslužitelje, srednje razine sigurnosti, uz korištenje softverskog spremnika ključa. Ovaj tip certifikata ima definiran OID: **1.3.124.1104.5.12.3.3.2.** Generiranje ključeva ovog certifikata obavlja skrbnik u softverskom kriptografskom modulu na svojoj udaljenoj lokaciji. Izdavanje ovog certifikata je u skladu s normom HRN ETSI/EN 319 411-3 (NCP) [12] i izdaje ga Fina RDC 2015 CA. Certifikat vrijedi dvije godine.

Ekstenzije profila certifikata specifične za SSL certifikat razine 2 (NCP) definirane su u Tablici 7.10.

Ekstenzija	Kritično	Atribut	Vrijednost
subjectAltName	NE	dNSName ili iPAddress	Puni kvalificirani naziv poslužitelja (FQDN) ili IP adresa poslužitelja, (najmanje jedan zapis/stavak).
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit
extKeyUsage	NE	serverAuth	1.3.6.1.5.5.7.3.1
		clientAuth	1.3.6.1.5.5.7.3.2
certificatePolicies	NE	policyIdentifier	OID: 1.3.124.1104.5.12.3.3.2
		cPSuri	http://rdc.fina.hr/RDC2015/FinaRDC2015-CP5-1-hr.pdf http://rdc.fina.hr/RDC2015/FinaRDC2015-CP5-1-en.pdf
		policyQualifierID	CPS

Tablica 7.10. Ekstenzije profila specifične za Poslovni SSL certifikat razine 2 (NCP)

- **SSL certifikat razine 3 (NCP+)** – Normalizirani certifikat za poslužitelje, visoke razine sigurnosti, uz korištenje HSM modula. Ovaj tip certifikata ima definiran OID: **1.3.124.1104.5.12.3.4.3.** Generiranje ključeva ovog certifikata obavlja skrbnik u HSM modulu na svojoj udaljenoj lokaciji. Izdavanje ovog certifikata je u skladu s normom HRN ETSI/EN 319 411-3 (NCP+) [12] i izdaje ga Fina RDC 2015 CA. Certifikat vrijedi jednu godinu.

Ekstenzije profila certifikata specifične za SSL certifikat razine 3 (NCP+) definirane su u Tablici 7.11.

Ekstenzija	Kritično	Atribut	Vrijednost
subjectAltName	NE	dNSName ili iPAddress	Puni kvalificirani naziv poslužitelja (FQDN) ili IP adresa poslužitelja, (najmanje jedan zapis/stavak).
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit
extKeyUsage	NE	serverAuth	1.3.6.1.5.5.7.3.1
		clientAuth	1.3.6.1.5.5.7.3.2
certificatePolicies	NE	policyIdentifier	OID: 1.3.124.1104.5.12.3.4.2
		cPSuri	http://rdc.fina.hr/RDC2015/FinaRDC2015-CP5-1-hr.pdf http://rdc.fina.hr/RDC2015/FinaRDC2015-CP5-1-en.pdf
		policyQualifierID	CPS

Tablica 7.11. Ekstenzije profila specifične za Poslovni SSL certifikata razine 3 (NCP+)

U nastavku su opisane ekstenzije certifikata za aplikacije.

- **Aplikacijski certifikat razine 1 (NCP)** – Normalizirani certifikat za aplikacije, standardne razine sigurnosti, uz korištenje softverskog spremnika ključa. Ovaj tip certifikata ima definiran OID: **1.3.124.1104.5.12.5.3.1.** Generiranje ključeva ovog certifikata obavlja Fina RDC 2015 CA te se certifikat izdaje u PKCS#12 formatu. Izdavanje ovog certifikata je u skladu s normom HRN ETSI/EN 319 411-3 (NCP) [12] i izdaje ga Fina RDC 2015 CA. Certifikat vrijedi najviše pet godina.

  Osim u softverskom spremniku ključa na disku računala korisnik može privatni ključ koji odgovara javnom ključu za ovaj tip certifikata čuvati i na kriptografskom uređaju (*smart* kartica ili USB token) te ga štititi PIN-om.

Ekstenzije profila certifikata specifične za Aplikacijski certifikat razine 1 (NCP) definirane su u Tablici 7.12.

Ekstenzija	Kritično	Atribut	Vrijednost
subjectAltName	NE	dNSName ili iPAddress	Opcionalno. Sadrži e-mail adresu subjekta u IETF RFC 822 standardiziranom obliku.
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit
		dataEncipherment	Uključen dataEncipherment bit
extKeyUsage	NE	emailProtection	OID: 1.3.6.1.5.5.7.3.4
		clientAuth	OID: 1.3.6.1.5.5.7.3.2
certificatePolicies	NE	policyIdentifier	OID: 1.3.124.1104.5.12.5.3.1
		cPSuri	http://rdc.fina.hr/RDC2015/FinaRDC2015-CP5-1-hr.pdf http://rdc.fina.hr/RDC2015/FinaRDC2015-CP5-1-en.pdf
		policyQualifierID	CPS

Tablica 7.12. Ekstenzije profila specifične za Poslovni aplikacijski certifikat razine 1 (NCP)

- **Aplikacijski certifikat razine 2 (NCP)** – Normalizirani certifikat za aplikacije, srednje razine sigurnosti, uz korištenje softverskog spremnika ključa. Ovaj tip certifikata ima definiran OID: **1.3.124.1104.5.12.5.3.2.** Generiranje ključeva ovog certifikata obavlja skrbnik u softverskom kriptografskom modulu na svojoj udaljenoj lokaciji. Izdavanje ovog certifikata je u skladu s normom HRN ETSI/EN 319 411-3 (NCP) [12] i izdaje ga Fina RDC 2015 CA. Certifikat vrijedi dvije godine.

  Osim u softverskom spremniku ključa na disku računala korisnik može privatni ključ koji odgovara javnom ključu za ovaj tip certifikata čuvati i na kriptografskom uređaju (*smart* kartica ili USB token) te ga štititi PIN-om.

Ekstenzije profila certifikata specifične za Aplikacijski certifikat razine 2 (NCP) definirane su u Tablici 7.13.

Ekstenzija	Kritično	Atribut	Vrijednost
subjectAltName	NE	dNSName ili iPAddress	Opcionalno. Sadrži e-mail adresu subjekta u IETF RFC 822 standardiziranom obliku.
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit
		dataEncipherment	Uključen dataEncipherment bit
extKeyUsage	NE	emailProtection	OID: 1.3.6.1.5.5.7.3.4
		clientAuth	OID: 1.3.6.1.5.5.7.3.2
certificatePolicies	NE	policyIdentifier	OID: 1.3.124.1104.5.12.5.3.2
		cPSuri	http://rdc.fina.hr/RDC2015/FinaRDC2015-CP5-1-hr.pdf http://rdc.fina.hr/RDC2015/FinaRDC2015-CP5-1-en.pdf
		policyQualifierID	CPS

Tablica 7.13. Ekstenzije profila specifične za Poslovni aplikacijski certifikat razine 2 (NCP)

- **Aplikacijski certifikat razine 2 (NCP+)** – Normalizirani certifikat za aplikacije, srednje razine sigurnosti, uz korištenje SSCD uređaja. Ovaj tip certifikata ima definiran OID: **1.3.124.1104.5.12.5.4.2.** Generiranje ključeva ovog certifikata obavlja skrbnik na SSCD uređaju. Izdavanje ovog certifikata je u skladu s normom HRN ETSI/EN 319 411-3 (NCP+) [12]. Ove certifikate izdaje Fina RDC 2015 CA. Certifikat vrijedi dvije godine.

Ekstenzije profila certifikata specifične za Aplikacijski certifikat razine 2 (NCP+) definirane su u Tablici 7.14.

Ekstenzija	Kritično	Atribut	Vrijednost
subjectAltName	NE	dNSName ili iPAddress	Opcionalno. Sadrži e-mail adresu subjekta u IETF RFC 822 standardiziranom obliku.
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit
		dataEncipherment	Uključen dataEncipherment bit
extKeyUsage	NE	emailProtection	OID: 1.3.6.1.5.5.7.3.4
		clientAuth	OID: 1.3.6.1.5.5.7.3.2
certificatePolicies	NE	policyIdentifier	OID: 1.3.124.1104.5.12.5.4.2
		cPSuri	http://rdc.fina.hr/RDC2015/FinaRDC2015-CP5-1-hr.pdf http://rdc.fina.hr/RDC2015/FinaRDC2015-CP5-1-en.pdf
		policyQualifierID	CPS

Tablica 7.14. Ekstenzije profila specifične za Poslovni aplikacijski certifikat razine 2 (NCP+)

- **Aplikacijski certifikat razine 3 (NCP+)** – Normalizirani certifikat za aplikacije, visoke razine sigurnosti, uz korištenje HSM modula. Ovaj tip certifikata ima definiran OID: **1.3.124.1104.5.12.5.4.3.** Generiranje ključeva ovog certifikata izvodi skrbnik u HSM modulu na svojoj udaljenoj lokaciji. Izdavanje ovog certifikata je u skladu s normom HRN ETSI/EN 319 411-3 (NCP+) [12]. Ove certifikate izdaje Fina RDC 2015 CA. Certifikat vrijedi jednu godinu.

Ekstenzije profila certifikata specifične za Aplikacijski certifikat razine 3 (NCP+) definirane su u Tablici 7.15.

Ekstenzija	Kritično	Atribut	Vrijednost
subjectAltName	NE	dNSName ili iPAddress	Opcionalno. Sadrži e-mail adresu subjekta u IETF RFC 822 standardiziranom obliku.
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit
		dataEncipherment	Uključen dataEncipherment bit
extKeyUsage	NE	emailProtection	OID: 1.3.6.1.5.5.7.3.4
		clientAuth	OID: 1.3.6.1.5.5.7.3.2

Ekstenzija	Kritično	Atribut	Vrijednost
certificatePolicies	NE	policyIdentifier	OID: 1.3.124.1104.5.12.5.4.3
		cPSuri	http://rdc.fina.hr/RDC2015/FinaRDC2015-CP5-1-hr.pdf http://rdc.fina.hr/RDC2015/FinaRDC2015-CP5-1-en.pdf
		policyQualifierID	CPS

Tablica 7.15. Ekstenzije profila specifične za Poslovnog aplikacijskog certifikata razine 3 (NCP+)

- **Certifikat za potpis *Trusted* liste (NCP+)** – Normalizirani certifikat za potpis *Trusted* liste, srednje razine sigurnosti, uz korištenje SSCD uređaja. Ovaj tip certifikata ima definiran OID: **1.3.124.1104.5.12.8.4.2.** Generiranje ključeva izvodi CA u SSCD uređaju. Izdavanje ovog certifikata je u skladu s normom HRN ETSI/EN 319 411-3 (NCP+) [12]. Ove certifikate izdaje Fina RDC 2015 CA. Certifikat vrijedi najviše dvije godine.

Ekstenzije profila certifikata specifične za certifikat za *Trusted* Liste (NCP+) definirane su u tablici 7.16.

Ekstenzija	Kritično	Atribut	Vrijednost
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
extKeyUsage	NE	id-tsl-kp-tslSigning	OID: 0.4.0.2231.3.0
certificatePolicies	NE	policyIdentifier	OID: 1.3.124.1104.5.12.8.4.2
		cPSuri	http://rdc.fina.hr/RDC2015/FinaRDC2015-CP5-1-hr.pdf http://rdc.fina.hr/RDC2015/FinaRDC2015-CP5-1-en.pdf
		policyQualifierID	CPS

Tablica 7.16. Ekstenzije profila specifične za Poslovni certifikat za potpis Trusted liste (NCP+)

- **Certifikat za vremenski žig (NCP+)** – Normalizirani certifikat visoke razine sigurnosti uz korištenje HSM modula, za izradu naprednih vremenskih žigova. Ovaj tip certifikata ima definiran OID: **1.3.124.1104.5.12.52.4.3.** Generiranje ključeva ovog certifikata obavlja se u HSM modulu uz nadzor ovlaštenih osoba davatelja usluge izdavanja naprednih vremenskih žigova. Izdavanje ovog certifikata je u skladu s normom HRN ETSI/EN 319 411-3 (NCP+) [12] i izdaje se od strane Fina RDC 2015 CA. Certifikat vrijedi deset godina.

Ekstenzije profila certifikata specifične za certifikat za vremenski žig (NCP+) definirane su u Tablici 7.17.

Ekstenzija	Kritično	Atribut	Vrijednost
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
		nonRepudiation	Uključen nonRepudiation bit
extKeyUsage	DA	timeStamping	OID: 1.3.6.1.5.5.7.3.8

Ekstenzija	Kritično	Atribut	Vrijednost
certificatePolicies	NE	policyIdentifier	OID: 1.3.124.1104.5.12.52.4.3
		cPSuri	http://rdc.fina.hr/RDC2015/FinaRDC2015-CP5-1-hr.pdf http://rdc.fina.hr/RDC2015/FinaRDC2015-CP5-1-en.pdf
		policyQualifierID	CPS

Tablica 7.17. Ekstenzije profila specifične za certifikat za vremenski žig (NCP+)

- **Certifikat za potpis odgovora OCSP servisa (NCP+)** – Normalizirani certifikat za potpis odgovora OCSP servisa, visoke razine sigurnosti, uz korištenje HSM modula. Ovaj tip certifikata ima definiran OID: **1.3.124.1104.5.12.9.4.3.** Generiranje ključeva ovog certifikata obavlja se u HSM modulu uz nadzor ovlaštenih osoba u Fina PKI. Izdavanje ovog certifikata je u skladu s normom HRN ETSI/EN 319 411-3 (NCP+) i preporukom RFC 6960 [25] te se izdaje od strane Fina RDC 2015 CA. Certifikat vrijedi dvanaest mjeseci.

Ekstenzije profila certifikata specifične za certifikat za potpis odgovora OCSP servisa (NCP+) definirane su u Tablici 7.18.

Ekstenzija	Kritično	Atribut	Vrijednost
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
		nonRepudiation	Uključen nonRepudiation bit
extKeyUsage	NE	OCSPSigning	OID: 1.3.6.1.5.5.7.3.9
ocsp-nocheck	NE		OID: 1.3.6.1.5.5.7.48.1.5, vrijednost NULL
certificatePolicies	NE	policyIdentifier	Visoka razina sigurnosti: OID: 1.3.124.1104.5.12.9.4.3
		cPSuri	http://rdc.fina.hr/RDC2015/FinaRDC2015-CP5-1-hr.pdf http://rdc.fina.hr/RDC2015/FinaRDC2015-CP5-1-en.pdf
		policyQualifierID	CPS

Tablica 7.18. Ekstenzije profila specifične za certifikat za potpis odgovora OCSP servisa (NCP+)

4. Fina RDC administrativni certifikati

Administrativne certifikate izdaje Fina RDC 2015 CA. Ova grupa certifikata namijenjena je za administrativnu uporabu unutar sustavu certificiranja FINE te se ovi certifikati izdaju na SSCD uređaju ovlaštenim zaposlenicima FINE.

SSCD uređaj sadrži sljedeći tip certifikata.

- **Administrativni N2 certifikat (NCP+)** – Administrativni normalizirani certifikat srednje razine sigurnosti ima definiran OID: **1.3.124.1104.5.12.6.4.2**. Izdavanje ovog certifikata je u skladu s normom HRN ETSI/EN 319 411-3 (NCP+) [12] i izdaje ga Fina RDC 2015 CA. Certifikat vrijedi dvije godine.

Ekstenzije profila specifične za Administrativni normalizirani certifikat (NCP+) definirane su u Tablici 7.19.

Ekstenzija	Kritično	Atribut	Vrijednost
subjectAltName	NE	rfc822Name	Opcionalno. Sadrži *e-mail* adresu potpisnika u IETF RFC 822 standardiziranom obliku.
Key Usage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit
		dataEncipherment	Uključen dataEncipherment bit
extKeyUsage	NE	emailProtection	OID: 1.3.6.1.5.5.7.3.4
		clientAuth	OID: 1.3.6.1.5.5.7.3.2
certificatePolicies	NE	policyIdentifier	OID: 1.3.124.1104.5.12.6.4.2
		cPSuri	http://rdc.fina.hr/RDC2015/FinaRDC2015-CP5-1-hr.pdf http://rdc.fina.hr/RDC2015/FinaRDC2015-CP5-1-en.pdf
		policyQualifierID	CPS

Tablica 7.19. Ekstenzije profila specifične za Administrativni autentifikacijski N2 certifikat (NCP+)

7.1.2.2. Fina RDC-TDU 2015 certifikati

Podjela certifikata koje izdaje Fina RDC-TDU 2015 CA po grupama korisnika:

1. Fina RDC-TDU 2015 certifikati za krajnje korisnike;
2. Fina RDC-TDU 2015 certifikati za IT opremu.

Certifikati izdani od Fina RDC-TDU 2015 CA imaju zajedničke ekstenzije profila certifikata definirane u Tablici 7.20.

Ekstenzija	Kritično	Atribut	Vrijednost
CRLDistributionPoints	NE	DistributionPoint	[1]URI: http://rdc.fina.hr/RDC-TDU2015/FinaRDC-TDUCA2015.crl URI: ldap://rdc-tdu-ldap2.fina.hr/CN=Fina RDC-TDU 2015, O=Financijska agencija, C=HR?certificateRevocationList;binary [2] DirName:/C=HR/O=Financijska agencija/CN=Fina RDC-TDU 2015/CN=CRLx
Authority Information Access	NE	id-ad-ocsp	http://ocsp.fina.hr
		id-ad-caIssuers	http://rdc.fina.hr/RDC-TDU2015/FinaRDC-TDUCA2015.cer

Tablica 7.20. Zajedničke ekstenzije svih certifikata izdanih od Fina RDC-TDU 2015 CA

1. Fina 2015 RDC-TDU certifikati za krajnje korisnike

Certifikate za državne dužnosnike i zaposlenike u tijelima državne uprave izdaje Fina RDC-TDU 2015 CA.

Fina e-kartica za TDU i **Fina e-token za TDU** na *smart* kartici, odnosno USB tokenu sadrži TDU potpisni Q2 certifikat (QCP+) i/ili TDU autentifikacijski N2 certifikat (NCP+).

- **TDU potpisni Q2 certifikat (QCP+)** – Potpisni kvalificirani certifikat srednje razine sigurnosti za državne dužnosnike i zaposlenike u tijelima državne uprave koji se koristi isključivo za izradu naprednog elektroničkog potpisa te ima definiran OID: **1.3.124.1104.5.22.2.2.2**. Izdaje se na SSCD uređaju u skladu s normom HRN ETSI/EN 319 411-2 [11] i izdaje ga Fina RDC-TDU 2015 CA. Certifikat vrijedi dvije godine.

Ekstenzije profila certifikata specifične za TDU potpisni Q2 certifikat (QCP+) definirane su u Tablici 7.21.

Ekstenzija	Kritično	Atribut	Vrijednost
subjectAltName	NE	rfc822Name	Opcionalno. Sadrži e-mail adresu potpisnika u IETF RFC 822 standardiziranom obliku.
KeyUsage	DA	nonRepudiation	Uključen nonRepudiation bit
certificatePolicies	NE	policyIdentifier	policyIdentifier: 1.3.124.1104.5.22.2.2.2
		cPSuri	http://rdc.fina.hr/RDC-TDU2015/FinaRDC-TDU2015-CP5-1-hr.pdf http://rdc.fina.hr/RDC-TDU2015/FinaRDC-TDU2015-CP5-1-en.pdf
		policyQualifierID	CPS
qCStatements	NE	esi4-qcStatement-1	Id-etsi-qcs-QcCompliance
		esi4-qcStatement-4	Id-etsi-qcs-QcSSCD
		esi4-qcStatement-5	id-etsi-qcs-QcPDS https://rdc.fina.hr/RDC-TDU2015/FinaRDC-TDU2015-PDSt5-1-hr.pdf https://rdc.fina.hr/RDC-TDU2015/FinaRDC-TDU2015-PDSt5-1-en.pdf

Tablica 7.21. Ekstenzije profila specifične za TDU potpisni Q2 certifikat (QCP+)

- **TDU autentifikacijski N2 certifikat (NCP+)** – Autentifikacijski normalizirani certifikat srednje razine sigurnosti za državne dužnosnike i zaposlenike u tijelima državne uprave koji se koristi za jaku autentifikaciju, elektronički potpis i enkripciju te ima definiran OID: **1.3.124.1104.5.22.2.4.2**. Izdaje na SSCD uređaju u skladu s normom HRN ETSI/EN 319 411-3 (NCP+) [12] i izdaje se od strane Fina RDC-TDU 2015 CA. Certifikat vrijedi dvije godine.

Ekstenzije profila certifikata specifične za TDU autentifikacijski N2 certifikat (NCP+) definirane su u Tablici 7.22.

Ekstenzija	Kritično	Atribut	Vrijednost
subjectAltName	NE	rfc822Name	Opcionalno. Sadrži e-mail adresu potpisnika u IETF RFC 822 standardiziranom obliku.
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit
		dataEncipherment	Uključen dataEncipherment bit

Ekstenzija	Kritično	Atribut	Vrijednost
extKeyUsage	NE	emailProtection	OID: 1.3.6.1.5.5.7.3.4
		clientAuth	OID: 1.3.6.1.5.5.7.3.2
certificatePolicies	NE	policyIdentifier	OID: 1.3.124.1104.5.22.2.4.2
		cPSuri	http://rdc.fina.hr/RDC-TDU2015/FinaRDC-TDU2015-CP5-1-hr.pdf http://rdc.fina.hr/RDC-TDU2015/FinaRDC-TDU2015-CP5-1-en.pdf
		policyQualifierID	CPS

Tablica 7.22. Ekstenzije profila specifične za TDU autentifikacijski N2 certifikat (NCP+)

2. Fina 2015 RDC-TDU certifikati za IT opremu

Grupa certifikata za IT opremu sadrži tip certifikata Certifikat za potpis odgovora OCSP servisa (NCP+).

- **Certifikat za potpis odgovora OCSP servisa (NCP+)** – Normalizirani certifikat za potpis odgovora OCSP servisa, visoke razine sigurnosti, uz korištenje HSM modula. Ovaj tip certifikata ima definiran OID: **1.3.124.1104.5.22.9.4.3.** Generiranje ključeva ovog certifikata obavlja se u HSM modulu uz nadzor ovlaštenih osoba davatelja usluge odgovora OCSP servisa. Izdavanje ovog certifikata je u skladu s normom IETF RFC 6960 X.509 [25] i izdaje se od strane Fina RDC-TDU 2015 CA. Certifikat vrijedi 12 mjeseci.

Ekstenzije profila certifikata specifične za certifikat za potpis odgovora OCSP servisa (NCP+) definirane su u Tablici 7.23.

Ekstenzija	Kritično	Atribut	Vrijednost
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
		nonRepudiation	Uključen nonRepudiation bit
extKeyUsage	NE	OCSPSigning	OID: 1.3.6.1.5.5.7.3.9
ocsp-nocheck	NE		OID: 1.3.6.1.5.5.7.48.1.5, vrijednost NULL
certificatePolicies	NE	policyIdentifier	Visoka razina sigurnosti: OID: 1.3.124.1104.5.22.9.4.3
		cPSuri	http://rdc.fina.hr/RDC-TDU2015/FinaRDC-TDU2015-CP5-1-hr.pdf http://rdc.fina.hr/RDC-TDU2015/FinaRDC-TDU2015-CP5-1-en.pdf
		policyQualifierID	CPS

Tablica 7.23. Ekstenzije profila specifične za potpis odgovora OCSP servisa (NCP+)

7.1.3. Identifikator objekta (OID) algoritama

Algoritmi s pripadajućim OID identifikatorima za sve certifikate koji se izdaju u Fina PKI produkcijskoj hijerarhiji zasnovanoj na Fina Root CA prikazani su u tablici 7.24.

Algoritam	OID
sha256WithRSAEncryption	1.2.840.113549.1.1.11
rsaEncryption	1.2.840.113549.1.1.1

Tablica 7.24. 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

Ne koristi se.

7.1.6. Identifikator objekta (OID) općih pravila certificiranja

Ekstenzija *Certificate Policies* certifikata koji se izdaju u Fina PKI produkcijskoj hijerarhiji zasnovanoj na Fina Root CA sadrži odgovarajući OID općih pravila certificiranja naveden u Tablici 1.1. u točki 1.1.2. ovih Općih pravila.

7.1.7. Uporaba ekstenzije *Policy Constraints*

Ne koristi se.

7.1.8. Sintaksa i semantika kvalifikatora općih pravila

Kvalifikator općih pravila u ekstenziji certifikata su dva pokazivača u URI formatu koji sadrže internetsku adresu dokumenta ovih Općih pravila na hrvatskom i engleskom jeziku.

7.1.9. Procesne semantike za kritičnu ekstenziju *Certificate Policies*

Nije primjenjivo.

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

Koristi se X.509 verzija 2.

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 7.25.

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 7.25. 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

Koristi se verzija: 1 (0x0).

7.3.2. OCSP ekstenzije

U odgovor Fina OCSP servisa uključene su slijedeće ekstenzije:

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

8. PROVJERA USKLAĐENOSTI

Inspekcijski nadzor nad radom Fina PKI reguliran je Zakonom o elektroničkom potpisu [1], [2] i [3], a provodi ga ministarstvo nadležno za gospodarstvo.

Nadzor nad radom davatelja usluga certificiranja 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.

Unutarnju kontrolu provođenja propisanih postupaka vezanih uz rad Fina PKI i provedbu unutarnjeg procesa odobravanja rada Fina CA-ova sukladno pravilima definiranim u ovim Općim pravilima provodi Fina PMA.

Provjera usklađenosti izdavanja certifikata provodi se sukladno Zakonu o elektroničkom potpisu [1], [2] i [3], podzakonskim propisima [4], [5], [6], [7] donijetih temeljem Zakona.

Provjera usklađenosti izdavanja kvalificiranih certifikata dodatno se provodi sukladno normi HRN ETSI/EN 319 411-2 [11]. Provjera usklađenosti izdavanja normaliziranih certifikata dodatno se provodi sukladno normi HRN ETSI/EN 319 411-3 [12], u dijelu općih pravila za NCP odnosno NCP+, a provjera usklađenosti izdavanja *lightweight* certifikata provodi se sukladno normi HRN ETSI/EN 319 411-3 [12] u dijelu općih pravila za LCP.

Provjera usklađenosti certifikata provodi se i sukladno zahtjevima iz dokumenta CA/Browser Forum Baseline Requirements [33]

Naredne točke ovog poglavlja reguliraju provođenje unutarnje provjere usklađenosti.

8.1. Učestalost ili okolnosti provjere usklađenosti

Provjera usklađenosti rada Fina CA-ova provodi se redovito, najmanje jedanput godišnje.

Provjeru usklađenosti potrebno je provesti i prije početka rada novog Fina CA te nakon značajnijih promjena u radu Fina PKI, odnosno nakon katastrofe ili sumnje u kompromitiranje sustava.

8.2. Identitet/kvalifikacije ocjenitelja

Interni ocjenitelji moraju:

- raspolagati znanjima i razumijevanjem odredbi normi HRN ETSI/EN 319 411-2 [11]i HRN ETSI/EN 319 411-3 [12] te odredbi iz normizacijskog dokumenta CWA 14167-1 [17];
- raspolagati aktualnim znanjima i vještinama iz PKI područja te područja informacijske sigurnosti;
- poznavati zakonsku regulativu iz područja davanja usluga certificiranja.

8.3. Odnos ocjenitelja s tijelom koje se ocjenjuje

Interni ocjenitelji usklađenosti moraju biti dovoljno organizacijski odvojeni od Fina CA-a kako bi obavljali neovisnu/neutralnu provjeru.

8.4. Predmeti provjera

Interni ocjenitelji provjeravaju postupaju li Fina CA-ovi prema Općim pravilima, internim CPS_{QC} i CPS_{NQC} dokumentima te ostaloj mjerodavnoj internoj dokumentaciji. Detaljnije odredbe nalaze se u internim CPS_{QC} i CPS_{NQC} dokumentima.

8.5. Mjere u slučaju neusklađenosti

U slučaju utvrđivanja neusklađenosti u radu Fina CA-ova, interni ocjenitelj izrađuje izvješće i dostavlja ga Fina PMA na osnovu kojeg Fina PMA izrađuje plan akcija, mjera i postupaka koji će se, u ovisnosti o težini neusklađenosti, u danom roku poduzeti kako bi se otklonile utvrđene neusklađenosti.

Ukoliko je u radu Fina CA-ova utvrđena značajna neusklađenost u odnosu na zahtjeve propisane ovim Općim pravilima, Fina PMA će dati zahtjev za prekid izdavanja certifikata s onim CP OID-om za koje je tvrđena neusklađenost ili će dati zahtjev za poduzimanje koraka kako bi u razumnom roku otklonila neusklađenost. U slučaju prekida izdavanja certifikata Fina PMA će odobriti nastavak izdavanja certifikata, odnosno naprednih vremenskih žigova, nakon što ocjenitelj utvrdi da je postignuta propisana usklađenost.

Za vrijeme prekida izdavanja certifikata zbog utvrđene značajne neusklađenosti, Fina CA može izdavati samo certifikate u kojima je naznačeno da služe za interne i testne svrhe te mora osigurati da ti certifikati ne budu dostupni ni jednom drugom korisniku

Fina CA i Fina RA mreža moraju voditi interni dnevnik vremenskih razdoblja u kojima nisu radili u skladu s ovim Općim pravilima s navedenim razlozima neusklađenosti.

8.6. Priopćavanje rezultata

Fina PMA kao nadležno tijelo, dužno je izvještaj o provjeri usklađenosti i plan akcija, mjera i postupaka koje će se poduzeti ukoliko su otkrivene neusklađenosti dostaviti svim odgovornim osobama unutar Fina PKI sustava koje su odgovorne za rad pojedinih dijelova sustava u kojima je izvedena provjera usklađenosti.

U cilju dokazivanja usklađenosti, korisnicima i pouzdajućim stranama je na zahtjev dostupan izvještaj o provjeri usklađenosti koju je obavio interni ili vanjski neovisni ocjenitelj.

U slučaju da rezultat provjere usklađenosti utječe na ostale sudionike Fina PKI, Fina PMA će na repozitorijima iz točke 2.2. ovih Općih pravila objaviti sažetak provjere usklađenosti koji je relevantan korisnicima i ostalim sudionicima.

Rezultate vanjske provjere usklađenosti Fina može javno objaviti. Rezultati se u tom slučaju objavljuju na internetskim stranicama repozitorija iz točke 2.2

9. OSTALE POSLOVNE I PRAVNE ODREDBE

9.1. Naknade za usluge

Fina i vanjski ugovoreni RA, sukladno uvjetima iz sklopljenog ugovora, moraju obavijestiti korisnike ili pouzdajuće strane o svim uslugama koje će se naplaćivati. Ukoliko posebnim ugovorom nije drugačije određeno, usluge se naplaćuju sukladno cjeniku Fine. Cjenik svih usluga koje se naplaćuju objavljen je na internetskim stranicama repozitorija http://www.fina.hr/finadigicert.

Fina zadržava pravo izmjene cjenika. Izmjene cjenika biti će objavljene na navedenoj adresi internetskih stranica repozitorija.

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 može odrediti i naplaćivati primjerenu naknadu za pristup certifikatima.

9.1.3. Naknade za opoziv i pristup informacijama o statusu certifikata

Fina naplaćuje naknadu za uslugu opoziva certifikata te može odrediti i naplaćivati primjerenu naknadu za suspenziju i reaktivaciju certifikata. Fina može odrediti i naplaćivati primjerenu naknadu za davanje informacija o statusu certifikata.

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, najam i održavanje opreme za elektronički potpis i enkripciju, i sl.

Za pristup ovim Općim pravilima ne naplaćuju se naknade.

9.1.5. Povrat naknada

Povrat naknade Fina korisnicima isplaćuje u slučaju pogrešne uplate ili preplate.

9.2. Financijska odgovornost

Fina kao davatelj usluga certificiranja raspolaže financijskim sredstvima koja osiguravaju nesmetano pružanje usluga certificiranja neovisno o broju korisnika usluga i za cijelo vrijeme obavljanja usluga certificiranja.

9.2.1. Pokrivenost osiguranjem

Fina kao davatelj usluga certificiranja ima osiguran rizik od odgovornosti za štete koje nastanu obavljanjem usluga izdavanja kvalificiranih i nekvalificiranih certifikata.

Fina dodatno osigurava imovinu policom osiguranja koja pokriva osiguranje od rizika požara, vremenskih nepogoda, poplava, eksplozija i slično te osiguranja od loma stroja (industrijski lom) kojima se pokrivaju moguće nastale štete od ispada ili oštećenja instalacija i/ili strojne opreme, kao i osiguranje od loma stakla.

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.

Povjerljivi su i svi podaci koji se odnose na način i na sredstva kojim Fina CA-ovi upravlja certifikatima.

Povjerljivi su i svi privatni ključevi korisnika koje generiraju Fina CA-ovi i Fina LRA. Ukoliko Fina CA skladišti nekvalificirane certifikate standardne razine sigurnosti, skladištenje ključeva se provodi na siguran način sukladno točki 6.2.3 ovih Općih pravila. Privatne ključeve koje Fina CA ne skladišti, dostavlja korisniku, a najkasnije po dostavi korisniku njihove eventualne kopije na svojoj lokaciji Fina CA uništava na siguran način.

9.3.2. Podaci koji se ne smatraju povjerljivim poslovnim podacima

Poslovni podaci u bilo kojem obliku koje na bilo koji način između sebe razmjene sudionici u svezi s uspostavom i pružanjem usluge certificiranja, a koje sudionici ne označe povjerljivim, ili određenom vrstom ili stupnjem tajnosti, ili koji po svojoj prirodi nisu povjerljivi, jer se njihovim neovlaštenim otkrivanjem ne bi mogla prouzročiti šteta sudioniku, su podaci koji se ne smatraju povjerljivim poslovnim podacima.

Poslovni podaci koji se ugrađuju u sadržaj certifikata, koji se prikazuju u javnim evidencijama i/ili registrima, koji se za potrebe davanja usluge certificiranja moraju propisano voditi, 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

Fina primjenjuje odredbe Zakona o zaštiti osobnih podataka [9] i drugih propisa kojima je uređena zaštita osobnih podataka te tajnost podataka u Republici Hrvatskoj.

9.4.1. Plan zaštite osobnih podataka

Fina planira i provodi propisane tehničke, kadrovske i organizacijske mjere za zaštitu osobnih podataka od slučajne ili namjerne zlouporabe, uništenja, gubitka, neovlaštenih promjena ili dostupa.

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 davanje usluga certificiranja. Osobni podaci koje prikupi Fina ili vanjski ugovoreni RA i koji nisu sadržaj certifikata, koji se ne prikazuju u javnim evidencijama i/ili registrima koji se za potrebe davanja usluge certificiranja moraju propisano voditi, su povjerljivi osobni podaci koje Fina propisano 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, koji se prikazuju u javnim evidencijama i/ili registrima, koji se za potrebe davanja usluge certificiranja moraju propisano voditi, su osobni podaci koji zbog dostupnosti svima zainteresiranima nisu povjerljivi.

9.4.4. Odgovornost za zaštitu osobnih podataka

Fina i vanjski ugovoreni RA odgovorni su za zaštitu osobnih podatka, sukladno odredbama Zakona o zaštiti osobnih podataka [9] i drugih propisa, posebno onih kojima je uređena zaštita osobnih podataka u Republici Hrvatskoj.

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 osobne podatke samo temeljem pisane privole korisnika koja se može dati u zahtjevu za izdavanje certifikata ili kasnije.

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 Finino vlasništvo i bez Fininog izričitog dopuštenja nije dozvoljeno njeno neovlašteno korištenje.

Softver trećih strana koji se koristi u Fina PKI koristi se u skladu s odredbama prava korištenja.

9.6. Obveze i odgovornosti

9.6.1. Obveze i odgovornosti CA

Fina, kao davatelj usluga certificiranja, pri davanju usluga izdavanja i upravljanja životnim ciklusom certifikata primjenjuje Zakone [1], [2] i [3], podzakonske propise [4], [5], [6] i [7] donijete temeljem Zakona o elektroničkom potpisu [1], [2] i [3], obvezujuće međunarodne norme i preporuke, Opća pravila davanja usluga certificiranja Fina Root CA [34], ova Opća pravila te CPS_{QC} i CPS_{NQC} dokumente. Pri davanju usluga certificiranja Fina može primjenjivati i druge interne akte koji se temelje na ovim Općim pravilima.

Akte koji mogu biti javno dostupni Fina objavljuje na internetskim stranicama repozitorija iz točke 2.2 ovih Općih pravila.

Fina na internetskim stranicama repozitorija iz točke 2.2 ovih Općih pravila objavljuje sve obavijesti i informacije o promjenama u radu koje na bilo koji način mogu utjecati na sudionike Fina PKI.

Fina, kao davatelj usluga certificiranja, preko Fina RDC 2015 i Fina RDC-TDU 2015, izdaje kvalificirane certifikate u skladu s odredbama norme HRN ETSI/EN 319 411-2 [11], a nekvalificirane certifikate u skladu s odredbama norme HRN ETSI/EN 319 411-3 [12].

Tijekom pružanja usluge izdavanja certifikata i upravljanja životnim ciklusom certifikata Fina RDC 2015 i Fina RDC-TDU 2015 poštuju sve zahtjeve i odredbe propisane ovim Općim pravilima.

Fina se obvezuje da će CA usluge obavljati s pažnjom dobrog stručnjaka.

Prije izrade certifikata Fina RDC 2015 i Fina RDC-TDU 2015 moraju provjeriti autentičnost podataka o registraciji dostavljenih od strane RA mreže.

Fina CA-ovi izdaju certifikat temeljeći ga na pouzdano utvrđenom identitetu potpisnika ili skrbnika, poslovnog subjekta, osobe ovlaštene za zastupanje i drugim podacima o poslovnom subjektu.

Fina objavljuje izdani certifikat sukladno točki 4.4.2 ovih općih pravila.

Fina na temelju zahtjeva fizičke osobe i/ili poslovnog subjekta po provedenom propisanom postupku, opoziva ili suspendira certifikat te ga objavljuje u listi opozvanih certifikata.

Fina osigurava objavu ispravne liste opozvanih certifikata.

Fina u svom poslovanju primjenjuje organizacijske i tehničke mjere zaštite ključeva i certifikata.

Fina u svom poslovanju koristi podatke potpisnika, skrbnika, poslovnog subjekta i osobe ovlaštene za zastupanje. Povjerljivost podataka koji se sukladno točkama 9.3 i 9.4 smatraju povjerljivim Fina štiti i te podatke koristiti isključivo za potrebe usluga certificiranja iz opsega ovih Općih pravila te dodatnih usluga certificiranja iz skupa Fina PKI usluga (npr. izdavanje naprednih vremenskih žigova).

Fina osigurava da rad Fina RA mreže bude u skladu sa zakonskom regulativom o elektroničkom potpisu, ovim Općih pravilima te drugim aktima Fine za obavljanje CA usluga.

Fina osigurava da potpisnik, odnosno skrbnik posjeduje privatni ključ čiji se pripadajući javni ključ dostavlja na certificiranje.

Fina omogućava da se par ključeva subjekta generira na siguran način i da je tajnost privatnog ključa osigurana sukladno odredbama norme HRN ETSI/EN 319 411-2 [11]ili HRN ETSI/EN 319 411-3 [12], ovisno o tipu zahtijevanog certifikata.

Fina osigurava odgovarajući SSCD i njegovu zaštićenu dostavu potpisniku, odnosno skrbniku.

Fina provodi zahtijevane sigurnosne mjere za zaštitu prostora i opreme sustava certificiranja.

Fina sukladno najboljoj poslovnoj praksi osigurava nesmetan rad i maksimalnu raspoloživost usluga certificiranja.

Fina rješava zastoje i greške u radu sustava u najkraćem mogućem roku.

Fina planira održavanje i daljnji razvoj sustava certificiranja sukladno normama i razvojem tehnologije.

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

Fina je odgovorna za štetu uzrokovanu korisnicima ili pouzdajućim stranama koje ostvaruju razumno pouzdanje u certifikat u slučaju da ne ispuni slijedeće uvjete:

- provjeri točnost podataka u vrijeme registracije korisnika i da, ovisno o tipu traženog certifikata, izdani certifikat sadržava sve komponente opisane u poglavlju 7.1 ovih Općih pravila;
- osigura da je potpisnik ili skrbnik u vrijeme izdavanja certifikata posjedovao privatni ključ čiji je pripadajući javni ključ ugrađen u certifikat ili, ukoliko se par ključeva generira na lokaciji Fina CA ili Fina LRA, osigura siguran način generiranja i dostave privatnog ključa i pripadajućih aktivacijskih podataka;
- provede opoziv certifikata u pripadajućoj listi opozvanih certifikata po zahtjevu korisnika, osim ako Fina dokaže kako je djelovala s dužnom pažnjom.

Fina odgovara za štetu uzrokovanu nepoštivanjem mjerodavnih odredbi iz ovih Općih pravila u radu RA mreže. Ova odgovornost između Fine i vanjskih RA uređuje se ugovorom.

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 dana isteka zadnjeg obnovljenog certifikata za istog korisnika;
- osiguravanje od gubitka ili povrede povjerljivosti, cjelovitosti i dostupnosti arhiviranih podataka korisnika, na način propisan 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, privatne ključeve i aktivacijske podatke te ih koristiti u skladu s odredbama Zakona o elektroničkom potpisu [1], [2] i [3], odgovarajućim propisima i ovim Općim pravilima;

- poduzeti odgovarajuće mjere zaštite sredstva za izradu elektroničkog potpisa, 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 svog certifikata u slučaju kompromitiranja privatnog ključa, gubitka ili oštećenja sredstva za izradu elektroničkog potpisa, 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 u roku od dva dana od nastalih promjena, sukladno točki 4.8. ovih Općih pravila;
- djelovati u skladu sa svim ostalim odredbama iz ovih Općih pravila koje se odnose na obveze korisnika.

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, odnosno zatražiti promjenu podataka o skrbniku ukoliko se radi o poslovnim certifikatima izdanim za IT opremu.

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 biti će 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:

- koristila certifikat u svrhe propisane ovim Općim pravilima, 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;
- provjerila da certifikat nije istekao u vrijeme ostvarenja pouzdanja te da certifikat nije opozvan ili suspendiran, a što pouzdajuća strana treba utvrditi provodeći provjeru statusa certifikata temeljem zadnje izdane CRL kako je propisano u CP-u;
- provjerila da su svi podaci o identitetu subjekta certifikata ispravno prikazani aplikacijom u koju se može pouzdati;
- ako je u pitanju elektronički potpis, provjerila da je elektronički potpis izrađen privatnim ključem koji odgovara javnom ključu u certifikatu za vrijeme perioda valjanosti 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 se, ne poštujući propise i ova Opća pravila te protivno gore utvrđenim obvezama i odgovornostima iz ove točke, pouzdala u nevažeći certifikat (opozvani, istekli ili suspendirani certifikat), 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

Osim onog što je za Finu izričito navedeno u točki 9.6 ovih Općih pravila, Fina kao davatelj usluga certificiranja ne odgovora ni za koje drugo jamstvo ili odgovornost, posebno ne u slučaju ako bi do odgovornosti Fine prema danim jamstvima došlo zbog povrede jamstava i odgovornosti drugih sudionika navedenih u točki 9.6 Općih pravila.

Fina ne odgovara za uporabu certifikata izdanog od strane drugog davatelja usluga certificiranja ili za uporabu svog CA certifikata izvan Fina CA domene.

Fina nije odgovorna za štete, uključujući indirektne i specijalne 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 proizašle iz veze s uslugama certificiranja:

- štete pretrpljene u vremenu od opoziva certifikata do izdavanja sljedeće CRL;
- štete zbog neautorizirane uporabe korisničkih ključeva i certifikata;
- štete nastale uporabom certifikata u primjenama koje nisu dopuštene ovim Općim pravilima;
- štete prouzročene lažnom ili nemarnom uporabom certifikata ili CRL-a;
- štete nastale kao rezultat neispravnosti i pogrešaka u softveru i hardveru subjekta i pouzdajuće strane.

RA mreža nije odgovorna za štete, uključujući indirektne i specijalne 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 proizašle iz veze s uslugama certificiranja nastale kao rezultat prijevarnog davanja podataka i predstavljanja korisnika tijekom procesa identifikacije i potvrde identiteta ako je provjeru podataka provodila 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 3.500.000,00 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 1.4. Razine sigurnosti za certifikate koje izdaju Fina CA-ovi, na način prikazan u Tablici 9.1.

Kategorija certifikata	Maksimalna FININA financijska odgovornost		
	Po kategoriji	Po transakciji	Ukupno
Nekvalificirani certifikati standardne razine sigurnosti	do 100.000 kn	do 8.000 kn	3.500.000 kn
Nekvalificirani certifikati srednje razine sigurnosti	do 600.000 kn	do 80.000 kn	
Kvalificirani certifikati srednje razine sigurnosti	do 2.000.000 kn	do 80.000 kn	
Nekvalificirani certifikati visoke razine sigurnosti	do 800.000 kn	do 400.000 kn	

Tablica 9.1. Maksimalna FININA financijska odgovornost

9.9. Naknada štete

Svaki sudionik odgovara oštećenom za štetu koju je počinio zbog nepoštivanja odredbe ovih Općih pravila i važećih relevantnih propisa.

Potpisnik odnosno pravna ili fizička osoba, u čije ime potpisnik djeluje i koju predstavlja, odgovora oštećenom odnosno svakom drugom sudioniku ako ishodi i koristi certifikat izdan od Fina CA temeljem prijevarno danih podataka u zahtjevu za izdavanje certifikata.

Pouzdajuća strana odgovora oštećenom odnosno svakom drugom sudioniku ako se pouzda u izdani certifikat bez provjere njegove valjanosti opisane u točki 9.6.4 Općih pravila ili ga koristi protivno svrhama određenim ovim Općim pravilima.

Fina je odgovorna osobi koja se pouzdaje u certifikat samo ako je ta odgovornost jasno uspostavljena ugovorom, ovim Općim pravilima, pripadajućim internim CPS_{QC} [34], odnosno CPS_{NQC} [37] dokumentom ili hrvatskom zakonskom regulativom.

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.

9.10.3. Posljedice prestanka važenja i nastavak djelovanja

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

Novi dokument Općih pravila ne utječe na važenje certifikata koji su izdani primjenom prethodnih dokumenata Općih pravila. Certifikati izdani primjenom prethodnih Općih pravila važe do njihova isteka pri čemu se mogu obnoviti primjenom Općih pravila iz novog dokumenta.

9.11. Pojedinačne obavijesti i komunikacija sa sudionicima

Pojedinačne obavijesti i druga službena komunikacija treba se provoditi dopisima koji se dostavljaju u papirnatom obliku ili elektronički.

Kontaktni podaci za dostavu dopisa prema Fini	
Poštanska adresa:	Fina Centar elektroničkog poslovanja, (za Fina RDC) Ulica grada Vukovara 70 10000 Zagreb Hrvatska

E-mail:	info.rdc@fina.hr
Telefax:	+385-1-6304-081

U slučaju dostave elektroničkom poštom dopis mora biti potpisan naprednim elektroničkim potpisom pošiljatelja.

9.12. Izmjene i dopune

9.12.1. Procedure izmjena i dopuna

Ova Opća pravila revidiraju se po potrebi. Za sve izmjene i dopune odgovoran je Fina PMA.

Fina PMA može bez obavijesti unositi tipografske ispravke, promjene kontakt podataka te druge manje ispravke koji ne utječu bitno na sudionike.

Sve izmjene ovih Općih pravila koje mogu bitno utjecati na sudionike zahtijevaju njihovo obavještavanje. U pravilu, takve izmjene uvjetuju i izmjenu OID-a Općih pravila.

Svi sudionici mogu na kontakt adresu Fina PMA iz točke 1.5 ovih Općih pravila poslati dopis s prijedlogom za ispravke pogrešaka za prijedlog nadopuna ili izmjena ovog dokumenta. U dopis treba navesti kontakt podatke 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

Kopija ovog dokumenta dostupna je u elektroničkom obliku na internetskim stranicama repozitorija iz točke 2.2. ovih Općih pravila.

Datum objave i datum stupanja na snagu novoobjavljenog dokumenta Općih pravila naznačeni su na njegovoj naslovnoj strani kao i na internetskim stranicama na kojima je objavljen.

9.12.3. Okolnosti pod kojima se mora mijenjati OID

Manje izmjene sadržaja u dokumentu Općih pravila koje ne utječu bitno na sudionike ne uvjetuju izmjene OID-a dokumenta.

Veće izmjene u dokumentu Općih pravila koje mogu utjecati na sudionike zahtijevaju i izmjenu OID-a Općih pravila. U pravilu, Fina PMA inkrementalno određuje novi OID za novu verziju dokumenta.

9.13. Postupak rješavanja sporova

U slučaju spora ili neslaganja među sudionicima 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.

Potpisnik odnosno pravna ili fizička osoba u čije ime potpisnik djeluje i koju predstavlja može Fini uputiti prigovor ako smatra da u njegovu slučaju postoji odstupanje sadržaja usluge u odnosu na ugovoreno. Fina će povodom prigovora odgovoriti podnositelju prigovora. Prigovor i odgovor na prigovor upućuju se pisano u papirnatom ili elektroničkom obliku na način opisan u točki 9.11. ovih Općih pravila.

U slučaju spora ili neslaganja između Fine (kao davatelja usluge certificiranja uređene ovim Općim pravilima) i potpisnika odnosno pravne ili fizičke osobe u čije ime potpisnik djeluje i koju predstavlja, povodom prigovora o navodnom odstupanju sadržaja usluge u odnosu na ugovoreno, 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.

U slučaju spora ili neslaganja između Fine, kao davatelja usluge certificiranja uređene ovim Općim pravilima, i vanjskog ugovorenog RA, postupak rješavanja spora reguliran je međusobnim ugovorom.

9.14. Važeći propisi

Za tumačenje odredaba ovih Općih pravila mjerodavne su odredbe Zakona o elektroničkom potpisu [1], [2] i [3], podzakonskih akata donesenih temeljem tog zakona [4], [5], [6] i [7] te propisa, normizacijskih dokumenata i preporuka na koje iste upućuju.

9.15. Usklađenost s važećim propisima

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

9.16. Razne odredbe

Fina u svojstvu davatelja usluga certificiranja može sa sudionicima sklopiti dodatni ugovor ukoliko to nije protivno zakonskim propisima.