FINA
PRAVILNIK O POSTUPCIMA CERTIFICIRANJA ZA KVALIFICIRANE CERTIFIKATE
(dokument za javnu objavu)

Verzija 5.0

Datum stupanja na snagu: 7.12.2015.

OID Dokumenta: 1.3.124.1104.5.0.0.2.5.0

Informacije o dokumentu

Ime dokumenta:	Fina - Pravilnik o postupcima certificiranja za kvalificirane certifikate (dokument za javnu objavu)
OID dokumenta:	1.3.124.1104.5.0.0.2.5.0
Tip dokumenta:	Pravilnik o postupcima certificiranja za kvalificirane certifikate (CPS_{QC})
Oznaka distribucije	Javno
Vlasnik dokumenta	Fina
Kontakt	pma@fina.hr

Povijest izmjena

Verzija	Datum	Razlog izmjene
3.0	15.07.2002.	
3.1	15.9.2002.	Dopuna tipova certifikata i ispravci uočenih grešaka
3.2	31.03.2003.	Dopuna postupaka registracije i izdavanja certifikata, izmjena u razinama sigurnosti klasa certifikata
4.0	6.11.2013.	Usklađivanje s pravilnicima [5] i [6], Popisom normizacijskih dokumenata [7] te s preporukom IETF RFC 3647 [18]
4.1	1.10.2015.	Ugradnja Izmjena i dopuna Pravilnika o postupcima certificiranja za kvalificirane certifikate 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.

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 319 412-5 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)

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

[14] ETSI TS 119 403 - Electronic Signatures and Infrastructures (ESI);Trust Service Provider Conformity Assessment

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

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

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

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

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

[20] IETF RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

[21] IETF RFC 5322 - Internet Message Format

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

[23] 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)

[24] HRN ISO/IEC 27001:2006 Informacijska tehnologija – Sigurnosne tehnike – Sustavi upravljanja informacijskom sigurnošću – Zahtjevi (ISO/IEC 27001:2005)

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

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

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

[28] NIST FIPS PUB 186-3: Digital Signature Standard (DSS)

[29] ITU-T Recommendation X.509:2000 / ISO/IEC 9594-8:2001: Information technology – Open Systems Interconnection – The Directory: Public-key attribute certificate frameworks

[30] ITU-T Recommendation X.501:2008 - Information technology – Open Systems Interconnection – The Directory: Models

[31] CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v1.2.3

Javni Finini dokumenti

[32] Fina – Opća pravila davanja usluga certificiranja Fina Root CA, v1.0

[33] Fina – Opća pravila davanja usluga certificiranja, v5.0

Interni Finini dokumenti

[34] Fina – Pravilnik o postupcima certificiranja Fina Root CA, CPS_{ROOT}, v1.0

[35] Fina PKI - Pravilnik o postupcima certificiranja za nekvalificirane certifikate, CPS_{NQC}, v5.0

1. UVOD

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 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, pri tom 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 izdao certifikate za njemu 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 [32].

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).

Postupci certificiranja koji se odnose se na Fina Root CA i na cijelu Fina PKI hijerarhiju zasnovanu na Fina Root CA opisani su u dokumentu Pravilnik o postupcima certificiranja Fina Root CA, CPS_{ROOT} [34].

1.1.1. Opseg i namjena

Ovaj **Fina - Pravilnik o postupcima certificiranja za kvalificirane certifikate (dokument za javnu objavu)**, (u daljnjem tekstu CPS_{QC}) odgovara dokumentu „Posebna unutarnja pravila o postupcima izdavanja certifikata i zaštiti sustava certificiranja“ definiranom u Pravilniku o evidenciji davatelja usluga certificiranja [4] i opisuje postupke i procedure koje primjenjuje Fina PKI na izdavanje i upravljanje životnim ciklusom produkcijskih kvalificiranih digitalnih certifikata (u daljnjem tekstu: kvalificirani certifikati), a sukladno zahtjevima iz Fina

PKI - Općih pravila davanja usluga certificiranja (u daljnjem tekstu: Opća pravila) [33] u dijelu koji se odnose na izdavanje **kvalificiranih certifikata**.

Ovaj CPS_{QC} dokument namijenjen javnom objavljivanju predstavlja **izvadak Fininog internog Pravilnika o postupcima certificiranja za kvalificirane certifikate, verzija 5.0** te pruža sudionicima Fina PKI informacije o Fina PKI postupcima i procedurama, ne otkrivajući pri tome povjerljive poslovne podatke Fine sadržane u internim pravilnicima, procedurama i drugim internim dokumentima Fine.

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 su usklađeni 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 [12] i preporuke IETF RFC 3739 [19]. Navedeni kvalificirani certifikati imaju oznaku QCP+.

Produkcijski kvalificirane certifikati iz opsega ovog CPS_{QC} dokumenata, zajedno s produkcijskim certifikatima iz opsega CPS_{NQC} dokumenata, čine Registar digitalnih certifikata (Fina RDC), a koji se sastoji od dva certifikacijska tijela (CA) iz opsega ovog CPS_{QC} dokumenta: Fina RDC 2015 i Fina RDC-TDU 2015.

CPS_{QC} je usklađen s dokumentom Opća pravila [33] u dijelu koji se odnosi na kvalificirane certifikate.

Opća pravila [33] objavljena su na internetskoj stranici http://www.fina.hr/finadigicert.

U okviru ovog CPS_{QC} dokumenta pod produkcijskim CA-ovima unutar Fina PKI podrazumijevaju se Fina RDC 2015 i Fina RDC-TDU 2015 (u daljnjem tekstu, zajedničkim imenom: Fina CA-ovi). U dijelovima ovog CPS_{QC} dokumenta u kojima se koristi termin Fina CA, svi postupci i procedure navedene u pojedinim točkama dokumenta koje provode Fina CA-ovi su obvezujuće za oba produkcijska Fina CA koja djeluju unutar Fina PKI. Ukoliko postoje razlike u provedbi postupaka i procedura između Fina RDC CA i Fina RDC-TDU 2015 iste će biti posebno naznačene u točkama u kojima se takve razlike pojavljuju.

1.1.2. Tipovi certifikata

Fina kao davatelj usluga certificiranja za korisnike izdaje sljedeće grupe kvalificiranih certifikata iz opsega ovog CPS_{QC} dokumenta:

- Fina RDC 2015 osobni kvalificirani certifikati;
- Fina RDC 2015 poslovni kvalificirani certifikati;
- Fina RDC-TDU 2015 kvalificirani certifikati.

Svaki tip certifikata ima naziv i jedinstven OID pravila certificiranja (CP-OID).

Tablica 1.1. prikazuje tipove kvalificiranih certifikata iz opsega CPS_{QC} ovog dokumenta s nazivima i pripadajućim CP OID-ovima, po grupama za pojedini Fina CA.

Fina Registar digitalnih certifikata (Fina RDC)		
Fina RDC 2015		
Fina RDC 2015 osobni kvalificirani certifikati	Osobni potpisni Q2 certifikat (QCP+)	CP OID: 1.3.124.1104.5.12.1.2.2
Fina RDC 2015 poslovni kvalificirani certifikati	Poslovni potpisni Q2 certifikat (QCP+)	CP OID: 1.3.124.1104.5.12.2.2.2
Fina RDC-TDU 2015		
Fina RDC-TDU 2015 kvalificirani certifikati	TDU potpisni Q2 certifikat (QCP+)	CP OID: 1.3.124.1104.5.22.2.2.2

Tablica 1.1. Tipovi certifikata

1.2. Naziv dokumenta i identifikacijski podaci

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

- Naziv dokumenta: Fina - Pravilnik o postupcima certificiranja za kvalificirane certifikate (dokument za javnu objavu)
- Verzija: 5.0
- Datum stupanja na snagu: 7.12.2015.
- OID: 1.3.124.1104.5.0.0.2.5.0

1.3. Sudionici u PKI

Sudionici Fina PKI iz opsega ovog CPS_{QC} dokumenta su fizičke osobe, tijela unutar Fine i pravni subjekti koji u Fina PKI sudjeluju kao korisnici usluga certificiranja, ili kao davatelji pojedinih podusluga vezanih uz obavljanje poslova certificiranja, a koje Fina koristi za potrebe obavljanja usluga certificiranja.

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 Authorities*, LRA-ovi);
- korisnici;
- pouzdajuće strane;
- ostali sudionici:
  - proizvođači IT opreme za PKI;
  - proizvođači sigurnih uređaja (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 procedure te za kontrolu provođenja istih.

1.3.2. Certifikacijska tijela

Certifikacijska tijela u Fina PKI iz opsega ovog CPS_{QC} dokumenta su Fina RDC 2015 i Fina RDC-TDU 2015 (zajedničkim imenom: Fina CA-ovi). Fina CA-ovi su obvezni usluge izdavanja certifikata i upravljanja životnim ciklusom izdanih certifikata obavljati sukladno postupcima iz ovog CPS_{QC} dokumenta koji je usklađen s Općim pravilima [33].

Obaveze i odgovornosti Fina CA-ova navedeni su u točki 9.6.1 ovog CPS_{QC} dokumenta. Postupci koje Fina CA-ovi provode u cilju ispunjenja zahtjeva za kvalificirane certifikate iz Općih pravila [33] opisani su u ovom CPS_{QC} dokumentu.

1.3.2.1. Fina RDC 2015

Fina RDC 2015 iz opsega ovog CPS_{QC} dokumenta izdaje certifikate za sljedeće grupe tipova kvalificiranih certifikata:

- Fina RDC 2015 osobni kvalificirani certifikati;
- Fina RDC 2015 poslovni kvalificirani certifikati.

Osnovni podaci o Fina RDC 2015 certifikatu dani su u tablici 1.2.:

Polje	Vrijednost za Fina RDC 2015 CA
Version	V3, vrijednost="2"
serialNumber	Serijski broj certifikata s entropijom od 32 bita (duljina serijskog broja:12 ili 13 bajtova)
signatureAlgorithm	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)
Issuer	cn=Fina Root CA, o=Financijska agencija, c=HR
Validity	NotBefore: Datum i vrijeme izdavanja NotAfter: 10 godina nakon datuma i vremena izdavanja
Subject	cn=Fina RDC 2015, o=Financijska agencija, c=HR
SubjectPublicKeyInfo	rsaEncryption (OID: 1.2.840.113549.1.1.1), javni ključ duljine 4096 bitova

Tablica 1.2. Osnovni podaci o Fina RDC 2015 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

Fina RDC-TDU 2015 iz opsega ovog CPS_{QC} dokumenta izdaje certifikate državnim dužnosnicima i zaposlenicima u tijelima državne uprave.

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

Polje	Vrijednost za Fina RDC-TDU 2015
Version	V3, vrijednost="2"
serialNumber	Serijski broj certifikata s entropijom od 32 bita (duljina serijskog broja:12 ili 13 bajtova)
signatureAlgorithm	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)
Issuer	cn=Fina Root CA, o=Financijska agencija, c=HR
Validity	NotBefore: Datum i vrijeme izdavanja NotAfter: 10 godina nakon datuma i vremena izdavanja
Subject	cn=Fina RDC-TDU 2015, o=Financijska agencija, c=HR
SubjectPublicKeyInfo	rsaEncryption (OID: 1.2.840.113549.1.1.1), javni ključ duljine 4096 bitova

Tablica 1.3. Osnovni podaci o Fina RDC-TDU 2015 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 obavljaju se u registracijskim uredima Fine. Za potrebe registracije korisnika za Fina CA, Fina ima s drugim poslovnim subjektima sklopljene ugovore o obavljanju usluga 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 čine Središnji Fina RA kao dio Odjela RDC, te mreža lokalnih registracijskih ureda u poslovnoj mreži Fine (u daljnjem tekstu: Fina LRA). Poslove registracije korisnika u Fina LRA obavljaju zaposlenici Fine u organizacijskim jedinicama Odsjek registra računa u regionalnim centrima, odnosno podružnicama, poslovnicama i poslovnim jedinicama (u daljnjem tekstu LRA službenici). Iznimno, poslove registracije korisnika obavljaju službenici Središnjeg Fina RA. Poslovima registracije u Fina RA mreži koordinira Središnji Fina RA koji je središnja komunikacijska točka Fina RA mreže. Popis aktualnih registracijskih ureda Fina LRA nalazi se na internetskoj adresi http://www.fina.hr/finadigicert.

Mreža vanjskog ugovorenog RA je mreža lokalnih registracijskih ureda poslovnog subjekta s kojim je Fina sklopila ugovor o obavljanju usluga registracije za Fina CA-ove. 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 je obvezna registraciju korisnika za izdavanje certifikata provoditi sukladno postupcima opisanim u ovom CPS_{QC} dokumentu.

Obveze i odgovornosti Fina RA mreže i vanjskih ugovorenih RA navedene su u točki 9.6.2 ovog CPS_{QC} dokumenta.

1.3.4. Korisnici

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

Usluge certificiranja iz opsega ovog CPS_{QC} dokumenta koje korisnici ugovaraju su usluge iz područja izdavanja i upravljanja životnim vijekom kvalificiranih certifikata.

Korisnici Fina PKI mogu biti:

- fizičke osobe – građani; i
- poslovni subjekti.

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

Da bi korisnici mogli koristiti usluge certificiranja korisnici trebaju obaviti proceduru registracije i predaje zahtjeva te prihvatiti obveze i odgovornosti koje su navedene u točki 9.6.3 Općih pravila [33]. U sklopu procedure registracije korisnici s Finom sklapaju ugovor o obavljanju usluga certificiranja. Ukoliko korisnik podnosi zahtjev za osobnim certifikatom ugovor potpisuje i sklapa fizička osoba – građanin (potpisnik). Kod poslovnih certifikata ugovor potpisuje pripadajuća osoba (potpisnik), a ovlaštena osoba poslovnog subjekta potpisuje i ovjerava ugovor u ime poslovnog subjekta kojeg predstavlja. TDU sklapaju s Finom ugovor o obavljanju usluge certificiranja koji ima funkciju krovnog ugovora. Ovaj ugovor potpisuje i ovjerava ovlaštena osoba TDU. Svaka pripadajuća osoba (potpisnik) iz TDU u sklopu registracije sklapa s Finom pojedinačni ugovor kojeg potpisuje pripadajuća osoba (potpisnik) te kojeg ovjerava ovlaštena osoba TDU potpisom i pečatom.

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

1.3.4.1. Subjekti certificiranja

Pri izradi kvalificiranog certifikata u certifikat se ugrađuju identifikacijski podaci subjekta certificiranja za kojeg se certifikat izdaje. Subjekt certificiranja kod izdavanja kvalificiranog certifikata može biti fizička osoba-građanin ili pripadajuća osoba. Podaci o subjektu sastavni su dio certifikata.

1.3.5. Pouzdajuće strane

Pouzdajuće strane su fizičke osobe ili poslovni subjekti koje 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.

Obveze i odgovornosti pouzdajuće strane navedene su u točki 9.6.4 CPS_{QC} dokumenta.

1.3.6. Ostali sudionici

Ostali sudionici Fina PKI su pravne osobe koje ne pružaju niti 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 procjenitelji i sl.

1.4. Uporaba certifikata

Na temelju namjene, dozvoljene uporabe i ograničenja uporabe tipa certifikata pouzdajuća strana odlučuje da li je pojedini tip certifikata prikladan i pouzdan za korištenje i prihvaćanje. Pouzdajuća strana je odgovorna za prihvaćanje i ostvarivanje razumnog pouzdanja u kvalificirani certifikat. Pri donošenju odluke o prihvaćanju kvalificiranog certifikata 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 dokument Opća pravila [33], odnosno ovaj CPS_{QC} dokument;
- 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.

Fina CA-ovi izdaju kvalificirane certifikate srednje razine sigurnosti.

Certifikati srednje razine sigurnosti su prikladni za uporabu u transakcijama koje imaju umjerenu vrijednost. Primjena certifikata srednja razine sigurnosti prikladna je u okolinama u kojima potencijalna zlouporaba certifikata može nanijeti umjerenu štetu ili u okolinama u

kojima je rizik od zlouporabe certifikata umjeren. Preporučeni financijski limit za srednju razinu sigurnosti certifikata je do 80.000 kn.

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

Fina RDC 2015 i Fina RDC-TDU 2015 potpisni QCP+ kvalificirani certifikati usklađeni su s općim pravilima QCP public + SSCD normizacijskog dokumenta HRN ETSI/EN 319 411-2 [11] i njihova je uporaba ograničena isključivo na podršku naprednom elektroničkom potpisu u smislu Zakona o elektroničkom potpisu [1], [2] i [3].

Ova točka obuhvaća sljedeće tipove certifikata:

- Osobni potpisni Q2 certifikat (QCP+), izdaje se fizičkim osobama – građanima, za privatnu uporabu. Fizička osoba – građanin može ovaj certifikat koristiti i za poslovnu uporabu, ukoliko pri tome 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 izdaju potpisnicima isključivo na SSCD uređaj, primjerice na adekvatnu *smart* karticu ili USB token.

Ekstenzija *keyUsage* je u ovim certifikatima označena kritičnom te isključivo ima vrijednost postavljenu na *nonRepudation*. 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.

1.4.2. Zabrane uporabe certifikata

Sve uporabe kvalificiranih certifikata različite od uporaba navedenih u točki 1.4.1 ovog CPS_{QC} dokumenta su zabranjene.

1.5. Administracija CPS_{QC} dokumenta

1.5.1. Organizacija odgovorna za održavanje CPS_{QC} dokumenta

Za izradu i održavanje CPS_{QC} dokumenta odgovorno je tijelo za upravljanje pravilima certificiranja Fina PMA (vidi točku 1.3. CPS_{QC} dokumenta).

1.5.2. Kontakt podaci

Kontakt podaci za administraciju i sadržaj ovog CPS_{QC} dokumenta:

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_{QC} dokumenta s Općim pravilima

Uskladivost CPS_{QC} dokumenta s Općim pravilima [33] utvrđuje Fina PMA.

1.5.4. Procedure odobravanja CPS_{QC} dokumenta

Da bi se CPS_{QC} dokument mogao primjenjivati prethodno mora biti odobren od strane Fina PMA. Početak važenja i stupanja CPS_{QC} dokumenta određuje Fina PMA.

Nakon izmjene zakonske regulative, popisa obvezujućih normizacijskih dokumenata, poslovnog procesa vezanog za izdavanje kvalificiranih certifikata ili izmjene Općih pravila davanja usluga certificiranja Fina Root CA [33] ili Općih pravila [33], a koja utječu na postupke iz opsega CPS_{QC} dokumenta, provodi se revizija CPS_{QC} dokumenta provjerom usklađenosti s:

- novom zakonskom regulativom;
- novim normizacijskim dokumentima;
- novim Općim pravilima davanja usluga certificiranja Fina Root CA [32], Općim pravilima [33], odnosno novim Pravilnikom o postupcima certificiranja Fina Root CA [34].

Nakon provedenog usklađenja, Fina PMA odobrava novi CPS_{QC} dokument.

Početak važenja novog CPS_{QC} dokumenta određuje se na osnovu procjene spremnosti sustava certificiranja na rad po novim procedurama propisanih ovim dokumentom. Stupanjem na snagu nove verzije CPS_{QC} dokumenta započinje i primjena postupaka koji su njime opisani.

1.6. Definicije i kratice

1.6.1. Definicije

DEFINICIJA	ZNAČENJE
CA privatni potpisni ključ	Privatni ključ CA koji s javnim CA ključem čini par CA ključeva. CA privatni potpisni ključ se koristi 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 izdao i potpisao taj isti CA, tj. subjekt certificiranja je isti CA koji sam sebi i izdaje certifikat. CA root certifikat sadrži javni ključ i naziv CA koji je izdao certifikat.
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 npr. usluga izdavanja vremenskog žiga, usluga izrade elektroničkog potpisa, usluga verifikacije elektroničkog potpisa, usluga dugotrajnog čuvanja elektronički potpisanih zapisa i sl.
Davatelj usluga izdavanja kvalificiranih certifikata	Pravna ili fizička osoba koja izdaje kvalificirane certifikate.
Dekripcija	Proces u kriptografiji kojim se enkriptirani podaci pretvaraju u razumljive podatke, korištenjem dekripcijskog ključa i dekripcijskog algoritma.
Dekripcijski ključ	Ključ koji se koristi uz dekripcijski algoritam za dekripciju podataka u cilju dobivanja razumljivih podataka iz enkriptiranih. Kod asimetrične kriptografije dekripcija podataka se obavlja korištenjem privatnog ključa primatelja. Kod elektroničkog potpisa dekripcija sažetka potpisanih podataka se obavlja javnim ključem potpisnika.

DEFINICIJA	ZNAČENJE
Digitalni potpis	Podaci koji se dodaju podatkovnom skupu ili kriptografska transformacija podatkovnog skupa koja omogućuje njegovom primatelju dokazivanje izvornosti i cjelovitosti podatkovnog slupa 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.
Elektronički zapis	Cjelovit skup podataka koji su elektronički generirani, poslani, primljeni ili sačuvani na elektroničkom, magnetnom, optičkom ili drugom mediju. Sadržaj elektroničkog zapisa uključuje sve oblike pisanog i drugog teksta, podatke, slike i crteže, karte, zvuk, glazbu, govor, računalne baze podataka.
Enkripcija	Proces u kriptografiji kojim se podaci mijenjaju tako da se informacije učine nerazumljivim za subjekte koje ne posjeduju odgovarajući dekripcijski ključ. Uporabom dekripcijskog ključa u postupku dekripcije ove se informacije ponovno mogu učiniti razumljivim.
Enkripcijski ključ	Ključ koji se koristi uz enkripcijski algoritam u cilju enkripcije podataka. Kod asimetrične kriptografije enkripcija podataka se obavlja korištenjem javnog ključa primatelja. Kod elektroničkog potpisa enkripcija sažetka se obavlja privatnim ključem potpisnika.
Fina LRA	LRA (lokalni registracijski ured) u Fina poslovnoj mreži.
Fina PKI	Infrastruktura javnog ključa (PKI) uspostavljena u Fini koja je namijenjena za pružanje usluga certificiranja fizičkim osobama – građanima, poslovnim subjektima i tijelima državne uprave, a koja je uspostavljena kao treća strana od povjerenja (engl. *Trusted Third Party*).
Fina RDC	Registar digitalnih certifikata kojeg vodi Fina za pružanje usluga izdavanja i upravljanja životnim ciklusom digitalnih certifikata.
Generiranje ključeva	Proces koji izrađuje niz simbola koji čine kriptografski ključ.
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 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.

DEFINICIJA	ZNAČENJE
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 (ako je javno objavljen kao dekripcijski ključ) ili za enkripciju podataka (ako je javno objavljen kao enkripcijski ključ).
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	Općenito, za usluge certificiranja: Fizička osoba-građanin ili poslovni subjekt kojima davatelj usluga certificiranja daje usluge, odnosno s kojim sklapa ugovor o korištenju usluga certificiranja. Za uslugu izdavanja vremenskog žiga: Fizička osoba-građanin ili poslovni subjekt kojima davatelj usluga izdavanja vremenskog žiga daje uslugu, odnosno s kojim sklapa ugovoru o pružanju usluge izdavanja vremenskog žiga.
Kriptografski modul	Softver ili uređaj određene razine sigurnosti koji: • generira par ključeva; i/ili • štiti kriptografske informacije; i/ili • obavlja kriptografske funkcije.
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.
***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.

DEFINICIJA	ZNAČENJE
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.
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).
***Online* provjera statusa certifikata (OCSP)**	Provjera statusa valjanosti certifikata koja se obavlja *online*. Primjer *online* provjere statusa certifikata je i provjera opozvanosti certifikata pomoću *online* preuzete CRL. Ako se *online* provjera statusa certifikata obavlja preko CRL, provjerava se samo zadnje izdana CRL.
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.
Oporavak certifikata	Postupak ponovnog izdavanja certifikata s novim parom ključeva, s istim DN-om i novim periodom valjanosti certifikata koji se provodi prije nastupanja rokova za obnovu certifikata.
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.
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.
Policy Management Authority (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.

DEFINICIJA	ZNAČENJE
Poslovni subjekt	1. Pravne osobe, primjerice • trgovačka društva; • kreditne i financijske institucije; • javne i privatne ustanove; • udruge s pravnom osobnošću; • neprofitne i nevladine organizacije s pravnom osobnošću; • fondovi s pravnom osobnošću; • jedinice lokalne i područne (regionalne) samouprave (općine, gradovi i županije) i dr. 2. Tijela javne vlasti, primjerice • tijela državne vlasti; • tijela državne uprave; • državne agencije i dr. 3. Fizičke osobe s registriranom djelatnošću, primjerice • obrtnici; • odvjetnici; • javni bilježnici; • javni ovršitelji i dr.
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	Za certifikat: Primatelj certifikata, koji djeluje temeljem razumnog pouzdanja u certifikat. Certifikat omogućuje pouzdajućoj strani provjeru cjelovitost i izvornosti elektronički potpisanog zapisa odnosno provjeru identiteta subjekta. Za vremenski žig: Primatelj vremenskog žiga koji se pouzdaje u taj vremenski žig.
Povjerljive uloge	Uloge o kojima ovisi sigurnost rada davatelja usluga izdavanja kvalificiranih certifikata. Povjerljive uloge (engl. Trusted Roles) i pripadne odgovornosti moraju biti jasno određene. Povjerljive uloge i odgovornosti opisane su 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).

DEFINICIJA	ZNAČENJE
Prihvaćanje certifikata	Postupci i radnje podnositelja zahtjeva za izdavanje certifikata na osnovu kojih se može smatrati da je certifikat prihvaćen od strane potpisnika ili skrbnika. Npr., može se smatrati da je certifikat prihvaćen ukoliko je potpisnik ili skrbnik potpisao prihvaćanje izdanog certifikata ili ako CA unutar određenog vremena nije primio nikakvu reklamaciju od korisnika. Korisnik može poslati potpisanu poruku o prihvaćanju certifikata ili korisnik može poslati potpisanu poruku kojom odbija prihvatiti certifikat s time da u poruci naznači razlog za odbijanje certifikata i označi polja u certifikatu koja nisu točna ili potpuna.
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.
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.
RA/LRA službenik	Ovlašteni zaposlenik lokalnog registracijskog ureda, odnosno registracijskog ureda koji obavlja registraciju, uz identifikaciju i potvrđivanje identiteta korisnika.
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.

DEFINICIJA	ZNAČENJE
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 liste 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.
Registracijski ured (RA)	Pravna ili fizička osoba ovlaštena od CA i zadužena za identifikaciju i potvrdu identiteta podnositelja zahtjeva za izdavanje, opoziv, suspenziju, reaktivaciju ili oporavak 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, za potpis koda 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 elektroničke identifikacije	Materijalna i/ili nematerijalna jedinica koja sadrži osobne identifikacijske podatke i koja se koristi za autentikaciju na *online* uslugu.

DEFINICIJA	ZNAČENJE
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.
Sredstvo za verificiranje potpisa	Odgovarajuća računalna oprema ili računalni program koji se koristi za primjenu podataka za verificiranje 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, središnji državni uredi Vlade Republike Hrvatske, državne upravne organizacije i uredi državne uprave u županijama ili druga tijela državne uprave utvrđena mjerodavnim važećim zakonom.
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.
Vanjski LRA	Lokalni registracijski ured pod ingerencijom vanjskog ugovornog 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 1.4. - Definicije

1.6.2. Kratice

KRATICA	PUNI NAZIV	ZNAČENJE
CA	Certification Authority	Certifikacijsko tijelo
CP	Certification Policy	Opća pravila davanja usluga certificiranja
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
CRL	Certificate Revocation List	Lista opozvanih certifikata
CSP	Certification Service Provider	Davatelj usluga certificiranja
DN	Distinguished Name	Razlikovno ime
DNS	Domain Name System	Sustav za prevođenje naziva računala u odgovarajuće IP adrese
DR	*Disasier Recovery*	Oporavak od katastrofe
ISO	International Standards Organization	Međunarodna organizacija za normizaciju
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
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
SW	Software	Programska podrška

KRATICA	PUNI NAZIV	ZNAČENJE
TDU	Tijelo (ili tijela) državne uprave	Tijelo (ili tijela) državne uprave
TLS	Transport Layer Security	Kriptografski protokol za sigurnu razmjenu podataka putem Interneta
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 1.5. - Kratice

2. OBJAVE I ODGOVORNOSTI ZA REPOZITORIJ

2.1. Identifikacija tijela koje vodi repozitorij

Fina PKI repozitorije vodi Fina kao davatelj usluga certificiranja. Fina je odgovorna za rad Fina PKI repozitorija kao i za objavu dokumenata i informacija na repozitorijima. Fina PKI repozitorij iz domene kvalificiranih certifikata čine sljedeća dva repozitorija:

- Fina RDC 2015 repozitorij čiji sadržaj operativno ažurira Fina RDC 2015;
- Fina RDC-TDU 2015 repozitorij čiji sadržaj operativno ažurira Fina RDC-TDU 2015.

Pojedini repozitorij se sastoji od dijela dostupnog preko internetskih stranica i dijela dostupnog preko LDAP poslužitelja.

2.2. Objava informacija o certificiranju

Na Fina PKI repozitorijima javno se objavljuju sljedeći dokumenti i informacije o davanju usluga certificiranja:

2.2.1. Fina RDC 2015 repozitorij

Na internetskim stranicama objavljeni su sljedeći dokumenti i informacije:

- Aktualna Opća pravila davanja usluga certificiranja;
- Prijašnje verzije Općih pravila davanja usluga certificiranja;
- Uvjeti pružanja usluga certificiranja;
- Opis važećih profila certifikata;
- Cjenik PKI usluga;
- Obrasci zahtjeva za izdavanje certifikata;
- Obrasci ugovora o obavljanju usluga certificiranja;
- Obrasci zahtjeva za opoziv, suspenziju, reaktivaciju ili oporavak certifikata;
- Obrasci punomoći;
- Informacije o Fina RDC 2015 certifikatu;
- Objedinjena CRL sustava Fina RDC 2015;
- Informacije o zakonskoj regulativi iz područja elektroničkog potpisa i davanja usluga certificiranja;
- Informacije o postojanju dokumenata važnim za poslovanje koji ne mogu biti u cijelosti ili uopće objavljeni zbog osjetljivosti ili tajnosti sadržaja;
- Aktualne lokacije Fina RA/LRA ureda;
- Korisničke upute;
- Obavijesti korisnicima vezane uz davanje usluga certificiranja;
- Ostale informacije vezane uz rad Fina RDC 2015.

Preko internetske stranice repozitorija moguće je pretraživanje javnog imenika certifikata koje je izdao Fina RDC 2015.

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

U strukturi javnog imenika javno se objavljuju:

- izdani kvalificirani certifikati;
- objedinjena CRL i segmentirana CRL sustava Fina RDC 2015.

Informacije objavljene na javnom imeniku dostupne su sa adrese ldap://rdc-ldap2.fina.hr.

Adrese Fina RDC 2015 repozitorija na kojima se objavljuju CRL navedene su u točki 4.10.1 CPS_{QC} dokumenta.

2.2.2. Fina RDC-TDU 2015 repozitorij

Na internetskim stranicama se objavljuju sljedeći dokumenti i informacije:

- Aktualna Opća pravila davanja usluga certificiranja;
- Prijašnje verzije Općih pravila davanja usluga certificiranja;
- Uvjeti pružanja usluga certificiranja;
- Izjava o pružanju usluga certificiranja;
- Opis važećih profila certifikata;
- Cjenik PKI usluga;
- Obrasci zahtjeva za izdavanje certifikata;
- Obrasci ugovora o obavljanju usluga certificiranja;
- Obrasci zahtjeva za opoziv, suspenziju, reaktivaciju ili oporavak certifikata;
- Obrasci punomoći;
- Informacije o Fina RDC-TDU 2015 certifikatu;
- Objedinjena CRL sustava Fina RDC-TDU 2015;
- Informacije o zakonskoj regulativi iz područja elektroničkog potpisa i davanja usluga certificiranja za TDU;
- Informacije o postojanju dokumenata važnim za poslovanje koji ne mogu biti u cijelosti ili uopće objavljeni zbog osjetljivosti ili tajnosti sadržaja;
- Aktualne lokacije Fina RA/LRA ureda;
- Korisničke upute;
- Obavijesti korisnicima vezane uz davanje usluga certificiranja;
- Ostale informacije vezane uz rad Fina RDC-TDU 2015.

Objavljeni sadržaj na internetskoj stranici dostupan je s adrese http://www.fina.hr/finadigicert.

U strukturi javnog imenika javno se objavljuju:

- svi izdani kvalificirani certifikati;
- objedinjena CRL i segmentirana CRL sustava Fina RDC-TDU 2015.

Informacije objavljene na javnom imeniku dostupne su sa adrese ldap://rdc-ldap2.fina.hr.

Adrese Fina RDC-TDU 2015 repozitorija na kojima se objavljuju CRL navedene su u točki 4.10.1 CPS_{QC} dokumenta.

U Fina PKI repozitorijima nisu javno objavljeni dokumenti koji predstavljaju povjerljivi dio internih pravila certificiranja.

2.2.3. Postupci objave sadržaja i upravljanja repozitorijem

Trajanje važenja i prestanak važenja Općih pravila [33] definirani su u točkama 9.10.1. i 9.10.2. Općih pravila [33], a određuje ih i odobrava Fina PMA. Prijašnje verzije dokumenta ostaju objavljene na repozitoriju, uz naznaku vremenskog perioda kad su vrijedile.

Obavijesti korisnicima, informacije o zakonskim aktima objavljuju se po početku primjene zakonskih akata u Fina PKI.

Informacije o certifikatima Fina CA-ova objavljuju se po njihovu izdavanju.

Dokumente o uvjetima pružanja usluga, korisničke upute, obrasce zahtjeva, ugovora i punomoći odobrava Fina PMA. Objava ovih dokumenata obavlja se bez prethodne najave, a starije verzije dokumenata brišu se iz repozitorija.

Certifikati se automatski objavljuju na repozitoriju odmah po njihovom izdavanju, ukoliko je korisnik prethodno odobrio njihovu javnu objavu.

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

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

2.3. Vrijeme ili učestalost objavljivanja

Opća pravila, drugi dokumenti i ostale informacije iz točaka 2.2.1 i 2.2.2 ovog dokumenta objavljuju se po potrebi, nakon odobrenja Fina PMA.

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 Općih pravila.

Online informacije o statusu izdanih certifikata dostupne su putem Fina OCSP 2015 servisa koji je opisan u točki 4.9.9. ovog CPS_{QC} dokumenta.

2.4. Kontrole pristupa repozitoriju

Informacije objavljene na repozitoriju su javno dostupne za sve sudionike Fina PKI. Pristup repozitoriju javno je dostupan samo s dozvolom čitanja objavljenog sadržaja.

Pristup repozitoriju uz mogućnost izmjene sadržaja imaju samo ovlašteni zaposlenici Fine.

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

3. IDENTIFIKACIJA I POTVRĐIVANJE IDENTITETA SUBJEKTA

Prije izdavanja certifikata Fina provodi pravovaljanu identifikaciju i potvrđivanje identiteta subjekta sukladno postupcima danim ovim CPS_{QC} dokumentom.

Postupke identifikacije i potvrđivanja identiteta subjekta za Fina PKI provodi RA mreža koju čine Fina RA mreža i mreža pojedinog vanjskog ugovorenog RA. Fina RA mrežu čine Središnji Fina RA i Fina LRA. Djelatnici ovlašteni za registraciju u RA mreži obavljaju poslove registracije sukladno CPS_{QC} dokumentu.

3.1. Određivanje imena

3.1.1. Tipovi imena

U polje „Subject“ svakog kvalificiranog certifikata upisuju se autentični podaci o potpisniku. Dio polja „Subject“ kvalificiranih certifikata sadrži ime i prezime potpisnika. Polje „Subject“ osobnih certifikata sadrži naziv mjesta prebivališta potpisnika, dok za poslovne certifikate „Subject“ sadrži naziv mjesta sjedišta poslovnog subjekta. Polje „Subject“ u kvalificiranim certifikatima je usklađeno s normom X.501 [30] i preporukom IETF RFC 3739 [19].

Polje „Subject“ u kvalificiranim certifikatima sadrži ime i prezime osobe iz identifikacijske isprave koju prihvaća Fina PKI, sukladno točki 3.2.3.1 ovog CPS_{QC} dokumenta te identifikator u obliku višekomponentnog serijskog broja kojim se osigurava jedinstvenost polja „Subject“ kvalificiranih certifikata unutar Fina CA. Višekomponentni serijski broj sadrži identifikator države, jedinstveni jedanaesteroznamenkasti broj te dva broja, sukladno opisu danom u točki 3.1.4. ovog CPS_{QC} dokumenta.

U kvalificiranim certifikatima koje izdaju Fina CA-ovi polje „Subject“ dodatno sadrži i skraćeni naziv te identifikator poslovnog subjekta. Skraćeni naziv poslovnog subjekta je identičan onom upisanom u nadležni registar. Ukoliko nadležni registar ne dodjeli skraćeni naziv poslovnog subjekta, u polje „Subjekt“ se upisuje puno ime poslovnog subjekta. Ukoliko skraćeni naziv poslovnog subjekta, ili puni naziv poslovnog subjekta (ako skraćeni naziv nije dodijeljen), sadrži više od 50 znakova, isti se dodatno skraćuje na 50 znakova izbacivanjem znakova s desne strane te se tako dodatno skraćen upisuje u polje „Subject“ certifikata. Pravila za kreiranje identifikatora poslovnog subjekta opisana su u točki 3.1.4. ovog CPS_{QC} dokumenta.

Ukoliko bilo koji podatak koji se unosi u polje „Subjekt“ sadrži posebne znakove ili slova koja nisu sadržana u engleskoj ili hrvatskoj abecedi, takvi znakovi se zamjenjuju najbližim znakom engleske abecede. Znakovi koji predstavljaju posebne znakove od tehničkog značaja za sustav certificiranja u potpunosti se izbacuju.

3.1.2. Smislenost imena

Smislenost imena u polju „Subject“ koja identificiraju fizičku osobu i poslovni subjekt te smislenost nazive mjesta i države osigurava se primjenom pravila prikazanim u tablici 3.1.

Naziv grupe certifikata	Pravilo za smislenost elemenata polja Subject
Fina RDC 2015 osobni kvalificirani certifikati	• commonName: Ime i prezime potpisnika • localityName: Mjesto prebivališta potpisnika • countryName: HR
Fina RDC 2015 poslovni kvalificirani certifikati	• commonName: Ime i prezime potpisnika • localityName: Mjesto sjedišta poslovnog subjekta • organizationName: Skraćeni naziv i identifikator poslovnog subjekta • countryName: HR
Fina RDC-TDU 2015 kvalificirani certifikati	• commonName: Ime i prezime potpisnika • localityName: Mjesto sjedišta TDU • organizationalUnit: Podorganizacijska jedinica TDU 2. razine (opcionalno) • organizationalUnit: Podorganizacijska jedinica TDU 1. razine (opcionalno) • organizationName: Skraćeni naziv i identifikator TDU • countryName: HR

Tablica 3.1. Pravila za određivanje elemenata polja „Subject“

Kada se za vrijednost atributa i polja certifikata primjenjuje preporuka IETF RFC 5322 [21] smislenost imena i naziva se ne provjerava. Preporuka IETF RFC 5322 [21] se u kvalificiranim certifikatima primjenjuje samo za nazive u polju „Subject Alternative Name“ koja imaju oblik e-mail adrese.

3.1.3. Anonimnost korisnika ili pseudonimnost

Anonimnost i pseudonimnost korisnika nije podržana.

3.1.4. Pravila tumačenja raznih oblika imena

Tumačenje oblika imena po X.501 [30] normi za kvalificirane certifikate provodi se prema tablici 3.2.

Poslovni kvalificirani certifikati			
Polje po X.501	**Fina RDC 2015**	**Fina RDC-TDU 2015**	**Pojašnjenje**
Country (C)	HR	HR	Dvoslovčani ISO kod države, HR za Hrvatsku
Organization (O)	Naziv poslovnog subjekta i identifikator poslovnog subjekta	Naziv tijela državne uprave i identifikator TDU	Naziv poslovnog subjekta ili TDU, dvoslovčani ISO kod države sjedišta poslovnog subjekta ili TDU te jedanaesteroznamenkasti broj. Za poslovne subjekte kojima je dodijeljen OIB i za TDU jedanaesteroznamenkasti broj je OIB poslovnog subjekta ili TDU. Za poslovne subjekte kojima nije dodijeljen OIB i nisu registrirani u Hrvatskoj jedanaesteroznamenkasti je broj jedinstveni broj kojeg dodjeljuje Fina CA.
Organization Unit (OU)	Ne koristi se	Naziv podorganizacijske jedinice	Certifikati izdani od strane Fina RDC-TDU 2015 podržavaju do dvije podorganizacijske jedinice unutar TDU
Locality (L)	Mjesto sjedišta poslovnog subjekta	Mjesto sjedišta TDU	Mjesto sjedišta poslovnog subjekta

Poslovni kvalificirani certifikati			
Polje po X.501	**Fina RDC 2015**	**Fina RDC-TDU 2015**	**Pojašnjenje**
Serial Number (SN)	Identifikator pripadajuće osobe (potpisnika)	Identifikator pripadajuće osobe (potpisnika)	Identifikator se sastoji od dvoslovčanog ISO koda države prebivališta pripadajuće osobe, jedanaesteroznamenkastog broja, te dva broja W i Z koji predstavljaju oznake koje imaju interno značenje za Fina PKI. Za potpisnike kojima je dodijeljen OIB jedanaesteroznamenkasti broj je OIB potpisnika. Za potpisnike kojima nije dodijeljen OIB i nemaju prebivalište u Hrvatskoj, jedanaesteroznamenkasti je broj jedinstveni broj kojeg dodjeljuje Fina CA.
Common Name (CN)	Ime i prezime pripadajuće osobe (potpisnika)	Ime i prezime pripadajuće osobe (potpisnika)	Ime i prezime pripadajuće osobe (potpisnika) iz identifikacijske isprave.
Osobni kvalificirani certifikati			
Polje po X.501	**Fina RDC 2015 2015**	**Fina RDC-TDU 2015**	**Pojašnjenje**
Country (C)	HR	Ne primjenjuje se.	Dvoslovčani ISO kod države, HR za Hrvatsku.
Organization (O)	OSOBNI	Ne primjenjuje se.	Interna klasifikacija osobnog certifikata
Locality (L)	Mjesto prebivališta fizičke osobe – građanina	Ne primjenjuje se.	Mjesto prebivališta fizičke osobe-građanina (potpisnika)

Osobni kvalificirani certifikati			
Polje po X.501	**Fina RDC 2015**	**Fina RDC-TDU 2015**	**Pojašnjenje**
Serial Number (SN)	Identifikator fizičke osobe – građanina	Ne primjenjuje se.	Identifikator se sastoji od dvoslovčanog ISO koda države prebivališta fizičke osobe – građanina, jedanaesteroznamenkastog broja, te dva broja W i Z koji predstavljaju oznake koje imaju interno značenje za Fina PKI. Za fizičke osobe – građanine kojima je dodijeljen OIB jedanaesteroznamenkasti broj je OIB potpisnika. Za fizičke osobe – građanine kojima nije dodijeljen OIB i nemaju prebivalište u Hrvatskoj, jedanaesteroznamenkasti je broj jedinstveni broj kojeg dodjeljuje Fina CA.
Common Name (CN)	Ime i prezime fizičke osobe – građanina	Ne primjenjuje se.	Ime i prezime fizičke osobe (potpisnika) iz identifikacijske isprave.

Tablica 3.2. Tumačenje oblika imena po X.501 normi

Tumačenje oblika imena prema preporuci IETF RFC 5322 [21] u Fina PKI kvalificiranim certifikatima primjenjuje se samo za nazive u ekstenziji certifikata *Subject Alternative Name* koja imaju oblik e-mail adrese i tumačimo ih kao e-mail adresu.

Tumačenje oblika imena po X.501 [30] normi u Fina PKI za CRL provodi se prema tablici 3.3.

Polje po X.501	Fina RDC 2015	Fina RDC-TDU 2015	Pojašnjenje
Country (C)	HR	HR	Država sjedišta davatelja usluge certificiranja, Hrvatska
Organization (O)	Financijska agencija	Financijska agencija	Davatelj usluga certificiranja
Organization Unit (OU)	Fina RDC 2015	Fina RDC-TDU 2015	Naziv certifikacijskog tijela

Polje po X.501	Fina RDC 2015	Fina RDC-TDU 2015	Pojašnjenje
Common Name (CN)	CRLn	CRLn	Identifikator segmentirane CRL (CRLn). Sa n se označava broj segmenta segmentirane CRL. (npr. CRL1 je prvi segment CRL).

Tablica 3.3. Tumačenje oblika imena po X.501 normi u Fina PKI za CRL

3.1.5. Jedinstvenost imena

Skup podataka u polju „Subject“ čini razlikovno ime subjekta certificiranja (engl. *Distinguished Name, DN*) sukladno preporuci IETF RFC 3739 [19] i normi X.501 [30].

Jedinstvenost razlikovnog imena u Fina PKI kvalificiranim certifikatima osigurava se vrijednošću atributa „SerialNumber“ unutar razlikovnog imena.

Fina CA samostalno kontrolira i dodjeljuje vrijednost atributa „SerialNumber“ u razlikovnom imenu da bi ostvarila jedinstvenost imena subjekata.

3.1.6. Prepoznavanje, potvrđivanje identiteta i uloga zaštitnog znaka

Nema odredbi.

3.2. Inicijalno utvrđivanje identiteta

3.2.1. Metoda dokazivanja posjeda privatnog ključa

3.2.1.1. Dokazivanje posjeda privatnog ključa za QCP+ certifikate

Za izdavanje tipova kvalificiranih certifikata za koje je propisano izdavanje na SSCD uređaju (tipovi certifikata QCP+ iz točke 1.1.2. ovog CPS_{QC} dokumenta), subjektovi se ključevi uvijek generiraju unutar SSCD uređaja. Fina podržava generiranje ključeva za potpisnika na SSCD uređaju na lokaciji Fina CA, Središnjeg Fina RA, Fina LRA ili na lokaciji korisnika.

a) Ključeve na SSCD uređaju generiraju Fina CA ili Središnji Fina RA na svojoj lokaciji

Ukoliko generiranje ključeva obavlja Fina CA, odnosno Središnji Fina RA, na svojoj lokaciji, za dokazivanje da subjekt posjeduje privatni ključ koristi se postupak kojeg osigurava Fina CMS sustav. Ovaj postupak se primjenjuje za izdavanje kvalificiranih QCP+ certifikata za fizičke osobe – građane, pripadajuće osobe u poslovnim subjektima i TDU. RA/LRA službenik SSCD uređaj uručuje potpisniku uz njegovu prethodnu neposrednu identifikaciju.

b) Ključeve na SSCD uređaju generira Fina LRA na svojoj lokaciji

Ukoliko generiranje ključeva obavlja Fina LRA na svojoj lokaciji, za dokazivanje da subjekt posjeduje privatni ključ koristi se postupak kojeg osigurava Fina CMS sustav. Ovaj postupak primjenjuje se za izdavanje kvalificiranih QCP+ certifikata za fizičke osobe – građane, pripadajuće osobe u poslovnim subjektima i TDU. SSCD uređaj s pripadajućim ključevima za potpisnika i izdanim kvalificiranim QCP+ certifikatom ovlaštena osoba u Fina LRA uručuje potpisniku uz njegovu prethodnu neposrednu identifikaciju.

c) Ključevi se na SSCD uređaju generiraju na korisničkoj lokaciji

Ukoliko se generiranje ključeva obavlja na korisničkoj lokaciji, za dokazivanje da subjekt posjeduje privatni ključ koristi se jedan od sljedeća dva postupka:

- postupak s uporabom Fina CMS sustava – upotrebljava se za izdavanje kvalificiranih QCP+ certifikata za fizičke osobe – građane te pripadajuće osobe u poslovnim subjektima i TDU koji se izdaju na SSCD uređaj;
- postupak s uporabom CMS sustava vanjskog ugovorenog RA – upotrebljava se za izdavanje kvalificiranih QCP+ certifikata za pripadajuće osobe u poslovnim subjektima koji se izdaju na SSCD uređaj, a koji su registrirani od strane vanjskog ugovorenog RA koji ima vlastiti CMS sustav.

Postupci se temelje na uručenju SSCD uređaja prethodno registriranom potpisniku, uz njegovu neposrednu identifikaciju te korištenju autentifikacije i sigurne *online* komunikacije prema SSCD uređaju za vrijeme izdavanja certifikata.

3.2.2. Potvrda identiteta poslovnog subjekta

U cilju potvrde identiteta poslovnog subjekta, pripadajuća osoba navodi točno i cjelovito popunjene podatke o poslovnom subjektu u zahtjevu za izdavanje certifikata, koji mora biti potpisan i ovjeren od strane osobe ovlaštene za zastupanje.

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

- izvornik ili presliku uz predočenje izvornika važećeg izvatka iz nadležnog registra, sukladno zakonima i propisima Republike Hrvatske radi dokaza upisa u nadležni

registar poslovne djelatnosti ili zakon, odnosno drugi propis temeljem kojeg je poslovni subjekt osnovan ako nije određeno da se poslovni subjekt upisuje u registar;
- obavijest Državnog zavoda za statistiku o razvrstavanju prema nacionalnoj klasifikaciji djelatnosti (NKD);
- presliku identifikacijske isprave fizičke osobe ovlaštene za zastupanje poslovnog subjekta.

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

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

1. provjerava se cjelovitost, autentičnost i valjanost dokumentacije za registriranje poslovnog subjekta;
2. provjerava se je li poslovni subjekt upisan u nadležni registar ako je po propisima dužan upisati se u isti, odnosno akt nadležnog organa ili propis o osnivanju poslovnog subjekta, ako poslovni subjekt nije dužan upisati se u registar;
3. Fina RA/LRA dodatno provjerava točnost provjerljivih podataka upisanih u zahtjevu. Provjera se provodi temeljem upita na nacionalni OIB sustav kroz Fina RA aplikaciju za podatke koji su dohvatljivi iz OIB sustava;
4. provjerava se ovlaštenje osobe ovlaštene za zastupanje poslovnog subjekta i točnost njenih osobnih podataka. Ukoliko ovlaštena osoba za zastupanje ovlasti opunomoćenika, provjerava se dokument punomoći na osnovu potpisa s preslike identifikacijske isprave fizičke osobe ovlaštene za zastupanje, te se provjeravaju podaci opunomoćenika na osnovu dostavljene preslike njegove identifikacijske isprave uz prethodnu provjeru ovlaštenja osobe ovlaštene za zastupanje poslovnog subjekta;

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

Iznimno, u slučaju promjene podataka o poslovnom subjektu sadržanih u certifikatu popisanih u točki 3.1.1. ovog CPS_{QC} dokumenta, potpisnik je dužan u zakonskom roku dostaviti dokaze o promjeni podataka, a službenik u RA mreži, uz prethodnu provjeru, unosi izmjenu podataka o poslovnom subjektu.

U slučaju već registriranog poslovnog subjekta kojem novi zahtjev za izdavanje certifikata ili ugovor potpisuje ovlaštena osoba koja nije prije registrirana u Fina RA/LRA, prilikom

podnošenja zahtjeva za izdavanje certifikata nužno je dostaviti novi, valjani izvod iz nadležnog registra kojim se potvrđuju ovlasti navedene osobe ovlaštene za zastupanje, te preslika osobne iskaznice te ovlaštene osobe. Procedura provjere tada je istovjetna inicijalnoj proceduri provjere identiteta poslovnog subjekta. Ukoliko u novom rješenju nadležnog registra, već registrirana ovlaštena osoba više nije navedena, istu službenik u RA mreži briše iz liste registriranih ovlaštenih osoba tog poslovnog subjekta u Fina RA aplikaciji.

U slučaju promjene podataka o poslovnom subjektu koji nisu sadržanu u certifikatu popisanih u točki 3.1.1. ovog CPS_{QC} dokumenta, potpisnik je dužan dostaviti dokaze o promjeni podataka prilikom predaje slijedećeg zahtjeva za izdavanje ili obnovu certifikata, a službenik u RA mreži, uz prethodnu provjeru, unosi izmjenu podataka o poslovnom subjektu.

Poslovni subjekt odgovara za točnost i ispravnost dostavljenih podataka.

3.2.3. Potvrda identiteta fizičke osobe

Inicijalnu identifikaciju i potvrđivanje identiteta fizičke osobe u Fina PKI provodi Fina RA mreža ili vanjski ugovoreni RA postupcima neposredne identifikacije i potvrđivanja identiteta fizičke osobe sukladno točki 3.2.3.2 ovog CPS_{QC} dokumenta. Identifikaciju i potvrđivanje identiteta fizičke osobe iznimno provodi i Središnji Fina RA..

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

Dodatno, za hrvatske državljane, prikupljaju se podaci o datumu i mjestu rođenja, te mjesto prebivališta. Ove dodatne podatke RA prikuplja upitom na nacionalni OIB sustav i potpisnik u zahtjevu ih ne mora unositi. Provjera točnosti tih podataka usporedbom istih u priloženoj dokumentaciji i usporedbom s podacima u nacionalnom OIB sustavu je obveza Fina RA/LRA službenika.

Identifikacija fizičkih osoba koji su strani državljani može se provesti na dva načina, ovisno o tome je li stranom državljaninu dodijeljen OIB u Republici Hrvatskoj. U slučaju da strani državljanin ima dodijeljen OIB, identifikacija se obavlja na način identičan identifikaciji hrvatskih građana. U slučaju da strani državljanin nema dodijeljen OIB, identifikacija stranog državljanina provodi se uvidom u prihvatljivu identifikacijsku ispravu za stranca, definiranu u točki 3.2.3.1. ovog CPS_{QC} dokumenta.

Dodatno, za potpisnike koji su strani državljani, prikupljaju se podaci o datumu i mjestu rođenja, te mjesto prebivališta. Ove dodatne podatke Fina RA/LRA prikuplja i provjerava točnosti tih podataka usporedbom istih u priloženoj dokumentaciji.

Identifikacija fizičkih osoba – građana koji su u ulozi opunomoćenika potpisnika, u svrhu podnošenja zahtjeva, preuzimanja SSCD uređaja sa ili bez privatnog ključa u ime potpisnika, provodi se neposrednom identifikacijom uz uvid u prihvatljivu identifikacijsku ispravu iz točke 3.2.3.1. ovog CPS_{QC} dokumenta. Dodatno, opunomoćenik mora donijeti potvrdu statusa u

obliku punomoći potpisane od strane potpisnika u čije ime preuzima SSCD uređaj sa ili bez privatnog ključa. U slučaju da opunomoćenik preuzima SSCD uređaj sa ili bez privatnog ključa, u ime potpisnika - pripadajuće osobe pravnog subjekta, punomoć mora uz potpis biti ovjerena i pečatom poslovnog subjekta.

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

3.2.3.1. Prihvatljive vrste identifikacijskih isprava

Podnositelji zahtjeva za izdavanje certifikata (potpisnici 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. Provođenje neposredne identifikacije

Neposredna identifikacija provodi se u fizičkoj prisutnosti fizičke osobe, temeljem važeće prihvatljive identifikacijske isprave koja je opisana u točki 3.2.3.1. ovog CPS_{QC} dokumenta, a kojom se potvrđuje njen identitet. Ovaj postupak se provodi na lokacijama RA mreže ili na drugoj lokaciji u prisutnosti ovlaštenog službenika u RA mreži, a može ga provoditi i ovlašteni djelatnik Središnjeg Fina RA.

Potpisnik uvijek mora biti identificiran neposrednom identifikacijom - prilikom podnošenja zahtjeva ili prilikom preuzimanja SSCD uređaja sa ili bez privatnog ključa

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

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

3.2.3.3. Provođenje 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.

Kao posredni dokaz potvrde identiteta podnositelja zahtjeva ne prihvaća se dokaz u elektroničkom obliku potpisan privatnim ključem koji odgovara javnom ključu u certifikatu za koji se traži opoziv ili suspenzija, osim u slučaju potpisivanja zahtjeva za raskid ugovora o obavljanju usluga certificiranja.

3.2.4. Informacije o korisniku koje se ne provjeravaju

Informacije o korisniku koje se ne provjeravaju su:

- naziv podorganizacijske jedinice TDU;
- telefonski brojevi.

Za točnost i cjelovitost gore navedenih informacija jamči i odgovara potpisnik.

3.2.5. Provjera identiteta ovlaštenih osoba

Zahtjev za izdavanje Fina CA poslovnih certifikata uz pečat potpisuje i osoba ovlaštena za zastupanje poslovnog subjekta te time potvrđuje istinitost podataka u zahtjevu.

Osoba ovlaštena za zastupanje poslovnog subjekta uz pečat potpisuje i ugovor o obavljanju usluga certificiranja za poslovne subjekte, odnosno ugovor o obavljanju usluga izdavanja digitalnih certifikata zaposlenicima TDU.

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

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

Tekst pečata mora biti istovjetan tekstu naziva poslovnog subjekta u punom ili skraćenom nazivu kako je upisan u nadležni registar, a mogu se prihvatiti i određene razlike u pečatu u odnosu na podatke u priloženoj dokumentaciji ukoliko se usporedbom pečata i podataka u priloženoj dokumentaciji može utvrditi da se radi o istom poslovnom subjektu.

Zahtjev za izdavanje Fina CA poslovnih certifikata, odnosno ugovor, uz pečat može potpisati i fizička osoba koju poslovni subjekt posebnom punomoći ovlasti za potpisivanje zahtjeva za izdavanje certifikata, odnosno ugovora o obavljanju usluga certificiranja.

Fizička osoba iz prethodnog stavka dužna je RA mreži dostaviti izvornik ili javno ovjerenu presliku gore navedene posebne punomoći.

Zahtjev za izdavanje Fina CA poslovnih certifikata, zahtjev za opoziv, suspenziju, reaktivaciju ili oporavak certifikata, ugovor o obavljanju usluga certificiranja za poslovne subjekte te ugovor o obavljanju usluga izdavanja digitalnih certifikata zaposlenicima TDU može se elektronički potpisati naprednim elektroničkim potpisom sukladno gore navedenim ovlaštenjima. U tom slučaju identitet potpisnika utvrđuje se naprednim elektroničkim potpisom s važećim kvalificiranim certifikatom.

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

Službenik u RA mreži je dužan utvrditi identitet osobe ovlaštene za zastupanje, odnosno opunomoćenika osobe ovlaštene za zastupanje poslovnog subjekta koja je uz pečat potpisala zahtjev ili ugovor. Utvrđivanje identiteta osobe ovlaštene za zastupanje, odnosno njenog opunomoćenika, provodi se provjerom podataka iz dostavljene dokumentacije za utvrđivanje pravnog subjektiviteta i identiteta navedene u točki 3.2.2. ovog CPS_{QC} dokumenta i usporedbom s podacima iz preslike prihvatljive i važeće identifikacijske isprave osobe ovlaštene za zastupanje, odnosno njenog opunomoćenika. Vrste prihvatljivih identifikacijskih isprava navedene su u točki 3.2.3.1. ovog CPS_{QC} dokumenta. Dodatno, vrši se upit na nacionalni OIB sustav i provjeravaju se svi podaci koje OIB sustav sadrži u odnosu na podatke iz preslike identifikacijske isprave.

3.2.6. Kriteriji interoperabilnosti

Kvalificirani certifikati koje za subjekte izdaju Fina RDC 2015 i Fina RDC-TDU 2015 su namijenjeni za korištenje u elektroničkom poslovanju unutar i izvan Republike Hrvatske te zadovoljavaju međunarodne norme za njihovu prekograničnu uporabu. Kvalificirani 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 kvalificiranog certifikata se provodi postupak generiranja novog para subjektovih ključeva te se provodi postupak izdavanja novog certifikata sukladno točki 4.7. CPS_{QC} dokumenta.

Identifikacija i potvrđivanje identiteta korisnika kod obnove certifikata uz generiranje novog para ključeva provodi se na dva osnovna načina sukladno točkama 3.3.1.1. odnosno 3.3.1.2. ovog CPS_{QC} dokumenta.

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

Postupak identifikacije i potvrđivanja identiteta kod obnove certifikata može se provoditi na lokaciji RA mreže ili dolaskom LRA agenta na lokaciju potpisnika. Postupak identifikacije i potvrđivanja identiteta potpisnika provodi se sukladno odredbama točke 3.2.3. CPS_{QC} dokumenta.

Gdje je primjenjivo, identifikacija i potvrđivanje identiteta poslovnog subjekta provodi se sukladno odredbama točaka 3.2.2. i 3.2.5. CPS_{QC} dokumenta.

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

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

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

Ukoliko se postupak obnove QCP+ kvalificiranog certifikata obavlja na udaljenoj lokaciji, identifikacija i potvrđivanje identiteta potpisnika se obavlja prijavom na Fina CMS sustav važećim Poslovnim autentifikacijskim N2 certifikatom (NCP+). Prijavom se ostvaruje dvostrana autentificirana i zaštićena SSL/TLS komunikacija i uspostavlja udaljeni nadzor Fina CMS sustavom.

Ukoliko je potpisnik registriran od strane vanjskog ugovorenog RA te je Poslovni potpisni Q2 certifikat (QCP+) inicijalno izdan korištenjem CMS sustava vanjskog ugovorenog RA, identifikacija i potvrđivanje identiteta potpisnika se obavlja prijavom potpisnika na CMS sustav vanjskog ugovorenog RA važećim Poslovnim autentifikacijskim N2 certifikatom (NCP+). Prijavom se ostvaruje dvostrana autentificirana i zaštićena SSL/TLS komunikacija i uspostavlja udaljeni nadzor CMS sustava.

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

Certifikat koji je istekao ili je opozvan ne može biti osnova za podnošenje zahtjeva za izdavanje, obnovu ili izmjenu podataka u certifikatu.

U slučaju da korisnik koji ima opozvan ili istekao certifikat tada se za ponovno izdavanje certifikata identifikacija i potvrda identiteta korisnika provodi sukladno proceduri inicijalnog utvrđivanja identiteta iz točke 3.2.ovog CPS_{QC} dokumenta. Po pozitivnoj identifikaciji, potvrdi identiteta i zaprimanju točnog i cjelovitog zahtjeva za izdavanje certifikata, korisniku se izdaje novi certifikat s novim parom ključeva i novim periodom valjanosti certifikata.

3.4. Identifikacija i potvrđivanje identiteta korisnika 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.

Postupci opoziva i suspenzije certifikata opisani su u točki 4.9. ovog CPS_{QC} dokumenta.

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 ovog CPS_{QC} dokumenta.

Podnositelj zahtjeva za opoziv poslovnih certifikata izdanih fizičkim osobama te certifikata za TDU može biti potpisnik ili osoba ovlaštena za zastupanje poslovnog subjekta.

Identifikacija i potvrđivanje identiteta podnositelja zahtjeva provodi se postupkom neposredne identifikacije u registracijskom uredu RA mreže na temelju identifikacijske isprave podnositelja zahtjeva.

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.

Podnositelj zahtjeva za opoziv poslovnih certifikata izdanih fizičkim osobama te certifikata za TDU može biti potpisnik ili osoba ovlaštena za zastupanje poslovnog subjekta.

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.

Putem telefona podnositelj zahtjeva za opozivom certifikata može provesti samo postupak suspenzije, a postupak opoziva može se provesti naknadno, na neki od načina navedenih u točki 4.9.3. ovog CPS_{QC} dokumenta.

3.4.4. Podnošenje zahtjeva za opoziv putem telefaksa

Fina CA ne podržava postupak opoziva certifikata putem telefaksa.

Putem telefaksa podnositelj zahtjeva za opozivom certifikata može provesti samo postupak suspenzije, a postupak opoziva može se provesti naknadno, na neki od načina navedenih u točki 4.9.3. ovog CPS_{QC} dokumenta.

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

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

Identifikacija i potvrđivanje identiteta podnositelja zahtjeva provodi se postupkom posredne identifikacije iz točke 3.2.3.3. ovog CPS_{QC} dokumenta, tj. 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. ovog CPS_{QC} dokumenta.

Podnositelj zahtjeva za suspenziju poslovnih certifikata izdanih fizičkim osobama te certifikata za TDU može biti potpisnik ili osoba ovlaštena za zastupanje poslovnog subjekta.

Identifikacija i potvrđivanje identiteta podnositelja zahtjeva provodi se postupkom neposredne identifikacije u registracijskom uredu RA mreže na temelju identifikacijske isprave podnositelja zahtjeva.

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.

Podnositelj zahtjeva za suspenziju poslovnih certifikata izdanih fizičkim osobama te certifikata za TDU može biti potpisnik ili osoba ovlaštena za zastupanje poslovnog subjekta.

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 web stranicama http://www.fina.hr/finadigicert.

Ukoliko je zahtjeva 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, 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. Zahtjevi zaprimljeni telefaksom u uredovno vrijeme Središnjeg Fina RA bit će obrađeni isti dan, a zahtjevi zaprimljeni izvan uredovnog vremena Fina RA bit će obrađeni sljedeći radni dan.

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, 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 kvalificiranih certifikata podnose 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

Usluge registracije korisnika sa zaprimanjem zahtjeva za izdavanje kvalificiranih certifikata te provođenje identifikacije i potvrđivanje identiteta korisnika za Fina CA obavlja RA mreža.

Odgovornost vanjskog RA za propuste u obavljanju ugovorenih usluga regulirana je ugovorom sklopljenim s Finom. Odgovornost prema sudionicima Fina PKI sustava za propuste u radu RA mreže ima Fina kao davatelj usluga certificiranja.

Fina RA mreža i vanjski ugovoreni RA-ovi određuje jednu ili više osoba koje provode identifikaciju i potvrđivanje identiteta u skladu s ovim CPS_{QC} dokumentom i Općim pravilima [33].

4.1.2.1. Proces podnošenja zahtjeva za izdavanje certifikata

Zahtjev za izdavanje kvalificiranih certifikata može biti namijenjen isključivo za izdavanje kvalificiranih certifikata ili može biti kombiniran sa zahtjevom za izdavanje normaliziranih certifikata, ukoliko se i kvalificirani i normalizirani certifikat istovremeno izdaju na isti SSCD uređaj. Zahtjev za izdavanje certifikata mora biti potpun, točan i cjelovit te mora biti potpisan čime se potvrđuje istinitost podataka u zahtjevu.

Zahtjev za izdavanje kvalificiranih osobnih certifikata potpisuje fizička osoba – građanin.

Zahtjev za izdavanje kvalificiranih Fina RDC 2015 poslovnih certifikata ili Fina RDC-TDU 2015 certifikata potpisuje pripadajuća osoba. Ovakav zahtjev, dodatno ovjerava pečatom i potpisuje osoba ovlaštena za zastupanje poslovnog subjekta.

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

Pravila za potpisivanje zahtjeva za izdavanje certifikata od strane osobe ovlaštene za zastupanje jednaka su za potpisivanje zahtjeva u papirnatom obliku kao i za potpisivanje zahtjeva u elektroničkom obliku. Ova pravila su navedena u točki 3.2.5. ovog CPS_{QC} dokumenta. Zahtjev u papirnatom obliku se dodatno ovjerava pečatom poslovnog subjekta.

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

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

Registracija korisnika provodi se postupkom koji je opisan u točkama 3.2.2., 3.2.3. i 3.2.5. ovog CPS_{QC} dokumenta.

4.1.2.2. Odgovornosti i obveze u procesu podnošenja zahtjeva za izdavanje certifikata

Korisnici koji podnose zahtjev za izdavanje kvalificiranog certifikata s Finom sklapaju odgovarajući ugovor o obavljanju usluga certificiranja kojim prihvaćaju Opća pravila davanja usluga certificiranja i Uvjete pružanja usluga certificiranja te time između ostalog prihvaćaju odgovornosti i obveze u procesu podnošenja zahtjeva za izdavanje certifikata.

Odgovornosti i obveze korisnika u procesu podnošenja zahtjeva za izdavanje certifikata su:

- 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 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, odnosno potpisnik, pristaje da Fina PKI koristi i obrađuje podatke sukladno propisima te izjavama i potvrdama iz zahtjeva za izdavanja certifikata te da su suglasni 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 svojim pravilima.

Obveze i o odgovornosti RA mreže su navedene u Poglavlju 9.6.2. ovog CPS_{QC} dokumenta.

Obveze i odgovornosti Fina CA su navedene u Poglavlju 9.6.1. ovog CPS_{QC} dokumenta.

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. ovog CPS_{QC} dokumenta.

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

- nakon zaprimanja zahtjeva za izdavanje certifikata na kojem je označeno izdavanje kvalificiranog certifikata, službenik u Fina RA mreži pregledava zaprimljeni zahtjev radi kontrole, sukladno postupcima opisanim u točkama 3.2.2., 3.2.3. i 3.2.5. ovog CPS_{QC} dokumenta;
- ukoliko zahtjev nije točno i u cijelosti popunjen te pravilno potpisan i ovjeren pečatom (ukoliko je to primjenjivo), službenik u RA mreži mora odbiti takav zahtjev i zahtijevati ispravno i točno ispunjen, potpisan i pečatom ovjeren zahtjev;
- ukoliko je zaprimljen zahtjev za izdavanje poslovnog certifikata ili certifikata za TDU, službenik u RA mreži provjerava jesu li poslovni subjekt podnositelja i sam podnositelj zahtjeva već registrirani. Ako zapis o registraciji podnositelja ili poslovnog subjekta ne postoji u Fina RA sustavu, kroz Fina RA aplikaciju i provjeru upitom na nacionalni OIB sustav (ukoliko je primjenjivo), kreiraju se zapisi o registraciji;
- ukoliko se radi o zahtjevu za osobnim kvalificiranim certifikatom, službenik u Fina RA mreži provjerava je li podnositelj zahtjeva već registriran. Ako zapis o registraciji podnositelja ne postoji u RA bazi, kroz Fina RA aplikaciju i provjeru upitom na nacionalni OIB sustav (ukoliko je primjenjivo), kreiraju se zapisi o registraciji;
- službenik u Fina RA mreži postavlja status podnositelja na „pripremljeno“ čime se u Fina RA aplikaciji naznačuje odobrenje zahtjeva. Tom prilikom generira se i razlikovno ime (*Distinguished Name*, DN) subjekta;
- službenik u Fina RA mreži odobreni zahtjev prosljeđuje na daljnju obradu u Fina CA.

4.2.2. Odobravanje ili odbijanje zahtjeva za izdavanje certifikata

Odobravanje ili odbijanje zahtjeva za uslugu izdavanja certifikata provodi službenik u registracijskom uredu RA mreže u kojem je korisnik podnio zahtjev. Ukoliko službenik u RA mreži odbije zahtjev za izdavanje certifikata, pismenim ili usmenim putem obavještava podnositelja o odbijanju zahtjeva i razlozima odbijanja istog. Ukoliko je podnositelj fizički prisutan u uredu RA mreže, podnositelj se obavještava usmenim putem. Ukoliko podnositelj nije fizički prisutan u uredu RA mreže, obavještava se telefonskim pozivom ili porukom na e-mail adresu iz zahtjeva.

Zahtjev za izdavanje certifikata može se odbiti zbog:

- Netočnih podataka;
- Nepravilno potpisanog ili nepravilno ovjerenog zahtjeva, odnosno ugovora;
- Nepotpune ili neispravne priložene dokumentacije;
- Prethodnih neodgovarajućih postupaka i nepoštivanja ugovornih obveza korisnika;
- Zakonske zabrane.

4.2.3. Vrijeme obrade zahtjeva za izdavanje certifikata

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

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

4.3. Izdavanje certifikata

Nakon primitka zahtjeva za izdavanje certifikata i provedenih procesa provjere i odobrenja navedenih u točki 4.2. i točkama 3.2.2., 3.2.3 i 3.2.5. ovog CPS_{QC} dokumenta, Fina CA izdaje certifikat.

4.3.1. Radnje Fina CA tijekom izdavanja certifikata

Generiranje korisničkih ključeva za pojedine tipove kvalificiranih certifikata tijekom njihova izdavanja provodi se u skladu s točkom 6.1.1.3. ovog CPS_{QC} dokumenta.

a) Ključeve na SSCD uređaju generira Fina CA ili Središnji Fina RA na svojoj lokaciji

- po primitku narudžbe za izdavanje certifikata iz RA aplikacije Fina CA za svaki registrirani SSCD uređaj u Fina CMS sustavu generira i enkriptira zaseban PIN;
- ovlaštene osobe u Fina CA, odnosno u Središnjem Fina RA, generiraju ključeve u SSCD uređaju povezanim sa podnositeljem zahtjeva i prosljeđuju njegov javni ključ na certificiranje;
- Fina CA certificira javni ključ izdajući korisniku certifikat odgovarajućeg profila;
- ovlaštena osoba u Fina CA, odnosno u Središnjem Fina RA, upisuje certifikat u odgovarajući SSCD uređaj;
- SSCD uređaj s pripadajućim parom ključeva i certifikatom ovlaštena osoba u Fina CA, odnosno u Središnjem Fina RA, prosljeđuje sigurnom dostavom u RA mrežu;
- enkriptirani PIN SSCD uređaja dostavlja se korisniku putem e-mail poruke ili se uručuje korisniku pri neposrednoj identifikaciji u RA mreži.

b) Ključeve na SSCD uređaju generira Fina LRA na svojoj lokaciji

- Fina CA, odnosno Središnjem Fina RA, registrira SSCD uređaje u Fina CMS sustavu;
- Fina LRA povezuje registrirani SSCD uređaj s registriranim potpisnikom iz baze registriranih korisnika;
- Fina LRA generiraa ključeve u SSCD uređaju povezanim sa podnositeljem zahtjeva i prosljeđuje njegov javni ključ na certificiranje;
- Fina CA certificira javni ključ izdajući korisniku certifikat odgovarajućeg profila;
- Fina LRA upisuje certifikat u odgovarajući SSCD uređaj;
- SSCD uređaj s pripadajućim parom ključeva i certifikatom ovlaštena osoba u Fina LRA uručuje korisniku pri neposrednoj identifikaciji;
- enkriptirani PIN SSCD uređaja dostavlja se korisniku putem e-mail poruke ili se uručuje korisniku pri neposrednoj identifikaciji u Fina LRA.

c) Ključevi se na SSCD uređaju generiraju na korisničkoj lokaciji

Ukoliko se ključevi na SSCD uređaju generiraju pod nadzorom Fina CA kroz Fina CMS sustav primjenjuje se sljedeći postupak:

- po primitku narudžbe za izdavanje certifikata iz RA aplikacije Fina CA za svaki registrirani SSCD uređaj u Fina CMS sustavu generira i enkriptira zaseban PIN;
- Fina CMS sustav putem e-mail poruke potpisniku dostavlja enkriptirani PIN;
- po iniciranju postupka certificiranja od strane potpisnika na udaljenoj korisničkoj lokaciji uporabom Fina CMS sustava, Fina CMS sustav inicira postupak generiranja korisničkih ključeva u potpisnikovom SSCD uređaju;
- Fina CMS sustav pripadajući korisnički javni ključ šalje u formatu PKCS#10 zahtjeva u Fina CA na postupak izdavanja certifikata;
- Fina CA certificira javni ključ izdajući korisniku certifikat odgovarajućeg profila i štićenim kanalom ga prosljeđuje u CMS sustav;
- Fina CMS sustav upisuje izdani certifikat na potpisnikov SSCD uređaj te inicira provjeru izdanog certifikata;
- ukoliko provjera izdanog certifikata daje negativan rezultat, podnositelja se upućuje na iniciranje ili zamjenu SSCD uređaja u RA mrežu.

Iznimno, ukoliko vanjski ugovoreni RA koristi vlastiti CMS sustav, za Poslovni potpisni Q2 certifikat (QCP+) primjenjuje se sljedeći postupak:

- po iniciranju postupka certificiranja od strane potpisnika, CMS sustav vanjskog RA inicira postupak generiranja korisničkih ključeva u potpisnikovom SSCD uređaju;
- CMS sustav vanjskog RA izrađuje PKCS#10 format zahtjeva s pripadajućim javnim ključem, koji se dodatno potpisuje i s elektroničkim potpisom vanjskog RA;
- CMS sustav vanjskog RA takav PKCS#10 format zahtjeva dostavlja u Fina CA;

- po primitku PKCS#10 zahtjeva, Fina CA provjerava valjanost elektroničkog potpisa vanjskog RA i potpisnika, a time i cjelovitost i autentičnost podataka u zahtjevu. Dodatno Fina CA provjerava da li je korisnik registriran u Fina RA sustavu;
- ukoliko potpis vanjskog RA ili potpisnika nije valjan ili korisnik nije registriran u Fina RA sustavu, zahtjev se odbija;
- Fina CA certificira javni ključ izdajući korisniku certifikat odgovarajućeg profila;
- Fina CA prosljeđuje izdani certifikat na CMS sustav vanjskog RA;
- CMS sustav vanjskog RA upisuje certifikat na potpisnikov SSCD uređaj te inicira provjeru izdanog certifikata;
- ukoliko provjera izdanog certifikata daje negativan rezultat, vanjski RA podnositelja upućuje na iniciranje ili zamjenu SSCD uređaja.

4.3.2. Obavještavanje korisnika od strane CA o izdavanju certifikata

Potpisnika o mogućnosti preuzimanja certifikata, službenik RA mreže obavještava telefonski. U slučaju da službenik RA mreže nije uspio telefonski obavijestiti potpisnika, obavijest potpisniku službenik RA mreže šalje e-mailom. Ukoliko potpisnik nije u Zahtjev za izdavanje certifikata naveo e-mail adresu, potpisnik se obavještava poštom.

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

Ukoliko potpisnik 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

4.4.1. Provedba prihvaćanja certifikata

Sukladno točki 3.2.1. ovog CPS_{QC} dokumenta, po obavještavanju potpisnika o izdavanju certifikata, potpisnik preuzima certifikat ovisno o tipu certifikata i načinu njegova izdavanja, na jedan od sljedećih načina:

- u registracijskom uredu RA mreže, zajedno s generiranim korisničkim ključevima na SSCD uređaju;
- *online* kroz Fina CMS sustav;
- *online* kroz CMS sustav vanjskog RA.

Potpisnik je dužan 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 treba odbiti prihvaćanje certifikata te o tome što prije obavijestiti Fina CA na e-mail adresu info.rdc@fina.hr ili osobno u registracijskom uredu RA mreže i pri tom navesti razloge neprihvaćanja istog. RA mreža pri tome prosljeđuje obavijest u Fina CA. Po primitku obavijesti Fina CA provodi opoziv, odnosno suspenziju

navedenog certifikata po postupku opisanom u točki 4.9. ovog CPS_{QC} dokumenta. Ukoliko je provedena suspenzija certifikata, Fina nakon identifikacije potpisnika u roku iz točke 4.9.16. i sukladno točki 4.9.3. ovog CPS_{QC} dokumenta opoziva certifikat, te omogućava izdavanje novog certifikata s potrebnim izmjenama, a na temelju zahtjeva za izdavanje certifikata.

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

Ukoliko potpisnik 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 certifikat prihvatio.

Upute za registraciju/preuzimanje certifikata nalaze se na stranicama repozitorija iz točke 2.2. ovog CPS_{QC} dokumenta. Pri dostavi autentifikacijskih podataka za preuzimanje certifikata potpisnik elektroničkom poštom dobiva i pripadnu uputu.

4.4.2. Objava izdanog certifikata od strane CA

Ukoliko je potpisnik odobrio javnu objavu certifikata, Fina CA odmah nakon izdavanja objavljuje izdani korisnikov certifikat u javnom imeniku pripadnog repozitorija iz točke 2.2. ovog CPS_{QC} dokumenta.

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 nije odobrio javnu objavu certifikata, 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 o obavljanju usluga certificiranja i u skladu sa propisima iz Općih pravila [33], potpisnik se obvezuje:

- na korištenje privatnog ključa i pripadajućeg certifikata samo u svrhe propisane Općim pravilima [33];
- da koristi privatni ključ i pripadajući certifikat samo tijekom perioda valjanosti certifikata, odnosno ne koristi privatni ključ i certifikat nakon njegova isteka, opoziva ili tijekom suspenzije;
- da od trenutka kad je privatni ključ u jedinstvenom posjedu potpisnika štiti privatni ključ od krađe, gubitka, izmjena, kompromitiranja i neovlaštene uporabe;
- čuvati aktivacijske podatke 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 izgubljen, ukraden ili postoji sumnja u bilo kakvo kompromitiranje privatnog ključa;
  - kada potpisnik 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 od strane Fina CA treba:

- koristiti certifikat isključivo u svrhe propisane u točki 1.4. ovog CPS_{QC} dokumenta.;
- obaviti provjeru isteka certifikata;
- obaviti provjeru statusa certifikata u kojeg namjerava ostvariti pouzdanje koristeći aktualnu i provjerenu CRL izdanu od strane Fina CA koji je izdao certifikat;
- provesti provjeru certifikata prema postupcima za validaciju certifikacijske staze, sukladno dokumentu IETF RFC 5280 [20];
- 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;
- u slučaju postojanja sumnji u ispravnost postupka kojim aplikacija pouzdajuće strane, temeljem gore navedenih odredbi iz ove točke, provjerava certifikat, pouzdajuća strana treba:
  - uvidom u certifikat utvrditi da li je certifikat istekao;
  - uvidom u važeću i provjerenu CRL utvrditi da li je certifikat opozvan ili suspendiran;
  - uvidom u prikaz certifikata provjeriti certifikacijsku stazu 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

Sukladno odredbama u točki 4.6. Općih pravila [33], Fina CA obnovu certifikata provodi na način da se za svakog postojećeg potpisnika čiji je certifikat pred istekom generira novi par ključeva i izdaje novi certifikat za istog potpisnika. DN novog certifikata jednak je DN-u certifikata koji je pred istekom. Postupak obnove kvalificiranih certifikata uz generiranje novog para ključeva je detaljno opisan u točki 4.7. ovog CPS_{QC} dokumenta.

Osim u postupku obnove certifikata korisnik može, podnošenjem zahtjeva za oporavak certifikata, pod određenim uvjetima, navedenim u točki 4.7.1., zatražiti ponovno izdavanje certifikata s novim parom ključeva, s istim DN-om i novim periodom valjanosti certifikata.

Oporavak certifikata je postupak koji se provodi prije nastupanja roka za obnovu certifikata.

Postupak obnove certifikata opisan je u točki 4.7. ovog CPS_{QC} dokumenta.

4.6.1. Razlozi za obnovu certifikata

Vidi točku 4.7.1.

4.6.2. Tko može tražiti obnovu certifikata

Vidi točku 4.7.2.

4.6.3. Obrada zahtjeva za obnovu certifikata

Vidi točku 4.7.3.

4.6.4. Obavještavanje korisnika o obnovi certifikata

Vidi točku 4.7.4.

4.6.5. Provedba prihvaćanja obnovljenog certifikata

Vidi točku 4.7.5.

4.6.6. Objava obnovljenog certifikata od strane CA

Vidi točku 4.7.6.

4.6.7. Obavještavanje drugih strana o obnovi certifikata

Vidi točku 4.7.7.

4.7. Obnova certifikata uz generiranje novog para ključeva

4.7.1. Razlozi za obnovu certifikata uz generiranje novog para ključeva

Obnova certifikata uz generiranje novog para ključeva se provodi ukoliko 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 ponovno izdavanje certifikata s novim parom ključeva, s istim korisničkim podacima i novim periodom valjanosti certifikata, a provodi se u slučaju kvara na kriptografskom uređaju 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 niti 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 korisniku izdati novi certifikat uz generiranje novog para ključeva, a čiji se DN razlikuje od DN-a u certifikatu čiji se oporavak traži, u komponenti W serijskog broja sukladno tablici 3.2 ovog CPS_{QC}.

4.7.2. Tko može zatražiti certificiranje novog javnog ključa

Potpisnik je ovlašten za podnošenje zahtjeva za obnovu ili oporavak pripadajućih certifikata.

Zahtjev za obnovu ili oporavak certifikata uvijek potpisuje potpisnik.

Zahtjev za obnovu ili oporavak poslovnih certifikata te certifikata za TDU dodatno potpisuje osoba ovlaštena za zastupanje poslovnog subjekta, odnosno TDU.

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

Za tipove certifikata iz točke 6.1.1.3. koriste se sljedeći postupci:

a) Ključeve na SSCD uređaju generira Fina CA na svojoj lokaciji

- potpisnik u RA mreži ili na drugom za to određenom mjestu predaje zahtjev za obnovu ili oporavak certifikata uz pravilnu identifikaciju sukladno točki 3.3.1.1. ovog CPS_{QC} dokumenta;
- službenik u RA mreži provodi odobravanje ili odbijanje zahtjeva sukladno postupcima za odobravanje ili odbijanje zahtjeva za izdavanjem certifikata iz točke 4.2.2. ovog CPS_{QC} dokumenta;
- Fina CA obavlja izdavanje certifikata sukladno postupku opisanom u točki 4.3.1. ovog CPS_{QC} dokumenta;
- Fina CA opoziva stari certifikat.

b) Ključeve na SSCD uređaju generira Fina LRA na svojoj lokaciji

- potpisnik u RA mreži ili na drugom za to određenom mjestu predaje zahtjev za obnovu ili oporavak certifikata uz pravilnu identifikaciju sukladno točki 3.3.1.1. ovog CPS_{QC} dokumenta;
- službenik u RA mreži provodi odobravanje ili odbijanje zahtjeva sukladno postupcima za odobravanje ili odbijanje zahtjeva za izdavanjem certifikata iz točke 4.2.2. ovog CPS_{QC} dokumenta;
- Fina LRA obavlja radnje sukladno postupku opisanom u točki 4.3.1.1. stavak b) ovog CPS_{QC} dokumenta.
- Fina CA opoziva stari certifikat.

c) Ključevi se na SSCD uređaju generiraju na korisničkoj lokaciji

Ukoliko se ključevi na SSCD uređaju generiraju pod nadzorom Fina CA kroz Fina CMS sustav primjenjuje se sljedeći postupak za obnovu certifikata:

- potpisnik se valjanim certifikatom na pripadajućem SSCD uređaju i aktivacijskim podacima spaja na Fina CMS sustav te se ostvaruje SSL/TLS zaštićena komunikacija uz dvostranu autentifikaciju. Udaljenim radom kroz CMS web sučelje potpisnik dobiva uvid u trenutne podatke o svojem važećem certifikatu te informacije o tome koji certifikat može obnoviti (ukoliko posjeduje više certifikata);
- potpisnik na Fina CMS sustavu 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 iniciranja obnove certifikata, potpisnik može zahtijevati njegovu obnovu na način da kroz Fina CMS sustav potvrdi slanje zahtjeva za obnovu certifikata. Tom se prilikom izrađeni zahtjev potpisnik elektronički potpisuje trenutno važećim certifikatom te ga Fina CMS

obrađuje, provjerava i pohranjuje. Ukoliko podaci o važećem certifikatu nisu točni, potpisnik je dužan obavijestiti Fina CA o izmjenama unutar certifikata;

- ukoliko je elektronički potpis zahtjeva uspješno verificiran i podaci u zahtjevu uspješno provjereni, na osnovu zahtjeva Fina CMS aplikacija inicira generiranje novog para ključeva na korisničkom SSCD uređaju, te se na korisničkoj lokaciji formira PKCS#10 potpisani zahtjev s novogeneriranim javnim ključem koji se ostvarenom zaštićenom komunikacijom prosljeđuje u Fina CA na certificiranje;
- Ukoliko elektronički potpis zahtjeva nije uspješno verificiran, Fina CMS javlja grešku, a potpisnik provodi postupak sukladno postupku za inicijalno izdavanje certifikata;
- Fina CMS sustav pripadajući javni ključ šalje u formatu PKCS#10 zahtjeva u Fina CA na postupak izdavanja certifikata;
- Fina CA certificira javni ključ izdajući potpisniku certifikat odgovarajućeg profila i štićenim kanalom ga prosljeđuje u CMS sustav;
- Fina CMS sustav upisuje izdani certifikat na potpisnikov SSCD uređaj te inicira provjeru izdanog certifikata;
- ukoliko provjera izdanog certifikata daje negativan rezultat, podnositelja se upućuje na iniciranje ili zamjenu SSCD uređaja u RA mrežu;
- Fina CA opoziva stari certifikat.

Iznimno, ukoliko vanjski ugovoreni RA koristi vlastiti CMS sustav, za Poslovni potpisni Q2 certifikat (QCP+) primjenjuje se sljedeći postupak obnove certifikata:

- po iniciranju postupka obnove certifikata od strane potpisnika, CMS sustav vanjskog RA inicira postupak generiranja ključeva u potpisnikovom SSCD uređaju;
- CMS sustav vanjskog RA izrađuje PKCS#10 format zahtjeva i dostavlja ga u Fina CA;
- po primitku PKCS#10 zahtjeva, Fina CA provjerava je li korisnik registriran u Fina RA sustavu;
- ukoliko korisnik nije registriran u Fina RA sustavu, zahtjev se odbija;
- Fina CA certificira javni ključ izdajući korisniku certifikat odgovarajućeg profila;
- Fina CA prosljeđuje izdani certifikat na CMS sustav vanjskog RA;
- CMS sustav vanjskog RA upisuje certifikat na potpisnikov SSCD uređaj te inicira provjeru izdanog certifikata;
- ukoliko provjera izdanog certifikata daje negativan rezultat, vanjski RA podnositelja upućuje na iniciranje ili zamjenu SSCD uređaja.

Za sve tipove QCP+ certifikata postupak oporavka obavlja se samo na način opisan u stavkama a) ili b) ove točke. Nakon izdavanja certifikata kroz postupak oporavka Fina CA opoziva certifikat čiji se oporavak traži.

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

Fina središnji RA, odnosno vanjski ugovoreni RA, tijekom mjeseca koji prethodi mjesecu u kojem istječe certifikat, pisanim putem obavještava potpisnika o skorom isteku certifikata te ga poziva na obnovu certifikata uz generiranje novog para ključeva. Potpisnicima koji su u zahtjevu za izdavanje certifikata dostavili e-mail adresu, obavijest se šalje e-mailom, a ostalim potpisnicima obavijest se šalje poštom.

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. ovog CPS_{QC} dokumenta.

4.7.6. Objavljivanje certifikata po obnovi s generiranje novog para ključeva

Objavljivanje certifikata po obnovi s generiranjem novog para ključeva provodi se sukladno točki 4.4.2. ovog CPS_{QC} dokumenta.

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 sukladno točki 4.4.3. ovog CPS_{QC} dokumenta.

4.8. Izmjene unutar certifikata

Potpisnici 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 obavlja izmjene unutar certifikata samo za certifikat koji nije opozvan, nije suspendiran ili nije istekao.

4.8.1. Razlozi za izmjene unutar certifikata

U slučaju da je certifikat izdan kao osobni, poslovni ili certifikat za TDU, razlozi izmjena podataka u certifikatu su promjena bilo kojeg od sljedećih podataka:

- imena ili prezimena potpisnika;
- naziva poslovnog subjekta;
- izmjene identifikatora poslovnog subjekta, ukoliko poslovnom subjektu nije dodijeljen OIB;
- 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.

4.8.2. Tko može zatražiti izmjene unutar certifikata

Izmjene unutar certifikata može zatražiti potpisnik, a zahtjev se potpisuje sukladno pravilima potpisivanja navedenim u točki 3.2.5.

4.8.3. Obrada zahtjeva za izmjenama unutar certifikata

Potpisnik u RA mrežu podnosi zahtjev za izmjene unutar certifikata i dostavlja onaj dio dokumentacije određene u točki 3.2. ovog CPS_{QC} dokumenta kojom se dokazuje novonastala izmjena.

Izmjene unutar certifikata Fina CA provodi opozivanjem postojećeg certifikata i izdavanjem novog certifikata s novim parom ključeva te izmijenjenim podacima u certifikatu. Opoziv starog certifikata se provodi sukladno točki 4.9. ovog CPS_{QC} dokumenta, a izdavanje novog certifikata se obavlja sukladno točkama 4.2., 4.3. i 4.4. ovog CPS_{QC} dokumenta.

4.8.4. Obavještavanje korisnika o izdavanju izmijenjenog certifikata

Pri izdavanju certifikata u procesu izmjene Fina CA provodi iste postupke kao i za obavještavanje opisano u točki 4.3.2. ovog CPS_{QC} dokumenta.

4.8.5. Provedba prihvaćanja izmijenjenog certifikata

Provedba prihvaćanja izmijenjenog certifikata provodi se sukladno točki 4.4.1. ovog CPS_{QC} dokumenta.

4.8.6. Objavljivanje izmijenjenog certifikata od strane CA

Objavljivanje izmijenjenog certifikata Fina CA provodi se na način opisan u točki 4.4.2. ovog CPS_{QC} dokumenta.

4.8.7. Obavještavanje drugih strana o izdavanju izmijenjenog certifikata

Obavještavanje drugih strana o izdavanju izmijenjenog certifikata Fina CA provodi se na način opisan u točki 4.4.3. ovog CPS_{QC} dokumenta.

4.9. Opoziv i suspenzija certifikata

4.9.1. Razlozi za opoziv

Fina CA opoziva certifikate iz 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 ili sredstva na kojem se ključ čuva;
- u slučaju gubitka ili trajne nedosupnosti privatnog ključa;
- ako se pojavi osnovana sumnja da privatni ključ ili aktivacijski podaci nisu više u jedinstvenom posjedu potpisnika 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 korisnik iz bilo kojeg razloga nema više potrebu koristiti certifikat;
- ako Fina CA smatra da certifikat nije izdan sukladno zahtjevu ili navodima iz ovog CPS_{QC} dokumenta;
- u slučaju otkaza ugovora o obavljanju usluge certificiranja, od strane korisnika.

Ako korisnik ili potpisnik ne izvršava svoje obveze u skladu s ovim CPS_{QC} dokumentom i potpisanim ugovorima, Fina CA opoziva certifikat prema nalogu voditelja Centra elektroničkog poslovanja ili prema nalogu Fina PMA. 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 te certifikata za TDU može podnijeti potpisnik 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 tražiti opoziv bilo kojeg izdanog certifikata uz odobrenje voditelja Centra elektroničkog poslovanja ili Fina PMA.

Fina CA o obavljenom opozivu certifikata pisanim putem obavještava pripadajućeg potpisnika te, ukoliko je to primjenjivo, i korisnika. Potpisnicima i korisnicima koji su u zahtjevu za izdavanje certifikata dostavili e-mail adresu, obavijest se šalje e-mailom, a ostalim potpisnicima i korisnicima obavijest se šalje poštom.

4.9.3. Procedura za zahtjev za opozivom

Zahtjev za opoziv certifikata je u obliku obrasca Zahtjev za opoziv, suspenziju, reaktivaciju ili oporavak certifikata dostupan na internetskim stranicama Fina PKI repozitorija iz točke 2.2. ovog CPS_{QC} dokumenta. Navedeni zahtjev treba odmah po nastupanju razloga za opoziv, koji su navedeni u točki 4.9.1. ovog CPS_{QC} dokumenta, točno i cjelovito ispuniti, potpisati i u najkraćem uredovnom roku dostaviti u Fina PKI na jedan od sljedećih načina:

- osobnom dostavom u registracijski ured RA mreže u uredovno vrijeme:

  Popunjen i vlastoručno potpisan Zahtjev za opoziv, suspenziju, reaktivaciju ili oporavak certifikata, uz osobnu identifikaciju podnositelja prema postupku opisanom u točki 3.4.1. ovog CPS_{QC} dokumenta predaje se službeniku u RA mreži.

- poštanskom dostavom ili preko dostavljača na adresu registracijskog ureda u RA mreži:

  Popunjen i vlastoručno potpisan zahtjev za opoziv certifikata, uz neposrednu identifikaciju podnositelja prema postupku opisanom u točki 3.4.2. ovog CPS_{QC} dokumenta poštanskom dostavom ili preko dostavljača dostavlja se u registracijski ured u RA mreži.

- elektroničkom dostavom zahtjeva za opoziv na e-mail adresu:

  Dostava popunjenog zahtjeva za opoziv certifikata koji je potpisan naprednim elektroničkim potpisom podnositelja zahtjeva i identifikacija podnositelja obavlja se prema postupku opisanom u točki 3.4.5. Ukoliko podnositelj potpisuje zahtjev sa privatnim ključem koji odgovara certifikatu koji se opoziva, valjanost potpisa se prihvaća samo u slučajevima raskida ugovora o obavljanju usluge certificiranja od strane korisnika i kada je razlog opoziva prestanak odnosa koji je bio razlog da se potpisniku izda certifikat kojim će kao pripadajuća osoba djelovati u ime fizičke ili pravne osobe. Ukoliko podnositelj dostavi nepotpun zahtjev koji je valjano potpisan, a na temelju podataka u zahtjevu nije moguće provesti opoziv, Fina CA će umjesto traženog opoziva provesti suspenziju certifikata sukladno točki 4.9.15. ovog CPS_{QC} dokumenta, ukoliko zahtjev ima dovoljno podataka za provođenje suspenzije.

Pri zaprimanju zahtjeva za opoziv po osobnoj dostavi zahtjeva službenik u RA mreži provodi sljedeći postupak:

- službenik u RA mreži provjerava cjelovitost, autentičnost i točnost zahtjeva i podataka upisanih u zahtjevu;
- ukoliko zahtjev i podaci upisani u zahtjevu nisu cjeloviti autentični i točni službenik u RA mreži odbija zahtjev i traži od podnositelja cjelovito, autentično i točno ispunjavanje zahtjeva;
- službenik u RA mreži provjerava podnositelja zahtjeva identifikacijom i potvrđivanjem identiteta sukladno točki 3.4.1. ovog CPS_{QC} dokumenta;

- ukoliko provjera podnositelja nije uspješna službenik u RA mreži mora odbiti zahtjev za opoziv certifikata;
- službenik u RA mreži zahtjev za opozivom prosljeđuje u Fina CA na postupak opoziva.

Pri zaprimanju zahtjeva za opoziv poštanskom dostavom ili preko dostavljača na adresu registracijskog ureda u RA mreži:

- službenik u RA mreži provjerava cjelovitost, autentičnost i točnost zahtjeva i podataka upisanih u zahtjevu;
- ukoliko zahtjev i podaci upisani u zahtjevu nisu cjeloviti autentični i točni službenik u RA mreži odbija zahtjev i obavještava podnositelja o razlogu odbijanja zahtjeva;
- službenik u RA mreži provjerava podnositelja zahtjeva identifikacijom i potvrđivanjem identiteta sukladno točki 3.4.2. ovog CPS_{QC} dokumenta;
- ukoliko provjera podnositelja nije uspješna službenik u RA mreži mora odbiti zahtjev za opoziv certifikata te o tome obavještava podnositelja;
- službenik u RA mreži zahtjev za opozivom prosljeđuje u Fina CA na postupak opoziva.

Postupak Fina CA pri zaprimanju zahtjeva za opoziv od strane službenika u RA mreži:

- na osnovu zahtjeva za opozivom, ovlaštena osoba Fina CA ili Središnjeg Fina RA opoziva certifikat izmjenom njegova statusa i objavom nove CRL u kojoj je sadržana informacija o opozvanosti certifikata;
- Fina CA o obavljenom opozivu obavještava potpisnika i osobu ovlaštenu za zastupanje ukoliko je to primjenjivo.

Ukoliko je Fina CA zaprimio zahtjev za opoziv certifikata e-mailom direktno od podnositelja ili vanjskog ugovorenog RA, Fina CA obavlja sljedeće radnje:

- ovlaštena osoba Fina CA ili Središnjeg Fina RA provjerava elektronički potpis na zahtjevu za opoziv;
- ovlaštena osoba Fina CA ili središnjeg RA provjerava točnost i cjelovitost podataka u zahtjevu za opoziv;
- ovlaštena osoba Fina CA ili središnjeg RA opoziva certifikat i objavljuje novu CRL u kojoj je sadržana informacija o opozvanosti certifikata;
- ukoliko podnositelj dostavi nepotpun zahtjev, certifikat se suspendira na osnovu zahtjeva, sukladno točki 4.9.15. ovog CPS_{QC} dokumenta, ukoliko zahtjev ima dovoljno podataka za provođenje suspenzije, a podnositelj se e-mailom obavještava o grešci te poziva na ponovnu dostavu zahtjeva za opozivom certifikata;
- Fina CA o obavljenom opozivu e-mailom obavještava potpisnika, odnosno osobu ovlaštenu za zastupanje ukoliko je to primjenjivo.

4.9.4. Poček zahtjeva za opozivom

Podnositelji zahtjeva za opoziv certifikata iz točke 4.9.2. ovog CPS_{QC} dokumenta trebaju u najkraćem razumnom roku od nastanka razloga za opoziv navedenih u točki 4.9.1. ovog CPS_{QC} 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, službenici u Fina RA mreži i djelatnici Fininog Centra za odnose s korisnicima mogu suspendirati certifikat prije njegova opoziva. Razlozi suspenzije su navedeni u točki 4.9.13. ovog CPS_{QC} dokumenta.

Neposredno nakon opoziva certifikata, Fina CA mijenja status certifikata te izdaje i objavljuje 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

Prije ostvarenja pouzdavanja u certifikat, pouzdajuća strana mora provesti provjeru statusa certifikata u cilju utvrđivanja njegove opozvanosti ili suspenzije, a u skladu s postupcima navedenim u točki 4.5.2. ovog CPS_{QC} dokumenta. Ako je pouzdajućoj strani u danom trenutku nemoguće dobiti informacije o statusu certifikata, tada mora odbiti uporabu certifikata do trenutka kada bude u mogućnosti dobiti informacije o statusu.

4.9.7. Učestalost izdavanja CRL

CRL za Fina RDC 2015 izdaje i potpisuje Fina RDC 2015, a CRL za Fina RDC-TDU 2015 izdaje i potpisuje Fina RDC-TDU 2015. Ove CRL objavljuju se odmah po opozivu, suspenziji ili reaktivaciji bilo kojeg certifikata izdanog od pripadnog Fina CA.

Fina CA izdaje i odmah objavljuje pripadnu CRL najmanje jedanput u roku od 24 sata od vremena izdavanja zadnje aktualne, još važeće CRL.

4.9.8. Maksimalno kašnjenje za CRL

Maksimalno kašnjenje CRL od trenutka njenog izdavanja do trenutka objave u redovitim uvjetima je uvijek manje od dvije minute.

4.9.9. *Online* dostupnost provjere opozvanih certifikata/statusa certifikata

CRL je primarno dostupna kroz LDAP imenik, te sekundarno kroz internetsku adresu odgovarajućeg repozitorija, kao što je to opisano u točki 4.10.1. ovog CPS_{QC} dokumenta. Podaci o pristupnim točkama za dohvat CRL sadržani su u svakom izdanom certifikatu.

Fina CA-ovi podržavaju *online* provjeru statusa opozvanosti izdanih certifikata putem Fina OCSP 2015 servisa čiji je rad temeljen na OCSP protokolu.

Informacija o statusu opozvanosti certifikata korištenjem Fina OCSP 2015 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.

4.9.10. Zahtjevi na *online* provjeru opozvanih certifikata

Za *online* preuzimanje CRL, pouzdajuće strane moraju imati pristup internetu te koristiti web preglednike ili aplikacije koje su u mogućnosti preuzeti CRL s internetskih adresa i protokolima navedenim u točki 4.10.1. ovog CPS_{QC} dokumenta.

4.9.11. Drugi dostupni načini objave opozvanih certifikata

Nije podržano.

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

Nema uvjeta.

4.9.13. Razlozi za suspenziju

Fina CA suspendira certifikat u slučajevima:

- kada korisnik ili potpisnik radi sumnji navedenih u točki 4.9.1. ovog CPS_{QC} dokumenta 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. ovog CPS_{QC} dokumenta, 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 ili osoba ovlaštena za zastupanje poslovnog subjekta.

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

Osoba ovlaštena za zastupanje poslovnog subjekta može podnijeti zahtjeva za suspenziju certifikata pripadajuće osobe.

Službenik u RA mreži može podnijeti zahtjev za suspenziju certifikata kojeg je podnio korisnik ili potpisnik, ili može podnijeti zahtjev u ime RA mreže. Zahtjev za suspenziju certifikata koji je podnesen u ime RA mreže autorizira neposredni voditelj službenika u RA mreži koji podnosi zahtjev.

Fina CA može tražiti suspendiranje bilo kojeg izdanog certifikata uz odobrenje Fina PMA.

Fina CA o obavljenoj suspenziji certifikata pisanim putem obavještava pripadajućeg potpisnika te, ukoliko je to primjenjivo, i korisnika. Potpisnicima i korisnicima koji su u zahtjevu za izdavanje certifikata dostavili e-mail adresu, obavijest se šalje e-mailom, a ostalim potpisnicima i korisnicima obavijest se šalje poštom.

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

Zahtjev za reaktivaciju poslovnih certifikata izdanih fizičkim osobama te certifikata za TDU podnosi potpisnik, 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 je u obliku obrasca Zahtjev za opoziv, suspenziju, reaktivaciju ili oporavak certifikata dostupan na internetskim stranicama Fina PKI repozitorija iz točke 2.2. ovog CPS_{QC} dokumenta. Zahtjev treba odmah po nastupanju razloga za suspenziju koji su opisani u točki 4.9.13. ovog CPS_{QC} dokumenta, točno i cjelovito ispuniti, potpisati i u najkraćem uredovnom roku dostaviti u Fina PKI na jedan od sljedećih načina:

- Osobnom dostavom u registracijski ured RA mreže u uredovno vrijeme:

  Popunjen i vlastoručno potpisan zahtjev suspenziju, uz osobnu identifikaciju podnositelja prema postupku opisanom u točki 3.4.6. ovog CPS_{QC} dokumenta predaje se službeniku u RA mreži.

- Poštanskom dostavom ili preko dostavljača na adresu registracijskog ureda u RA mreži:

  Popunjen i vlastoručno potpisan zahtjev za suspenziju, uz identifikaciju podnositelja prema postupku opisanom u točki 3.4.7. ovog CPS_{QC} dokumenta poštanskom dostavom ili preko dostavljača dostavlja se u registracijski ured u RA mreži.

- Telefonskim pozivom na Finin Centar za odnose s korisnicima:

  Podnositelj zahtjeva navodi sljedeće podatke za specificiranja certifikata za suspenziju:

  - serijski broj certifikata ili
  - ime i prezime potpisnika i serijski broj (ukoliko postoji u DN-u certifikata), naziv poslovnog subjekta u slučaju da se traži suspenzija poslovnog certifikata.

  Podnositelj zahtjeva navodi sljedeće podatke u cilju identifikacije:

  - ime i prezime podnositelja zahtjeva;
  - OIB podnositelja zahtjeva;
  - naziv poslovnog subjekta (ukoliko se traži opoziv poslovnog certifikata);
  - kontakt broj telefona ili e-mail adresa podnositelja zahtjeva.

  Djelatnik Centara za odnose s korisnicima dobivene odgovore za identifikaciju podnositelja zahtjeva provjerava uspoređujući ih s podacima upisanim u RA bazi za certifikat za koji se traži suspenzija.

  Ukoliko je zahtjev za suspenzijom zaprimljen u uredovno vrijeme Fina CA, Centara za odnose s korisnicima po provjeri podataka zahtjev za suspenzijom zahtjev prosljeđuje u Fina CA.

  Ukoliko je telefonski zahtjev za suspenzijom certifikata zaprimljen izvan uredovnog vremena Fina CA, ovlaštena osoba Centara za odnose s korisnicima po provjeri podataka provodi suspenziju certifikata. Fina CA mijenja statusa certifikata i objavljuje novu CRL u kojoj je sadržana informacija o suspendiranosti certifikata. Ovlaštena osoba Centara za odnose s korisnicima o obavljenoj suspenziji obavještava potpisnika i osobu ovlaštenu za zastupanje ukoliko je to primjenjivo.

- Putem telefaksa:

Dostava popunjenog i vlastoručno potpisanog zahtjeva za suspenziju i identifikacija podnositelja obavlja se telefaksom prema postupku opisanom u točki 3.4.9. ovog CPS_{QC} dokumenta.

- Elektroničkom dostavom zahtjeva za opoziv na e-mail adresu:

Dostava popunjenog zahtjeva za suspenziju certifikata koji je potpisan naprednim elektroničkim potpisom podnositelja zahtjeva i identifikacija podnositelja obavlja se prema postupku opisanom u točki 3.4.10.

Postupak službenika u RA mreži pri zaprimanju zahtjeva za suspenzijom certifikata po osobnoj dostavi:

- službenik u RA mreži provjerava cjelovitost, autentičnost i točnost zahtjeva i podataka upisanih u zahtjevu;
- ukoliko zahtjev i podaci upisani u zahtjevu nisu cjeloviti autentični i točni službenik u RA mreži odbija zahtjev i traži od podnositelja cjelovito, autentično i točno ispunjavanje zahtjeva;
- službenik u RA mreži provjerava podnositelja zahtjeva identifikacijom i potvrđivanjem identiteta sukladno točki 3.4.6. ovog CPS_{QC} dokumenta;
- ukoliko provjera podnositelja nije uspješna službenik u RA mreži mora odbiti zahtjev za suspenziju certifikata;
- službenik u RA mreži prosljeđuje zahtjev u Fina CA na postupak suspenzije.

Pri zaprimanju zahtjeva za suspenziju poštanskom dostavom ili preko dostavljača na adresu registracijskog ureda u RA mreži:

- službenik u RA mreži provjerava cjelovitost, autentičnost i točnost zahtjeva i podataka upisanih u zahtjevu;
- ukoliko zahtjev i podaci upisani u zahtjevu nisu cjeloviti autentični i točni službenik u RA mreži odbija zahtjev i obavještava podnositelja o razlogu odbijanja zahtjeva;
- službenik u RA mreži provjerava podnositelja zahtjeva identifikacijom i potvrđivanjem identiteta sukladno točki 3.4.6. ovog CPS_{QC} dokumenta;
- ukoliko provjera podnositelja nije uspješna službenik u RA mreži mora odbiti zahtjev za suspenziju certifikata te o tome obavještava podnositelja;
- službenik u RA mreži zahtjev za suspenziju prosljeđuje u Fina CA na postupak suspenzije.

Postupak Fina CA pri zaprimanju zahtjeva za suspenzijom certifikata od strane službenika u RA mreži:

- na osnovu zahtjeva za suspenzijom, ovlaštena osoba Fina CA ili Središnjeg Fina RA suspendira certifikat izmjenom njegova statusa i objavom nove CRL u kojoj je sadržana informacija o suspendiranosti certifikata;
- Fina CA o obavljenoj suspenziji obavještava potpisnika i osobu ovlaštenu za zastupanje ukoliko je to primjenjivo.

Ukoliko je Fina CA zaprimio zahtjev za suspenziju certifikata e-mailom direktno od podnositelja ili vanjskog ugovorenog RA, Fina CA obavlja sljedeći postupak:

- ovlaštena osoba Fina CA ili Središnjeg Fina RA provjerava napredni elektronički potpis na zahtjevu za suspenziju;

- ovlaštena osoba Fina CA ili središnjeg RA provjerava točnost i cjelovitost podataka u zahtjevu za suspenziju;
- ovlaštena osoba Fina CA ili središnjeg RA suspendira certifikat i objavljuje novu CRL u kojoj je sadržana informacija o suspendiranosti certifikata;
- Fina CA o obavljenoj suspenziji e-mailom obavještava potpisnika i osobu ovlaštenu za zastupanje ukoliko je to primjenjivo.

Po suspenziji certifikata korisnik ili potpisnik mogu tražiti opoziv ili reaktivaciju certifikata.

Postupak u slučaju opoziva suspendiranog certifikata je opisana u točki 4.9.3. ovog CPS_{QC} dokumenta.

4.9.15.2. Procedura za zahtjev za reaktivaciju

Zahtjev za reaktivaciju certifikata je u obliku obrasca Zahtjev za opoziv, suspenziju, reaktivaciju ili oporavak certifikata dostupan na internetskim stranicama Fina PKI repozitorija iz točke 2.2. ovog CPS_{QC} dokumenta. Zahtjev treba točno i cjelovito ispuniti, potpisati i dostaviti u Fina PKI na jedan od slijedećih načina:

- Osobnom dostavom u registracijski ured RA mreže u uredovno vrijeme:

  Popunjen i vlastoručno potpisan zahtjev za reaktivaciju, uz neposrednu identifikaciju podnositelja prema postupku opisanom u točki 3.4.1. ovog CPS_{QC} dokumenta predaje se službeniku u RA mreži.

- Poštanskom dostavom ili preko dostavljača na adresu registracijskog ureda u RA mreži:

  Popunjen i vlastoručno potpisan zahtjev za reaktivaciju, uz identifikaciju podnositelja prema postupku opisanom u točki 3.4.2. ovog CPS_{QC} dokumenta poštanskom dostavom ili preko dostavljača dostavlja se u registracijski ured u RA mreži.

- Elektroničkom dostavom zahtjeva za opoziv na e-mail adresu:

  Dostava popunjenog zahtjeva za reaktivaciju koji je potpisan naprednim elektroničkim potpisom podnositelja zahtjeva i identifikacija podnositelja obavlja se prema postupku opisanom u točki 3.4.5.

Postupak službenika u RA mreži pri zaprimanju zahtjeva za reaktivacijom certifikata po osobnoj dostavi:

- službenik u RA mreži provjerava cjelovitost, autentičnost i točnost zahtjeva i podataka upisanih u zahtjevu;
- ukoliko zahtjev i podaci upisani u zahtjevu nisu cjeloviti autentični i točni službenik u RA mreži odbija zahtjev i traži od podnositelja cjelovito, autentično i točno ispunjavanje zahtjeva;
- službenik u RA mreži provjerava podnositelja zahtjeva identifikacijom i potvrđivanjem identiteta sukladno točki 3.4.1. CPS_{NQC} dokumenta;

- ukoliko provjera podnositelja nije uspješna službenik u RA mreži mora odbiti zahtjev za reaktivaciju certifikata;
- službenik u RA mreži prosljeđuje zahtjev za reaktivacijom u Fina CA na postupak reaktivacije.

Pri zaprimanju zahtjeva za reaktivaciju poštanskom dostavom ili preko dostavljača na adresu registracijskog ureda u RA mreži:

- službenik u RA mreži provjerava cjelovitost, autentičnost i točnost zahtjeva i podataka upisanih u zahtjevu;
- ukoliko zahtjev i podaci upisani u zahtjevu nisu cjeloviti autentični i točni službenik u RA mreži odbija zahtjev i obavještava podnositelja o razlogu odbijanja zahtjeva;
- službenik u RA mreži provjerava podnositelja zahtjeva identifikacijom i potvrđivanjem identiteta sukladno točki 3.4.2. ovog CPS_{QC} dokumenta;
- ukoliko provjera podnositelja nije uspješna službenik u RA mreži mora odbiti zahtjev za reaktivaciju certifikata te o tome obavještava podnositelja;
- službenik u RA mreži zahtjev za reaktivaciju prosljeđuje u Fina CA na postupak reaktivacije.

Ukoliko je Fina CA zaprimio zahtjev za reaktivaciju certifikata e-mailom direktno od podnositelja ili vanjskog ugovorenog RA, Fina CA obavlja sljedeći postupak:

- ovlaštena osoba Fina CA ili Središnjeg Fina RA provjerava napredni elektronički potpis na zahtjevu za reaktivaciju;
- ovlaštena osoba Fina CA ili središnjeg RA provjerava točnost i cjelovitost podataka u zahtjevu za reaktivaciju;
- ovlaštena osoba Fina CA ili središnjeg RA reaktivira certifikat i objavljuje novu CRL u kojoj se više ne nalazi informacija o suspendiranosti certifikata;
- Fina CA o obavljenoj reaktivaciji e-mailom obavještava potpisnika i osobu ovlaštenu za zastupanje ukoliko je to primjenjivo.

Ukoliko zahtjev nije potpun ili postoje drugi niže navedeni razlozi zbog čega se certifikat ne može reaktivirati, službenik u RA mreži odbija zahtjev za reaktivacijom. Nakon prestanka razloga radi kojih certifikat nije smio biti reaktiviran, podnositelj zahtjeva može ponovno zatražiti reaktivaciju certifikata.

Zahtjev za reaktivaciju se može odbiti zbog:

- netočnih podataka;
- nepravilno potpisanog ili nepravilno ovjerenog zahtjeva;
- prethodnih neodgovarajućih postupaka i nepoštivanja ugovornih obveza korisnika;
- zakonske zabrane.

Postupak Fina CA pri zaprimanju zahtjeva za reaktivacijom certifikata:

- na osnovu zahtjeva za reaktivacijom, ovlaštena osoba Fina CA ili Središnjeg Fina RA reaktivira certifikat izmjenom njegova statusa i objavom nove CRL u kojoj više nije sadržana informacija o suspendiranosti certifikata;

- Fina CA o obavljenoj suspenziji obavještava potpisnika i osobu ovlaštenu za zastupanje ukoliko je to primjenjivo.

Ukoliko je Fina CA zaprimio zahtjev za reaktivaciju certifikata e-mailom direktno od podnositelja ili vanjskog ugovorenog RA, Fina CA obavlja sljedeći postupak:

- ovlaštena osoba Fina CA ili Središnjeg Fina RA provjerava napredni elektronički potpis na zahtjevu za reaktivaciju;
- ovlaštena osoba Fina CA ili središnjeg RA provjerava točnost i cjelovitost podataka u zahtjevu za reaktivaciju;
- ovlaštena osoba Fina CA ili središnjeg RA reaktivira certifikat i objavljuje novu CRL u kojoj više nije sadržana informacija o suspendiranosti certifikata;
- Fina CA o obavljenoj reaktivaciji e-mailom obavještava potpisnika, i osobu ovlaštenu za zastupanje ukoliko je to primjenjivo.

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 CRL ili OCSP servisa.

CRL liste Fina CA certifikata objavljuju se na javnom imeniku i na web poslužitelju repozitorija određenog Fina CA. Na javnom imeniku objavljuju se objedinjena i segmentirana CRL, a na web poslužitelju objavljuje se objedinjena CRL.

Adrese objave CRL sadržane su u ekstenziji *CRLDistributionPoints* u svakom izdanom certifikatu i upisane su sljedećim redoslijedom:

1. adresa objedinjene CRL na web poslužitelju;
2. adresa objedinjene CRL na javnom imeniku;
3. adresa segmentirane CRL na javnom imeniku, uključujući i brojčanu oznaku segmenta.

Navedeni redoslijed označava redoslijed kojim pouzdajuća strana treba dohvaćati CRL:

1. ako aplikacija pouzdajuće strane podržava rad sa segmentiranom CRL, aplikacija s web poslužitelja dohvaća objedinjenu CRL,
2. ako web poslužitelj nije dostupan, objedinjenu CRL aplikacija dohvaća s javnog LDAP imenika,
3. ako aplikacija pouzdajuće strane podržava rad sa segmentiranom CRL, aplikacija s javnog imenika dohvaća određeni segment segmentirane CRL.

4.10.1.1. Adrese za dohvat CRL liste Fina RDC 2015 certifikata

Adresa objedinjene CRL liste Fina RDC 2015 certifikata na web poslužitelju je: http://rdc.fina.hr/RDC2015/FinaRDCCA2015.crl.

Na internetskim stranicama http://www.fina.hr/finadigicert CRL je moguće dohvatiti u DER, PEM i tekstualnom formatu.

Adresa objedinjene CRL liste Fina RDC 2015 certifikata na javnom imeniku je:

ldap://rdc-ldap2.fina.hr/cn=Fina%20RDC%202015,o=Financijska%20agencija, c=HR?certificateRevocationList%3Bbinary

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

CN=CRL1, CN=Fina RDC 2015, O=Financijska agencija, C=HR

Oznaka x u CN=CRLx označava segment CRL.

4.10.1.2. Adrese za dohvat CRL liste Fina RDC-TDU 2015 certifikata

Adresa objedinjene CRL liste Fina RDC-TDU 2015 certifikata na web poslužitelju je: http://rdc.fina.hr/RDC-TDU2015/FinaRDC-TDUCA2015.crl.

Na internetskoj stranici http://www.fina.hr/finadigicert CRL je moguće dohvatiti u DER, PEM i tekstualnom formatu.

Adresa objedinjene CRL liste Fina RDC-TDU 2015 certifikata na javnom imeniku:

ldap://rdc-tdu-ldap2.fina.hr/cn=Fina%20RDC-TDU%202015,o=Financijska%20agencija, c=HR?certificateRevocationList%3Bbinary

Adresa segmentirane CRL liste Fina RDC-TDU 2015 certifikata na javnom imeniku je: CN=CRL1, CN=Fina RDC-TDU 2015, O=Financijska agencija, C=HR

Oznaka x u CN=CRLx označava segment CRL.

4.10.2. Dostupnost usluga

Dostupnost CRL koje izdaju i objavljuju Fina CA-ovi je 24 sata na dan i 7 dana u tjednu. U slučaju ispada sustava, nastanka okolnosti koje su izvan kontrole Fine ili utjecaja više sile, usluga je dostupna maksimalno moguće vrijeme, u skladu sa najboljim poslovnim praksama.

4.10.3. Opcionalna svojstva

Nema odredbi.

4.11. Kraj korištenja

Ako korisnik namjerava otkazati ugovor o obavljanju usluga certificiranja, mora prema RA mreži uputiti zahtjev za otkaz ugovora o obavljanju usluga certificiranja.

Korisnik može otkazati ugovor u pisanom obliku bez obrazloženja.

Fina će otkazati ugovor u slučaju kad:

- poslovni subjekt ili potpisnik ne ispunjavaju uvjete koji su navedeni u Općim pravilima [33] i Uvjetima pružanja usluga certificiranja, ili
- poslovni subjekt ili potpisnik postupaju protivno odredbama ugovora o obavljanju usluga certificiranja.

Otkaz ugovora znači i opoziv svih certifikata izdanih po ugovoru o obavljanju usluga certificiranja.

Adrese lokacija registracijskih ureda Fina RA mreže su na web dijelu repozitorija iz točke 2.2. ovog CPS_{QC} dokumenta. Adresa davatelja usluga certificiranja navedena je u točki 9.11. ovog CPS_{QC} dokumenta.

Nakon otkaza ugovora Fina CA će opozvati sve certifikate na koje se odnosi taj ugovor.

4.12. Sigurno skladištenje i oporavak privatnog ključa

Fina CA ne obavlja pohranu i oporavak korisničkih ključeva kvalificiranih certifikata.

4.12.1. Pravila i prakse sigurnog skladištenja i povrata privatnog ključa

Ne primjenjuje se.

4.12.2. Pravila i prakse enkapsulacije ključa sesije

Ne primjenjuje se.

5. PROVJERA SUSTAVA, UPRAVLJANJA I RADNIH POSTUPAKA

Fina kao davatelj usluga certificiranja koji izdaje kvalificirane certifikate primjenjuje adekvatne mjere fizičke zaštite sustava izdavanja kvalificiranih certifikata. Ove mjere zaštite imaju jednu od ključnih uloga u ostvarivanju povjerenja u izdane kvalificirane certifikate Fine.

U ovom poglavlju prikazan je opis sustava fizičke zaštite koji se provodi u Fina PKI sustavu za izdavanje kvalificiranih certifikata. Detaljniji opis sustava fizičke zaštite uređaja, opreme i podataka koji se upotrebljavaju u Fina PKI sustavu nalazi se u Fininim internim dokumentima.

5.1. Kontrole fizičke sigurnosti

Fina kao davatelj usluga certificiranja koji izdaje kvalificirane certifikate primjenjuje mjere fizičke zaštite sustava izdavanja kvalificiranih certifikata u skladu s poslovnom politikom Fine, važećom zakonskom regulativom i međunarodnim preporukama.

Fina primjenjuje mjere fizičke zaštite sustava izdavanja kvalificiranih certifikata radi ograničavanja pristupa hardverskim i softverskim komponentama sustava kao što su poslužitelji, radne stanice, kriptografski moduli, mrežni uređaji i pripadajući softver u Fina CA-ovima, arhivi i repozitoriju kao i za pristup podacima registriranih fizičkih osoba i poslovnih subjekata. Fizički pristup navedenoj opremi je opisan u točki 5.2.1. ovog CPS_{QC} dokumenta.

5.1.1. Lokacija objekta i njegova konstrukcija

Finin produkcijski sustav izdavanja kvalificiranih certifikata Fine nalazi se u zgradi Fine, u posebnom prostoru izdvojenom za tu namjenu, uz primjenu više razina fizičke i tehničke zaštite. Smještaj produkcijskog sustava izdavanja kvalificiranih certifikata Fine udovoljava sigurnosnim zahtjevima iz zakonske regulative.

Sekundarni sustav certificiranja Fine nalazi se na izdvojenoj udaljenoj lokaciji i 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 u odnosu na primarni sustav udovoljava jednakim ili višim sigurnosnim zahtjevima.

5.1.2. Fizički pristup

Fizički pristup Fina CA sustavu, Fina RA sustavu, repozitoriju i arhivi su štićeni sukladno važećoj zakonskoj regulativi i internim propisima, te se o svakom pristupu vodi evidencija.

Fizički pristup podacima koje prikuplja RA mreža imaju samo ovlašteni zaposlenici Fina CA i 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

Svi uređaji i prostor Fininog sustava izdavanja kvalificiranih certifikata smještenog u Fina PKI štićenom prostoru imaju rezervno napajanje osigurano uređajem za neprekidno napajanje u konfiguraciji s dizel agregatom koje omogućuje neprekidan i pouzdani rad sustava izdavanja kvalificiranih certifikata do ponovne uspostave primarnog napajanja.

U svim prostorijama u kojima se nalazi oprema sustava izdavanja kvalificiranih certifikata instalirani su klima uređaji za održavanje propisanog radnog okruženja.

5.1.4. Opasnost od poplave

Oprema Fininog sustava za izdavanje kvalificiranih certifikata nalazi se u prostoru koji je osiguran od poplave.

5.1.5. Protupožarna zaštita

Finin sustav za izdavanje kvalificiranih certifikata zaštićen je automatskim sustavom protupožarne zaštite sukladno propisanoj i važećoj zakonskoj regulativi.

5.1.6. Pohrana medija

Mediji sa sigurnosnim kopijama podataka Fina CA-ova, središnjeg Fina RA sustava, kopijama sadržaja repozitorija, mediji s elektroničkom arhivom te mediji sa sigurnosnim kopijama programske opreme iz sustava izdavanja kvalificiranih certifikata pohranjuju se na dvije odvojene štićene lokacije na siguran način kako bi se zaštitili od oštećenja, otuđenja ili neovlaštenog pristupa.

5.1.7. Zbrinjavanje otpada

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

Zbrinjavanje otpada iz Fina PKI štićenog prostora odvija se pod nadzorom ovlaštenih zaposlenika koji obavljaju poslove iz područja Fina PKI.

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

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

5.1.8. Sigurnosne kopije na drugoj lokaciji

Sigurnosne kopije Fina CA-ova, središnjeg Fina RA sustava, sadržaja repozitorija i arhive u elektroničkom obliku, sigurnosne kopije programske opreme te kopija dnevnika sustava koji se vode u papirnatom obliku pohranjuju se u drugom štićenom prostoru na izdvojenoj lokaciji.

Sigurnosne kopije koje se pohranjuju u drugom štićenom prostoru na izdvojenoj lokaciji se, u odnosu na njihove originale, čuvaju uz primjenu jednake ili više razine mjera fizičke zaštite.

5.2. Kontrola procedura

5.2.1. Povjerljive uloge

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

Povjerljive uloge dodjeljuju se ovlaštenim osobama iz nadležnih organizacijskih dijelova Fine.

5.2.2. Broj osoba potrebnih za obavljanje zadataka

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

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

5.2.3. Identifikacija i potvrđivanje identiteta za svaku ulogu

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

5.2.4. Uloge koje zahtijevaju odvajanje dužnosti

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

- Službeniku za sigurnost, Službeniku središnjeg RA Fine, odnosno LRA službeniku ne smije biti dodijeljena uloga Službenika za nadzor sustava;
- Administratoru sustava ne smije biti dodijeljena uloga Službenika za sigurnost ili uloga Službenika za nadzor sustava.

5.3. Provjere osoblja

5.3.1. Kvalifikacije, radno iskustvo i zahtjevi za provjerom osoblja

Pri zapošljavanju osoblja na poslovima Fina CA uzimaju se u obzir zahtjevi za odgovarajućom stručnom spremom za svaku povjerljivu, odnosno korisničku ulogu.

Prije početka rada u Fina CA kandidati moraju imati odgovarajuća stručna znanja u radu s PKI tehnologijom, stručna znanja za postupke zaštite računalne opreme i programa koji se koriste u Fina CA sustavima.

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

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

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

Fina CA osoblje kontinuirano usavršava specijalistička znanja i vještine.

5.3.5. Učestalost i slijed izmjene zaposlenika

Ne primjenjuje se.

5.3.6. Kazne za neovlaštene radnje

Prema osobama koje ne postupaju sukladno Fininim Općim pravilima [33], ovom CPS_{QC} dokumentu i drugim internim pravilnicima i dokumentima Fina PKI poduzeti će se odgovarajuće stegovne sankcije u skladu s internim aktima Fine.

U slučaju izvođenja neovlaštene radnje ili zlonamjerne radnje koju je izvela ovlaštena osoba Fina CA primjenjuju se odredbe važeće zakonske regulative i internih akata Fine.

Takvoj osobi biti će zabranjen rad na poslovima u Fina PKI.

5.3.7. Zahtjevi za vanjske suradnike

Zahtjevi za vanjske suradnike opisani su u internim dokumentima Fine.

5.3.8. Dokumentacija koja je dostupna osoblju

Svakom zaposleniku dostupna je dokumentacija potrebna za obavljanje njegovih radnih zadataka, koja uključuje interne i vanjske materijale za edukaciju, te radne upute i procedure za obavljanje pojedinih poslova u Fina PKI, sukladno dodijeljenoj povjerljivoj ili privilegiranoj korisničkoj 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 prate se i pregledavaju periodički. 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 u Fina CA štite se mehanizmima i postupcima koji osiguravaju povjerljivost i cjelovitost dnevnika te ne dozvoljavaju izmjenu zapisa, kao ni jednostavno brisanje ili uništenje zapisa.

Tako zaštićeni dnevnici sustava na zahtjev su raspoloživi samo ovlaštenim osobama, posebice u svrhu pružanja dokaza o certifikatu 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)

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

5.4.7. Obavještavanje subjekta uzročnika događaja

Fina će, po potrebi, obavijestiti subjekta koji je uzrokovao bilježenja zapisa o događaju.

5.4.8. Procjena ranjivosti

Rezultati analize dnevnika sustava koriste se za procjenu ranjivosti sustava.

Analiza dnevnika sustava i praćenje provedbe svih propisanih postupaka provodi se od strane ovlaštenih osoba u Fina PKI.

5.5. Arhiviranje zapisa

5.5.1. Tipovi arhiviranih zapisa

Arhiviraju se minimalno sljedeći zapisi Fina PKI sustava 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;
- kvalificirani 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 uređaje;
- dnevnici povjerljivih sustava;
- relevantni zapisnici vezani uz rad i održavanje Fina PKI sustava;
- drugi dokumenti Fina PKI, sukladno važećim propisima.

Svaki zapis koji se arhivira sadržava podatak o vremenu koje 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

Generiranje novog para potpisnih ključeva Fina CA provodi se pravovremeno prije njihova isteka perioda valjanosti.

Fina CA par potpisnih ključeva mora biti generiran na način opisan u točki 6.1 ovog CPS_{QC} dokumenta.

O planiranoj promjeni Fina CA ključa, Fina CA će pravovremeno obavijestiti sudionike Fina PKI objavom na internetskoj stranici repozitorija Fina CA za kojeg se provodi promjena ključa (vidi točke 2.2.1. i 2.2.2. CPS_{QC} dokumenta). Novi Fina CA certifikat dostupan je sudionicima Fina PKI putem javnog imenika i internetskih stranica pripadnog repozitorija iz točke 2.2 ovog CPS_{QC} dokumenta.

Novi Fina CA certifikat dostavljat će se potpisnicima, skrbnicima i pouzdajućim stranama na način na koji se dostavlja postojeći Fina CA *root* certifikat, sukladno točki 6.1.4. ovog CPS_{QC} dokumenta.

5.7. Oporavak od kompromitiranja ili nepogode

Fina PKI ima planove za očuvanje i oporavak sustava nakon nepogode, koji uključuju i postupke u slučaju kompromitiranja privatnog Fina CA ključa te u slučaju hardverskih i softverskih kvarova i grešaka na kritičnim komponentama Fina CA sustava.

Internim planovima obuhvaćeni su postupci očuvanja i oporavka sustava za slučaj povrede pravila pristupa Fina CA sustavu, elementarnih nepogoda, požara, prekida napajanja i komunikacijskih kanala, puknuća vodovodnih cijevi, otuđenja ili kompromitiranja podataka i sl.

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

5.7.1. Postupci u slučaju nepogode 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, Fina će:

- zaustaviti izdavanje certifikata od strane Fina CA čiji je privatni ključ kompromitiran;
- opozvati pripadajući certifikat Fina CA čiji je privatni ključ kompromitiran;
- opozvati sve certifikate izdane uporabom kompromitiranog privatnog ključa;
- obavijestiti Fina RA/LRA i vanjske ugovorene RA;
- obavijestiti korisnike s kojima ima sklopljen ugovor o obavljanju usluga certificiranja;
- obavijestiti pouzdajuće strane putem obavijesti na internetskim stranicama repozitorija iz točke 2.2. ovog CPS_{NQC} dokumenta;
- ustanoviti uzroke koji su prouzročili kompromitiranost Fina CA privatnog potpisnog ključa;
- generirati novi par Fina CA potpisnih ključeva;
- izdati novi Fina CA certifikat;
- objaviti novi Fina CA certifikat korisnicima i pouzdajućim stranama;
- započeti s izdavanjem certifikata potpisujući ih s novim Fina CA privatnim potpisnim ključem;
- osigurati da se CRL liste potpisuju uporabom novog ključa.

U slučaju da korišteni kriptografski algoritmi i parametri prestanu pružati zahtijevanu sigurnost i zaštitu Fina će:

- obavijestiti svakog korisnika s kojima ima sklopljen ugovor o obavljanju predmetnih usluga e će na internetskoj stranici repozitorija Fina CA (vidi točke 2.2.1. i 2.2.2. ovog CPS_{QC} dokumenta) objaviti obavijest za pouzdajuće strane o kompromitiranju kriptografskih algoritama;
- opozvati sve certifikate na koje se to odnosi.

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/LRA. Detaljnije odredbe vezane uz prekid rada vanjskog ugovorenog RA određuju se međusobnim ugovornim obvezama.

slučaju prestanka obavljanja usluga certificiranja za pojedini Fina CA koji prestaje s radom, Fina će:

- obavijestiti svakog korisnika i sve poslovne subjekte s kojima ima sklopljen ugovor o obavljanju predmetnih usluga ili je u poslovnom odnosu u svezi davanja usluga certificiranja koje pruža Fina CA te ministarstvo nadležno za gospodarstvo, najmanje tri mjeseca prije prestanka obavljanja usluga certificiranja Fina CA;
- o mogućem prestanku rada pojedinog Fina CA na internetskoj stranici repozitorija Fina CA koji prestaje s radom (vidi točke 2.2.1. i 2.2.2. ovog CPS_{QC} dokumenta) objaviti obavijest za pouzdajuće strane, najmanje tri mjeseca prije prestanka obavljanja usluga izdavanja kvalificiranih certifikata od strane Fina CA koji prestaje s radom;
- osigurati kod drugog davatelja usluga certificiranja nastavak obavljanja usluga izdavanja kvalificiranih certifikata za korisnike kojima je Fina CA izdao kvalificirane certifikate, ukoliko postoji davatelj takve usluge iste kvalitete usluge kao i Fina CA, a koji je s time suglasan
- ukoliko nema drugog davatelja usluga koji bi osigurao nastavak obavljanja usluga certificiranja Fina CA će opozvati sve izdane kvalificirane certifikate te o tome odmah obavijestiti ministarstvo nadležno za gospodarstvo;
- dostaviti svu dokumentaciju u svezi s obavljanjem usluga izdavanja kvalificiranih certifikata drugom davatelju usluga na kojega prenosi obveze s osnove obavljanja usluga izdavanja kvalificiranih certifikata za Fina CA koji prestaje s radom, odnosno ministarstvu nadležnom za gospodarstvo, ukoliko nema drugog davatelja usluga;
- nastaviti održavati prikupljene podatke korisnika kojima je Fina CA izdao kvalificirane certifikate, a koji su prikupljeni u postupku registracije, pružanje informacija o statusu opozvanosti izdanih certifikata te arhiviranje dnevnika sustava vezanih uz događaje okruženja vjerodostojnog sustava, događaje upravljanja ključevima i certifikatima, u vremenskom periodu koji je naveden u točki 5.5.2. ovog CPS_{QC} dokumenta ili će s drugim poslovnim subjektom ugovoriti održavanje istih;
- nastaviti održavati podatke nužne za pružanje dokaza u sudskim, upravnim i drugim postupcima, navedene u točki 5.5.1. ovog CPS_{QC} dokumenta za Fina CA koji prestaje s radom u vremenskom periodu koji je naveden u točki 5.5.2. ovog CPS_{QC} dokumenta, ili će s drugim poslovnim subjektom ugovoriti održavanje istih;
- ukinuti sva ovlaštenja eventualno podugovorenim poslovnim subjektima koji u ime Fina CA sudjeluju u bilo kojem dijelu procesa izdavanja kvalificiranih certifikata;
- za Fina CA koji prestaje s radom uništiti pripadne privatne potpisne ključeve i sve njihove kopije.

6. PROVJERA TEHNIČKE SIGURNOSTI

Zahtjevi na tehničku sigurnost i primijenjene mjere zaštite u Fina PKI određene su vrstom usluga koje pružaju njeni pojedini dijelovi.

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

6.1. Generiranje i instalacija para ključeva

6.1.1. Generiranje para ključeva

6.1.1.1. Generiranje para Fina CA ključeva

Postupak generiranja para Fina CA ključeva provodi se ceremonijom generiranja Fina CA ključeva kojoj prisustvuju ovlaštene osobe. Generiranje para ključeva pokreću ovlaštene osobe Fina CA uz nadzor ovlaštenih osoba Fina PMA. Fina CA par ključeva generira se na siguran način u HSM modulu koji zadovoljava zahtjeve iz točke 6.2.1. ovog CPS_{QC} dokumenta.

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

6.1.1.2. Generiranje para RA ključeva

Ovlaštene osobe u Fina RA mreži koriste Poslovni potpisni Q2 certifikat (QCP+). Generiranje para ključeva za ovaj tip certifikata opisano je u točki 6.1.1.3. ovog CPS_{QC} dokumenta, pri čemu je potpisnik iz navedene točke ovlaštena osoba Fina RA mreže, a korisnička lokacija je lokacija unutar Fina RA mreže.

6.1.1.3. Generiranje para ključeva za QCP+ certifikate korisnika

Ovaj postupak se primjenjuje za sljedeće tipove certifikata:

- Osobni potpisni Q2 certifikat (QCP+);
- Poslovni potpisni Q2 certifikat (QCP+) i
- TDU potpisni Q2 certifikat (QCP+).

Parovi ključeva za QCP+ certifikate potpisnika se generiraju na SSCD uređajima.

Ukoliko Fina CA generira potpisnikov par ključeva, ključevi se na SSCD uređaju generiraju u Fina PKI štićenom prostoru, uz nadzor i upravljanje Fina CMS sustava.

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

Ukoliko svoj par ključeva generira potpisnik tada se ključevi na SSCD uređaju generiraju na korisničkoj lokaciji, po preuzimanju SSCD uređaja u RA mreži, uz osobnu identifikaciju

potpisnika te po primitku aktivacijskih podataka. Potpisnik svoj par ključeva generira na jedan od sljedeća dva načina:

- Ukoliko je potpisnik registriran u Fina RA mreži ili je potpisnik registriran u RA mreži vanjskog ugovorenog RA koji u postupku ne koristi vlastiti CMS, potpisnik se autentificira na udaljeni Fina CMS sustav sigurnom SSL/TLS komunikacijom, koristeći dobivene aktivacijske podatke i pripadajući SSCD. U tom postupku, pod udaljenim *online* nadzorom i upravljanjem Fina CMS sustava potpisnik na SSCD uređaju generira svoj par ključeva.
- Ukoliko je potpisnik registriran u RA mreži vanjskog ugovorenog RA i ukoliko potpisnik generira ključ za Poslovni potpisni Q2 certifikat (QCP+), vanjski ugovoreni RA po odobrenju Fine u postupku može koristiti vlastiti CMS sustav. Potpisnik se autentificira na udaljeni CMS sustav vanjskog ugovorenog RA sigurnom SSL komunikacijom, koristeći dobivene aktivacijske podatke i pripadajući SSCD. U tom postupku, pod udaljenim *online* nadzorom i upravljanjem CMS sustava vanjskog ugovorenog CA potpisnik na SSCD uređaju generira svoj par ključeva.

6.1.2. Dostava privatnog ključa korisniku

Ukoliko Fina CA generira privatni ključ povezan s kvalificiranim certifikatom za ovlaštene osobe u Fina RA mreži, tada se privatni ključ osobno, na SSCD uređaju, uručuje ovlaštenoj osobi, uz prethodnu neposrednu identifikaciju.

Ukoliko svoj privatni ključ povezan s kvalificiranim certifikatom na SSCD uređaju, pod udaljenim nadzorom Fina CA, generira ovlaštena osoba u Fina RA mreži, smatra se da svoj privatni ključ ovlaštena osoba već posjeduje.

U slučaju da Fina CA ili Središnji Fina RA generira privatni ključ za potpisnika, unutar SSCD uređaja, tada se SSCD uređaj s privatnim ključem zaštićenim kanalom dostavlja u Fina RA mrežu te se osobno uručuje identificiranom potpisniku.

U slučaju da Fina LRA generira privatni ključ za potpisnika unutar SSCD uređaja, tada se SSCD uređaj s privatnim ključem osobno uručuje identificiranom potpisniku.

Ako potpisnik na svojoj lokaciji pod udaljenim nadzorom Fina CA generira privatni ključ na SSCD uređaju, smatra se da ga potpisnik već posjeduje.

6.1.3. Dostava javnog ključa CA-u

Ukoliko javni ključ generira Središnji Fina RA, Fina LRA ili potpisnik, tada se javni ključ u Fina CA dostavlja na način koji sigurno povezuje potvrđeni identitet potpisnika i pripadajući javni ključ koji se dostavlja na certificiranje. Postupci dostave koriste PKCS#10 format zahtjeva koji je potpisan privatnim ključem potpisnika.

Dostava korisničkog javnog ključa u PKCS#10 formatu obavlja se elektroničkim putem korištenjem Fina CMS sustava koji ostvaruje SSL/TLS komunikacijski kanal nakon uspješno provedene autentifikacije potpisnika.

6.1.4. Dostava CA javnog ključa pouzdajućim stranama

Javni ključ za provjeru Fina CA potpisa se pouzdanim kanalom dostavlja potpisnicima, u Fina CA certifikatu. Fina CA certifikat je pouzdajućim stranama dostupan i na pripadnim internetskim stranicama repozitorija iz točke 2.2. ovog CPS_{QC} dokumenta. Izvornost Fina CA certifikata objavljenog na internetskim stranicama osigurava se dostavom njegova sažetka pouzdanim kanalom.

6.1.5. Duljine ključeva

Duljine ključeva certifikata iz opsega ovog CPS_{QC} dokumenta su sljedeće:

- 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 par ključeva duljine 2048 bita;
- par ključeva za osobne i poslovne kvalificirane certifikate je RSA duljine 2048 bita.

6.1.6. Generiranje i provjera kvalitete parametara javnog ključa

Kod generiranja parametara javnog ključa u HSM modulima i SSCD uređajima Fina CA koristi parametre generirane za RSA algoritam po normama FIPS 186-3 (ili novija) ili ANSI X9.31.

Kod generiranja parametara javnog ključa u SSCD uređaju koriste se parametri generirani za RSA algoritam po normi ANS X9.31.

Kvaliteta parametara javnih ključeva koji se generiraju na lokaciji Fina CA osigurana je od strane proizvođača opreme u kojoj se ključevi generiraju korištenjem kvalitetnih generatora slučajnih brojeva, proizvedenih u skladu s normama FIPS 186-3 (ili novija) ili ANS X9.31.

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

Fina CA-ovi koriste privatne potpisne ključeve za potpisivanje izdanih certifikata te odgovarajuće CRL liste (X.509 v3 KeyUsage Extension: *keyCertSign, cRLSign*).

Ovlaštene osobe u Fina RA mreži koriste privatne ključeve za napredni elektronički potpis (X.509 v3 KeyUsage Extension: *nonRepudiation*).

Ključevi kvalificiranih certifikata potpisnika namijenjeni su za napredni elektronički potpis (X.509 v3 KeyUsage Extension: *nonRepudiation*).

6.2. Zaštita privatnog ključa i tehnike upravljanja kriptografskim modulom

6.2.1. Norme i upravljačke funkcije kriptografskog modula

Fina CA privatni ključevi generiraju se u HSM modulu koji zadovoljava zahtjeve prema FIPS 140-2 [27], razina 3 ili viša.

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 [26] ili FIPS 140-2 [27], razina 2 ili više;
- CEN/ISSS SSCD-PP definiran dokumentom CWA 14169 [16], ili
- zahtjeve primijenjenih jednako vrijednih sigurnosnih kriterija.

Ovlaštene osobe Fina RA mreže posjeduju certifikate srednje razine sigurnosti te se njihovi privatni ključevi generiraju u SSCD uređaju.

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-ovi 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.

6.2.3. Sigurno skladištenje privatnog ključa (key escrow)

Sigurno skladištenje privatnih Fina CA ključeva izvan Fine se ne primjenjuje.

Fina CA ne skladišti potpisnikov privatni ključ nakon što je on isporučen potpisniku.

6.2.4. Sigurnosno kopiranje privatnog ključa

Sigurnosno kopiranje Fina CA privatnog ključa provodi se pod najmanje dualnom kontrolom ovlaštenog osoblja Fina CA s povjerljivim ulogama. Kada se nalazi izvan kriptografskog modula privatni Fina CA ključ je isključivo u enkriptiranom obliku. Sigurnosne kopije privatnog Fina CA ključa čuvaju se na odvojenim i adekvatno štićenim lokacijama.

Fina CA nikada ne provodi sigurnosno kopiranje privatnih ključeva potpisnika.

6.2.5. Arhiviranje privatnog ključa

Privatni ključevi se ne arhiviraju.

6.2.6. Prijenos privatnog ključa u ili iz kriptografskog modula

Prijenos privatnog ključa subordiniranog Fina CA u ili iz kriptografskog modula opisan je u točki 6.2.6. dokumenta Pravilnik o postupcima certificiranja Fina Root CA, CPS_{ROOT} [34].

Prijenos privatnog ključa Fina OCSP 2015 servisa te privatnog ključa Fina QTSA 2015 provodi se na jednak način kao i prijenos privatnih ključeva subordiniranih Fina CA-ova.

Prijenos privatnog ključa potpisnika u ili iz SSCD uređaja nije dozvoljen.

6.2.7. Spremanje privatnog ključa u kriptografskom modulu

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

6.2.8. Metoda aktivacije privatnog ključa

Pokretanje CA servisa za izradu certifikata te aktivacija privatnog Fina CA ključa u hardverskom kriptografskom modulu provodi se pod dualnom kontrolom ovlaštenih osoba Fina CA. Jednom aktiviran, privatni ključ ostaje aktiviran bez vremenskog ograničenja.

Privatni potpisni ključ Fina RA/LRA službenika aktivira samo pripadajući Fina RA/LRA službenik korištenjem PIN-a za pripadni SSCD uređaj. Za vrijeme dok je privatni ključ aktivan Fina RA/LRA službenik nadzire njegovu uporabu i SSCD uređaj.

Aktivaciju privatnog ključa kvalificiranih certifikata izvodi samo pripadajući potpisnik korištenjem odgovarajućeg PIN-a za pripadni SSCD uređaj. Za vrijeme dok je privatni ključ aktivan potpisnik nadzire njegovu uporabu i SSCD uređaj.

Samo potpisnik zna PIN za aktivaciju privatnog ključa na SSCD uređaju. Potpisnik izvodi aktivaciju privatnog ključa na način u kojem PIN i dalje ostaje tajan. Vrijeme u kojem privatni ključ ostaje aktiviran nije određeno.

6.2.9. Metoda deaktivacije privatnog ključa

Metode deaktivacije privatnog ključa primjenjuju se za deaktivaciju privatnog ključa nakon prestanka potrebe za njegovim korištenjem, odmah nakon njegove upotrebe ili nakon završetka svih aktivnosti u kojem je postojala ponavljajuća potreba za korištenje privatnog ključa.

Deaktivacija privatnog ključa subordiniranog Fina CA, kao i deaktivacija privatnih ključeva za potpis odgovora Fina OCSP 2015 servisa opisana je u točki 6.2.9. CPS_{ROOT} dokumenta [34].

SSCD uređaji potpisnika koji su aktivirani ne smiju biti ostavljeni bez nadzora. Nakon prestanka potrebe za korištenjem privatnog potpisnog ključa potpisnik mora deaktivirati privatni ključ.

Deaktivaciju privatnog ključa obavlja potpisnik fizičkim vađenjem ili odspajanjem SSCD uređaja, odnosno pouzdanom logičkom deaktivacijom propisanom od strane proizvođača SSCD uređaja.

Pouzdanu logičku deaktivaciju SSCD uređaja može obaviti i korisnička aplikacija ili operacijski sustav koji koristi pouzdane metode logičke deaktivacije propisane od proizvođača SSCD uređaja.

6.2.10. Metoda uništavanja privatnog ključa

Privatni ključevi Fina CA-ova uništavaju se nakon prestanka potrebe za njihovim korištenjem, odnosno na kraju njihovog životnog ciklusa.

Postupak uništavanja privatnih ključeva Fina CA provodi se na način opisan u točki 6.2.10. CPS_{ROOT} dokumenta [34].

Nema odredbi za obavezno uništavanje privatnih ključeva potpisnika.

6.2.11. Ocjena kriptografskog modula

Ocjena kriptografskih modula provodi se prema normama za kriptografske module navedenim u točki 6.2.1. ovog CPS_{QC} dokumenta.

6.3. Ostali vidovi upravljanja parom ključeva

6.3.1. Arhiviranje javnog ključa

Javni ključevi Fina CA i korisnički javni ključevi svih subjekata kojima su izdani kvalificirani certifikati arhiviraju se u cilju omogućavanje verifikacije naprednih elektroničkih potpisa, posebice u svrhu pružanja dokaza o kvalificiranim certifikatima u sudskim, upravnim i drugim postupcima.

Javni ključevi Fina CA se arhiviraju na način da se arhiviraju Fina CA certifikati koji su izdani za te javne ključeve.

Fina CA-ovi arhiviraju javne ključeve svih subjekata arhivirajući certifikate koji su izdani za te javne ključeve.

Arhiviranje javnih ključeva provodi se na rok propisan u točki 5.5.2. ovog CPS_{QC} dokumenta.

Sigurnosna kopija arhiviranih ključeva izrađuje se i čuva sukladno točki 5.5.4. ovog CPS_{QC} dokumenta.

6.3.2. Periodi valjanosti certifikata i korištenja para ključeva

Predviđeni rok valjanosti certifikata i korištenja para ključeva prikazan je u tablici 6.1.

Certifikat	Rok
Fina Root CA certifikat	20 godina
Certifikat za Fina RDC 2015 i Fina RDC-TDU 2015 CA	10 godina
Certifikat za potpis odgovora OCSP servisa	12 mjeseci
Kvalificirani certifikat srednje razine sigurnosti	2 godine

Tablica 6.1. - Rokovi uporabe certifikata

Privatni ključevi vrijede od početka do isteka valjanosti odgovarajućeg certifikata. Certifikat i pripadajući privatni ključ ne smiju se upotrebljavati nakon isteka roka valjanosti certifikata.

Period valjanosti svakog izdanog certifikata definiran je vrijednostima navedenim u osnovnom polju *Validity*. U točki 7.1. ovog CPS_{QC} dokumenta dani su podaci za vrijednost polja *Validity* za sve tipove certifikata iz opsega ovog dokumenta.

Period valjanosti certifikata i pripadajućeg privatnog ključa može se u tijeku perioda valjanosti trajno ili privremeno skratiti opozivom, odnosno suspenzijom certifikata.

6.4. Aktivacijski podaci

Za zaštitu pristupa privatnim ključevima u Fina PKI upotrebljavaju se PIN, zaporka ili drugi tip aktivacijskih podataka.

6.4.1. Generiranje i instalacija aktivacijskih podataka

Generiranje i instalacija aktivacijskih podataka za privatni ključ Fina Root CA te za privatne ključeve subordiniranih Fina CA-ova, kao i generiranje i instalacija aktivacijskih podataka za privatne ključeve Fina OCSP 2015 opisano je u točki 6.4.1. dokumenta CPS_{ROOT} [34].

Aktivacijske podatke za privatne ključeve LRA službenika i za korisničke privatne ključeve smještene u SSCD uređajima generiraju ovlaštene osobe Fina CA na siguran način u Fina PKI štićenom prostoru.

6.4.2. Zaštita aktivacijskih podataka

Zaštita aktivacijskih podataka povezanih s privatnim ključem Fina Root CA, subordiniranih Fina CA-ova te aktivacijskih podataka povezanih s privatnim ključem za Fina OCSP 2015 servis opisana je u točki 6.4.2. dokumenta CPS_{ROOT} [34].

Aktivacijski podaci koje generira Fina CA za korisničke privatne ključeve dostavljaju se potpisniku odvojenim distribucijskim kanalom od kanala isporuke SSCD uređaja. Preporuka je da potpisnik promijeni aktivacijske podatke pri prvoj aktivaciji ključa.

Preporuka je da se aktivacijske podatke ne zapisuje. Ukoliko se aktivacijski podaci ipak zapisuju, oni moraju biti pohranjeni na zaštićeni način tako da su dostupni samo pripadajućem potpisniku te se ne smiju pohranjivati zajedno s pripadajućim SSCD uređajem.

6.4.3. Ostale odredbe o aktivacijskim podacima

Ukoliko aktivacijske podatke za kvalificirane certifikate generira Fina CA, aktivacijski podaci se iz Fina CA ili RA mreže e-mailom ili preporučenom poštanskom pošiljkom šalju potpisniku. Ukoliko se aktivacijski podaci za privatni ključ koji se nalazi u SSCD uređaju šalju e-mailom, aktivacijski podaci su enkriptirani.

Ukoliko aktivacijski podaci trebaju biti preneseni, tada za vrijeme prijenosa aktivacijski podaci moraju biti zaštićeni od krađe, gubitka, izmjena, kompromitiranja i neovlaštene uporabe. Lokacija na koju se aktivacijski podaci prenose mora imati jednaku ili višu razinu sigurnosti od lokacije s koje se aktivacijski podaci prenose.

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 normizacijskim dokumentom HRN ETSI/EN 319 411-2 [11] , te sa zahtjevima iz dokumenta CA/Browser Forum Baseline Requirements [31].

6.5.2. Ocjena računalne sigurnosti

Sigurnosne mjere koje se odnose na računalnu sigurnost periodički se ispituju sukladno normama iz točke 6.5.1. ovog CPS_{QC} dokumenta.

6.6. Tehničko upravljanje životnim ciklusom

Fina PKI provođenjem redovitih periodičkih kontrola sustava i sigurnosnih kontrola upravljanja sustavom certificiranja osigurava usklađenost tehničkog upravljanja životnim ciklusom Fina CA sustava sukladno zahtjevima navedenim u normizacijskom dokumentu HRN ETSI/EN 319 411-2 [11].

6.6.1. Upravljanje razvojem sustava

Plan za upravljanje konfiguracijom Fina PKI sustava sadrži jasan prikaz trenutnog stanja, popis dokumentacije nastale u sklopu izrade informacijskog sustava, mjere za osiguranje

kvalitete, procjenu ranjivosti, softverski dizajn,sistemski test i definicije kontrolnih mehanizama.

6.6.2. Provjera upravljanja sigurnošću

Postupci i oblici zaštite Fina CA informacijskog sustava usklađeni su s normizacijskim dokumentom HRN ISO/IEC 27001 [24].

6.6.3. Provjera sigurnosti životnog ciklusa

Fina CA osoblje provodi provjeru svih dijelova sustava certificiranja u odnosu na sigurnost, pouzdanost i kvalitetu djelovanja, u skladu s propisanim procedurama i postupcima, osiguravajući na taj način da Fina CA sustavi rade ispravno i u skladu s implementiranom konfiguracijom sustava.

Provjera Fina CA sustava provodi se prije početka obavljanja usluga, nakon značajnih promjena u sustavu certificiranja za vrijeme obavljanja usluga, te redovito najmanje jedanput godišnje.

Najveći vremenski razmak između dva postupka provjere nije duži od jedne godine.

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.

6.8. Usluga vremenskog žiga

Ne primjenjuje se.

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 opsegu ovog CPSQC dokumenta.

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 [12].

Profili CRL koje izdaju subordinirani Fina CA-ovi usklađeni su s preporukom IETF RFC 5280 [20].

Profili OCSP odgovora Fina OCSP i Fina RDC servisa usklađen je s preporukom IETF RFC 6960 [22].

7.1. Profil certifikata

Subordinirani Fina CA-ovi izdaju certifikate prema profilima koji su određeni Općim pravilima [33]. 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).

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 kvalificirani certifikati

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

1. Fina 2015 RDC osobni kvalificirani certifikati;
2. Fina 2015 RDC poslovni kvalificirani 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 kvalificirani certifikati

Osobni kvalificirani certifikati namijenjeni su fizičkim osobama – građanima za osobnu uporabu, a izdaje ih Fina RDC 2015 CA.

- **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-CP5-0-hr.pdf http://rdc.fina.hr/RDC2015/FinaRDC2015-CP5-0-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-PDS5-0-en.pdf https://rdc.fina.hr/RDC2015/FinaRDC2015-PDS5-0-hr.pdf

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

2. Fina RDC 2015 poslovni kvalificirani certifikati

Poslovni kvalificirani certifikati namijenjeni su za poslovnu uporabu te se ovi certifikati izdaju pripadajućim osobama unutar poslovnog subjekta, a izdaje ih Fina RDC 2015 CA.

- **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 7.4.

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-CP5-0-hr.pdf http://rdc.fina.hr/RDC2015/FinaRDC2015-CP5-0-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-PDS5-0-en.pdf https://rdc.fina.hr/RDC2015/FinaRDC2015-PDS5-0-hr.pdf

Tablica 7.4. Ekstenzije profila specifične za Poslovni potpisni Q2 certifikat (QCP+)

7.1.2.2. Fina RDC-TDU 2015 kvalificirani certifikati

Fina RDC-TDU 2015 CA izdaje Fina RDC-TDU 2015 kvalificirane certifikate za krajnje korisnike.

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.

- **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 7.5.

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-CP5-0-hr.pdf http://rdc.fina.hr/RDC-TDU2015/FinaRDC-TDU2015-CP5-0-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-PDS5-0-hr.pdf https://rdc.fina.hr/RDC-TDU2015/FinaRDC-TDU2015-PDS5-0-en.pdf
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-calssuers	http://rdc.fina.hr/RDC-TDU2015/FinaRDC-TDUCA2015.cer

Tablica 7.5. Ekstenzije profila specifične za TDU potpisni Q2 certifikat (QCP+)

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 7.6.

Algoritam	OID
sha256WithRSAEncryption	1.2.840.113549.1.1.11
rsaEncryption	1.2.840.113549.1.1.1

Tablica 7.6. Algoritmi s pripadajućim OID identifikatorima

7.1.4. Oblici naziva

Oblici naziva za subordinirane Fina CA-ove opisani su u točki 1.3.2. ovog CPS_{QC} dokumenta.

Oblici naziva za certifikate koje izdaju subordinirani Fina CA-ovi opisani su u točkama 3.1.1. i 3.1.4. ovog CPS_{QC} dokumenta.

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. ovog CPS_{QC} dokumenta.

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 Općih pravila [33] 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 [20].

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 7.7.

Ekstenzije	Kritično	Vrijednost
crlExtensions		
cRLNumber	NO	Jednolično rastući serijski broj CRL duljine 24 bita.
AuthorityKeyIdentifier	NO	SHA-1 hash vrijednost duljine 160 bita
crlEntryExtensions		
reasonCode	NO	Kod razloga opoziva certifikata

Tablica 7.7. Ekstenzije CRL liste i elemenata unosa CRL listi koje izdaju Fina CA-ovi

7.3. OCSP profil

Profil odgovora Fina OCSP servisa usklađen je s preporukom IETF RFC 6960 [22].

7.3.1. Broj(evi) verzije

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 pravila i postupaka vezanih uz rad Fina PKI i provedbu unutarnjeg procesa odobravanja rada Fina CA sukladno pravilima definiranim u Općim pravilima [33] i postupcima iz CPS_{QC} dokumenta provode interni ocjenitelji iz Ureda za upravljanja politikom e-Poslovanja.

Provjera usklađenosti izdavanja kvalificiranih certifikata provodi se sukladno normizacijskom dokumentu HRN ETSI/EN 319 411-2 [11].

Zapisi o obavljenim provjerama usklađenosti na zahtjev mogu biti dostupni vanjskim ocjeniteljima pri njihovoj provjeri usklađenosti Fina PKI sustava. Odobrenje za davanje zapisa o obavljenim provjerama usklađenosti vanjskim ocjeniteljima daje Fina PMA.

Naredne točke ovog poglavlja reguliraju provođenje unutarnje provjere usklađenosti.

8.1. Učestalost ili okolnosti provjere usklađenosti

Učestalost provjera usklađenosti rada Fina PKI provodi se najmanje jedanput godišnje. Provjera usklađenosti se provodi i prije početka rada novog Fina CA, te nakon znatnih promjena u radu Fina PKI sustava, odnosno nakon nepogode ili sumnje u kompromitiranje sustava.

8.2. Identitet/kvalifikacije ocjenitelja

Interni ocjenitelji moraju:

- raspolagati znanjima i razumijevanjem odredbi norme HRN ETSI/EN 319 411-2 [11] i normizacijskog dokumenata CWA 14167-1 [15];
- raspolagati aktualnim znanjima i vještinama iz PKI područja i informacijske sigurnosti;
- poznavati zakonsku regulativu iz područja davanja usluga certificiranja.

8.3. Odnos ocjenitelja s tijelom koje se ocjenjuje

Interni ocjenitelji usklađenosti su organizacijski i hijerarhijski odvojeni od Fina CA kako bi mogli obavljati neovisnu/neutralnu provjeru usklađenosti.

8.4. Predmeti provjera

Interni ocjenitelji provjeravaju postupa li Fina CA prema Općim pravilima [33] i CPS_{QC} dokumentu.

Provjera usklađenosti sustava za izdavanje certifikata provodi se u odnosu na sigurnost, pouzdanost i kvalitetu djelovanja

Provjera dokumentacije sustava obuhvaća provjeru usklađenosti dokumentacije sa zahtjevima zakonske regulative o elektroničkom potpisu i usklađenosti s normom HRN ETSI/EN 319 411-2 [11].

Provjerom implementacije sustava provodi se provjera usklađenosti sustava sa zakonskom regulativom o elektroničkom potpisu, Općim pravilima [33], CP_{QC} dokumentom i normom HRN ETSI/EN 319 411-2 [11].

8.5. Mjere u slučaju neusklađenosti

U slučaju utvrđivanja neusklađenosti u radu Fina CA, interni ocjenitelj izrađuje izvještaj i dostavlja ga Fina PMA na osnovu kojeg Fina PMA izrađuje plan akcija, mjera i postupaka koje će Fina CA poduzeti u danom roku kako bi se otklonile neusklađenosti navedene u izvješću ocjenitelja.

Ukoliko je u radu Fina CA utvrđena neusklađenost koja značajno utječe na mogućnost zadovoljenja uvjeta za kvalificirane certifikate sukladno Direktivi [10] i CPS_{QC} dokumentu, Fina PMA će dati zahtjev za prekid izdavanja kvalificiranih certifikata s CP OID-ovima iz opsega CPS_{QC} dokumenta, ili će dati zahtjev da Fina CA poduzme korake kako bi u razumnom roku otklonila neusklađenost. U slučaju prekida izdavanja certifikata, Fina PMA će odobriti nastavak izdavanja certifikata nakon što ocjenitelj utvrdi da je Fina CA postigla propisanu 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/LRA vode interne dnevnike sustava s popisom vremenskih razdoblja u kojima nisu radili u skladu CPS_{QC} dokumentom, s navedenim razlozima tih neusklađenosti.

8.6. Priopćavanje rezultata

Fina PMA kao nadležno tijelo, dužan 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 provedena 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. CPS_{QC} dokumenta objaviti sažetak provjere usklađenosti koji je relevantan korisnicima i ostalim sudionicima Fina PKI sustava.

Svi dokumenti interne provjere usklađenosti na zahtjev su dostupni vanjskim ocjeniteljima koji provode provjeru usklađenosti Fina PKI sustava.

9. OSTALE POSLOVNE I PRAVNE STAVKE

9.1. Naknade za usluge

Fina i RA mreža informiraju korisnike i pouzdajuće strane o cijeni i načinu naplate usluga koje naplaćuje Fina kao davatelj usluga certificiranja. Informiranje korisnika o cijeni i načinu naplate obavljaju RA/LRA službenici u RA mreži, te osobe u Fini zadužene za promociju i prodaju proizvoda i usluga. Informiranje o cijenama i naplati usluga obavlja se i objavom cjenika i drugih mjerodavnih informacija na internetskim stranicama Fina RDC 2015 i Fina RDC-TDU 2015 repozitorija iz točke 2.2. CPS_{QC} dokumenta.

Ukoliko posebnim ugovorom nije drugačije određeno, usluge se naplaćuju prema cjenicima objavljenim na navedenim internetskim stranicama repozitorija.

9.1.1. Naknade za izdavanje ili obnovu certifikata

Fina, sukladno objavljenom cjeniku ili na temelju posebnog ugovora, naplaćuje naknadu za usluge izdavanja i obnove Fina RDC 2015 i Fina RDC-TDU 2015 kvalificiranih certifikata.

9.1.2. Naknade za pristup certifikatu

Fina ne naplaćuje naknadu za pristup certifikatima.

9.1.3. Naknade za opoziv i pristup informacijama o statusu certifikata

Fina, sukladno objavljenom cjeniku ili na temelju posebnog ugovora, naplaćuje naknadu za uslugu opoziva certifikata, te ne naplaćuje naknadu za uslugu suspenzije i reaktivacije certifikata.

Fina ne naplaćuje naknadu za uslugu davanje informacija o statusu certifikata.

9.1.4. Naknade za ostale usluge

Fina ili vanjski ugovoreni RA, sukladno objavljenom cjeniku ili na temelju posebnog ugovora, naplaćuje naknadu za sljedeće usluge i proizvode vezane uz izdavanje kvalificiranih certifikata:

- usluga registriranja poslovnog subjekta i fizičke osobe – građanina;
- promjena podataka u certifikatu;
- čitač *smart* kartice;
- neposredna identifikacija potpisnika i isporuka certifikata na SSCD uređaju na korisničkoj lokaciji;
- najam i održavanje opreme za napredni elektronički potpis i enkripciju.

Za pristup Općim pravilima [33] i drugoj javno objavljenoj dokumentaciji na web dijelu repozitorija iz točke 2.2. CPS_{QC} dokumenta, Fina ne naplaćuje naknadu.

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 iz opsega ovog CPS_{QC} dokumenta, neovisno o broju korisnika usluga i za cijelo vrijeme obavljanja usluga certificiranja.

9.2.1. Pokrivenost osiguranjem

Fina, kao davatelj usluga certificiranja koji izdaje kvalificirane certifikate, ima osiguran rizik od odgovornosti za štete koje nastanu obavljanjem usluga izdavanja kvalificiranih certifikata. Polica osiguranja mora glasiti na ukupan iznos od najmanje 2.000.000,00 kuna.

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, te osiguranje od loma stakla.

Fina može od vanjskog ugovorenog RA-a zahtijevati da se, sukladno uvjetima iz Općih pravila [33] i na odgovarajuće iznose, 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 upravlja certifikatima.

Povjerljivi su i svi privatni ključevi povezani s kvalificiranim certifikatima koje generira Fina CA i Fina LRA. Ukoliko ove ključeve generira Fina CA oni se generiraju na SSCD uređaju, sukladno točki 6.1.1.3. ovog $CPS_{QC,}$ dokumenta, te se SSCD uređaj s ključevima i certifikatima dostavlja potpisniku. Pri tom Fina CA ne izrađuju i ne pohranjuje nikakve kopije korisničkih ključeva (vidi točke 6.2.3. i 6.2.4. ovog CPS_{QC} dokumenta).

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 usluga certificiranja, a koje sudionici ne označe povjerljivim, ili određenom vrstom ili stupnjem tajnosti, ili koji po svojoj prirodi nisu povjerljivi jer se njihovim neovlaštenim otkrivanje ne bi mogla prouzročiti šteta sudioniku, jesu podaci koji se ne smatraju povjerljivim poslovnim podacima.

Poslovni podaci koji se ugrađuju u sadržaj certifikata, a koji se prikazuju u javnim evidencijama i/ili registrima ne smatraju se povjerljivim poslovnim podacima.

Poslovni podaci koji se ugrađuju u sadržaj certifikata, te se ne smatraju povjerljivim poslovnim podacima su:

- skraćeni naziv poslovnog subjekta, odnosno puni naziv ukoliko poslovni subjekt ne posjeduje skraćeni naziv;
- OIB poslovnog subjekta;
- matični broj poslovnog subjekta kojeg dodjeljuje Državni zavod za statistiku;
- naziv podorganizacijske jedinice (za Fina RDC-TDU 2015 certifikate);
- mjesto sjedišta poslovnog subjekta;
- država sjedišta poslovnog subjekta.

Sljedeći poslovni podaci koji se prikazuju u javnim evidencijama i/ili registrima, koji se moraju propisano voditi, ne smatraju se povjerljivim poslovnim podacima:

- popis osoba ovlaštenih za zastupanje i njihov model zastupanja;
- puni naziv poslovnog subjekta;
- glavna djelatnost;
- ulica i kućni broj adrese sjedišta poslovnog subjekta.

9.3.3. Odgovornost za zaštitu povjerljivih poslovnih podataka

Svaki sudionik Fina PKI obvezan je štititi povjerljive poslovne podatke iz točke 9.3.1. CPS_{QC} dokumenta, koje je saznao na bilo koji način, sukladno propisima koji uređuju zaštitu podataka prema vrsti podatka, odnosno vrsti i stupnju tajnosti podataka. U protivnom sam odgovara za nastalu štetu.

9.4. Zaštita osobnih podataka

Fina primjenjuje odredbe Zakona o zaštiti osobnih podataka [9] i drugih propisa, posebno onih 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 te prikupljaju 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, su povjerljivi osobni podaci koje Fina propisano štiti.

Osobni podaci koji se prikupljaju pri registraciji potpisnika i osobe ovlaštene za zastupanje, ili nakon toga, a koji se smatraju povjerljivima, te ih Fina propisano štiti su:

- MBG osobe;
- datum rođenja;
- ulica i kućni broj adrese prebivališta;
- državljanstvo;
- podaci o identifikacijskoj ispravi osobe;
- kontakt broj telefona, mobitela i telefaksa;
- kontakt poštanska adresa.

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, su osobni podaci koji zbog dostupnosti svim sudionicima Fina PKI nisu povjerljivi.

Osobni podaci koji se prikupljaju pri registraciji korisnika ili nakon toga, a koji se zbog dostupnosti svim sudionicima Fina PKI ne smatraju povjerljivima su:

- ime i prezime potpisnika;
- OIB potpisnika;
- pripadnost potpisnika poslovnom subjektu;
- mjesto prebivališta;
- država prebivališta;
- e-mail adresa potpisnika.

9.4.4. Odgovornost za zaštitu osobnih podataka

Fina, kao davatelj usluga certificiranja, i vanjski ugovoreni RA odgovorni su za zaštitu osobnih podataka 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, kao davatelj usluga certificiranja ovlaštena je, osim za potrebe ispunjenja zakonskih, odnosno ugovornih obveza po ugovorima kojima se uređuju usluge certificiranja, koristiti osobne podatke samo temeljem pisane privole potpisnika. Potpisnik svoju privolu za korištenja osobnih podataka daje Fini u zahtjevu za izdavanje certifikata.

9.4.6. Dostupnost podataka mjerodavnim tijelima

Fina, kao davatelj usluga certificiranja, ne daje na dostup podatke iz točaka 9.3.1 i 9.4.2 ovog CPS_{QC} dokumenta, osim ako joj to nalažu zakonski propisi, Opća pravila [33] 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

Opća pravila [33], kao i druga dokumentacija objavljena na internetskim stranicama Fina RDC 2015 i Fina RDC-TDU 2015 repozitorija iz točke 2.2. ovog CPS_{QC} dokumenta je Finino vlasništvo i bez njena izričita ovlaštenja nije dozvoljeno njeno neovlašteno korištenje.

Svaka stvar ili djelo koje je predmet nekog od prava intelektualnog vlasništva, vezano uz davanje usluga certificiranja koje su u opsegu Općih pravila [33], neovisno pripada li Fini ili drugom sudioniku, zaštićeno je sukladno relevantnim propisima.

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

Sudionici Fina PKI dužni su poštovati prava intelektualnog vlasništva.

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 kvalificiranih certifikata primjenjuje Zakon [1], [2] i [3], podzakonske propise [4], [5] i [6] donijete temeljem Zakona [1], [2] i [3], obvezujuće međunarodne norme i preporuke, Opća

pravila [33] i CPS_{QC}. Pri davanju usluga certificiranja iz opsega ovog CPS_{QC} dokumenta Fina primjenjuje i druge akte navedene u ovom CPS_{QC} dokumentu.

Akte koji su namijenjeni za javnu objavu Fina objavljuje na internetskim stranicama odgovarajućeg Fina CA repozitorija iz točke 2.2. CPS_{QC} dokumenta.

Fina CA na navedenim internetskim stranicama repozitorija objavljuje sve obavijesti i informacije o promjenama u radu koje na bilo koji način utječu ili mogu utjecati na sudionike Fina PKI.

Fina CA-ovi izdaju kvalificirane certifikate usklađene s X.509 v3 normom [29], preporukom RFC 3739 [19] te s normizacijskim dokumentom HRN ETSI/EN 319 412-5 [12], a u skladu s odredbama normizacijskog dokumenta HRN ETSI/EN 319 411-2 [11].

Tijekom pružanja usluge izdavanja kvalificiranih certifikata i upravljanja njihovim životnim ciklusom, Fina CA-ovi poštuju sve zahtjeve i odredbe propisane Općim pravilima [33] i CPS_{QC} dokumentom.

Fina CA-ovi obavljaju usluge iz opsega ovog CPS_{QC} dokumenta s pažnjom dobrog stručnjaka.

Prije iniciranja izrade certifikata Fina CA-ovi verificiraju elektronički potpisane podatke o registriranom korisniku koji su dostavljeni od strane RA mreže. Time se utvrđuje identitet RA/LRA kao pošiljatelja i provjerava cjelovitost zaprimljenih podataka o registriranom korisniku.

Fina CA-ovi izdaju certifikat koji je temeljen na aktivnostima pouzdanog utvrđivanja identiteta potpisnika, poslovnog subjekta, identiteta osoba ovlaštenih za zastupanje, kao i utvrđivanje drugih podataka o poslovnom subjektu.

Ukoliko je korisnik pristao na javnu objavu njegova certifikata, Fina CA objavljuje izdani certifikat u javnom imeniku odgovarajućeg repozitorija Fina, a sukladno točki 2.2. CPS_{QC} dokumenta.

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

Fina će suspendirati certifikat i suspendirane certifikate objaviti u listi opozvanih certifikata, te o tom obavijestiti pripadajućeg korisnika:

- ako Fina raspolaže dokazima ili opravdano sumnja da je privatni ključ kompromitiran;
- ako Fina smatra da je prilikom izdavanja certifikata učinjen propust.

Fina CA osigurava objavu ispravne liste opozvanih certifikata.

Fina CA u svom poslovanju primjenjuje organizacijske i tehničke mjere zaštite ključeva i certifikata, te zaštite podataka potpisnika, poslovnog subjekta i osobe ovlaštene za

zastupanje, a koji se smatraju povjerljivima sukladno točki 9.4. CPS_{QC} dokumenta. Ove podatke Fina, kao davatelj usluga certificiranja, koristiti isključivo za potrebe usluga certificiranja iz opsega CPS_{QC} dokumenta i drugih usluga iz područja Fina PKI (npr. vremenski žig).

Fina, kao davatelj usluga certificiranja, osigurava rad RA mreže u skladu s odredbama Zakona [1], [2] i [3], podzakonskih propisa [4], [5] i [6] donesenih temeljem Zakona, Općih pravila [33], CPS_{QC} dokumenta, te drugih akata Fine u svezi davanja usluga certificiranja. Rad vanjskih ugovorenih RA reguliran je kroz ugovor o obavljanju poslova registracije.

Fina CA osigurava metodu kojom potpisnik dokazuje posjedovanje privatnog ključa čiji se pripadajući javni ključ dostavlja na certificiranje.

Fina CA osigurava uvjete da se par ključeva potpisnika generira na siguran način i da je tajnost privatnog ključa osigurana sukladno odredbama norme HRN ETSI/EN 319 411-2 [11] za sve certifikate čiji se parovi ključeva generiraju u Fina CA, odnosno čije parove ključeva korisničkoj lokaciji generira potpisnik uz udaljeni nadzor Fina CA, odnosno ugovorenog RA.

Fina CA osigurava da odgovarajući SSCD na siguran način bude dostavljen u RA mrežu u cilju njegove dostave potpisniku, u skladu s normom HRN ETSI/EN 319 411-2 [11]. Postupak u slučajevima kad Fina CA izdaje certifikate na SSCD uređajima za potpisnike koji su registrirani od strane vanjskog ugovorenog RA, postupak dostave SSCD uređaja reguliran je kroz ugovor o obavljanju poslova registracije kojeg sklapaju Fina i vanjski RA.

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

Fina CA, sukladno najboljoj poslovnoj praksi, osigurava nesmetan rad i maksimalnu moguću raspoloživost usluga certificiranja, osim u slučajevima:

- unaprijed planiranog održavanja sustava;
- neplaniranog zastoja uslijed otklanjanja posljedica kvara sustava;
- neplaniranog zastoja uslijed ispada infrastrukture izvan nadležnosti Fine;
- nedostupnosti zbog više sile ili izuzetnih događaja.

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

Fina, kao davatelj usluga certificiranja, planira održavanje i daljnji razvoj sustava certificiranja sukladno priznatim normama i razvoju tehnologije.

U slučaju prekida poslovanja pojedinog Fina CA, Fina će postupiti sukladno točki 5.8. ovog CPS_{QC} dokumenta.

Fina, kao davatelj usluge certificiranja, odgovara za štetu uzrokovanu korisnicima ili pouzdajućim stranama koje ostvaruju razumno pouzdanje u certifikat u slučaju da Fina CA ne ispuni sljedeće uvjete:

- provjeri točnost i cjelovitost podataka u vrijeme registracije korisnika i da, ovisno o tipu traženog certifikata, izdani certifikat sadrži sve komponente opisane u poglavlju 7.1. CPS_{QC} dokumenta;
- osigura da je potpisnik u vrijeme izdavanja certifikata posjedovao privatni ključ čiji je pripadajući javni ključ ugrađen u certifikat, ili ukoliko se par ključeva generira na lokaciji CA ili Fina LRA, osigura siguran način generiranja i dostave privatnog ključa i pripadajućih aktivacijskih podataka;
- provede opoziv, odnosno suspenziju certifikata, te objavu statusa opozvanosti ili suspenzije certifikata u pripadajućoj listi opozvanih certifikata po zahtjevu korisnika, osim ako Fina CA dokaže kako je djelovala s dužnom pažnjom.

Fina, kao davatelj usluga certificiranja, odgovara za štetu uzrokovanu nepoštivanjem mjerodavnih odredbi iz ovog CPS_{QC} dokumenta u radu RA mreže. Ovu odgovornost Fina prema vanjskim ugovorenim RA-ovima uređuje ugovorom o obavljanju poslova registracije.

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 CPS_{QC} dokumentom;
- čuvanje i zaštita prikupljenih podataka na način i u skladu sa zakonima na koje se poziva CPS_{QC} dokument;
- prosljeđivanje cjelovitih, točnih i provjerenih podataka o korisnicima na daljnju obradu u Fina CA;
- arhiviranje zahtjeva i prikupljene dokumentacije na način propisan CPS_{QC} dokumentom;
- osiguravanje od gubitka ili povrede povjerljivosti, cjelovitosti i dostupnosti arhiviranih podataka korisnika, na način propisan CPS_{QC} dokumentom.
- osiguranje SSCD uređaja i njegova zaštićena dostava potpisniku u skladu s CPS_{QC} dokumentom.

Vanjski ugovoreni RA uz ove obveze moraju poštovati i obveze proizašle iz ugovora o obavljanju poslova registracije sklopljenog s Finom.

9.6.3. Obveze i odgovornosti korisnika

Korisnik je dužan:

- u procesu registracije predstaviti se na način propisan u poglavlju 3. i u točki 4.1.2.2 ovog CPS_{QC} dokumenta;
- pažljivo koristiti i čuvati sredstvo za izradu elektroničkog potpisa, privatne ključeve i aktivacijske podatke, te ih koristiti u skladu s odredbama Zakona [1], [2] i [3], odgovarajućim propisima i ovim CPS_{QC} dokumentom;

- poduzeti odgovarajuće mjere zaštite sredstva za izradu elektroničkog potpisa, privatnog ključa i aktivacijskih podataka od neovlaštenog pristupa i uporabe u skladu s poglavljem 6. ovog CPS_{QC} dokumenta;
- 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 . ovog CPS_{QC} dokumenta;
- u registracijski ured dostaviti 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 ovog CPS_{QC} dokumenta;
- djelovati u skladu sa svim ostalim odredbama iz ovog CPS_{QC} dokumenta 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.

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 navedenim obvezama i obavezama iz ugovora o obavljanju usluga certificiranja biti će opozvan certifikat te će izgubiti sva prava proizašla iz ugovora.

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 Općim pravilima [33] i ovim CPS_{QC} dokumentom, pod okolnostima u kojima je pouzdanje razumno i u dobroj namjeri, te pod okolnostima koje su bile 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 ovom CPS_{QC} dokumentu;
- provjerila da su svi podaci o identitetu potpisnika u certifikatu ispravno prikazani aplikacijom u koju se može pouzdati;

- u slučaju verificiranja naprednog elektroničkog potpisa, 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 su navedeni u točki 4.9.6. ovog CP_{QC} dokumenta.

Pouzdajuća strana koja se, ne poštujući propise i Opća pravila [33], te protivno gore utvrđenim obvezama i odgovornostima iz ove točke CPS_{QC} dokumenta, pouzdala u nevažeći (istekli, opozvani 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. ovog CPS_{QC} dokumenta, 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. ovog CPS_{QC} dokumenta.

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, za slučaj nezgode, 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:

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

RA mreža nije odgovorna za štete uključujući indirektne, 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 s postupcima iz ovog CPS_{QC} dokumenta i zahtjevima iz Općih pravila [33].

9.8. Ograničenja odgovornosti

Finina ukupna financijska odgovornost za kvalificirane certifikate izdane prema Općim pravilima i ovom CPS_{QC} dokumentu i za transakcije obavljene na temelju pouzdavanja u tako izdane certifikate iznosi najviše 2.000.000 kuna.

Ako nije posebnim ugovorom ili na drugi način određeno, Finina maksimalna financijska odgovornost prema korisniku i pouzdajućoj strani koja se razumno pouzdaje u kvalificirani certifikat ograničava se, sukladno preporučenim financijskim limitima određenim u točki 1.4. ovog CPS_{QC} dokumenta na način prikazan u Tablici 9.1.

Kategorija certifikata	Maksimalna Finina financijska odgovornost		
	Po kategoriji	Po transakciji	Ukupno
Kvalificirani certifikati srednje razine sigurnosti	do 2.000.000 kn	do 80.000 kn	2.000.000 kn

Tablica 9.1. Maksimalna Finina financijska odgovornost za kvalificirane certifikate

9.9. Naknada štete

Svaki sudionik odgovora oštećenom za štetu koju je počinio zbog nepoštovanja odredbi Općih pravila [33], ovog CPS_{QC} dokumenta 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. ovog CPS_{QC} dokumenta, ili ga koristi protivno svrhama određenim Općim pravilima [33] i ovom CPS_{QC} dokumentu.

Fina je odgovorna osobi koja se pouzdaje u certifikat samo ako je ta odgovornost jasno uspostavljena ugovorom, Općim pravilima [33], ovim CPS_{QC} dokumentom ili hrvatskom zakonskom regulativom.

9.10. Trajanje i prestanak važenja

9.10.1. Trajanje

Ovaj CPS_{QC} dokument važi do stupanja na snagu novog CPS_{QC} dokumenta ili do objave prestanka njegova važenja. Nova verzija CPS_{QC} dokumenta ili prestanak važenja biti će objavljena interno u Fina CA te u Fina središnjem RA. Na internetskim stranicama Fina RDC 2015 i Fina RDC-TDU 2015 repozitorija iz točke 2.2. ovog CPS_{QC} dokumenta može se objaviti prilagođena verzija novog CPS_{QC} dokumenta koja ne sadrži tajne podatke. Novi CPS_{QC} dokument će imati naznačen datum stupanja na snagu. Novom CPS_{QC} dokumentu biti će dodijeljena nova verzija, te će u njemu biti naznačene obavljene izmjene.

O potrebi izmjena i/ili dopunama CPS_{QC} dokumenta, o objavi nove verzije dokumenta te o broju njegove verzije odlučuje Fina PMA.

9.10.2. Prestanak važenja

Stupanjem na snagu nove verzije CPS_{QC} dokumenta za sve certifikate izdane prema ovom dokumentu ostaju važiti one odredbe iz ovog dokumenta koje se ne mogu smisleno zamijeniti odredbama nove verzije CPS_{QC} dokumenta.

Prestanak važenja ovog CPS_{QC} dokumenta nije vezan i ne utječe na važenje certifikata izdanih primjenom ovog dokumenta.

Fina može za pojedine odredbe važećeg CPS_{QC} dokumenta izraditi izmjene i dopune, kao što je to navedeno u točki 9.12. Općih pravila [33] i ovog CPS_{QC} dokumenta.

9.10.3. Posljedice prestanka važenja i nastavak djelovanja

Stupanjem na snagu novog CPS_{QC} dokumenta, na sve se certifikate izdane od tog dana primjenjuju odredbe iz novog dokumenta.

Novi CPS_{QC} dokumenta ne utječe na važenje certifikata koji su izdani primjenom prethodnih CPS_{QC} dokumenata. Certifikati izdani primjenom prethodnih CPS_{QC} dokumenata važe do njihova isteka, pri čemu se mogu obnoviti samo primjenom odredbi iz novog CPS_{QC} dokumenta.

9.11. Pojedinačne obavijesti i komunikacija sa sudionicima

Pojedinačne obavijesti i druga službena komunikacija provodi se 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

Tablica 9.2. Kontaktni podaci za dostavu dopisa prema Fini

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

CPS_{QC} dokument revidira se po potrebi i nakon svake izmjene Općih pravila [33]. Za sve izmjene i dopune odgovoran je Fina PMA.

Fina PMA može bez obavijesti i promjene verzije dokumenta unositi tipografske ispravke, promjene kontakt podataka, te druge manje ispravke koji ne utječu bitno na sudionike.

Sve izmjene CPS_{QC} dokumenta koje mogu bitno utjecati na sudionike zahtijevaju njihovo obavješćivanje. Takve izmjene uvjetuju i izmjenu OID-a CPS_{QC} dokumenta.

Svi sudionici mogu na kontakt adresu Fina PMA iz točke 1.4 ovog CPS_{QC} dokumenta poslati dopis s prijedlogom za ispravke pogrešaka, za prijedlog nadopuna ili izmjena ovog dokumenta. U dopis treba navesti kontakt podatke osobe koja je poslala promjenu. Fina PMA može prihvatiti, prilagoditi ili odbiti predložene promjene nakon razmatranja istih.

9.12.2. Mehanizmi obavještavanja i vremenski periodi

Dokument CPS_{QC} je interni dokument Fine i ne objavljuje se javno. Javno se može objaviti verzija CPS_{QC} dokunmenta koja ne sadrži tajne podatke. Takav dokument objavljuje na internetskim stranicama repozitorija Fina CA iz točke 2.2. ovog CPS_{QC} dokumenta.

9.12.3. Okolnosti pod kojima se mora mijenjati OID

Manje izmjene sadržaja u CPS_{QC} dokumentu koje ne utječu bitno na sudionike ne uvjetuju izmjene OID-a dokumenta.

Veće izmjene u CPS_{QC} dokumenta koje mogu utjecati na sudionike zahtijevaju i izmjenu OID-a CPS_{QC} dokumenta. 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 usluga certificiranja sukladno ovom CPS_{QC} dokumentu, 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. ovog CPS_{QC} dokumenta.

U slučaju spora ili neslaganja između Fine, kao davatelja usluga certificiranja sukladno ovom CPS_{QC} dokumentu 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 usluga certificiranja, sukladno ovom CPS_{QC} dokumentu i vanjskog ugovorenog RA, postupak rješavanja spora reguliran je međusobnim ugovorom.

9.14. Važeći propisi

Za tumačenje odredbi ovog CPS_{QC} dokumenta mjerodavne su odredbe Zakona o elektroničkom potpisu [1], [2] i [3], podzakonskih akata [4], [5], [6] i [7] donijetih temeljem tog zakona, odredbe Općih pravila [33] te propisa, normi i preporuka na koje iste upućuju.

9.15. Usklađenost s važećim propisima

Ovaj CPS_{QC} dokument i davanje usluga certificiranja koje su obuhvaćene ovim CPS_{QC} dokumentom usklađeni su s propisima iz točke 9.14. ovog CPS_{QC} dokumenta.

9.16. Razne odredbe

Fina, u svojstvu davatelja usluga certificiranja, može sa sudionicima Fina PKI sklopiti dodatni ugovor, ukoliko to nije protivno zakonskim propisima.

Fina osigurava da sklopljeni ugovori sadrže odgovarajuće odredbe usklađene s odredbama ovog CPS_{QC} dokumenta, Općih pravila [33] te da ti ugovori omogućuju ugovornim stranama zaštitu interesa sukladno Općim pravilima [33].