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

Verzija 4.0

Datum stupanja na snagu: 7.11.2013.

OID Dokumenta: 1.3.124.1104.5.0.0.3.4.0

Informacije o dokumentu

Ime dokumenta:	FINA PKI - Pravilnik o postupcima certificiranja za nekvalificirane certifikate (dokument za javnu objavu)
OID dokumenta:	1.3.124.1104.5.0.0.3.4.0
Tip dokumenta:	Pravilnik o postupcima certificiranja za nekvalificirane certifikate (CPS_{NQC})
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 [4] i [5] i s preporukom IETF RFC 3647 [18]

SADRŽAJ

AUTORSKA PRAVA

REFERENCE

Temeljni zakon

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

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

Podzakonski akti

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

[4] 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)

[5] Pravilnik o izmjenama o 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)

[6] 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)

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

Ostali zakoni

[8] Zakon o zaštiti osobnih podataka (NN106/2012)

Direktive Europskog parlamenta

[9] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

Normizacijski dokumenti

[10] 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)

[11] HRN ETSI/EN 319 411-3 V1.1.1:2013 Elektronički potpisi i infrastrukture (ESI) – Zahtjevi za opća pravila i sigurnost za vjerodostojne davatelje usluga koji izdaju certifikate – 3. dio: Opća pravila za certifikacijska tijela koja izdaju certifikate s javnim ključem (EN 319 411-3 V1.1.1:2013)

[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] HRS ETSI/TS 102 023 V 1.2.2:2009 Elektronički potpisi i infrastrukture (ESI) – Zahtjevi za osobe ovlaštene za otiskivanje vremena (ETSI TS 102 023 V1.2.2:2008)

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

[15] CEN Workshop Agreement 14169:2004 - Secure signature-creation devices “EAL 4+”

[16] IETF RFC 3161 (2001) Internet X.509: Public Key Infrastructure: Time Stamp Protocol (TSP)

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

[20] IETF RFC 5322 - Internet Message Format

[21] 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)

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

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

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

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

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

FININI dokumenti

[27] FINA PKI - Opća pravila davanja usluga certificiranja, ver. 4.0

[28] FINA PKI - Opća pravila davanja usluga izdavanja vremenskog žiga, ver. 1.2

1. UVOD

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

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] – [5] i europskom Direktivom o elektroničkim potpisima [9] te samim time i s mjerodavnim međunarodnim normama iz djelokruga davanja usluga certificiranja. FINA neprekidno prati potrebe korisnika, razvoj tehnologije i promjene u mjerodavnim normama iz područja davanja usluga certificiranja te sukladno tome unapređuje i usklađuje svoj PKI sustav, pri tom nastojeći svoje proizvode i usluge što više prilagoditi zahtjevima za međugraničnu interoperabilnost.

1.1. Pregled

1.1.1. Opseg i namjena

Ovaj **FINA PKI - Pravilnik o postupcima certificiranja za nekvalificirane certifikate (dokument za javnu objavu),** (u daljnjem tekstu CPS_{NQC}), odgovara dokumentu „Interni pravilnik o postupcima certificiranja“ definiranom u Pravilniku o evidenciji davatelja usluga certificiranja [3] i opisuje postupke i procedure koje primjenjuje FINA PKI na izdavanje i upravljanje životnim ciklusom produkcijskih digitalnih certifikata koji se ne smatraju kvalificiranim certifikatima u smislu Zakona o elektroničkom potpisu [1] i [2], (u daljnjem tekstu: nekvalificirani certifikati), a sukladno zahtjevima iz FINA PKI - Općih pravila pružanja usluga certificiranja (u daljnjem tekstu Opća pravila) [27] u dijelu koji se odnose na izdavanje **nekvalificiranih certifikata**.

Ovaj CPS_{NQC} dokument namijenjen javnom objavljivanju predstavlja **izvadak FININOG internog Pravilnika o postupcima certificiranja za nekvalificirane certifikate** 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.

FINA PKI, sukladno Općim pravilima [27], izdaje sljedeće vrste nekvalificiranih certifikata: normalizirane certifikate i *lightweight* certifikate.

Normalizirani certifikati su certifikati u smislu Zakona o elektroničkom potpisu [1] i [2] te se koriste za podršku elektroničkom potpisu. Normalizirani certifikati s oznakom NCP su usklađeni s općim pravilima za NCP (*Normalized Certificate Policy*) norme HRN ETSI/EN 319 411-3 [11], a normalizirani certifikati s oznakom NCP+ su usklađeni s općim pravilima za NCP+ (*Extended Normalized Certificate Policy*) norme HRN ETSI/EN 319 411-3 [11]. Pored

podrške elektroničkom potpisu, normalizirani certifikati se mogu koristiti i za druge potrebe kao što su jaka autentifikacija i enkripcija.

***Lightweight* certifikati** su certifikati u smislu Zakona o elektroničkom potpisu [1] i [2] te se koriste za podršku elektroničkom potpisu. *Lightweight* certifikati su usklađeni s općim pravilima za LCP (*Lightweight Certificate Policy*) norme HRN ETSI/EN 319 411-3 [11]. Pored podrške elektroničkom potpisu, *lightweight* certifikati se mogu koristiti i za druge potrebe kao što su jaka autentifikacija i enkripcija. Navedeni *lightweight* certifikati imaju oznaku LCP.

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

Nekvalificirane certifikate u FINA PKI izdaje i njihovim životnim ciklusom upravlja FINA Registar digitalnih certifikata (FINA RDC) preko svoja dva produkcijska certifikacijska tijela (CA): FINA RDC CA i FINA RDC-TDU CA.

CPS_{NQC} je usklađen s dokumentom Opća pravila [27] u dijelu koji se odnosi na nekvalificirane certifikate. Opća pravila [27] dostupna su na internetskoj stranici http://rdc.fina.hr/cp/cp4-0.pdf.

Pored postupaka i procedura za izdavanje i upravljanje životnim ciklusom nekvalificiranih certifikata, ovaj CPS_{NQC} obuhvaća postupke i procedure koje primjenjuje FINA PKI na davanje usluge izdavanja vremenskog žiga čija su opća pravila opisana u dokumentu FINA PKI - Opća pravila davanja usluga izdavanja vremenskog žiga [28], (u daljnjem tekstu: Opća pravila davanja usluga izdavanja vremenskog žiga) u točkama u kojima se ovaj CPS_{NQC} odnosi na tu uslugu. Opća pravila davanja usluga izdavanja vremenskog žiga [28] dostupna su na internetskoj stranici http://tsa.fina.hr .

U okviru ovog CPS_{NQC} dokumenta pod produkcijskim CA unutar FINA PKI podrazumijevaju se FINA RDC CA i FINA RDC-TDU CA (u daljnjem tekstu, zajedničkim imenom: FINA CA-ovi). U dijelovima ovog CPS_{NQC} 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 CA 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 nekvalificiranih certifikata iz opsega ovog CPS_{NQC} dokumenta:

- FINA RDC osobni normalizirani certifikati;
- FINA RDC poslovni normalizirani certifikati;
- FINA RDC poslovni LCP certifikati;
- FINA RDC-TDU normalizirani certifikati;
- FINA RDC poslovni normalizirani certifikati za IT opremu;

- FINA RDC administrativni normalizirani certifikati (samo za ovlaštene zaposlenike FINE).

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

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

FINA Registar digitalnih certifikata (FINA RDC)		
FINA RDC CA		
FINA RDC osobni normalizirani certifikati	Osobni autentifikacijski N2 certifikat (NCP+)	CP OID: 1.3.124.1104.5.11.1.4.2
	Osobni autentifikacijski Win2 certifikat (NCP+)	CP OID: 1.3.124.1104.5.11.11.4.2
	Osobni soft certifikat (NCP)	CP OID: 1.3.124.1104.5.11.1.3.1
FINA RDC poslovni normalizirani certifikati	Poslovni autentifikacijski N2 certifikat (NCP+)	CP OID: 1.3.124.1104.5.11.2.4.2
	Poslovni autentifikacijski Win2 certifikat (NCP+)	CP OID: 1.3.124.1104.5.11.21.4.2
	Poslovni soft certifikat (NCP)	CP OID: 1.3.124.1104.5.11.2.3.1
FINA Registar digitalnih certifikata (FINA RDC)		
FINA RDC CA		
FINA RDC poslovni lightweight certifikati	Poslovni soft certifikat (LCP)	CP OID: 1.3.124.1104.5.11.2.5.1
FINA RDC poslovni normalizirani certifikati za IT opremu	SSL certifikat razine 2 (NCP)	CP OID: 1.3.124.1104.5.11.3.3.2
	SSL certifikat razine 3 (NCP+)	CP OID: 1.3.124.1104.5.11.3.4.3
	WinDC certifikat razine 2 (NCP)	CP OID: 1.3.124.1104.5.11.31.3.2
	WinDC certifikat razine 3 (NCP+)	CP OID: 1.3.124.1104.5.11.31.4.3
	Aplikacijski certifikat razine 1 (NCP)	CP OID: 1.3.124.1104.5.11.5.3.1
	Aplikacijski certifikat razine 2 (NCP)	CP OID: 1.3.124.1104.5.11.5.3.2
	Aplikacijski certifikat razine 2 (NCP+)	CP OID: 1.3.124.1104.5.11.5.4.2
	Aplikacijski certifikat razine 3 (NCP+)	CP OID: 1.3.124.1104.5.11.5.4.3
	Certifikat za potpis koda (NCP+)	CP OID: 1.3.124.1104.5.11.7.4.2
	Certifikat za vremenski žig (NCP+)	CP OID: 1.3.124.1104.5.11.52.4.3
FINA RDC administrativni normalizirani certifikati	Administrativni N2 certifikat (NCP+)	CP OID: 1.3.124.1104.5.1.6.4.2

FINA Registar digitalnih certifikata (FINA RDC)		
FINA RDC-TDU CA		
FINA RDC-TDU normalizirani certifikati	TDU autentifikacijski N2 certifikat (NCP+)	CP OID: 1.3.124.1104.5.21.2.4.2

Tablica 1.1. Tipovi certifikata

1.2. Naziv dokumenta i identifikacijski podaci

Naziv dokumenta: FINA PKI - Pravilnik o postupcima certificiranja za nekvalificirane certifikate (dokument za javnu objavu)
Verzija: 4.0
Datum stupanja na snagu: 7.11.2013.
OID: 1.3.124.1104.5.0.0.3.4.0

1.3. Sudionici u PKI

Sudionici FINA PKI iz opsega ovog CPS_{NQC} 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 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);
- davatelj usluga izdavanja vremenskog žiga (Time-Stamping Authority, TSA);
- registracijska mreža (RA mreža) koja se sastoji od registracijskih ureda (Registration Authorities, RA-ovi) 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.

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.

1.3.1. Certifikacijska tijela

Certifikacijska tijela u FINA PKI iz opsega ovog CPS_{NQC} dokumenta su FINA RDC CA i FINA RDC-TDU CA (zajedničkim imenom: FINA CA-ovi). FINA CA-ovi su obavezni usluge izdavanja certifikata i upravljanja životnim ciklusom izdanih certifikata obavljati sukladno postupcima iz ovog CPS_{NQC} dokumenta koji je usklađen s Općim pravilima [27].

Obaveze i odgovornosti FINA CA-ova navedeni su u točki 9.6.1 ovog CPS_{NQC} dokumenta. Postupci koje FINA CA-ovi provode u cilju ispunjenja zahtjeva za nekvalificirane certifikate iz Općih pravila [27] opisani su ovom CPS_{NQC} dokumentu.

1.3.1.1. FINA RDC CA

FINA RDC CA iz opsega ovog CPS_{NQC} dokumenta izdaje certifikate koji pripadaju sljedećim grupama tipova nekvalificiranih certifikata:

- FINA RDC osobni normalizirani certifikati;
- FINA RDC poslovni normalizirani certifikati;
- FINA RDC poslovni *lightweight* certifikati;
- FINA RDC poslovni normalizirani certifikati za IT opremu;
- FINA RDC administrativni certifikati.

Profili za svaki pojedini tip normaliziranog, odnosno *lightweight* certifikata kojeg izdaje FINA RDC CA prikazan je u točki 7.1 ovog dokumenta.

FINA RDC CA je izdao vlastiti samopotpisani (root) certifikat koji je namijenjen za provjeru certifikata koje izdaje FINA RDC CA.

Osnovni podaci o FINA RDC CA root certifikatu dani su u tablici 1.2.:

Polje	Vrijednost za FINA RDC CA
Version	V3, vrijednost="2"
serialNumber	3f 1b ce 21
signatureAlgorithm	sha1 s RSA enkripcijom
Issuer	ou=RDC, o=FINA, c=HR
Validity	NotBefore: 21. srpanj 2003 11:57:43 NotAfter: 21. srpanj 2023 12:27:43
Subject	ou=RDC, o=FINA, c=HR
SubjectPublicKeyInfo	AlgorithmIdentifier: RSA 2048 bit
SubjectKeyIdentifier	60-bitna SHA-1 s vodećim 0100 bitovima (po IETF RFC 5280): 47 45 00 6e f0 57 a6 c0
Thumbprint	Thumbprint algorithm: SHA-1 4c 4b ed f2 a8 d7 64 c1 fe dc 81 af d6 37 0f 50 30 7a 0a 12

Tablica 1.2. Osnovni podaci o FINA RDC CA root certifikatu

1.3.1.2. FINA RDC-TDU CA

RDC-TDU CA iz opsega ovog CPS_{NQC} dokumenta izdaje normalizirane certifikate državnim dužnosnicima i zaposlenicima u tijelima državne uprave.

Profili za normalizirani certifikat kojeg izdaje FINA RDC-TDU prikazan je u točki 7.1 ovog dokumenta.

FINA RDC-TDU CA je izdao vlastiti samopotpisani root certifikat koji je namijenjen za provjeru certifikata koje izdaje FINA RDC-TDU CA.

Osnovni podaci o FINA RDC-TDU CA root certifikatu dani su u tablici 1.3.:

Polje	Vrijednost za FINA RDC-TDU CA
Version	V3, vrijednost="2"
serialNumber	41 db f1 61
signatureAlgorithm	sha1 s RSA enkripcijom
Issuer	ou=RDC-TDU, o=FINA, c=HR
Validity	NotBefore: 5. siječanj 2005 14:23:47 NotAfter: 5. siječanj 2025 14:53:47
Subject	ou=RDC-TDU, o=FINA, c=HR
SubjectPublicKeyInfo	AlgorithmIdentifier: RSA 2048 bit
SubjectKeyIdentifier	60-bitna SHA-1 s vodećim 0100 bitovima (po IETF RFC 5280): 47 56 fb b4 e3 ce 3f 7d
Thumbprint	Thumbprint algorithm: SHA-1 6e 46 67 b5 5e 5e e3 4e ad 8c c2 1c fa a1 0b b8 bf c9 a5 30

Tablica 1.3. Osnovni podaci o FINA RDC-TDU CA root certifikatu

1.3.1.3. Davatelj usluga izdavanja vremenskog žiga

FINA kao davatelj usluga certificiranja ima uspostavljenu uslugu izdavanja vremenskog žiga kroz FINA Servis vremenske ovjere (u daljnjem tekstu: FINA TSA). FINA TSA je obavezan uslugu izdavanja vremenskog žiga obavljati sukladno postupcima iz ovog CPS_{NQC} dokumenta koji je u dijelu vezanom uz obavljanje usluge izdavanja vremenskog žiga usklađen s dokumentom Opća pravila davanja usluga izdavanja vremenskog žiga [28].

FINA TSA izrađuje vremenske žigove na TSU jedinici FINA Servis vremenske ovjere TSA1.

Profili vremenskog žiga kojeg izdaje FINA TSA prikazan je u točki 7.1 ovog dokumenta.

Obaveze i odgovornosti FINE kao davatelja usluga izdavanja vremenskog žiga navedene su u točki 9.6.6. ovog CPS_{NQC} dokumenta. Postupci koje FINA TSA provodi u cilju obavljanja usluge izdavanja vremenskog žiga opisani su ovom CPS_{NQC} dokumentu.

Osnovni podaci o FINA TSA certifikatu za potpis vremenskog žiga dani su u tablici 1.4.:

Polje	Vrijednost za FINA TSA
Version	V3, vrijednost="2"
serialNumber	3f 1c 8a 93
signatureAlgorithm	sha1 s RSA enkripcijom
Issuer	ou=RDC, o=FINA, c=HR
Validity	NotBefore: 08. lipnja 2006. 11:33:09 NotAfter: 08. lipnja 2016. 12:03:09

Polje	Vrijednost za FINA TSA
Subject	cn= SERVIS VREMENSKE OVJERE TSA1 o= FINA 00332852 c= HR
SubjectPublicKeyInfo	AlgorithmIdentifier: RSA 2048 bit
SubjectKeyIdentifier	60-bitna SHA-1 s vodećim 0100 bitovima (po IETF RFC 5280): 9 b9 41 ee f4 c4 63 e8
Thumbprint	Thumbprint algorithm: SHA-1 ac b8 44 fd d7 21 67 db 95 73 9d 3a 9e fe c6 23 e3 a5 6b 07
KeyUsage	digitalSignature, Non-Repudiation
EnhancedKeyUsage	Time Stamping (1.3.6.1.5.5.7.3.8)

Tablica 1.4. Osnovni podaci o certifikatu vremenskog žiga FINA TSA

1.3.2. 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, te mreža lokalnih registracijskih ureda u poslovnoj mreži FINE (u daljnjem tekstu: FINA LRA). Poslove registracije korisnika u FINA LRA obavljaju zaposlenici FINE 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://rdc.fina.hr, odnosno http://rdc-tdu.fina.hr.

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_{NQC} dokumentu.

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

1.3.3. Korisnici

Korisnici FINA PKI su osobe koje s FINOM ugovaraju korištenje usluga certificiranja. Usluge certificiranja iz opsega ovog CPS_{NQC} dokumenta koje korisnici ugovaraju su usluge iz područja izdavanja i upravljanja životnim vijekom nekvalificiranih certifikata te usluge izdavanja vremenskog žiga.

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 CA, dok za sve druge korisnike certifikate izdaje FINA RDC CA. Vremenske žigove za sve poslovne subjekte, uključujući i kategoriju TDU izdaje FINA TSA.

Da bi korisnici mogli koristiti usluge certificiranja korisnici trebaju obaviti proceduru registracije i predaje zahtjeva te prihvatiti obaveze i odgovornosti koje su opisane u točki 9.6.3 ovog CPS_{NQC} dokumenta. 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), odnosno skrbnik, a ovlaštena osoba poslovnog subjekta potpisuje i ovjerava ugovor u ime poslovnog subjekta kojeg predstavlja. TDU s FINOM sklapa ugovor o obavljanju usluge certificiranja koji ima funkciju krovnog ugovora. Ovaj ugovor potpisuje i ovjerava ovlaštena osoba TDU. Svaka pripadajuća osoba (potpisnik), odnosno skrbnik, iz TDU u sklopu registracije sklapa s FINOM pojedinačni ugovor kojeg potpisuje pripadajuća osoba – potpisnik, odnosno skrbnik, 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. Ukoliko je korisnik zatražio i ugovorio uslugu izdavanja vremenskog žiga omogućuje mu se korištenje ugovorene usluge.

1.3.3.1. Subjekti certificiranja

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

U slučaju kada je subjekt certificiranja IT oprema korisnik obvezatno određuje skrbnika certifikata. Skrbnik certifikata je 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 ili za potpis koda.

1.3.4. 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.

Prije ostvarenja razumnog pouzdanja u certifikat pouzdajuća strana mora provjeriti valjanost certifikata provjerom CRL liste te na temelju oznaka u certifikatu mora provjeriti sukladnost njegove uporabe s ovim CPS_{NQC} dokumentom.

Obaveze i odgovornosti pouzdajuće strane navedene su u točki 9.6.4 CPS_{NQC} dokumenta.

1.3.5. 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 sličnih 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 normalizirani certifikat koji ima određenu razinu sigurnosti. Pri donošenju odluke o prihvaćanju normaliziranog certifikata određene razine sigurnosti pouzdajuća strana treba razmotriti sljedeće:

- pravne zahtjeve za identifikaciju druge strane, npr. zaštita tajnosti informacija, pravna prihvatljivost elektroničkog potpisa kojeg se može primijeniti;
- sve činjenice koje se nalaze u certifikatu ili činjenice o kojima je pouzdajuća strana obaviještena, uključujući i dokument Opća pravila [27], odnosno ovaj CPS_{NQC} 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 pouzdanim 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 koji se oznakom razine sigurnosti primjenjuje na tipove certifikata.

U tablici 1.5. prikazane su razine sigurnosti za nekvalificirane certifikate koje izdaju FINA CA-ovi. Za svaku razinu sigurnosti u tablici je prikazan pripadajući opis područja primjene i preporučeni financijski limit.

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

Tablica 1.5. Razine sigurnosti za certifikate koje izdaju FINA CA-ovi

1.4.1. Primjerena uporaba FINA RDC i FINA RDC-TDU autentifikacijskih NCP+ normaliziranih certifikata

FINA RDC i FINA RDC-TDU autentifikacijski NCP+ normalizirani certifikati usklađeni su s NCP+ općim pravilima normizacijskog dokumenta HRN ETSI/EN 319 411-3 [11] i njihova je uporaba ograničena na podršku elektroničkom potpisu u smislu Zakona o elektroničkom potpisu [1] i [2], na jaku autentifikaciju i enkripciju ključa. Tipovi certifikata iz ove točke koji u nazivu imaju oznaku Win2 se mogu upotrebljavati za jaku autentifikaciju na Microsoft® Windows okolinu te imaju profil koji im to omogućuje i s tehnološke strane.

Ova točka obuhvaća sljedeće tipove certifikata:

- Osobni autentifikacijski N2 certifikat (NCP+), izdaje se fizičkim osobama – građanima, za privatnu uporabu. Fizička osoba – građanin može ovaj certifikat koristiti i za poslovnu uporabu, ukoliko pri tome nije nužno certifikatom dokazivati pripadnost poslovnom subjektu.
- Osobni autentifikacijski Win2 certifikat (NCP+), 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 autentifikacijski N2 certifikat (NCP+), izdaje se pripadajućim osobama u poslovnim subjektima koji nisu TDU, za poslovnu uporabu;
- Poslovni autentifikacijski Win2 certifikat (NCP+), izdaje se pripadajućim osobama u poslovnim subjektima koji nisu TDU, za poslovnu uporabu;
- TDU autentifikacijski N2 certifikat (NCP+), izdaje se državnim dužnosnicima i zaposlenicima u TDU, za službenu uporabu.

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

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

1.4.1.1. Primjerena uporaba FINA RDC autentifikacijskih NCP normaliziranih certifikata

FINA RDC autentifikacijski NCP normalizirani certifikati usklađeni su s NCP općim pravilima normizacijskog dokumenta HRN ETSI/EN 319 411-3 [11] i njihova je uporaba ograničena na podršku elektroničkom potpisu u smislu Zakona o elektroničkom potpisu [1] i [2], na jaku autentifikaciju i enkripciju ključa.

Ova točka obuhvaća sljedeće tipove certifikata:

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

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

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

1.4.1.2. Primjerena uporaba FINA RDC autentifikacijskih LCP lightweight certifikata

FINA RDC autentifikacijski LCP *lightweight* certifikati usklađeni su s LCP općim pravilima normizacijskog dokumenta HRN ETSI/EN 319 411-3 [11] i njihova je uporaba ograničena na podršku elektroničkom potpisu u smislu Zakona o elektroničkom potpisu [1] i [2], na jaku autentifikaciju i enkripciju ključa.

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

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

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

1.4.1.3. Primjerena uporaba FINA RDC SSL i WinDC poslužiteljskih normaliziranih certifikata

FINA RDC SSL i WinDC poslužiteljski certifikati usklađeni su s NCP, odnosno NCP+ općim pravilima normizacijskog dokumenta HRN ETSI/EN 319 411-3 [11], sukladno podacima iz niže navedenog popisa tipova certifikata obuhvaćenih ovom točkom. U istom su popisu navedene i pripadajuće razine sigurnosti.

Ova točka obuhvaća sljedeće tipove certifikata:

- SSL certifikat razine 2 (NCP), srednje razine sigurnosti, uz korištenje softverskog spremnika ključa
- SSL certifikat razine 3 (NCP+), visoke razine sigurnosti, uz korištenje adekvatnog HSM modula
- WinDC certifikat razine 2 (NCP), srednje razine sigurnosti, uz korištenje softverskog spremnika ključa
- WinDC certifikat razine 3 (NCP+), visoke razine sigurnosti, uz korištenje adekvatnog HSM modula

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

Tipovi certifikata iz popisa koji u nazivu imaju oznaku WinDC izdaju se za Windows Domain Controller te se koriste za jaku autentifikaciju korisnika Windows domene. Ovi tipovi certifikata imaju profil prilagođen opisanoj namjeni.

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

1.4.1.4. Primjerena uporaba FINA RDC aplikacijskih normaliziranih certifikata

FINA RDC aplikacijski certifikati usklađeni su s NCP, odnosno NCP+ općim pravilima normizacijskog dokumenta HRN ETSI/EN 319 411-3 [11], sukladno podacima iz niže navedenog popisa tipova certifikata obuhvaćenih ovom točkom. U istom su popisu navedene i pripadajuće razine sigurnosti.

Ova točka obuhvaća sljedeće tipove certifikata:

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

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

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

1.4.1.5. Primjerena uporaba FINA RDC certifikata za potpis koda

FINA RDC certifikat za potpis koda usklađeni su s NCP+ općim pravilima normizacijskog dokumenta HRN ETSI/EN 319 411-3 [11] te se izdaju poslovnom subjektu, uključujući i TDU. Ovaj tip certifikata jamči elektronički identitet poslovnog subjekta u svrhu provjere autentičnosti porijekla i osiguranje cjelovitosti softvera ili prikladnog oblika softverskog koda. Certifikat se smije koristiti samo za podršku digitalnog potpisa softvera, odnosno softverskog koda.

Ova točka se odnosi na sljedeći tip certifikata:

- Certifikat za potpis koda (NCP+).

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

Ekstenzija *keyUsage* ovih certifikata je označena kritičnom te ima vrijednost postavljenu na *digitalSignature*. Ovaj tip certifikata ima i dodatnu ekstenziju *extKeyUsage* koja nije označena kritično, a koja ima vrijednost postavljenu na *codeSigning*.

1.4.1.6. Primjerena uporaba FINA RDC certifikata za vremenski žig

FINA RDC certifikati za vremenski žig usklađeni su s NCP+ općim pravilima normizacijskog dokumenta HRN ETSI/EN 319 411-3 [11] te se izdaju poslovnom subjektu, uključujući i TDU isključivo za podršku potpisa servisa vremenskog žiga. Ovaj tip certifikata jamči elektronički identitet servisa vremenskog žiga.

Ova točka se odnosi na sljedeći tip certifikata:

- Certifikat za vremenski žig (NCP+).

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

Ekstenzija *keyUsage* ovih certifikata je označena kritičnom te ima vrijednost postavljenu na *digitalSignature* i *nonRepudation*. Ovaj tip certifikata ima i dodatnu ekstenziju *extKeyUsage* označenu kritičnom, a koja ima vrijednost postavljenu na *timeStamping*.

1.4.1.7. Primjerena uporaba FINA RDC administrativnih NCP+ normaliziranih certifikata

FINA RDC administrativni NCP+ normalizirani certifikati usklađeni su s NCP+ općim pravilima normizacijskog dokumenta HRN ETSI/EN 319 411-3 [11] i njihova je uporaba ograničena isključivo na radnje unutar sustava certificiranja FINE..

Ova točka se odnosi na sljedeći tip certifikata:

- Administrativni N2 certifikat (NCP+).

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

1.4.2. Zabrane uporabe certifikata

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

1.5. Administracija CPS_{NQC} dokumenta

1.5.1. Organizacija odgovorna za održavanje CPS_{NQC} dokumenta

Za izradu i održavanje ovog CPS_{NQC} dokumenta odgovorno je tijelo za upravljanje pravilima certificiranja, FINA PMA (vidi točku 1.3. CPS_{NQC} dokumenta).

1.5.2. Kontakt podaci

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

Poštanska adresa:

FINA

Sektor usluga za financijsku industriju i korporativne klijente

Odjel upravljanja politikom ePoslovanja

Koturaška cesta 43

10000 Zagreb

Hrvatska

telefax: 385-1-6304-081

e-mail: pma@fina.hr

1.5.3. Tijelo koje utvrđuje uskladivost CPS_{NQC} dokumenta s Općim pravilima

Uskladivost CPS_{NQC} dokumenta s Općim pravilima [27] utvrđuje FINA PMA.

1.5.4. Procedure odobravanja CPS_{NQC} dokumenta

Da bi se CPS_{NQC} dokument mogao primjenjivati prethodno mora biti odobren od strane FINA PMA. Početak i prestanak važenja CPS_{NQC} dokumenta određuje FINA PMA.

Nakon izmjene zakonske regulative, popisa obvezujućih normizacijskih dokumenata, poslovnog procesa vezanog za izdavanje nekvalificiranih certifikata i vremenskih žigova,

izmjene Općih pravila [27] ili Opća pravila davanja usluga izdavanja vremenskog žiga [28], a koja utječu na postupke iz opsega CPS_{NQC} dokumenta, provodi se revizija CPS_{NQC} dokumenta provjerom usklađenosti s:

- novom zakonskom regulativom;
- novim normizacijskim dokumentima;
- novim Općim pravilima [27];
- novim Općim pravilima davanja usluga izdavanja vremenskog žiga [28].

Nakon provedenog usklađenja, FINA PMA odobrava novi CPS_{NQC} dokument.

Početak važenja novog CPS_{NQC} dokumenta se određuje na osnovu procjene spremnosti sustava certificiranja na rad prema postupcima propisanih ovim dokumentom. Stupanjem na snagu nove verzije CPS_{NQC} 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.

DEFINICIJA	ZNAČENJE
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.
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.
Generiranje ključeva	Proces koji izrađuje niz simbola koji čine kriptografski ključ.

DEFINICIJA	ZNAČENJE
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.
Javni imenik	Informatički sustav u nadležnosti CA koji služi za *on-line* 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.
LCP certifikat	Vidi pojam „*Lightweight* certifikat“

DEFINICIJA	ZNAČENJE
***Lightweight* certifikat**	Certifikat koji pruža manje zahtjevnu razinu kvalitete usluge u odnosu na certifikate izdane sukladno Općim pravilima izdavanja kvalificiranih certifikata opisanim u HRN ETSI/EN 319 411-2, LCP certifikat.
Lista opozvanih certifikata (CRL)	Potpisana lista koja ukazuje na skup certifikata koji se od strane izdavatelja certifikata više ne smatraju važećim.
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).
***On-line* provjera statusa certifikata**	Provjera statusa valjanosti certifikata koja se obavlja *on-line*. Primjer *on-line* provjere statusa certifikata je i provjera opozvanosti certifikata pomoću *on-line* preuzete CRL. Ako se *on-line* 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.
Operativni period certifikata	Stvarno vrijeme valjanosti certifikata koje počinje vremenom početka važenja certifikata koje je označeno u certifikatu te završava najranijim od dva sljedeća događaja: • istekom roka valjanosti certifikata koje je označeno u certifikatu ili • trenutkom opoziva 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.

DEFINICIJA	ZNAČENJE
Par ključeva	Dva matematički povezana kriptografska ključa (privatni ključ i njegov odgovarajući javni ključ), koji imaju sljedeća svojstva: • jedan ključ iz para ključeva može biti korišten za enkripciju podataka, a koji se mogu dekriptirati samo korištenjem drugog ključa iz istog para ključeva, i • u slučaju poznavanja samo jednog ključa nije moguće (u razumnom vremenu i uz poznatu tehnologiju) otkriti drugi ključ.
Period valjanosti certifikata	Vremenski period tijekom kojeg vrijedi certifikat. Ovaj vremenski period počinje vremenom označenim u polju „vrijedi od“ i završava vremenom „vrijedi do“.
Podaci za izradu elektroničkog potpisa	Jedinstveni podaci, poput kodova ili privatnih kriptografskih ključeva, koje potpisnik koristi za izradu elektroničkog potpisa.
Podaci za verificiranje elektroničkog potpisa	Podaci poput kodova ili javnih kriptografskih ključeva, koji se koriste u svrhu verificiranja (ovjere) elektroničkog potpisa.
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.
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.

DEFINICIJA	ZNAČENJE
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 pravilima davanja usluga certificiranja (CP), odnosno Općim pravilima davanja usluga izdavanja vremenskog žiga.
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	Za certifikat: 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. Za vremenski žig: Fizička osoba zaposlena u poslovnom subjektu ili na drugi način povezana s poslovnim subjektom, a koja je od strane istog poslovnog subjekta autorizirana za korištenje usluge izdavanja vremenskog žiga.
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.

DEFINICIJA	ZNAČENJE
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.
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.
Registracijski ured (RA)	Za certifikate: Pravna ili fizička osoba ovlaštena od CA i zadužena za jednu ili više slijedećih radnji: identifikaciju i potvrdu identiteta tražitelja certifikata, prihvaćanje ili odbijanje zahtjeva za izdavanje certifikata, obradu zahtjeva za opoziv, suspenziju ili reaktivaciju certifikata, pokretanje opoziva, suspenzije ili reaktivacije certifikata, prihvaćanje ili odbijanje zahtjeva za obnovu certifikata. Za vremenski žig: Pravna ili fizička osoba ovlaštena od TSA zadužena za registraciju korisnika.
Sigurno sredstvo za izradu elektroničkog potpisa (SSCD)	Vidi pojam: „Sredstvo za izradu naprednog elektroničkog potpisa“.

DEFINICIJA	ZNAČENJE
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 ili za potpis koda. Skrbnik pokreće zahtjeve za izdavanje, obnovu, opoziv, suspenziju ili reaktivaciju certifikata te je kontakt osoba za taj certifikat.
Središnji RA	Središnji registracijski ured. Može registrirati korisnike, ali primarno je zadužen za koordiniranje cjelokupne RA mreže.
Sredstvo za izradu elektroničkog potpisa	Odgovarajuća računalna oprema ili računalni program kojeg potpisnik koristi pri izradi elektroničkog potpisa.
Sredstvo za izradu naprednog elektroničkog potpisa (SSCD)	Sredstvo za izradu elektroničkog potpisa koje osigurava: • da se podaci za izradu naprednoga elektroničkog potpisa mogu pojaviti samo jednom te da je ostvarena njihova sigurnost, • da se podaci za izradu naprednoga elektroničkog potpisa ne mogu ponoviti te da je potpis zaštićen od krivotvorenja pri korištenju postojeće raspoložive tehnologije, • da podatke za izradu naprednoga elektroničkog potpisa subjekt može pouzdano zaštititi protiv korištenja od strane drugih. Sredstvo za izradu naprednoga elektroničkog potpisa ne smije pri izradi naprednoga elektroničkog potpisa promijeniti podatke koji se potpisuju ili onemogućiti subjektu uvid u te podatke prije procesa izrade naprednoga elektroničkog potpisa.
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, pripadajuća osoba, poslovni subjekt i IT oprema (npr. poslužitelj, aplikacija i sl.). Podaci o subjektu sastavni su dio certifikata.
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 državni uredi Vlade Republike Hrvatske, državne upravne organizacije i uredi državne uprave u županijama ili druga tijela državne uprave utvrđena mjerodavnim važećim zakonom.
Tražitelj certifikata	Poslovni subjekt i/ili fizička osoba koja podnosi zahtjev za izdavanje certifikata, podnositelj zahtjeva.
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.

DEFINICIJA	ZNAČENJE
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.

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
ISO	International Standards Organization	Međunarodna organizacija za normizaciju
LCP	Lightweight Certificate Policy	Opća pravila certificiranja za *lightweight* (lagane) certifikate
LDAP	Lightweight Directory Access Protocol	Protokol za pristup informacijskim direktorijima
LRA	Local Registration Authority	Lokalni registracijski ured
NCP	Normalized Certificate Policy	Opća pravila certificiranja za normalizirane certifikate
OID	Object Identifier	Identifikator objekta
PIN	Personal Identification Number	Osobni tajni broj za aktivaciju smart kartice, USB

KRATICA	PUNI NAZIV	ZNAČENJE
		tokena ili sličnog uređaja
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
TDU	Tijelo (ili tijela) državne uprave	Tijelo (ili tijela) državne uprave
TSA	Time-Stamping Authority	Davatelj usluga izdavanja vremenskog žiga
TSU	Time-Stamping Unit	Jedinica za izradu vremenskog žiga
URL	Uniform Resource Locator	Internetska adresa određenog resursa
UTC	Coordinated Universal Time	Koordinirano svjetsko vrijeme

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 repozitorije čine sljedeći repozitoriji:

- FINA RDC repozitorij čiji sadržaj operativno ažurira FINA RDC CA;
- FINA RDC-TDU repozitorij čiji sadržaj operativno ažurira FINA RDC-TDU CA;
- FINA TSA repozitorij čiji sadržaj operativno ažurira FINA TSA.

Repozitoriji se mogu sastojati od dijela dostupnog preko internetskih stranica i dijela dostupnog preko LDAP poslužitelja.

2.2. Objava informacija o certificiranju

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

2.2.1. FINA RDC repozitorij

Na internetskim stranicama se objavljuju sljedeći dokumenti i informacije:

- Aktualna Opća pravila [27];
- Prijašnje verzije Općih pravila [27];
- 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 i reaktivaciju certifikata;
- Obrasci punomoći;
- Informacije o FINA RDC CA *root* certifikatu;
- Objedinjena CRL sustava FINA RDC CA;
- 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 CA.

Preko internetske stranice repozitorija moguće je pretraživanje javnog imenika certifikata koje je izdao FINA RDC CA .

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

U strukturi javnog imenika javno se objavljuju:

- izdani nekvalificirani certifikati;
- objedinjena CRL i segmentirana CRL sustava RDC CA.

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

Adrese FINA RDC repozitorija na kojima se objavljuju CRL liste navedene su u točki 4.10.1 ovog CPS_{NQC} dokumenta.

2.2.2. FINA RDC-TDU repozitorij

Na internetskim stranicama se objavljuju sljedeći dokumenti i informacije:

- Aktualna Opća pravila [27];
- Prijašnje verzije Općih pravila davanja usluga certificiranja [27];
- 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 i reaktivaciju certifikata;
- Obrasci punomoći;
- Informacije o FINA RDC-TDU CA root certifikatu;
- Objedinjena CRL sustava FINA RDC-TDU CA;
- 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 CA.

Objavljeni sadržaj na internetskoj stranici dostupan je s adrese http://rdc-tdu.fina.hr .

U strukturi javnog imenika javno se objavljuju:

- svi izdani normalizirani certifikati;
- objedinjena CRL i segmentirana CRL sustava FINA RDC-TDU CA.

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

Adrese FINA RDC-TDU repozitorija na kojima se objavljuju CRL liste navedene su u točki 4.10. CPS_{NQC} dokumenta.

2.2.3. FINA TSA repozitorij

FINA TSA repozitorij se sastoji samo iz dijela koji je javno objavljen na internetskim stranicama. Na FINA TSA repozitoriju javno se objavljuju sljedeći dokumenti i informacije:

- Aktualna Opća pravila davanja usluga izdavanja vremenskog žiga [28];
- Prijašnje verzije Općih pravila davanja usluga izdavanja vremenskog žiga [28];
- Izjava o davanju usluga izdavanja vremenskog žiga
- Uvjeti pružanja usluge vremenske ovjere;
- Cjenik usluga izdavanja vremenskog žiga;
- Obrazac zahtjeva za pristupanjem FINA Servisu vremenske ovjere;
- Informacije o certifikatu za potpis vremenskog žiga;
- 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 izdavanja vremenskog žiga;
- Ostale informacije vezane uz rad FINA TSA.

Objavljeni sadržaj FINA TSA repozitorija dostupan je s internetske adrese http://tsa.fina.hr .

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

2.2.4. Postupci objave sadržaja i upravljanja repozitorijem

Trajanje važenja i prestanak važenja Općih pravila [27] su definirani u točkama 9.10.1. i 9.10.2. Općih pravila [27], a određuje ih i odobrava FINA PMA. Prijašnje verzije dokumenta ostaju objavljene na repozitoriju, uz naznaku vremenskog perioda kad su vrijedile. Obavijesti o izmjenama i važenju dokumenta Opća pravila [27] objavljuju se najmanje 30 dana prije početka njihove primjene.

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

Informacije o root certifikatima FINA CA-ova i certifikatu za potpis vremenskog žiga objavljuju se po njihovu izdavanju.

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

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

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

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

2.3. Vrijeme ili učestalost objavljivanja

Opća pravila [27], drugi dokumenti i ostale informacije iz točaka 2.2.1. i 2.2.2. ovog CPS_{NQC} dokumenta se objavljuju po potrebi, nakon odobrenja FINA PMA.

Certifikati se u javnom imeniku objavljuju odmah po izdavanju.

Učestalost objave CRL lista za certifikate koje izdaju FINA CA je definirana u točki 4.9.7. ovog CPS_{NQC} dokumenta.

2.4. Kontrole pristupa repozitoriju

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

Pristup repozitoriju uz mogućnost izmjene sadržaja imaju samo ovlašteni zaposlenici u FINA CA.

FINA će osigurati 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_{NQC} 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 ovom CPS_{NQC} dokumentu.

3.1. Određivanje imena

3.1.1. Tipovi imena

U polje „Subject“ svakog nekvalificiranog certifikata upisuju se autentični podaci o subjektu certificiranja. Dio polja „Subject“ sadrži ime i prezime, odnosno naziv subjekta certificiranja. Također, polje „Subject“ osobnih certifikata sadrži naziv mjesta prebivališta potpisnika, dok za poslovne certifikate i poslovne certifikate za IT opremu polje „Subject“ sadrži naziv mjesta sjedišta poslovnog subjekta. Polje „Subject“ u nekvalificiranim certifikatima je usklađeno s normom X.501 [26] i preporukom IETF RFC 5280 [19].

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

Nazivi poslužitelja i aplikacija koji se upisuju u polje „Subject“ certifikata koji se izdaju za poslužitelje i aplikacije te sadržaj polja „Subject Alternative Name“ certifikata su u skladu s preporukom IETF RFC 5322 [20]. Nazivi poslužitelja/aplikacije mogu biti FQDN, IP adresa poslužitelja, odnosno naziv ili URL aplikacije/servisa. Pri registraciji FINA RA mreža provjerava vlasništvo nad domenom, odnosno IP adresnim područjem, iz naziva poslužitelja/aplikacije. Ako se u polje „Subject Alternative Name“ upisuje e-mail adresa, ona se prethodno provjerava.

Polje „Subject“ u certifikatima koji se izdaju za potpis koda sadrži skraćeni naziv poslovnog subjekta i njegov identifikator te mjesto sjedišta poslovnog subjekta.

U FINA RDC poslovnim certifikatima, FINA RDC-TDU certifikatima te FINA RDC poslovnim certifikatima za IT opremu polje „Subject“ sadrži ime i prezime, odnosno naziv subjekta certificiranja, skraćeni naziv i identifikator poslovnog subjekta. Skraćeni naziv poslovnog subjekta je identičan onom skraćenom nazivu 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 skraćeni naziv upisuje u polje „Subject“ certifikata. Pravila za kreiranje identifikatora poslovnog subjekta opisana su u točki 3.1.4. ovog CPS_{NQC} 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 se u potpunosti izbacuju.

3.1.2. Smislenost imena

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

Naziv grupe certifikata	Pravilo za smislenost elemenata polja Subject
FINA RDC osobni nekvalificirani certifikati	• commonName: Ime i prezime potpisnika • localityName: Mjesto prebivališta potpisnika • countryName: HR
FINA RDC poslovni nekvalificirani certifikati i	• commonName: Ime i prezime potpisnika • localityName: Mjesto sjedišta poslovnog subjekta • organizationName: Skraćeni naziv i identifikator poslovnog subjekta • countryName: HR
FINA RDC poslovni nekvalificirani certifikati za IT opremu	• localityName: Mjesto sjedišta poslovnog subjekta • organizationName: Skraćeni naziv i identifikator poslovnog subjekta • countryName: HR
FINA RDC-TDU nekvalificirani 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 [20] smislenost imena i naziva se ne provjerava.

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 [26] normi za nekvalificirane certifikate provodi se prema tablici 3.2.

Poslovni nekvalificirani certifikati			
Polje po X.501	**FINA RDC CA**	**FINA RDC-TDU CA**	**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 CA podržavaju do dvije podorganizacijske jedinice unutar TDU
Locality (L)	Mjesto sjedišta poslovnog subjekta	Mjesto sjedišta TDU	Mjesto sjedišta poslovnog subjekta

Poslovni nekvalificirani certifikati			
Polje po X.501	**FINA RDC CA**	**FINA RDC-TDU CA**	**Pojašnjenje**
Serial Number (SN)	- Identifikator pripadajuće osobe (potpisnika) - Ne koristi se za poslovne certifikate za IT opremu	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)	Poslovni certifikati za pripadajuće osobe: - Ime i prezime pripadajuće osobe (potpisnika) Certifikati za poslužitelje: - FQDN poslužitelja; ili - IP adresa poslužitelja Certifikati za aplikacije: - naziv aplikacije Za certifikate za potpis koda: - skraćeni naziv poslovnog subjekta	Ime i prezime pripadajuće osobe (potpisnika)	Za pripadajuće osobe: ime i prezime pripadajuće osobe (potpisnika) iz identifikacijske isprave. Za poslužitelje: FQDN ili IP adresa poslužitelja. Za potpis koda: skraćeni naziv poslovnog subjekta iz mjerodavnog registra.

Osobni nekvalificirani certifikati			
Polje po X.501	**FINA RDC CA**	**FINA RDC-TDU CA**	**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)
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 [20] u FINA PKI nekvalificiranim certifikatima primjenjuje se:

- za nazive u atributu „Common Name“ (CN) u slučajevima kad je subjekt certificiranja poslužitelj, tumačimo ih kao FQDN poslužitelja;
- za nazive u atributu „Common Name“ (CN) u slučajevima kad je subjekt certificiranja aplikacija, tumačimo ih kao naziv aplikacije;
- za nazive u ekstenziji certifikata „Subject Alternative Name“ koja imaju oblik e-mail adrese, tumačimo ih kao e-mail adresu, osim za autentifikacijske normalizirane

certifikate za Windows gdje ih tumačimo kao User Principal Name (UPN) u obliku email adrese.

Tumačenje oblika imena po X.501 [26] normi u FINA PKI za CRL liste provodi se prema tablici 3.3.

Polje po X.501	FINA RDC CA	FINA RDC-TDU CA	Pojašnjenje
Country (C)	HR	HR	Država sjedišta davatelja usluge certificiranja, Hrvatska
Organization (O)	FINA	FINA	Davatelj usluga certificiranja
Organization Unit (OU)	RDC	RDC-TDU	Naziv certifikacijskog tijela
Common Name (CN)	CRLn	CRLn	Identifikator segmentirane CRL liste (CRLn). Sa n se označava broj segmenta segmentirane CRL liste. (npr. CRL1 je prvi segment CRL liste).

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

3.1.5. Jedinstvenost imena

Skup podataka u polju „Subject“ čini razlikovno ime subjekta certificiranja (engl. *Distinguished Name, DN*) sukladno preporuci IETF RFC 5280 [19] i normi X.501 [26].

Jedinstvenost razlikovnog imena u FINA PKI nekvalificiranim certifikatima osigurava se sukladno preporuci IETF RFC 5280 [19] i normom X.501 [26] za:

- potpisnike osigurava se serijskim brojem (atribut SerialNumber) u razlikovnom imenu;
- poslužitelje se osigurava na način da se u atribut „Common Name“ (CN) razlikovnog imena certifikata upisuje jedinstveni FQDN poslužitelja ili IP adresa;
- aplikacije se osigurava na način da se u atribut „Common Name“ (CN) razlikovnog imena certifikata upisuje naziv aplikacije koji unutar istog poslovnog subjekta mora biti jedinstven;
- potpis koda osigurava se serijskim brojem (atribut SerialNumber) u razlikovnom imenu.

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 NCP+ certifikate

Za izdavanje tipova normaliziranih certifikata za koje je propisano izdavanje na SSCD uređaju (tipovi certifikata NCP+ iz točke 1.1.2. ovog CPS_{NQC} dokumenta), subjektovi se ključevi uvijek generiraju unutar SSCD uređaja. Potpisnik može odabrati jednu od sljedeće dvije mogućnosti:

- ključeve za potpisnika na SSCD uređaju generira FINA CA na svojoj lokaciji;
- ključeve za potpisnika na SSCD uređaju generira potpisnik na korisničkoj lokaciji.

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

Dokazivanje posjeda privatnog ključa, koji pripada odgovarajućem javnom ključu, sastoji se u kombinaciji procesa generiranja ključeva u SSCD uređaju i prosljeđivanja javnog ključa sustavu za izdavanje certifikata. Ovaj proces osigurava i nadgleda FINA CA unutar svoje lokacije (vidi točku 6.1.1.3. ovog CPS_{NQC} dokumenta). SSCD uređaj sa subjektovim ključevima i izdanim certifikatom se uz neposrednu identifikaciju dostavlja potpisniku odnosno skrbniku.

b) Ključevi se na SSCD uređaju generiraju na korisničkoj lokaciji

Dokazivanje posjeda privatnog ključa, koji pripada odgovarajućem javnom ključu, osigurava se sigurnom dostavom SSCD uređaja potpisniku odnosno skrbniku, sigurnim načinom slanja aktivacijskih podataka za SSCD potpisniku odnosno skrbniku, odvojenim zaštićenim kanalom, generiranjem ključeva na SSCD uređaju pod udaljenim *on-line* nadzorom FINA CA te korištenjem potpisanog PKCS#10 formata zahtjeva (vidi točku 6.1.1.3. ovog CPS_{NQC} dokumenta). Ukoliko zadovolji potrebne uvjete, udaljeni *on-line* nadzor umjesto FINA CA može osiguravati vanjski ugovoreni RA.

3.2.1.2. Dokazivanje posjeda privatnog ključa za NCP i LCP certifikate

Subjektovi ključevi za nekvalificirane NCP i LCP certifikate se generiraju i čuvaju u adekvatnom softverskom spremniku ključeva.

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

a) Ključeve NCP i LCP certifikata generira FINA CA na svojoj lokaciji

Ovaj postupak se primjenjuje za sljedeće tipove certifikata:

- Osobni soft certifikat (NCP);
- Poslovni soft certifikat (NCP); i
- Poslovni soft certifikat (LCP).

Ovisno o odluci skrbnika, ovaj postupak se primjenjuje i na Aplikacijski certifikat razine 1 (NCP).

Dokazivanje posjeda privatnog ključa, koji pripada odgovarajućem javnom ključu, sastoji se u kombinaciji procesa generiranja ključeva i prosljeđivanja javnog ključa sustavu za izdavanje certifikata. Ovaj proces osigurava i nadgleda FINA CA unutar svoje lokacije. Subjektov par ključeva i izdani certifikat dostavljaju se potpisniku odnosno skrbniku sigurnim autentificiranim *on-line* kanalom u PKCS#12 formatu (vidi točku 6.1.1.4. ovog CPS_{NQC} dokumenta).

b) Ključeve NCP certifikata generira skrbnik na korisničkoj lokaciji

Dokazivanje posjeda privatnog ključa, koji pripada odgovarajućem javnom ključu, osigurava se generiranjem subjektovog para ključeva u propisanoj kontroliranoj okolini na korisničkoj lokaciji, slanjem zahtjeva za izdavanje certifikata u potpisanom PKCS#10 formatu u FINA CA (vidi točku 6.1.1.4. ovog CPS_{NQC} dokumenta) te sigurnim načinom dostave aktivacijskih podataka za preuzimanje certifikata potpisniku odnosno skrbniku.

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_{NQC} dokumenta.

Iznimno, u slučaju promjene podataka o poslovnom subjektu sadržanih u certifikatu popisanih u točki 3.1.1. ovog CPS_{NQC} dokumenta potpisnik, odnosno skrbnik, 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_{NQC} dokumenta, potpisnik ili skrbnik 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.

3.2.2.1. Potvrda identiteta poslovnog subjekta kod pružanja usluga vremenskog žiga

U cilju potvrde identiteta poslovnog subjekta koji traži pružanje usluga vremenskog žiga, podnositelj zahtjeva navodi točno i cjelovito popunjene podatke o poslovnom subjektu i pripadajućim autentifikacijskim certifikatima u zahtjevu za pružanje usluga vremenskog žiga, koji mora biti potpisan i ovjeren od strane osobe ovlaštene za zastupanje.

Postupak potvrde identiteta provodi službenik FINA RA mreže na temelju upita na FINA RA aplikaciju i, ukoliko je to primjenjivo, na nacionalni OIB sustav. Službenik FINA RA uspoređuje podatke o poslovnom subjektu dostavljene na zahtjevu sa podacima u FINA RA aplikaciji te provjerava valjanost i povezanost autentifikacijskih certifikata i poslovnog subjekta. Prilikom pristupa usluzi vremenskog žiga tako provjereni autentifikacijski certifikati su potvrda identiteta korisnika usluge.

3.2.3. Potvrda identiteta fizičke osobe

Inicijalnu identifikaciju i potvrđivanje identiteta potpisnika, odnosno skrbnika u FINA PKI provodi FINA RA/LRA ili vanjski ugovoreni RA postupcima neposredne identifikacije i potvrđivanja identiteta fizičke osobe sukladno točki 3.2.3.2 ovog CPS_{NQC} dokumenta. Identifikaciju i potvrđivanje identiteta potpisnika, odnosno skrbnika, iznimno provodi i FINA Središnji RA.

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

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, odnosno skrbnik, 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 se može provesti na dva načina, ovisno o tome je li stranom državljaninu dodijeljen OIB u 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 se provodi uvidom u prihvatljivu identifikacijsku ispravu za stranca, definiranu u točki 3.2.3.1. ovog CPS_{NQC} dokumenta.

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

Identifikacija potpisnika stranih državljana koji podnose zahtjev za izdavanje LCP certifikata se ne provodi neposrednom identifikacijom. Ova identifikacija se provodi provjerom preslika

dvije različite identifikacijske isprave za stranca, definirane u točki 3.2.3.1. ovog CPS_{NQC} dokumenta, te provjerom telefonskim upitom na službeno registrirani broj poslovnog subjekta u kojem je potpisnik pripadajuća osoba. Ukoliko predstavnik poslovnog subjekta potvrdi identitet i pripadnost potpisnika poslovnom subjektu, smatra se da je provedena posredna identifikacija potpisnika koja zadovoljava norme za izdavanje LCP certifikata.

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_{NQC} 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 uređaja 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, odnosno skrbnik, i potvrđuje točnost i cjelovitost informacija u zahtjevu za izdavanje certifikata. Službenik u RA mreži potpisom ovjerava uspješnu i pravilnu identifikaciju potpisnika, odnosno skrbnika, te podatke upisuje u FINA RA aplikaciju ili zaštićenim putem dostavlja u FINA RA sustav.

3.2.3.1. Prihvatljive vrste identifikacijskih isprava

Potpisnici, skrbnici ili opunomoćenici potpisnika koji su hrvatski državljani, za izdavanje nekvalificiranih certifikata moraju dokazati svoj identitet valjanom osobnom iskaznicom ili putovnicom.

Potpisnici, skrbnici ili opunomoćenici potpisnika koji nisu hrvatski državljani dokazuju svoj identitet valjanom putnom ispravom s kojom su ušli u Republiku Hrvatsku, a mogu ga dokazati i valjanom osobnom iskaznicom za stranca. Iznimno, strani državljanin u ulozi potpisnika koji podnosi zahtjev za izdavanje LCP certifikata, može se identificirati i drugom javnom ispravom koja sadrži njegovu fotografiju, potpis i osobne podatke.

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_{NQC} 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 FINA središnjeg RA.

Potpisnik, odnosno skrbnik, uvijek mora biti identificiran neposrednom identifikacijom - prilikom podnošenja zahtjeva ili prilikom preuzimanja SSCD uređaja sa ili bez privatnog ključa, osim u slučaju izdavanja LCP certifikata.

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 važeće identifikacijske isprave upitom na nacionalni OIB sustav, osim za strane državljane koji nemaju dodijeljen OIB u Hrvatskoj.

3.2.3.3. Potvrda identiteta fizičke osobe kod pružanja usluga vremenskog žiga

U cilju potvrde identiteta fizičke osobe koja traži pružanje usluga vremenskog žiga, podnositelj zahtjeva navodi točno i cjelovito popunjene podatke o fizičkoj osobi i pripadajućim autentifikacijskim certifikatima u zahtjevu za pružanje usluga vremenskog žiga, koji mora biti potpisan od strane fizičke osobe.

Fizička osoba koja traži pružanje usluga vremenskog žiga mora imati pripadajući autentifikacijski certifikat izdan od strane FINA CA ili mora biti skrbnik autentifikacijskog certifikata izdanog od strane FINA CA. Postupak potvrde identiteta provodi službenik FINA RA mreže na temelju provjere povezanosti fizičke osobe i autentifikacijskog certifikata kojeg je fizička osoba navela u zahtjevu. Službenik FINA RA uspoređuje podatke o fizičkoj osobi dostavljene na zahtjevu sa podacima u FINA RA aplikaciji te provjerava valjanost i povezanost autentifikacijskih certifikata i fizičke osobe. Prilikom pristupa usluzi vremenskog žiga tako provjeren autentifikacijski certifikat je potvrda identiteta korisnika usluge.

3.2.4. Informacije o korisniku koje se ne provjeravaju

Informacije o korisniku koje se ne provjeravaju su:

- naziv podorganizacijske jedinice TDU;
- telefonski brojevi (ukoliko se na iste ne šalju autentifikacijski podaci).

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

3.2.5. Provjera identiteta ovlaštenih osoba

Na zahtjev za izdavanje FINA CA poslovnih certifikata se uz pečat potpisuje i osoba ovlaštena za zastupanje poslovnog subjekta te time potvrđuje istinitost podataka u zahtjevu.

Osoba ovlaštena za zastupanje poslovnog subjekta se uz pečat potpisuje i na ugovor o obavljanju usluga certificiranja za poslovne subjekte, odnosno na 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 iz prethodne rečenice 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.

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 ili reaktivaciju, 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_{NQC} 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_{NQC} 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

Nekvalificirani certifikati koje za subjekte izdaju FINA RDC CA i FINA RDC-TDU CA su namijenjeni za korištenje u elektroničkom poslovanju unutar i izvan prostora Republike Hrvatske te zadovoljavaju međunarodne norme za njihovu prekograničnu uporabu. Nekvalificirani certifikati za potpisnike zadovoljavaju odredbe europske Direktive o elektroničkim potpisima [9].

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

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

Kod redovne obnove nekvalificiranih certifikata se provodi postupak generiranja novog para subjektovih ključeva te se provodi redovna obnova certifikata sukladno točki 4.7. CPS_{NQC} dokumenta.

Identifikacija i potvrđivanje identiteta pri obnovi se provodi na dva osnovna načina sukladno točkama 3.3.1.1., odnosno 3.3.1.2. ovog CPS_{NQC} dokumenta.

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

Ovaj postupak provodi se za sljedeće tipove certifikata:

- Osobni soft certifikat (NCP);
- Poslovni soft certifikat (NCP);
- Poslovni soft certifikat (LCP);
- Aplikacijski certifikat razine 1 (NCP) koji se preuzimaju kroz FINA CMS sustav.

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

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

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

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

Ovaj postupak provodi se za slijedeće tipove certifikata:

- Osobni autentifikacijski N2 certifikat (NCP+);
- Osobni autentifikacijski Win2 certifikat (NCP+);
- Poslovni autentifikacijski N2 certifikat (NCP+);
- Poslovni autentifikacijski Win2 certifikat (NCP+);
- Administrativni N2 certifikat (NCP+);
- TDU autentifikacijski N2 certifikat (NCP+).

Postupak identifikacije i potvrđivanja identiteta kod redovne obnove certifikata zaštićenim elektroničkim putem uz udaljeni nadzor FINA CA obavlja se *on-line* pristupom valjanim certifikatom. Ukoliko zadovolji potrebne uvjete, udaljeni *on-line* nadzor umjesto FINA CA može osiguravati vanjski ugovoreni RA. Identifikacija i potvrđivanje identiteta korisnika odnosno skrbnika, obavlja se autentifikacijom i provjerom elektroničkog potpisa potpisnika odnosno skrbnika pri *on-line* podnošenju zahtjeva za redovnom obnovom certifikata.

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

Ovaj postupak provodi se za sve poslovne certifikate za IT opremu.

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

Identifikacija i potvrđivanje identiteta poslovnog subjekta provodi se sukladno odredbama točaka 3.2.2. i 3.2.5. CPS_{NQC} 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_{NQC} dokumenta.

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

3.3.2. Identifikacija i potvrđivanje identiteta korisnika za obnovu certifikata po opozivu

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 traži obnovu ili izmjenu podataka u certifikatu, korisnik identifikaciju i potvrdu identiteta obavlja sukladno proceduri inicijalnog utvrđivanja identiteta iz točke 3.2. ovog CPS_{NQC} dokumenta. Po pozitivnoj identifikaciji, potvrdi identiteta i zaprimanju točnog i cjelovitog zahtjeva za izdavanje certifikata, korisniku se izdaje novi certifikat.

3.4. Identifikacija i potvrđivanje identiteta korisnika kod zahtjeva za opoziv

Identifikacija i potvrđivanje identiteta u postupku opoziva normaliziranih certifikata provodi se neposrednom identifikacijom podnositelja zahtjeva koji traži opoziv u registracijskom uredu RA mreže ili u prisustvu ovlaštenog RA ili LRA službenika.

Identifikacija i potvrđivanje identiteta u postupku opoziva *lightweight* certifikata provodi se provjerom podataka o certifikatu, potpisniku i poslovnom subjektu koje putem e-mail poruke ili telefonskim putem dostavi podnositelj zahtjeva za opoziv, uz posrednu identifikaciju podnositelja zahtjeva. Izvornost podataka provjerava se inicijalno registriranom e-mail adresom, odnosno inicijalno registriranim telefonskim brojem korisnika te podacima koje korisnik dostavlja. Na osnovu provjere i izvornosti podataka vrši se opoziv *lightweight* certifikata.

Ako je zahtjev za opoziv certifikata poslan i potpisan elektronički, identitet korisnika utvrđuje se elektroničkim potpisom s važećim certifikatom.

Zahtjev za opoziv i reaktivaciju poslovnih certifikata, poslovnih certifikata za IT opremu i certifikata za TDU, uz pečat potpisuje osoba ovlaštena za zastupanje poslovnog subjekta, a zahtjev za suspenziju navedenih certifikata može uz pečat potpisati potpisnik, odnosno skrbnik ili ovlaštena osoba. Zahtjev za opoziv, suspenziju i reaktivaciju osobnog certifikata potpisuje potpisnik.

Identifikacija i potvrđivanje identiteta u postupku suspenzije certifikata, moguće je provesti prema proceduri za opoziv certifikata. Također, identifikacija i potvrđivanje identiteta u postupku suspenzije moguće je provesti i telefonskim putem. U tom slučaju ovlašteni agent provodi postupak identifikacije i potvrđivanja identiteta podnositelja zahtjeva na temelju upita i usporedbe odgovora sa zapisima pohranjenim u RA sustavu.

Ako je zahtjev za suspenziju certifikata poslan elektronički, identitet podnositelja zahtjeva utvrđuje se elektroničkim potpisom s važećim certifikatom.

Opoziv i suspenzija certifikata opisana je u točki 4.9. ovog CPS_{NQC} dokumenta.

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 nekvalificiranih 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 nekvalificiranih 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 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_{NQC} dokumentom i Općim pravilima [27].

4.1.2.1. Proces podnošenja zahtjeva za izdavanje certifikata

Zahtjev za izdavanje nekvalificiranih certifikata može biti namijenjen isključivo za izdavanje nekvalificiranih certifikata ili može biti kombiniran sa zahtjevom za izdavanje kvalificiranih certifikata, ukoliko se i nekvalificirani i kvalificirani 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 nekvalificiranih osobnih certifikata potpisuje fizička osoba-građanin.

Zahtjev za izdavanje nekvalificiranih FINA RDC poslovnih certifikata i FINA RDC poslovnih certifikata za IT opremu potpisuje pripadajuća osoba, odnosno skrbnik, a zahtjev za izdavanje normaliziranih FINA RDC TDU 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_{NQC} 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 nekvalificiranih certifikata predan u elektroničkom obliku, FINA 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_{NQC} dokumenta.

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

Korisnici koji podnose zahtjev za izdavanje nekvalificiranog certifikata, s FINOM sklapaju odgovarajući ugovor o obavljanju usluga certificiranja kojim prihvaćaju Opća pravila certificiranja [27] 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, odnosno skrbnik, kazneno i materijalno odgovara za točnost i ispravnost dostavljenih podataka o sebi;
- osoba ovlaštena za zastupanje poslovnog subjekta, odnosno poslovni subjekt, kazneno i materijalno odgovara za točnost i ispravnost dostavljenih podataka o sebi, poslovnom subjektu, pripadajućoj osobi ili drugom subjektu certificiranja;
- korisnik, potpisnik, odnosno skrbnik, 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_{NQC} dokumenta.

Obveze i odgovornosti FINA CA su navedene u Poglavlju 9.6.1. ovog CPS_{NQC} 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_{NQC} 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 nekvalificiranog 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_{NQC} 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, poslovnog certifikata za IT opremu 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, kreiraju se zapisi o registraciji;
- ukoliko se radi o zahtjevu za osobnim nekvalificiranim certifikatom, službenik u FINA RA mreži provjerava je li podnositelj zahtjeva već registriran. Ako zapis o registraciji podnositelja ne postoji u FINA RA sustavu, kreiraju se zapisi o registraciji;
- službenik u FINA RA mreži odobrava zahtjev. 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 se može 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.

4.3. Izdavanje certifikata

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

4.3.1. Radnje FINA CA tijekom izdavanja certifikata

4.3.1.1. Radnje FINA CA tijekom izdavanja NCP+ certifikata

Generiranje korisničkih ključeva za pojedine tipove NCP+ certifikata tijekom njihova izdavanja provodi se u skladu s točkom 6.1.1.3., 6.1.1.6., odnosno 6.1.1.7. ovog CPS_{NQC} dokumenta.

Za tipove certifikate iz točke 6.1.1.3. stavak a) provode se postupci opisani niže u stavkama a) i b). Za Administrativni N2 certifikat (NCP+) tip certifikata provodi se samo postupak naveden niže u stavci a).

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

- po primitku narudžbe za izdavanje certifikata iz RA aplikacije FINA CA za svaki registrirani SSCD uređaj generira i enkriptira zaseban PIN;
- FINA CA generira 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 CA upisuje certifikat u odgovarajući SSCD uređaj;
- SSCD uređaj s pripadajućim parom ključeva i certifikatom FINA CA prosljeđuje sigurnom dostavom u RA mrežu;
- FINA RA ovlaštena osoba potpisniku dostavlja enkriptirani PIN SSCD uređaja putem e-mail poruke ili ga uručuje pri neposrednoj identifikaciji;

b) Ključevi se na SSCD uređaju generiraju na korisničkoj lokaciji

Ukoliko se ključevi na SSCD uređaju generiraju pod nadzorom FINA CA primjenjuje se sljedeći postupak:

- po primitku narudžbe za izdavanje certifikata iz RA aplikacije, FINA CA za svaki registrirani SSCD uređaj generira i enkriptira zaseban PIN;
- FINA CA putem e-mail poruke potpisniku dostavlja enkriptirani PIN;

- po iniciranju postupka certificiranja od strane potpisnika na udaljenoj korisničkoj lokaciji prijavom na FINA CMS, inicira se postupak generiranja korisničkih ključeva u potpisnikovom SSCD uređaju;
- FINA CMS 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 prosljeđuje ga u CMS sustav;
- FINA CMS 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 autentifikacijski N2 certifikat (NCP+) 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 da li je 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 tipove NCP+ certifikata iz točke 6.1.1.3. stavak b), c) i d) te iz točke 6.1.1.6. ovog CPS_{NQC} dokumenta, uz korištenje FININOG alternativnog web servisa za preuzimanje certifikata, koristi se sljedeći postupak:

- po primitku narudžbe FINA CA kreira referentni broj i autorizacijski kod za subjekt certificiranja kojim se skrbniku omogućuje udaljeno preuzimanje certifikata;
- ukoliko je skrbnik već neposredno identificiran, FINA CA skrbniku šalje autorizacijski kod i referentni broj za jednokratnu prijavu na alternativni web servis, na način da se jedan od podataka skrbniku šalje SMS porukom, a drugi elektroničkom poštom na e-mail adresu skrbnika;
- ukoliko skrbnik nije prethodno neposredno identificiran, FINA CA službeniku u RA mreži dostavlja referentni broj i autorizacijski kod.
- službenik u RA mreži skrbniku osobno, uz neposrednu identifikaciju, uručuje navedene podatke za prijavu;

- po prijavi skrbnika na alternativni web servis za preuzimanje certifikata, skrbnik prosljeđuje zahtjev u PKCS#10 formatu u FINA CA;
- FINA CA provjerava valjanost PKCS#10 zahtjeva;
- ukoliko se pri provjeri javlja greška, FINA CA obavještava skrbnika o grešci;
- FINA CA certificira javni ključ izdajući korisniku certifikat odgovarajućeg profila;
- FINA CA omogućuje skrbniku preuzimanje izdanog certifikata putem web servisa.

4.3.1.2. Radnje FINA CA tijekom izdavanja NCP i LCP certifikata

Tijekom izdavanja NCP, odnosno LCP certifikata, generiranje ključeva korisnika provodi se za pojedine tipove certifikata u skladu s točkom 6.1.1.4., odnosno 6.1.1.5. ovog CPS_{NQC} dokumenta.

Za tipove certifikate iz točke 6.1.1.4. stavak a), stavak e) i točke 6.1.1.5. koristi se sljedeći postupak:

- po primitku narudžbe za izdavanje certifikata iz RA aplikacije FINA CA generira autentifikacijske podatke za prijavu na FINA CMS;
- FINA CA sustav putem e-mail i SMS poruke potpisniku, odnosno skrbniku, dostavlja autentifikacijske podatke;
- po iniciranju postupka certificiranja od strane potpisnika, odnosno skrbnika, FINA CMS generira korisničke ključeve na lokaciji FINA CA;
- FINA CMS pripadajući javni ključ šalje u formatu PKCS#10 zahtjeva u FINA CA na postupak izdavanja certifikata;
- FINA CA certificira javni ključ izdajući potpisniku, odnosno skrbniku, certifikat odgovarajućeg profila;
- FINA CA izrađuje PKCS#12 datoteku koja sadrži potpisnikov privatni ključ i certifikat. Potpisnik u FINA CMS upisuje aktivacijski podatak kojim se zaštićuje PKCS#12 datoteka;
- potpisnik kroz FINA CMS preuzima zaštićenu PKCS#12 datoteku i sprema u softverski spremnik ključeva i certifikata na svom uređaju.

Za tipove certifikate iz točke 6.1.1.4. stavak b), c) i d) uz korištenje FININOG alternativnog web servisa za preuzimanje certifikata, koristi se sljedeći postupak:

- po primitku narudžbe za izdavanje certifikata iz RA aplikacije FINA CA kreira referentni broj i autorizacijski kod subjekta certificiranja kojim se omogućuje skrbniku udaljeno preuzimanje certifikata;
- ukoliko je skrbnik u obrascu zahtjeva za izdavanje certifikata upisao broj mobitela i e-mail adresu i neposredno je identificiran, FINA CA skrbniku šalje autorizacijski kod i referentni broj za jednokratnu prijavu na alternativni web servis, na način da se jedan od podataka šalje skrbniku SMS porukom, a drugi elektroničkom poštom na e-mail adresu skrbnika;
- ukoliko skrbnik u obrascu zahtjeva za izdavanje certifikata nije upisao broj mobitela i e-mail adresu FINA CA službenika u RA mreži dostavlja referentni broj i autorizacijski kod;

- službenik u RA mreži skrbniku osobno, uz neposrednu identifikaciju, uručuju navedene podatke za prijavu;
- po prijavi skrbnika na alternativni web servis za preuzimanje certifikata, skrbnik prosljeđuje zahtjev u PKCS#10 formatu u FINA CA;
- FINA CA provjerava valjanost PKCS#10 zahtjeva;
- ukoliko se pri provjeri javlja greška, FINA CA obavještava skrbnika o grešci;
- FINA CA certificira javni ključ izdajući korisniku certifikat odgovarajućeg profila;
- FINA CA omogućuje skrbniku preuzimanje izdanog certifikata putem web servisa.

4.3.2. Obavještavanje korisnika od strane CA o izdavanju certifikata

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

Ukoliko potpisnik, odnosno skrbnik, preuzima certifikat *on-line*, tada je isti obaviješten o izdavanju certifikata od strane FINA CA u tijeku samog *on-line* preuzimanja certifikata.

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

4.4. Prihvaćanje certifikata

4.4.1. Provedba prihvaćanja certifikata

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

- u registracijskom uredu RA mreže, zajedno s generiranim korisničkim ključevima na SSCD uređaju;
- *on-line* kroz FINA CMS;
- *on-line* kroz CMS sustav vanjskog RA;
- *on-line* putem FININOG alternativnog web servisa.

Potpisnik, odnosno skrbnik, dužan je tijekom ili neposredno po obavljenom preuzimanju certifikata provesti provjeru sadržaja certifikata sukladno uputama dobivenim od FINA CA. Ukoliko ne prihvaća bilo koji dio sadržaja certifikata, potpisnik, odnosno skrbnik, treba odbiti prihvaćanje certifikata 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_{NQC} dokumenta. Ukoliko je provedena suspenzija certifikata, FINA nakon identifikacije potpisnika, odnosno skrbnika, u roku iz točke 4.9.16. i sukladno točki 4.9.3. ovog CPS_{NQC} dokumenta opoziva certifikat, te omogućava izdavanje novog certifikata s potrebnim izmjenama, a na temelju zahtjeva za izdavanje certifikata.

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

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

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

4.4.2. Objava izdanog certifikata od strane CA

Ukoliko je potpisnik, odnosno skrbnik, odobrio javnu objavu certifikata, FINA CA odmah nakon izdavanja objavljuje izdani korisnikov certifikat u javnom imeniku pripadnog repozitorija iz točke 2.2. ovog CPS_{NQC} 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, odnosno skrbnik, nije odobrio javnu objavu certifikata, isti 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 [27], potpisnik, odnosno skrbnik, se obvezuje:

- na korištenje privatnog ključa i pripadajućeg certifikata samo u svrhe propisane Općim pravilima [27];
- 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, odnosno skrbnika, štiti privatni ključ i njegove kopije (ukoliko je njihova izrada dozvoljena i moguća) 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, odnosno komponente IT opreme, izgubljen, ukraden ili postoji sumnja u bilo kakvo kompromitiranje privatnog ključa;
  - kada potpisnik, odnosno skrbnik, više nije u jedinstvenom posjedu privatnog ključa, tj. kada se sumnja u kompromitiranost aktivacijskih podataka;
  - da su podaci sadržani u certifikatu netočni.

4.5.2. Korištenje javnog ključa i certifikata od strane pouzdajuće strane

Pouzdajuća strana koja namjerava ostvariti pouzdanje u certifikat izdan od strane FINA CA treba:

- koristiti certifikat isključivo u svrhe propisane u točki 1.4. ovog CPS_{NQC} dokumenta;
- obaviti provjeru isteka certifikata;
- obaviti provjeru statusa certifikata u kojeg namjerava ostvariti pouzdanje koristeći aktualnu i provjerenu CRL listu izdanu od strane FINA CA koji je izdao certifikat;
- provesti provjeru certifikata prema postupcima za validaciju certifikacijske staze, sukladno dokumentu IETF RFC 5280 [19];
- 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 listu 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 [27], FINA CA obnovu certifikata provodi na način da se za svaki postojeći subjekt čiji je certifikat pred istekom generira novi par ključeva i izdaje novi certifikat. Postupak obnove nekvalificiranog certifikata uz generiranje novog para ključeva je detaljno opisan u točki 4.7. ovog CPS_{NQC} 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.

4.7.2. Tko može zatražiti certificiranje novog javnog ključa

Postupak obnove certifikata uz generiranje novog para ključeva može zatražiti, odnosno inicirati potpisnik, odnosno skrbnik.

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

Kod obnove certifikata, osnova za identifikaciju korisnika je postojeći certifikat. Na osnovu postojećeg certifikata i provjere njegove valjanosti, izdaje se certifikat s istim razlikovnim imenom i novim parom ključeva.

4.7.3.1. Obrada zahtjeva za obnovom NCP+ certifikata

Za tipove certifikate iz točke 6.1.1.3. stavak a) provode se postupci opisani niže u stavkama a) i b). Za Administrativni N2 certifikat (NCP+) tip certifikata provodi se samo postupak naveden niže u stavci a).

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 uz pravilnu identifikaciju sukladno točki 3.3.1.1. ovog CPS_{NQC} 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_{NQC} dokumenta;
- FINA CA obavlja izdavanje certifikata sukladno postupku opisanom u točki 4.3.1.1. stavak a) ovog CPS_{NQC} dokumenta.
- FINA CA opoziva stari certifikat.

b) Ključevi se na SSCD uređaju generiraju na korisničkoj lokaciji

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

- potpisnik se valjanim certifikatom na pripadajućem SSCD uređaju i aktivacijskim podacima spaja na FINA CMS te se ostvaruje SSL 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 kroz FINA CMS 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 potvrdi slanje zahtjeva za obnovu certifikata. Tom 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 su podaci iz zahtjeva uspješno provjereni, FINA CMS inicira generiranje novog para ključeva na korisničkom SSCD uređaju, te se PKCS#10 potpisani zahtjev s novogeneriranim javnim ključem prosljeđuje u FINA CA na certificiranje;
- ukoliko podaci iz zahtjeva nisu uspješno provjereni, FINA CMS javlja grešku, a potpisnik provodi postupak sukladno postupku za inicijalno izdavanje certifikata;
- FINA CMS pripadajući 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 prosljeđuje ga u FINA CMS;
- FINA CMS 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 autentifikacijski N2 certifikat (NCP+) primjenjuje se slijedeći postupak:

- 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 da li je 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 tipove NCP+ certifikata iz točke 6.1.1.3. stavak b), c) i d) te iz točke 6.1.1.6. ovog CPS_{NQC} dokumenta, uz korištenje FININOG alternativnog web servisa za preuzimanje certifikata, koristi se postupak identičan postupku za inicijalno izdavanje certifikata ovog tipa iz točke 4.3.1.1. ovog CPS_{NQC} dokumenta.

4.7.3.2. Obrada zahtjeva za obnovom NCP i LCP certifikata

Tijekom izdavanja NCP, odnosno LCP certifikata, generiranje ključeva korisnika provodi se za pojedine tipove certifikata u skladu s točkom 6.1.1.4., odnosno 6.1.1.5. ovog CPS_{NQC} dokumenta.

Za tipove certifikate iz točke 6.1.1.4. stavak a), stavak e) i točke 6.1.1.5. koristi se slijedeći postupak:

- potpisnik, odnosno skrbnik, se na FINA CMS prijavljuje autentifikacijskim certifikatom za kojeg namjerava pokrenuti postupak obnove te se pri tome ostvaruje SSL zaštićena komunikacija uz dvostranu autentifikaciju. Udaljenim radom kroz CMS web sučelje potpisnik, odnosno skrbnik, dobiva uvid u trenutne podatke o svojem važećem certifikatu te informacije o tome koji certifikat može obnoviti (ukoliko posjeduje više certifikata ili ukoliko je skrbnik više certifikata);
- potpisnik, odnosno skrbnik, kroz 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, odnosno skrbnik, može zahtijevati njegovu obnovu na način da kroz FINA CMS potvrdi slanje zahtjeva za obnovu certifikata. Tom se prilikom izrađeni zahtjev elektronički potpisuje trenutno važećim certifikatom, te ga FINA CMS obrađuje, provjerava i pohranjuje. Ukoliko podaci o važećem certifikatu nisu točni, potpisnik, odnosno skrbnik, je dužan obavijestiti FINA CA o izmjenama unutar certifikata;
- ukoliko su podaci iz zahtjeva uspješno provjereni FINA CMS inicira generiranje novog para ključeva, formira PKCS#10 potpisani zahtjev s novogeneriranim javnim ključem prosljeđuje u FINA CA na certificiranje;
- FINA CA certificira dostavljni javni ključ te izdani certifikat;
- FINA CA kreira PKCS#12 datoteku s privatnim ključem i pripadajućim certifikatom;
- potpisnik, odnosno skrbnik, u FINA CMS upisuje zaporku kojom se zaštićuje PKCS#12 datoteka te ju preuzima i sprema na računalo;
- FINA CA opoziva stari certifikat.

Za tipove certifikate iz točke 6.1.1.4. stavak b), c) i d) skrbnik uz korištenje FININOG alternativnog web servisa za preuzimanje certifikata provodi postupak identičan postupku za inicijalno izdavanje certifikata iz točke 4.3.1.2. ovog CPS_{NQC} dokumenta.

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, odnosno skrbnika, o skorom isteku certifikata te ga poziva na obnovu certifikata uz generiranje novog para ključeva. Potpisnicima, odnosno skrbnicima, koji su u zahtjevu za izdavanje certifikata dostavili e-mail adresu, obavijest se šalje e-mailom, a ostalim potpisnicima i skrbnicima 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 FINA CA provodi sukladno točki 4.4.1 ovog CPS_{NQC} dokumenta.

4.7.6. Objavljivanje certifikata po obnovi s generiranjem novog para ključeva

Objavljivanje certifikata po obnovi s generiranjem novog para ključeva provodi se sukladno točki 4.4.2 ovog CPS_{NQC} 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 FINA CA provodi sukladno točki ovog 4.4.3 CPS_{NQC} dokumenta.

4.8. Izmjene unutar certifikata

Potpisnici i skrbnici imaju obvezu informiranja FINA PKI o promjeni podataka koji ulaze u sadržaj certifikata u roku od dva dana kako je propisano Zakonom o elektroničkom potpisu [1] i [2] 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.

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

- naziva poslužitelja ili aplikacije;
- naziva poslovnog subjekta;
- podataka o mjestu središta poslovnog subjekta;
- e-mail adrese za certifikate koji sadrže e-mail adresu u „Subject alternative name“ ekstenziji certifikata;
- sadržaja ekstenzije certifikata.

4.8.2. Tko može zatražiti izmjene unutar certifikata

Izmjene unutar certifikata mogu zatražiti potpisnik, odnosno skrbnik.

4.8.3. Obrada zahtjeva za izmjenama unutar certifikata

Potpisnik, odnosno skrbnik, u RA mrežu podnosi zahtjev za izmjene unutar certifikata i dostavlja onaj dio dokumentacije određene u točki 3.2. ovog CPS_{NQC} 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_{NQC} dokumenta, a izdavanje novog certifikata se obavlja sukladno točkama 4.2., 4.3. i 4.4. ovog CPS_{NQC} dokumenta.

4.8.4. Obavještavanje korisnika o izdavanju izmijenjenog certifikata

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

4.8.5. Provedba prihvaćanja izmijenjenog certifikata

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

4.8.6. Objavljivanje izmijenjenog certifikata od strane CA

Objavljivanje izmijenjenog certifikata FINA CA provodi na način opisan u točki 4.4.2. ovog CPS_{NQC} 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_{NQC} dokumenta.

4.9. Opoziv i suspenzija certifikata

4.9.1. Razlozi za opoziv

FINA CA opoziva certifikate iz sljedećih razloga:

- ako neka od informacija sadržana 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;
- ako se pojavi osnovana sumnja da privatni ključ ili aktivacijski podaci nisu više u jedinstvenom posjedu potpisnika, odnosno skrbnika, ili ako dođe do otuđenja privatnog ključa ili aktivacijskih podataka;
- ako prestane odnos koji je bio razlog da se potpisniku izda certifikat kojim će kao pripadajuća osoba djelovati u ime fizičke ili pravne osobe;
- ako korisnik iz bilo kojeg razloga nema više potrebu koristiti certifikat izdan za IT opremu, aplikacije, potpis koda ili vremenski žig;
- ako FINA CA smatra da certifikat nije izdan sukladno zahtjevu ili navodima iz ovog CPS_{NQC} dokumenta;
- u slučaju raskida ugovora o obavljanju usluge certificiranja, od strane korisnika.

Ako korisnik, potpisnik ili skrbnik ne izvršava svoje obveze u skladu s ovim CPS_{NQC} dokumentom i potpisanim ugovorima, FINA CA opoziva certifikat prema nalogu voditelja Centra elektroničkog poslovanja ili prema nalogu FINA PMA.

4.9.2. Tko može tražiti opoziv

Potpisnici podnose zahtjev za opoziv pripadajućih certifikata.

Skrbnici podnose zahtjev za opoziv certifikata o kojima skrbe.

Osoba ovlaštena za zastupanje poslovnog subjekta može podnijeti zahtjeva za opoziv certifikata pripadajuće osobe i ostalih certifikata izdanih na temelju zahtjeva poslovnog subjekta.

Službenik u RA mreži može uputiti zahtjev za opoziv certifikata kojeg je podnio korisnik, potpisnik ili skrbnik, ili u ime RA mreže. Zahtjev za opoziv certifikata koji je podnesen u ime RA autorizira voditelj Centra elektroničkog poslovanja ili FINA PMA.

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, skrbnika te, ukoliko je to primjenjivo, i korisnika. Potpisnicima, odnosno skrbnicima, te korisnicima koji su u zahtjevu za izdavanje certifikata dostavili e-mail adresu, obavijest se šalje e-mailom, a ostalim potpisnicima, skrbnicima 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 ili reaktivaciju certifikata dostupan na web stranicama FINA PKI repozitorija iz točke 2.2. ovog CPS_{NQC} dokumenta. Navedeni zahtjev treba odmah po nastupanju razloga za opoziv, koji su navedeni u točki 4.9.1. ovog CPS_{NQC} dokumenta, točno i cjelovito ispuniti, potpisati i u najkraćem roku dostaviti u FINA PKI na jedan od slijedećih načina:

- osobnom dostavom u RA mrežu u uredovno vrijeme:

  Popunjen i ručno potpisan Zahtjev za opoziv, suspenziju ili reaktivaciju certifikata, uz neposrednu identifikaciju podnositelja prema postupku opisanom u točki 3.4. ovog CPS_{NQC} dokumenta predaje se službeniku u RA mreži.

- dostavom elektroničkom poštom direktno na FINA CA:

  Popunjen i potpisan naprednim elektroničkim potpisom podnositelja Zahtjev za opoziv, suspenziju ili reaktivaciju certifikata dostavlja se elektroničkom poštom na adresu info.rdc@fina.hr. Ukoliko podnositelj potpisuje zahtjev s 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_{NQC} dokumenta, ukoliko zahtjev ima dovoljno podataka za provođenje suspenzije.

- telefonskim pozivom na FININ Centar za odnose s korisnicima:

  Podnositelj zahtjeva navodi sljedeće podatke za specificiranje certifikata za opoziv:

  - serijski broj certifikata; ili
  - ime i prezime potpisnika i serijski broj (ukoliko postoji u DN-u certifikata); ili

- ime aplikacije ili FQDN poslužitelja, naziv poslovnog subjekta u slučaju da se podnosi zahtjev za opoziv poslovnog certifikata ili poslovnog certifikata za IT opremu.

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 Centra 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 opoziv.

Ukoliko je telefonski zahtjev za opoziv certifikata zaprimljen u uredovno vrijeme FINA CA, Centara za odnose s korisnicima po provjeri podataka zahtjev za suspenzijom prosljeđuje u FINA CA. FINA CA provodi suspenziju certifikata sukladno točki 4.9.15. ovog CPS_{NQC} dokumenta.

Ukoliko je telefonski zahtjev za opoziv certifikata zaprimljen izvan uredovnog vremena FINA CA, Centara za odnose s korisnicima po provjeri podataka provodi suspenziju certifikata sukladno točki 4.9.15. ovog CPS_{NQC} dokumenta.

Po primitku i provjeri telefonskog zahtjeva certifikat za koji se traži opoziv se samo suspendira sukladno točki 4.9.15. ovog CPS_{NQC} dokumenta. Opoziv certifikata će se provesti tek nakon dostave točno ispunjenog i potpisanog zahtjeva za opoziv u obliku obrasca i identifikacije podnositelja zahtjeva, bilo fizički sukladno točki 3.4. ovog CPS_{NQC} dokumenta, bilo posredno identifikacijom podnositelja temeljem valjanog certifikata.

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. ovog CPS_{NQC} dokumenta;
- ukoliko provjera podnositelja nije uspješna službenik u RA mreži mora odbiti zahtjev za opoziv certifikata;
- službenik u RA mreži izrađuje zahtjev za opozivom kroz RA aplikaciju i 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 RA opoziva certifikat izmjenom njegova statusa i objavom nove CRL liste u kojoj je sadržana informacija o opozvanosti certifikata;
- FINA CA o obavljenom opozivu obavještava potpisnika, skrbnika 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 sljedeći postupak:

- ovlaštena osoba FINA CA ili Središnjeg 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 listu 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_{NQC} 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, skrbnika i 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_{NQC} dokumenta trebaju u najkraćem razumnom roku od nastanka razloga za opoziv navedenih u točki 4.9.1. ovog CPS_{NQC} 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_{NQC} dokumenta.

Neposredno nakon opoziva certifikata, FINA CA mijenja status certifikata te izdaje i objavljuje novu CRL listu. 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_{NQC} 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 liste

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

CRL listu izdaje i odmah objavljuje pripadni FINA CA najmanje jedanput u roku od 24 sata od vremena izdavanja zadnje aktualne, još važeće CRL liste.

4.9.8. Maksimalno kašnjenje za CRL listu

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

4.9.9. On-line dostupnost provjere opozvanih certifikata/statusa certifikata

CRL lista 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_{NQC} dokumenta. Podaci o pristupnim točkama za dohvat CRL liste sadržani su u svakom izdanom certifikatu.

4.9.10. Zahtjevi na On-line provjeru opozvanih certifikata

Za *on-line* preuzimanje CRL liste, pouzdajuće strane moraju imati pristup internetu te koristiti web preglednike ili aplikacije koje su u mogućnosti preuzeti CRL liste s internetskih adresa i protokolima navedenim u točki 4.10.1. ovog CPS_{NQC} 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 certifikata

FINA CA suspendira certifikat u slučajevima:

- kada korisnik, potpisnik ili skrbnik radi sumnji navedenih u točki 4.9.1 CPS_{NQC} 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 CPS_{NQC} dokumenta, a za vrijeme dok FINA CA ili RA mreža provode sve potrebne provjere nužne za opoziv certifikata.

4.9.14. Tko može tražiti suspenziju certifikata

Potpisnici podnose zahtjev za suspenziju pripadajućih certifikata.

Skrbnici podnose zahtjev za suspenziju certifikata o kojima skrbe.

Osoba ovlaštena za zastupanje poslovnog subjekta može podnijeti zahtjeva za suspenziju certifikata pripadajuće osobe i ostalih certifikata izdanih na temelju zahtjeva poslovnog subjekta.

Službenik u RA mreži može podnijeti zahtjev za suspenziju certifikata kojeg je podnio korisnik, potpisnik ili skrbnik, 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, skrbnika te, ukoliko je to primjenjivo, i korisnika. Potpisnicima, odnosno skrbnicima te korisnicima koji su u zahtjevu za izdavanje certifikata dostavili e-mail adresu, obavijest se šalje e-mailom, a ostalim potpisnicima, skrbnicima i korisnicima obavijest se šalje poštom.

4.9.15. Procedura za zahtjev za suspenziju certifikata

Zahtjev za suspenziju certifikata je u obliku obrasca Zahtjev za opoziv, suspenziju ili reaktivaciju certifikata dostupan na internetskim stranicama FINA PKI repozitorija iz točke 2.2. ovog CPS_{NQC} dokumenta. Zahtjev treba odmah po nastupanju razloga za suspenziju koji su opisani u točki 4.9.13. ovog CPS_{NQC} dokumenta, točno i cjelovito ispuniti, potpisati i u najkraćem uredovnom roku dostaviti u FINA PKI na jedan od slijedećih načina:

- Osobnom dostavom u RA mrežu u uredovno vrijeme:

  Popunjen i ručno potpisan Zahtjev za opoziv, suspenziju ili reaktivaciju certifikata, uz neposrednu identifikaciju podnositelja prema postupku opisanom u točki 3.4. ovog CPS_{NQC} dokumenta predaje se službeniku 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) ili ime aplikacije ili FQDN poslužitelja, naziv poslovnog subjekta u slučaju da se traži opoziv 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 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 listi 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.

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. ovog CPS_{NQC} dokumenta;
- ukoliko provjera podnositelja nije uspješna RA/LRA službenik mora odbiti zahtjev za suspenziju certifikata;
- službenik u RA mreži izrađuje zahtjev za suspenziju kroz RA aplikaciju i prosljeđuje u FINA CA na postupak suspenzije.

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

- FINA CA ili Središnji RA suspendira certifikat izmjenom njegova statusa i objavom nove CRL liste u kojoj je sadržana informacija o suspendiranosti certifikata;
- FINA CA o obavljenoj suspenziji obavještava potpisnika i osobu ovlaštenu za zastupanje ukoliko je to primjenjivo.

Po suspenziji certifikata korisnik, potpisnik ili skrbnik može tražiti opoziv ili reaktivaciju certifikata.

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

Za reaktivaciju certifikata korisnik, potpisnik ili skrbnik treba popuniti Zahtjev za opoziv, suspenziju ili reaktivaciju certifikata i u zahtjevu označavaju reaktivaciju certifikata. Popunjen i ručno potpisan i ovjeren zahtjev, uz neposrednu identifikaciju podnositelja zahtjeva na osnovi prihvatljive identifikacijske isprave iz točke 3.2.3.1. ovog CPS_{NQC} dokumenta. službenik u RA mreži provjerava i prosljeđuje u odgovarajući FINA CA.

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

- 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. CPS_{NQC} dokumenta;
- ukoliko provjera podnositelja nije uspješna službenik u RA mreži mora odbiti zahtjev za reaktivaciju certifikata;
- službenik u RA mreži izrađuje zahtjev za reaktivaciju kroz RA aplikaciju i prosljeđuje u FINA CA na postupak reaktivacije.

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. U protivnom, službenik u RA mreži podnosi zahtjev za opozivom certifikata, a korisnik, odnosno potpisnik ili skrbnik mogu zatražiti izdavanje novog certifikata po obavljenom opozivu.

Zahtjev za reaktivaciju se može odbiti zbog:

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

Postupak FINA CA pri zaprimanju zahtjeva za reaktivacijom certifikata:

- FINA CA ili Središnji FINA RA reaktivira certifikat izmjenom njegova statusa i objavom nove CRL liste iz koje je brisana informacija o suspendiranosti certifikata;

- FINA CA o obavljenoj reaktivaciji obavještava potpisnika, skrbnika i osobu ovlaštenu za zastupanje ukoliko je to primjenjivo.

4.9.16. Ograničenje na trajanje suspenzije

Ukoliko certifikat ostane u stanju „suspendiran“ dulje od 60 dana, FINA CA opoziva certifikat i objavljuje CRL listu te korisnika obavještava o opozivu certifikata.

4.10. Usluge statusa Certifikata

4.10.1. Operativna svojstva

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 lista, a na web poslužitelju objavljuje se objedinjena CRL lista. Adrese objave CRL liste sadržane su u ekstenziji *CRLDistributionPoints* u svakom izdanom certifikatu i upisane su sljedećim redoslijedom:

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

Navedeni redoslijed označava redoslijed kojim pouzdajuća strana treba dohvaćati CRL listu:

1. ukoliko aplikacija pouzdajuće strane podržava rad sa segmentiranom CRL listom, aplikacija s javnog imenika dohvaća određeni segment segmentirane CRL liste;
2. ukoliko aplikacija pouzdajuće strane podržava rada s objedinjenom CRL listom, s javnog imenika dohvaća objedinjenu CRL listu;
3. ukoliko je javni imenik nedostupan aplikacija pouzdajuće strane objedinjenu CRL listu dohvaća s web poslužitelja.

4.10.1.1. Adrese za dohvat CRL liste FINA RDC certifikata

FINA RDC CA izdaje CRL listu te je objavljuje na sljedećim internetskim adresama:

Adresa segmentirane CRL liste FINA RDC certifikata na javnom imeniku je:

ldap://rdc-ldap.fina.hr/cn=CRL*x*,ou=RDC,o=FINA,c=HR?certificateRevocationList%3Bbinary
Oznaka x u cn=CRLx označava segment CRL liste.

Adresa objedinjene CRL liste FINA RDC certifikata na javnom imeniku je:

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

Adresa objedinjene CRL liste FINA RDC certifikata na web poslužitelju je:

http://rdc.fina.hr/crls/rdc.crl

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

4.10.1.2. Adrese za dohvat CRL liste FINA RDC-TDU certifikata

FINA RDC-TDU CA izdaje CRL listu te je objavljuje na sljedećim internetskim adresama:

Adresa Segmentirane CRL liste FINA RDC-TDU certifikata na javnom imeniku je:

ldap://rdc-tdu-ldap.fina.hr/cn=CRLx,ou=RDC-TDU,o=FINA,c=HR?certificateRevocationList%3Bbinary
Oznaka x u cn=CRLx označava segment CRL liste.

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

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

Adresa objedinjene CRL liste FINA RDC-TDU certifikata na internetskom poslužitelju je:

http://rdc-tdu.fina.hr/crls/rdc-tdu.crl

Na internetskoj stranici http://rdc-tdu.fina.hr CRL listu je moguće dohvatiti u DER, PEM i tekstualnom formatu.

4.10.2. Dostupnost usluga

Dostupnost CRL listi 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 raskinuti ugovor o obavljanju usluga certificiranja, mora prema RA mreži uputiti zahtjev za raskid ugovora o obavljanju usluga certificiranja.

Korisnik može otkazati ugovor u pisanom obliku bez obrazloženja.

FINA će otkazati ugovor u slučaju kad:

- poslovni subjekt, potpisnik ili skrbnik ne ispunjavaju uvjete koji su navedeni u Općim pravilima [27] i Uvjetima pružanja usluga certificiranja, ili

- poslovni subjekt, potpisnik ili skrbnik 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_{NQC} dokumenta. Adresa davatelja usluga certificiranja navedena je u točki 9.11. ovog CPS_{NQC} dokumenta.

Nakon raskida ugovora FINA CA će opozvati sve certifikate na koje se odnosi taj ugovor.

4.12. Sigurno skladištenje i oporavak privatnog ključa

Sigurno skladištenje korisničkih privatnih ključeva FINA CA provodi samo za NCP i LCP certifikate standardne razine sigurnosti koji se preuzimaju uporabom FINA CMS sustava i spremaju u softverski spremnik ključa.

4.12.1. Pravila i prakse sigurnog skladištenja i povrata privatnog ključa

Postupak sigurnog skladištenja privatnih ključeva je propisan na slijedeći način:

- FINA CMS generira korisnički par ključeva te javni ključ prosljeđuje u FINA CA na certificiranje;
- po primitku certifikata, FINA CMS kreira PKCS#12 datoteku koju korisnik može preuzeti;
- na početku procesa preuzimanja PKCS#12 datoteke, potpisnik, odnosno skrbnik, koristi tajni podatak uz pomoć kojeg se enkriptira sadržaj PKCS#12 datoteke na način da je ona čitljiva isključivo potpisniku, odnosno skrbniku;
- FINA CMS uništava čitljivi oblik korisničkog privatnog ključa na način koji onemogućava oporavak istog, a enkriptiranu PKCS#12 datoteku pohranjuje.

Oporavak ovako čuvane PKCS#12 datoteke s privatnim ključem je moguć samo od strane potpisnika, odnosno skrbnika, jer je za dekripciju privatnog ključa nužan tajni podatak koji je poznat samo potpisniku, odnosno skrbniku. Potpisnik, odnosno skrbnik, može pristupiti preuzimanju enkriptirane PKCS#12 datoteke isključivo nakon dvofaktorske autentifikacije na FINA CMS.

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 nekvalificirane i kvalificirane certifikate te vremenski žig primjenjuje adekvatne mjere fizičke zaštite sustava certificiranja. Mjere fizičke zaštite za izdavanje nekvalificiranih certifikata i vremenskog žiga jednake su mjerama fizičke zaštite koje su propisane za izdavanje kvalificiranih certifikata. Ove mjere zaštite imaju jednu od ključnih uloga u ostvarivanju povjerenja u izdane nekvalificirane certifikate i vremenske žigove FINE.

U ovom poglavlju prikazan je opis sustava fizičke zaštite koji se provodi u FINA PKI sustavu. Detaljniji opis sustava fizičke zaštite uređaja, opreme i podataka koji se upotrebljavaju u FINA PKI sustavu nalazi se u internim FININIM dokumentima.

5.1. Kontrole fizičke sigurnosti

FINA kao davatelj usluga certificiranja koji izdaje nekvalificirane certifikate i vremenski žigove primjenjuje mjere fizičke zaštite sustava u skladu s poslovnom politikom FINE, važećom zakonskom regulativom i međunarodnim preporukama.

FINA primjenjuje mjere fizičke zaštite sustava certificiranja 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_{NQC} dokumenta.

5.1.1. Lokacija objekta i njegova konstrukcija

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

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

5.1.2. Fizički pristup

Fizički pristup FINA CA sustavu, FINA TSA sustavu, FINA RA sustavu, repozitoriju i arhivi omogućen je isključivo ovlaštenim zaposlenicima FINE u skladu s njihovim povjerljivim ulogama i ovlastima.

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

Fizički pristup podacima koje prikuplja RA mreža imaju samo ovlašteni zaposlenici 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 certificiranja 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 certificiranja do ponovne uspostave primarnog napajanja.

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

5.1.4. Opasnost od poplave

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

5.1.5. Protupožarna zaštita

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

5.1.6. Pohrana medija

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

5.1.7. Zbrinjavanje otpada

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

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

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

5.1.8. Sigurnosne kopije na drugoj lokaciji

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

5.2. Kontrola procedura

5.2.1. Povjerljive uloge

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

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

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

5.2.2. Broj osoba potrebnih za obavljanje zadataka

Poslove u FINA PKI obavljaju isključivo ovlaštene osobe. FINA ima stalno zaposlen dovoljan broj stručnih osoba sa znanjem, iskustvom i kvalifikacijama koji je potreban u FINA PKI za davanja usluga iz opsega ovog CPS_{NQC} dokumenta.

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

5.2.3. Identifikacija i potvrđivanje identiteta za svaku ulogu

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

5.2.4. Uloge koje zahtijevaju odvajanje dužnosti

Zbog sigurnosnih zahtjeva u FINA PKI potrebno je odvajanje sljedećih dužnosti:

- Službenik za sigurnost ili RA službenik ne smiju obavljati poslove službenika za nadzor sustava;

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

5.3. Provjere osoblja

5.3.1. Kvalifikacije, radno iskustvo i zahtjevi za provjerom osoblja

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

5.3.2. Procedure provjere primjerenosti osoblja

Prije početka rada na poslovima FINA PKI, FINA provodi odgovarajuće provjere kandidata da bi procijenila njihovu sposobnost i pouzdanost u skladu sa 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 davanja usluga certificiranja [27], ovom CPS_{NQC} 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 bit će zabranjen rad na poslovima u FINA PKI.

5.3.7. Zahtjevi na 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 bilježe 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;
- izdavanje vremenskih žigova;
- 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 zaštićuju se mehanizmima i postupcima koji osiguravaju povjerljivost i cjelovitost dnevnika. Novi zapisi dnevnika vjerodostojnih sustava ne smiju se automatski zapisivati preko postojećih zapisa.

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

5.4.5. Postupci izrade sigurnosnih kopija dnevnika sustava

Novonastali dnevnici FINA PKI sustava se kopiraju te se njihove kopije pohranjuju na drugu lokaciju izdvojenu 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 koji je kombinacija 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;
- 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 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, FINA TSA 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, odnosno para potpisnih ključeva FINA TSU za FINA TSA provodi se pravovremeno prije isteka perioda valjanosti FINA CA, odnosno FINA TSA certifikata.

FINA CA, odnosno FINA TSU par potpisnih ključeva mora biti generiran na način opisan u točki 6.1 ovog CPS_{NQC} dokumenta.

Novi verifikacijski/root (samo-potpisani) certifikat FINA CA s novo-generiranim javnim ključem može se potpisati i postojećim privatnim ključem FINA CA koji će biti zamijenjen novo-generiranim javnim ključem.

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_{NQC} dokumenta). Novi FINA CA root certifikat dostupan je sudionicima FINA PKI putem javnog imenika i internetskih stranica pripadnog repozitorija iz točke 2.2. ovog CPS_{NQC} dokumenta.

Novi FINA CA root 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_{NQC} dokumenta.

Javni ključ TSU za provjeru potpisa vremenskog žiga FINA TSA nalazi se u certifikatu „SERVIS VREMENSKE OVJERE TSA1“ koji je objavljen na LDAP imeničkom poslužitelju rdc-ldap.fina.hr te na internetskim stranicama http://tsa.fina.hr.

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, odnosno privatnog FINA TSU ključa za FINA TSA, te u slučaju hardverskih i softverskih kvarova i grešaka na kritičnim komponentama FINA CA, odnosno FINA TSA sustava.

Internim planovima obuhvaćeni su postupci očuvanja i oporavka sustava za slučaj povrede pravila pristupa FINA CA, odnosno FINA TSA 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 nepogode.

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 kompromitiranosti ili sumnje u kompromitiranost FINA CA privatnog potpisnog ključa, FINA CA će o tome obavijestiti FINA PMA. FINA, kao davatelj usluga certificiranja, će:

- obavijestiti FINA RA/LRA i vanjske ugovorene RA;
- zaustaviti izdavanje certifikata od strane FINA CA;
- opozvati sve certifikate izdane uporabom toga ključa;
- obavijestiti svakog korisnika i sve poslovne subjekte s kojima ima sklopljen ugovor o obavljanju usluga certificiranja ili je u poslovnom odnosu te će na internetskoj stranici repozitorija kompromitiranog FINA CA (vidi točke 2.2.1. i 2.2.2. ovog CPS_{NQC} dokumenta) objaviti obavijest za pouzdajuće strane da se certifikati i informacije o statusu opozvanosti certifikata izdanih od FINA CA, čiji je privatni ključ kompromitiran ili se sumnja u njegovu kompromitiranost, više ne mogu smatrati valjanim;
- ustanoviti uzroke koji su prouzročili kompromitiranost FINA CA privatnog potpisnog ključa;
- generirati novi par FINA CA potpisnih ključeva;
- izdati novi FINA CA root certifikat;
- objaviti serijski broj kompromitiranog FINA CA certifikata u CRL koja će biti potpisana s novim FINA CA privatnim potpisnim ključem;
- omogućiti dostavu novog FINA CA root certifikata potpisnicima, skrbnicima i pouzdajućim stranama sukladno točki 6.1.4. ovog CPS_{NQC} dokumenta;
- započeti s izdavanjem certifikata potpisujući ih s novim FINA CA privatnim potpisnim ključem te ponovno izdati certifikate svim subjektima i osigurati da su sve CRL liste potpisane uporabom novog ključa.

U slučaju kompromitiranja ili sumnje u kompromitiranost FINA TSA privatnog potpisnog ključa, FINA CA će o tome obavijestiti FINA PMA. FINA, kao davatelj usluga certificiranja koji izdaje vremenski žig, će:

- zaustaviti izdavanje vremenskih žigova;

- obavijestiti FINA RA/LRA i vanjske ugovorene RA;
- provesti korake potrebne za opoziv FINA TSA certifikata;
- obavijestiti svakog korisnika i sve poslovne subjekte s kojima ima sklopljen ugovoru o pružanju usluge izdavanja vremenskog žiga te će na internetskoj stranici FINA TSA (vidi točku 2.1.2. dokumenta Opća pravila davanja usluga izdavanja vremenskog žiga [28]) objaviti obavijest za pouzdajuće strane da se certifikat više ne može smatrati valjanim;
- ustanoviti uzroke koji su prouzročili kompromitiranost FINA TSA privatnog potpisnog ključa;
- generirati novi par FINA TSA potpisnih ključeva;
- provesti korake potrebne za izdavanje novog FINA TSA certifikata;
- ponovno pokrenuti izdavanje vremenskih žigova potpisujući ih s novim FINA TSA potpisnih ključem.

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

- obavijestiti svakog korisnika i sve poslovne subjekte s kojima ima sklopljen ugovor o obavljanju predmetnih usluga ili je u poslovnom odnosu te će na internetskoj stranici repozitorija FINA CA (vidi točke 2.2.1. i 2.2.2. ovog CPS_{NQC} dokumenta), odnosno na internetskoj stranici FINA TSA (vidi točku 2.1.2. dokumenta Opća pravila davanja usluga izdavanja vremenskog žiga [28]) 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 određene su međusobnim ugovornim obvezama.

U slučaju prestanka rada FINA RA mreže FINA može drugoj pravnoj osobi ugovorom povjeriti obavljanje poslova registracije korisnika.

U slučaju prestanka obavljanja usluga certificiranja za pojedini FINA CA, odnosno FINA TSA 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, odnosno FINA TSA te Ministarstvo gospodarstva,

najmanje tri mjeseca prije prestanka obavljanja usluga certificiranja FINA CA, odnosno FINA TSA;

- o mogućem prestanku rada pojedinog FINA CA, odnosno FINA TSA, na internetskoj stranici repozitorija FINA CA koji prestaje s radom (vidi točke 2.2.1. i 2.2.2. ovog CPS_{NQC} dokumenta), odnosno na internetskoj stranici FINA TSA repozitorija (vidi točku 2.2.3. ovog CPS_{NQC} dokumenta), objaviti obavijest za pouzdajuće strane najmanje tri mjeseca prije prestanka obavljanja usluga certificiranja od strane FINA CA, odnosno FINA TSA;
- osigurati kod drugog davatelja usluga certificiranja nastavak obavljanja usluga certificiranja za korisnike kojima je FINA CA izdao nekvalificirane 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 nekvalificirane certifikate te o tome odmah obavijestiti Ministarstvo gospodarstva;
- osigurati kod drugog davatelja usluga izdavanja vremenskog žiga nastavak obavljanja usluga za korisnike s kojima je sklopljen ugovor o pružanju usluge izdavanja vremenskog žiga ukoliko postoji davatelj takve usluge iste kvalitete usluge kao FINA TSA te će o tome odmah obavijestiti Ministarstvo gospodarstva;
- osigurati ili prenijeti drugom pouzdanom poslovnom subjektu obvezu održavanja dostupnosti FINA TSA certifikata s javnim ključem pouzdajućim stranama u razumnom vremenskom periodu;
- dostaviti svu dokumentaciju u svezi s obavljanjem usluga certificiranja drugom davatelju usluga na kojega prenosi obveze s osnove obavljanja usluga certificiranja za FINA CA odnosno FINA TSA koji prestaje s radom, odnosno Ministarstvu gospodarstva, ukoliko nema drugog davatelja usluga;
- nastaviti održavati prikupljene podatke korisnika kojima je FINA CA izdao nekvalificirane certifikate, a koji su prikupljeni u postupku registracije, pružanje informacija o statusu opozvanosti izdanih certifikata te arhiviranje dnevnika sustava vezanih uz događaje okruženja povjerljivog sustava, događaje upravljanja ključevima i certifikatima u vremenskom periodu koji je naveden u točki 5.5.2. ovog CPS_{NQC} 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_{NQC} dokumenta za FINA CA, odnosno FINA TSA, koji prestaje s radom u vremenskom periodu koji je naveden u točki 5.5.2. ovog CPS_{NQC} dokumenta ili će s drugim poslovnim subjektom ugovoriti održavanje istih;
- ukinuti sva ovlaštenja eventualno podugovorenim poslovnim subjektima koji u ime FINA CA, odnosno FINA TSA, sudjeluju u bilo kojem dijelu procesa davanja usluga certificiranja;
- za FINA CA koji prestaje s radom uništiti pripadne privatne potpisne ključeve i sve njihove kopije;
- za FINA TSA provesti korake potrebne za opoziv FINA TSU certifikata te uništiti privatne TSU 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 CA ključeva kojoj prisustvuju za to ovlaštene osobe uz nadzor FINA PMA. FINA CA par ključeva generira se na siguran način unutar HSM modula u svojem štićenom prostoru na IT sastavu namijenjenom samo za usluge certificiranja. O provedenom generiranju ključeva vodi se zapisnik s priloženim dnevnicima sustava.

6.1.1.2. Generiranje para RA ključeva

Ovlaštene osobe u FINA RA mreži koriste Poslovni autentifikacijski N2 certifikat (NCP+). Generiranje para ključeva za ovaj tip certifikata opisano je u točki 6.1.1.3. ovog CPS_{NQC} 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 NCP+ certifikate korisnika

a) Osobni i poslovni NCP+ certifikati

Ovaj postupak se primjenjuje za sljedeće tipove certifikata:

- Osobni autentifikacijski N2 certifikat (NCP+);
- Osobni autentifikacijski Win2 certifikat (NCP+);
- Poslovni autentifikacijski N2 certifikat (NCP+);
- Poslovni autentifikacijski Win2 certifikat (NCP+); i
- TDU autentifikacijski N2 certifikat (NCP+).

Parovi ključeva za NCP+ osobne i poslovne certifikate korisnika se generiraju na SSCD uređajima. Parove ključeva generiraju ovlaštene osobe FINA CA, sukladno točki 5.2.2. ovog CPS_{NQC} dokumenta, ili svoj par ključeva generira potpisnik.

Ukoliko FINA CA generira korisnički par ključeva, ključevi se na SSCD uređaju generiraju FINA PKI štićenom prostoru.

Ukoliko svoj par ključeva generira potpisnik tada se ključevi na SSCD uređaju generiraju na korisničkoj lokaciji, po preuzimanju SSCD uređaja u RA mreži, uz neposrednu 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 sigurnom SSL komunikacijom, koristeći dobivene aktivacijske podatke i pripadajući SSCD. U tom postupku 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 autentifikacijski N2 certifikat (NCP+), 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 potpisnik na SSCD uređaju generira svoj par ključeva.

b) Certifikat za potpis koda (NCP+)

Ovaj postupak se primjenjuje za Certifikat za potpis koda (NCP+) certifikat. Generiranje parova ključeva za ovaj tip certifikata obavlja skrbnik na SSCD uređaju na svojoj udaljenoj lokaciji.

Potpisnik se autentificira na udaljeni FINA CMS sustav sigurnom SSL komunikacijom, koristeći dobivene aktivacijske podatke i pripadajući SSCD. U tom postupku potpisnik na SSCD uređaju generira svoj par ključeva.

c) Poslovni NCP+ certifikati za IT opremu, razine 3

Ovaj postupak se primjenjuje za sljedeće tipove certifikata:

- SSL certifikat razine 3 (NCP+);
- WinDC certifikat razine 3 (NCP+);
- Aplikacijski certifikat razine 3 (NCP+).

Generiranje parova ključeva za poslovne NCP+ certifikate za IT opremu, razine 3 obavlja skrbnik u HSM modulu na svojoj udaljenoj lokaciji.

d) Poslovni NCP+ certifikati za IT opremu, razine 2

Ovaj postupak se primjenjuje za Aplikacijski certifikat razine 2 (NCP+). Generiranje parova ključeva za ovaj tip certifikata obavlja skrbnik na SSCD uređaju na svojoj udaljenoj lokaciji.

6.1.1.4. Generiranje para ključeva za NCP certifikate

a) Osobni i poslovni NCP certifikati

Ovaj postupak se primjenjuje za sljedeće tipove certifikata:

- Osobni soft certifikat (NCP);

- Poslovni soft certifikat (NCP);

Parove ključeva za NCP osobne i poslovne certifikate korisnika generira FINA CMS unutar FINA PKI štićenog prostora.

b) SSL certifikat razine 2 (NCP)

Generiranje parova ključeva za SSL certifikat razine 2 (NCP) obavlja skrbnik u softverskom kriptografskom modulu na svojoj udaljenoj lokaciji. Pri generiranju ključeva skrbnik mora zadovoljiti tehničke uvjete propisane u točki 6.2.1. ovog CPS_{NQC} dokumenta.

c) WinDC certifikat razine 2 (NCP)

Generiranje parova ključeva za WinDC certifikat razine 2 (NCP) obavlja skrbnik u softverskom kriptografskom modulu na svojoj udaljenoj lokaciji. Pri generiranju ključeva skrbnik mora zadovoljiti tehničke uvjete propisane u točki 6.2.1. ovog CPS_{NQC} dokumenta.

d) Aplikacijski certifikat razine 2 (NCP)

Generiranje parova ključeva za Aplikacijski certifikat razine 2 (NCP) obavlja skrbnik u softverskom kriptografskom modulu na svojoj udaljenoj lokaciji. Pri generiranju ključeva skrbnik mora zadovoljiti tehničke uvjete propisane u točki 6.2.1. ovog CPS_{NQC} dokumenta.

e) Aplikacijski certifikat razine 1 (NCP)

Generiranje parova ključeva za Aplikacijski certifikat razine 1 (NCP) generira FINA CMS unutar FINA PKI štićenog prostora.

Ukoliko generiranje ključeva za NCP certifikate provodi potpisnik ili skrbnik, generiranje ključeva se provodi u sigurnoj okolini na korisničkoj lokaciji, pod potpunom kontrolom i odgovornosti isključivo potpisnika ili skrbnika, odnosno pravne osobe kojoj isti pripadaju. FINA CA za pojedini tip NCP certifikata prihvaća javni ključ propisane duljine i korištenih algoritama navedenih u profilima certifikata u poglavlju 7. ovog CPS_{NQC} dokumenta.

6.1.1.5. Generiranje para ključeva za LCP certifikate

Ovaj postupak se primjenjuje za Poslovni soft certifikat (LCP). Parove ključeva za ovaj tip certifikata generira FINA CMS unutar FINA PKI štićenog prostora.

6.1.1.6. Generiranje para TSU ključeva za TSA

TSU par ključeva za FINA TSA sustav mora biti generiran na takav način da se ni u jednom trenutku ne može pojaviti nezaštićen.

TSU par ključeva FINA TSA sustava izrađuje se i pohranjuje u kriptografskom modulu. Postupak generiranja ovih ključeva provodi stručno ovlašteno osoblje s povjerljivim ulogama uz minimalno dualnu kontrolu. Opis zahtjeva za izbor osoblja opisan je u poglavlju 5.3. ovog CPS_{NQC} dokumenta.

U postupku izrade kriptografskih ključeva za FINA TSA osigurana je njihova kontrola, posebno:

- generiranje TSU ključeva za potpisivanje vremenskih žigova FINA TSA izvode ovlaštene osobe s povjerljivim ulogama u FINA TSA sustavu, a postupak se izvodi u štićenom okruženju;
- generiranje TSU ključeva za potpisivanje FINA TSA vremenskih žigova obavlja se unutar zaštićenog kriptografskog modula koji zadovoljava zahtjeve navedene u točki 6.2.1. ovog CPS_{NQC} dokumenta;
- duljina TSU ključeva FINA TSA i algoritmi za potpisivanje vremenskog žiga su:
    - RSA kriptografski algoritam s dužinom ključa od 2048 bita;
    - *hash* algoritam SHA-1.

Par TSU ključeva se generira u HSM modulu, uz minimalno dualnu kontrolu ovlaštenih osoba davatelja usluga.

6.1.2. Dostava privatnog ključa korisniku

Ukoliko FINA CA generira privatni ključ povezan s NCP+ 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 NCP+ 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 generira privatni ključ za potpisnika, aplikaciju ili potpis koda unutar SSCD uređaja, tada se SSCD uređaj s privatnim ključem zaštićenim kanalom dostavlja u FINA RA mrežu te se osobno uručuje identificiranom potpisniku, odnosno skrbniku.

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

Ukoliko korisnički privatni ključ subjekta za NCP i LCP certifikate generira FINA CA, korisnički privatni ključ se dostavlja autentificiranom potpisniku ili skrbniku zaštićenim kanalom u PKCS#12 formatu uporabom FINA CMS-a.

Ako potpisnik ili skrbnik na svojoj lokaciji generira privatni ključ, smatra se da ga potpisnik, odnosno skrbnik već posjeduje.

6.1.3. Dostava javnog ključa CA-u

Ukoliko korisnički javni ključ ne generira FINA CA, javni ključ se u FINA CA dostavlja na način koji sigurno povezuje potvrđeni identitet subjekta i pripadajući javni ključ koji se

dostavlja na certificiranje. Postupci dostave koriste PKCS#10 format zahtjeva koji je potpisan privatnim ključem subjekta.

Dostava korisničkog javnog ključa u PKCS#10 formatu obavlja se elektroničkim putem korištenjem FINA CMS-a ili drugih FINA CA web servisa za slanje javnog ključa i preuzimanje certifikata, a koji ostvaruju SSL komunikacijski kanal nakon uspješno provedene autentifikacije potpisnika, odnosno skrbnika.

6.1.4. Dostava CA javnog ključa pouzdajućim stranama

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

6.1.5. Duljine ključeva

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

- par ključeva FINA CA za elektroničko potpisivanje certifikata i CRL: 2048 bita, RSA;
- par ključeva za ovlaštene osobe u FINA RA mreži: 1024 bita, RSA;
- par ključeva za IT opremu RA sustava: 1024 bita, RSA;
- par TSU ključeva za TSA: 2048 bita, RSA;
- par ključeva za osobne i poslovne nekvalificirane certifikate: 1024 bita, RSA;
- par ključeva za SSL i WinDC certifikate: 1024 bita, RSA;
- par ključeva za aplikacijske certifikate: 1024 bita ili 2048 bita, RSA;
- par ključeva za certifikate za potpis koda: 1024 bita, RSA;
- par ključeva za administrativne certifikate: 1024 bita, RSA.

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 [24] (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.

Kod generiranja parametara javnog ključa u softverskim kriptografskim modulima (za certifikate za poslužitelje ili aplikacije) skrbnik mora koristiti softverske kriptografske module kojima je generiranje parametara RSA javnog ključa usklađeno po normama FIPS 186-3 [24] ili novijem, ili ANS X9.31.

Kvaliteta parametara javnih ključeva koji se generiraju na lokaciji FINA CA i javnog ključa FINA TSU osigurana je od strane proizvođača opreme u kojoj se ključevi generiraju korištenjem kvalitetnih generatora slučajnih brojeva, proizvedenih u skladu s normama FIPS 186-3 [24] (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 ekstenzija *KeyUsage*: *keyCertSign, cRLSign*).

Ovlaštene osobe u FINA RA mreži koriste privatne ključeve za autentifikaciju na FINA RA sustav (X.509 v3 ekstenzija *KeyUsage*: *digitalSignature, keyEncipherment*).

FINA RA sustav koristi ključeve u svrhu autentifikaciju na FINA RA sustav, potpisivanje i enkripciju (X.509 v3 ekstenzija *KeyUsage*: *digitalSignature, keyEncipherment*).

FINA TSA sustav koristi privatne potpisne TSU ključeve za elektronički potpis vremenskih žigova (X.509 v3 ekstenzija *KeyUsage*: *digitalSignature, nonRepudiation;* ekstenzija extKeyUsage: *timeStamping*).

Ključevi nekvalificiranih certifikata potpisnika namijenjeni su za elektronički potpis, autentifikaciju i enkripciju (X.509 v3 ekstenzija *KeyUsage*: *digitalSignature, keyEncipherment*).

Ključevi SSL i WinDC certifikata namijenjeni su za elektronički potpis, autentifikaciju i enkripciju (X.509 v3 ekstenzija *KeyUsage*: *digitalSignature, keyEncipherment*).

Ključevi aplikacijskih certifikata namijenjeni su za elektronički potpis, autentifikaciju i enkripciju (X.509 v3 ekstenzija *KeyUsage*: *digitalSignature, keyEncipherment*).

Privatni ključevi za potpis koda namijenjeni su za elektronički potpis softverskog koda (X.509 v3 ekstenzija *KeyUsage*: *digitalSignature*; ekstenzija *extKeyUsage*: *codeSigning*).

Ključevi administrativnih certifikata namijenjeni su za elektronički potpis, autentifikaciju i enkripciju (X.509 v3 ekstenzija *KeyUsage*: *digitalSignature, keyEncipherment*).

6.2. Zaštita privatnog ključa i tehnike upravljanja kriptografskim modulom

6.2.1. Norme i upravljačke funkcije kriptografskog modula

FINA CA i FINA TSU privatni ključevi generiraju se u HSM modulu koji:

- zadovoljava zahtjeve prema FIPS 140-2 [23], razina 3 ili viša, ili;
- predstavlja vjerodostojan sustav osiguran razinom EAL 4 ili višom, u skladu s HRN ISO/IEC 15408 normom [21], ili primjenom jednako vrijednih sigurnosnih kriterija.

Svi korisnički ključevi za certifikate visoke razine sigurnosti moraju se generirati u korisničkom HSM modulu:

- koji zadovoljava zahtjeve prema FIPS 140-1 [22] ili FIPS 140-2 [23], razina 3 ili više, ili
- zahtjeve primijenjenih jednako vrijednih sigurnosnih kriterija.

Svi korisnički 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 [22] ili FIPS 140-2 [23], razina 2 ili više, ili
- CEN/ISSS SSCD-PP definiran dokumentom CWA 14169 [15], ili
- zahtjeve primijenjenih jednako vrijednih sigurnosnih kriterija.

Iznimno, za NCP certifikate srednje razine sigurnosti za poslužitelje i aplikacije/servise korisnički ključevi se mogu generirati u softverskom ili hardverskom kriptografskom modulu koji zadovoljava zahtjeve prema FIPS 140-1 [22] ili FIPS 140-2 [23], razina 1 ili zahtjeve primijenjenih jednako vrijednih sigurnosnih kriterija, uz primjenu dodatnih mjera fizičke zaštite i ICT sigurnosti.

U slučaju kada skrbnik generira ključeve za NCP certifikate standardne razine sigurnosti, svi ključevi moraju biti generirani u kriptografskom modulu koji:

- zadovoljava zahtjeve prema FIPS 140-1 [22] ili FIPS 140-2 [23], razina 1 ili viša; ili
- zahtjeve primijenjenih jednako vrijednih sigurnosnih kriterija;

te uz primjenu mjera fizičke zaštite i ICT sigurnosti.

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

Kontrola od strane više osoba sigurnosni je mehanizam koji zahtijeva višestruku autorizaciju za pristup FINA CA privatnom potpisnom ključu. Pristup FINA CA privatnom potpisnom ključu mora biti obavljen uz minimalno dualnu kontrolu ovlaštenih osoba FINA CA.

6.2.3. Sigurno skladištenje privatnog ključa (key escrow)

Sigurno skladištenje privatnih FINA CA, odnosno FINA TSU ključeva izvan FINE se ne primjenjuje.

Sigurno skladištenje korisničkih privatnih ključeva FINA CA izvodi samo za NCP i LCP certifikate standardne razine sigurnosti tako da su privatni ključevi pohranjeni u FINA CMS-u, u enkriptiranom PKCS#12 obliku. Oporavak tako čuvane PKCS#12 datoteke s privatnim ključem je moguć samo od strane potpisnika, odnosno skrbnika, jer se dekripcija privatnog ključa vrši tajnim podatkom koji je poznat samo potpisniku, odnosno skrbniku.

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 korisničkih privatnih ključeva generiranih na SSCD uređajima.

FINA CA obavlja sigurno skladištenje korisničkih privatnih ključeva samo za nekvalificirane certifikate standardne razine sigurnosti (NCP i LCP), na način opisan u točki 6.2.3. ovog CPS_{NQC} dokumenta.

Ako korisnički privatni ključ nije generiran na SSCD uređaju tada potpisnik, odnosno skrbnik, smije izraditi sigurnosnu kopiju privatnog ključa na mediju za pohranu podataka, ukoliko mu je to tehnički omogućeno.

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

Poslovni subjekt, potpisnik ili skrbnik je odgovoran za zaštitu kopija korisničkog privatnog ključa te je odgovoran u slučaju njihovog neovlaštenog korištenja na isti način kao i originala, kako je to opisano u točki 4.5.1. ovog CPS_{NQC} dokumenta.

Sigurnosno kopiranje privatnog TSU ključa FINA TSA izvodi se na jednak način kao i za FINA CA.

6.2.5. Arhiviranje privatnog ključa

Privatni ključevi se ne arhiviraju.

6.2.6. Prijenos privatnog ključa u ili iz kriptografskog modula

Ako privatni FINA CA ključ treba prenijeti iz jednoga kriptografskog modula u drugi, za vrijeme prijenosa privatni ključ mora biti propisano zaštićen dok je izvan kriptografskog modula. Ovaj postupak provode samo ovlaštene osobe FINA CA i FINA PMA uz minimalno dualnu kontrolu.

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

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

U svim navedenim slučajevima u kojima je dozvoljen prijenos privatnog ključa mora se osigurati da se:

- privatni ključ prenosi samo u kriptografski modul jednake ili više razine sigurnosti u odnosu na kriptografski modul iz kojega se privatni ključ prenosi;
- privatni ključ prije prijenosa adekvatno enkriptira kako bi bio zaštićen dok se nalazi izvan kriptografskog modula.

6.2.7. Spremanje privatnog ključa u kriptografskom modulu

Privatni ključevi FINA CA i privatni TSU ključevi FINA TSA se generiraju i čuvaju HSM modulom.

Kada se nalaze unutar HSM modula, navedeni privatni ključevi su za HSM modul u čitljivom izvornom obliku.

6.2.8. Metoda aktivacije privatnog ključa

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

Privatni ključ certifikata izdanog za poslužitelj, aplikaciju ili za potpis koda aktivira samo pripadajući skrbnik korištenjem odgovarajućeg aktivacijskog podataka. Za vrijeme dok je privatni ključ aktivan skrbnik osigurava pravilnost njegove uporabe.

Privatni ključ osobnog ili poslovnog certifikata izdanog potpisniku aktivira samo pripadajući potpisnik korištenjem odgovarajućeg aktivacijskog podataka. Za vrijeme dok je privatni ključ aktivan potpisnik nadzire njegovu uporabu.

Samo potpisnik, odnosno skrbnik znaju podatak za aktivaciju privatnog ključa. Potpisnik, odnosno skrbnik, provode aktivaciju privatnog ključa na način u kojem ostaje sačuvana tajnost aktivacijskog podatka. 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 FINA CA, odnosno privatnog TSU ključa FINA TSA, provodi se kada postoji neposredan zahtjev za privremenim obustavljanjem aktivnosti FINA CA, odnosno FINA TSA sustava, u slučajevima isteka perioda valjanosti privatnog ključa te u slučaju opoziva pripadajućeg certifikata. Deaktivacija privatnog ključa FINA CA, odnosno

privatnog TSU ključa FINA TSA provodi se pod minimalno dualnom kontrolom ovlaštenih osoba FINA CA s povjerljivim ulogama.

Svaka deaktivacija privatnog ključa FINA CA, odnosno privatnog TSU ključa FINA TSA bilježi se u dnevnicima sustava.

Korisnički kriptografski moduli koji su aktivirani ne smiju biti ostavljeni bez nadzora. Nakon prestanka potrebe za korištenjem privatnog potpisnog ključa potpisnik, odnosno skrbnik mora deaktivirati privatni ključ.

Ukoliko se korisnički privatni ključ nalazi u HSM modulu, njegovu deaktivaciju obavlja skrbnik na pouzdan način koji propisuje proizvođač modula. Ovisno o načinu izvedbe HSM modula deaktivacija se obavlja logičkom deaktivacijom HSM modula, fizičkim vađenjem ili odspajanjem aktivacijskog uređaja, odnosno vađenjem ili odspajanjem HSM modula.

Ukoliko se korisnički privatni ključ nalazi na SSCD uređaju, njegovu deaktivaciju obavlja potpisnik, odnosno skrbnik fizičkim vađenjem ili odspajanjem SSCD uređaja, odnosno pouzdanom logičkom deaktivacijom propisanom od strane proizvođača SSCD uređaja.

Ukoliko se korisnički privatni ključ nalazi u softverskom kriptografskom modulu, njegovu deaktivaciju obavlja potpisnik, odnosno skrbnik pouzdanom logičkom deaktivacijom propisanom od proizvođača softverskog kriptografskog modula ili isključivanjem računala na kojem se nalazi privatni ključ.

Pouzdanu logičku deaktivaciju HSM modula, SSCD uređaja i softverskog kriptografskog modula može obaviti i korisnička aplikacija ili operacijski sustav koji koristi pouzdane metode logičke deaktivacije propisane od proizvođača modula, odnosno SSCD uređaja.

6.2.10. Metoda uništavanja privatnog ključa

Privatni ključevi FINA CA, odnosno privatni TSU ključ FINA TSA uništavaju se nakon prestanka potrebe za njihovim korištenjem, odnosno na kraju njihovog životnog ciklusa.

Postupak uništavanja privatnih ključeva FINA CA, odnosno privatnog TSU ključa FINA TSA, provodi se od strane ovlaštenog osoblja FINA CA i FINA PMA s povjerljivim ulogama. Svako provedeno uništavanje privatnih ključeva FINA CA, odnosno privatnog TSU ključa FINA TSA, se dokumentira te se dokumentacija o provedenom uništenju arhivira, sukladno točki 5.5. ovog CPS_{NQC} dokumenta.

Nema odredbi za obavezno uništavanje privatnih ključeva certifikate za IT opremu Središnjeg FINA RA sustava, IT opremu vanjskih ugovorenih RA, poslovnih certifikata za IT opremu, te poslovnih i osobnih certifikata za potpisnike.

6.2.11. Ocjena kriptografskog modula

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

6.3. Ostali vidovi upravljanja parom ključeva

6.3.1. Arhiviranje javnog ključa

Javni ključevi FINA CA, javni TSU ključ FINA TSA te korisnički javni ključevi svih subjekata kojima su izdani certifikati arhiviraju se u cilju omogućavanje verifikacije elektroničkih potpisa i vremenskih žigova, posebice u svrhu pružanja dokaza o certifikatima i vremenskim žigovima u sudskim, upravnim i drugim postupcima.

Javni ključevi FINA CA i javni TSU ključ FINA TSA se arhiviraju na način da se arhiviraju FINA CA, odnosno FINA TSA 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 se provodi na rok propisan u točki 5.5.2. ovog CPS_{NQC} dokumenta.

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

6.3.2. Periodi valjanosti certifikata i korištenja para ključeva

Predviđeni rok uporabe certifikata i korištenja para ključeva po vrstama certifikata, prikazan je u tablici 6.1.

Certifikat	Rok
CA certifikat	20 godina
Certifikat za vremenski žig	10 godina
Certifikat standardne razine sigurnosti	5 godina
Certifikat srednje razine sigurnosti	2 godine
Certifikat visoke razine sigurnosti	1 godina

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_{NQC} 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

Aktivacijski podaci za FINA CA privatni ključ generiraju se u FINA PKI pod nadzorom ovlaštenih osoba FINA CA.

Aktivacijski podaci za FINA RA mrežu generiraju se i čuvaju na siguran način u FINA RDC CA.

Aktivacijski podaci za privatni TSU ključ FINA TSA generiraju se na isti način kao aktivacijski podaci za FINA CA privatni ključ.

Aktivacijske podatke za privatne ključeve za IT opremu Središnjeg FINA RA generiraju ovlaštene osobe FINA CA u FINA PKI štićenom prostoru.

Ukoliko FINA CA generira privatni ključ za IT opremu vanjskog ugovorenog RA, pripadajuće aktivacijske podatke generiraju ovlaštene osobe FINA CA u FINA PKI štićenom prostoru. Ukoliko se privatni ključ za opremu generira na lokaciji vanjskog ugovorenog RA, pripadajuće aktivacijske podatke generira skrbnik na lokaciji vanjskog ugovorenog RA.

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

Aktivacijski podatak za korisnički privatni ključ koji je smješten u HSM modulu generira skrbnik na svojoj lokaciji .

U slučajevima kada potpisnik ili skrbnik preuzimaju certifikate u obliku PKCS#12 datoteke koristeći FINA CMS sustav, privatni ključ se enkriptira zaporkom koju odabire potpisnik, odnosno skrbnik tijekom SSL štićene sjednice. Prilikom uvoza PKCS#12 datoteke u softverski spremnik računala potpisnik, odnosno skrbnik kreira zaporku kojom će se aktivirati privatni ključ u softverskom spremniku.

U slučajevima kada skrbnik preuzima certifikate koristeći ostale FINA CA web servise za slanje javnog ključa i preuzimanje certifikata, skrbnik kreira zaporku kojom će se aktivirati privatni ključ u softverskom spremniku.

6.4.2. Zaštita aktivacijskih podataka

Aktivacijski podaci za privatne ključeve FINA CA se čuvaju i štite na propisan način. Pristup aktivacijskim podacima imaju samo ovlaštene osobe FINA CA s povjerljivim ulogama uz dualnu kontrolu.

Zaštita aktivacijskih podataka za privatni TSU ključ FINA TSA realizirana je na isti način kao i zaštita aktivacijskih podataka FINA CA privatnog ključa.

Aktivacijski podaci za privatne ključeve IT opreme Središnjeg FINA RA se čuvaju i štite na propisan način. Pristup sigurnosnom spremniku imaju samo ovlaštene osobe FINA CA s povjerljivim ulogama uz dualnu kontrolu.

Aktivacijski podaci koje generira FINA CA za korisničke privatne ključeve dostavljaju se potpisniku, odnosno skrbniku odvojenim distribucijskim kanalom od kanala isporuke SSCD uređaja i/ili privatnog ključa. Preporuka je da potpisnik, odnosno skrbnik promijeni aktivacijske podatke pri prvoj aktivaciji ključa.

Ukoliko aktivacijske podatke za IT opremu vanjskih ugovorenih RA generira skrbnik na lokaciji vanjskog ugovorenog RA, isti je odgovoran za sigurnost i kvalitetu aktivacijskih podataka.

Ukoliko aktivacijske podatke generiraju potpisnik, odnosno skrbnik, isti je odgovoran za sigurnost i kvalitetu aktivacijskih podataka.

Za korisničke privatne ključeve koji se uvoze u softverski spremnik ključeva preporuča se da potpisnik, odnosno skrbnik kreira aktivacijske podatke kojima će se aktivirati privatni ključ.

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, odnosno skrbniku, te se ne smiju pohranjivati zajedno s pripadajućim kriptografskim modulom na kojem se nalazi štićeni korisnički privatni ključ.

6.4.3. Ostale odredbe o aktivacijskim podacima

Ukoliko aktivacijske podatke za korisničke nekvalificirane certifikate generira FINA CA, aktivacijski podaci se iz FINA CA ili RA mreže e-mailom ili preporučenom poštanskom pošiljkom šalju potpisniku, odnosno skrbniku. Ukoliko se aktivacijski podaci za privatni ključ koji se nalazi u SSCD uređaju šalju e-mailom, aktivacijski podaci su enkriptirani. Ukoliko se šalju aktivacijski podaci za privatni ključ koji se nalazi zaštićen u PKCS#12 datoteci, tada su aktivacijski podaci šalju kroz dva odvojena distribucijska kanala, na e-mail adresu, odnosno SMS porukom na broj mobilnog uređaja.

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 dokumentima HRS ETSI/TS 102 023 [13], HRN ETSI/EN 319 411-3 [11] te normizacijskim dokumentom HRN ETSI/EN 319 411-2 [10] u slučajevima kada ovaj postavlja strože zahtjeve na računalnu sigurnost.

6.5.2. Ocjena računalne sigurnosti

Vjerodostojni računalni sustavi FINA CA i FINA TSA iz točke 6.5.1. zadovoljavaju uvjete iz norme HRN ISO/IEC 15408 [21], odnosno normizacijskog dokumenta CWA 14167-1 [14].

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 319 411-3 [11], odnosno normizacijskom dokumentu ETSI/EN 319 411-2 [10] u slučajevima kada ovaj postavlja strože zahtjeve na sustav certificiranja. Za FINA TSA sustave upravlja se sukladno zahtjevima navedenim u normizacijskom dokumentu HRS ETSI/TS 102 023 [13].

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

FINA PKI osigurava usklađenost provjera upravljanja sigurnošću FINA PKI sustava s normom HRN ETSI/EN 319 411-3 [11] te normom HRN ETSI/EN 319 411-2 [10] u slučajevima kada ova postavlja strože zahtjeve na sustav certificiranja, kao i normizacijskim dokumentom HRS ETSI/TS 102 023 [13] za FINA TSA sustav.

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 i FINA TSA sustavi rade ispravno i u skladu s implementiranom konfiguracijom sustava.

Provjera FINA CA i FINA TSA 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

FINA PKI osigurava usklađenost mrežne sigurnosti s normom HRN ETSI/EN 319 411-3 [11] te normom HRN ETSI/EN 319 411-2 [10] u slučajevima kada ova postavlja strože zahtjeve na mrežnu sigurnost.

6.8. Uporaba vremenskog žiga

Ne primjenjuje se.

7. SADRŽAJ CERTIFIKATA, LISTA OPOZVANIH CERTIFIKATA I OCSP PROFILI

Ovo poglavlje sadrži opis profila nekvalificiranih certifikata i listi opozvanih certifikata (CRL) koje FINA kao davatelj usluga certificiranja kroz FINA CA izdaje sukladno Općim pravilima [27].

Detaljan opis profila nekvalificiranih certifikata i CRL listi uključuje verzije, ekstenzije i druge podatke vezane uz certifikate, odnosno CRL liste.

Profili normaliziranih certifikata koje izdaju FINA RDC CA i FINA RDC-TDU CA usklađeni su s normom HRN ETSI/EN 319 411-3 [11] u dijelu pravila za normalizirane certifikate (NCP) i preporukom IETF RFC 5280 [19].

Profil *lightweight* certifikata koje izdaje FINA RDC CA usklađen je s normom HRN ETSI/EN 319 411-3 [11] u dijelu pravila za *lightweight* certifikate (LCP) i preporukom IETF RFC 5280 [19].

7.1. Profil certifikata

7.1.1. Broj(evi) verzije

Podržana je i korištena X.509 verzija 3 certifikata.

7.1.1.1. FINA RCD certifikati

Podjela certifikata koje izdaje FINA RDC CA po grupama korisnika:

1. FINA RDC osobni certifikati;
2. FINA RDC poslovni certifikati;
3. FINA RDC poslovni certifikati za IT opremu;

Svi certifikati koje izdaje FINA RCD CA imaju zajedničke elemente za osnovna polja i ekstenzije profila certifikata definirane u Tablici 7.1.

Polje	Atribut	Vrijednost
Osnovna polja		
Version	Version	V3, vrijednost="2"
serialNumber	CertificateSerialNumber	32-bitni neponovljivi cijeli broj
signatureAlgorithm	AlgorithmIdentifier	sha1RSA (sha1 sa RSA enkripcijom) OID: 1.2.840.113549.1.1.5
signatureValue		Vrijednost potpisa izdavatelja certifikata
Issuer	organizationalUnit	RDC
	organizationName	FINA
	countryName	HR

Polje	Atribut		Vrijednost
Osnovna polja			
Validity	notBefore		Vrijeme izdavanja certifikata
	notAfter		Vrijeme izdavanja certifikata + vrijeme valjanosti certifikata (UTC format zapisa)
Polje	**Kritično**	**Atribut**	**Vrijednost**
Ekstenzije			
PrivateKeyUsagePeriod	NE	notBefore	Vrijeme izdavanja certifikata
		notAfter	Vrijeme izdavanja certifikata + vrijeme valjanosti certifikata (UTC format zapisa)
CRLDistributionPoints	NE	DistributionPoint	[1]DirName:/C=HR/O=FINA/OU=RDC/CN=CRL(x) [2]URI:ldap://rdc-ldap.fina.hr/ou=RDC,o=FINA,c=HR?certificateRevocationList%3Bbinary [3]URI:http://rdc.fina.hr/crls/rdc.crl
AuthorityKeyIdentifier	NE	keyIdentifier	60-bitna SHA-1 hash vrijednost ključa s vodećim 0100 bitovima (po IETF RFC 5280)
SubjectKeyIdentifier	NE	keyIdentifier	60-bitna SHA-1 hash vrijednost ključa s vodećim 0100 bitovima (po IETF RFC 5280)
BasicConstraints	NE	cA	cA: FALSE

Tablica 7.1. Zajednička osnovna polja i ekstenzije certifikata izdanih od FINA RDC CA

1. FINA RDC osobni normalizirani certifikati

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

FINA e-kartica za građane i **FINA e-token za građane** na pametnoj kartici, odnosno USB tokenu, sadrži jedan od slijedeća dva tipa certifikata:

- **Osobni autentifikacijski N2 certifikat (NCP+)** - Osobni autentifikacijski normalizirani certifikat srednje razine sigurnosti koji se koristi za jaku autentifikaciju, elektronički potpis i enkripciju te ima definiran OID: **1.3.124.1104.5.11.1.4.2**. Izdaje se na SSCD uređaju u skladu s normizacijskim dokumentom HRN ETSI/EN 319 411-3 (NCP+) [11] i izdaje ga FINA RCD CA. Certifikat vrijedi dvije godine.

Osnovna polja i ekstenzije profila certifikata specifična za Osobni autentifikacijski N2 certifikat (NCP+) definirana su u Tablici 7.2.

Polje	Atribut	Vrijednost
Osnovna polja		
Subject	commonName	Ime i prezime potpisnika
	serialNumber	Sukladno opisu za polje Serial Number (SN) za osobne certifikate u tablici 3.1. ovog CPS_{NQC} dokumenta, Z=2.
	localityName	Mjesto prebivališta potpisnika
	organizationName	OSOBNI
	countryName	HR

Polje	Atribut		Vrijednost
Osnovna polja			
subjectPublic KeyInfo	AlgorithmIdentifier		RSA 1024 bit
	subjectPublicKey		Javni ključ subjekta
Polje	**Kritično**	**Atribut**	**Vrijednost**
Ekstenzije			
subjectAltName	NE	rfc822Name	Opcionalno. Sadrži *e-mail* adresu potpisnika u IETF RFC 822 standardiziranom obliku.
CertificatePolicies	NE	policyIdentifier	Srednja razina sigurnosti OID: 1.3.124.1104.5.11.1.4.2
		policyQualifiers	CPS: http://rdc.fina.hr/cp/cp4-0.pdf
Key Usage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit

Tablica 7.2. Specifična osnovna polja i ekstenzije profila Osobnog autentifikacijskog N2 certifikata (NCP+)

- **Osobni autentifikacijski Win2 certifikat (NCP+)** - Osobni autentifikacijski normalizirani certifikat za Windows, srednje razine sigurnosti koji se koristi za jaku autentifikaciju na Windows domenu, za druge vidove jake autentifikacije, za elektronički potpis i enkripciju te ima definiran OID: **1.3.124.1104.5.11.11.4.2**. Izdaje se na SSCD uređaju u skladu sa normizacijskim dokumentom HRN ETSI/EN 319 411-3 (NCP+) [11] i izdaje ga FINA RCD CA. Certifikat vrijedi dvije godine.

Osnovna polja profila certifikata specifična za Osobni autentifikacijski Win2 certifikat (NCP+) definirana su u Tablici 7.3.

Polje	Atribut		Vrijednost
Osnovna polja			
Subject	commonName		Ime i prezime potpisnika
	serialNumber		Sukladno opisu za polje Serial Number (SN) za osobne certifikate u tablici 3.1. ovog CPS_{NQC} dokumenta, Z=2.
	localityName		Mjesto prebivališta potpisnika
	organizationName		OSOBNI
	countryName		HR
subjectPublic KeyInfo	AlgorithmIdentifier		RSA 1024 bit
	subjectPublicKey		Javni ključ subjekta
Polje	**Kritično**	**Atribut**	**Vrijednost**
Ekstenzije			
subjectAltName	NE	rfc822Name	Opcionalno. Sadrži *e-mail* adresu potpisnika u IETF RFC 822 standardiziranom obliku.
		otherName	User Principal Name (UPN) u obliku email adrese
CertificatePolicies	NE	policyIdentifier	Srednja razina sigurnosti OID: 1.3.124.1104.5.11.11.4.2
		policyQualifiers	CPS: http://rdc.fina.hr/cp/cp4-0.pdf
Key Usage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit

Polje	Kritično	Atribut	Vrijednost
Ekstenzije			
extKeyUsage	NE	Client Authentication	OID: 1.3.6.1.5.5.7.3.2
		Smart Card Logon	OID: 1.3.6.1.4.1.311.20.2.2
		Secure Email	OID: 1.3.6.1.5.5.7.3.4

Tablica 7.3. Specifična osnovna polja i ekstenzije profila Osobnog autentifikacijskog Win2 certifikata (NCP+)

FINA e-kartica za građane, odnosno FINA e-token za građane, može sadržavati navedene tipove certifikata u kombinacijama K1 – K5 prikazanim Tablicom 7.4.

Certifikat	OID	K1	K2	K3	K4	K5
Osobni potpisni Q2 (QCP+)	1.3.124.1104.5.11.1.2.2	X			X	X
Osobni autentifikacijski N2 (NCP+)	1.3.124.1104.5.11.1.4.2		X		X	
Osobni autentifikacijski Win2 (NCP+)	1.3.124.1104.5.11.11.4.2			X		X

Tablica 7.4. Kombinacije certifikata sadržanih na FINA e-kartici ili e-tokenu za građane

Postupci certificiranja za Osobni potpisni Q2 certifikat (QCP+) su opisani u CPS_{QC} dokumentu.

- **Osobni soft certifikat (NCP)** - Osobni autentifikacijski normalizirani certifikat standardne razine sigurnosti koji se izdaje u PKCS#12 formatu, a koristi se za jaku autentifikaciju, elektronički potpis i enkripciju s definiranim OID-om: **1.3.124.1104.5.11.1.3.1**. Izdavanje ovog certifikata je u skladu s normizacijskim dokumentom HRN ETSI/EN 319 411-3 (NCP) [11] i izdaje ga FINA RCD CA. Certifikat vrijedi pet godina.

Osnovna polja i ekstenzije profila certifikata specifične za Osobni soft certifikat (NCP) definirane su u Tablici 7.5.

Polje	Atribut	Vrijednost
Osnovna polja		
Subject	commonName	Ime i prezime potpisnika
	serialNumber	Sukladno opisu za polje Serial Number (SN) za osobne certifikate u tablici 3.1. ovog CPS_{NQC} dokumenta, Z=9.
	localityName	Mjesto prebivališta potpisnika
	organizationName	OSOBNI
	countryName	HR
subjectPublic KeyInfo	AlgorithmIdentifier	RSA 1024 bit
	subjectPublicKey	Javni ključ subjekta

Polje	Kritično	Atribut	Vrijednost
Ekstenzije			
subjectAltName	NE	rfc822Name	Opcionalno. Sadrži *e-mail* adresu potpisnika u IETF RFC 822 standardiziranom obliku.

Polje	Kritično	Atribut	Vrijednost
Ekstenzije			
CertificatePolicies	NE	policyIdentifier	Standardna razina sigurnosti OID: 1.3.124.1104.5.11.1.3.1
		policyQualifiers	CPS: http://rdc.fina.hr/cp/cp4-0.pdf
Key Usage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit

Tablica 7.5. Specifična osnovna polja i ekstenzije profila Osobnog soft certifikata (NCP)

2. FINA RDC poslovni certifikati

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

FINA poslovna e-kartica i **FINA poslovni e-token** na smart kartici ili USB tokenu sadrži jedan od dva niže navedena tipa certifikata:

- **Poslovni autentifikacijski N2 certifikat (NCP+)** - Poslovni autentifikacijski normalizirani certifikat srednje razine sigurnosti koji se koristi za jaku autentifikaciju, elektronički potpis i enkripciju te ima definiran OID: **1.3.124.1104.5.11.2.4.2**. Izdavanje ovog certifikata je u skladu s normizacijskim dokumentom HRN ETSI/EN 319 411-3 (NCP+) [11] i izdaje ga FINA RCD CA. Certifikat vrijedi dvije godine.

Osnovna polja i ekstenzije profila certifikata specifične za Poslovni autentifikacijski N2 certifikat (NCP+) definirane su u Tablici 7.6.

Polje	Atribut	Vrijednost
Osnovna polja		
Subject	commonName	Ime i prezime potpisnika
	serialNumber	Sukladno opisu za polje Serial Number (SN) za poslovne FINA RDC certifikate u tablici 3.1. ovog CPS_{NQC} dokumenta, Z=1.
	localityName	Mjesto sjedišta poslovnog subjekta
	organizationName	Sukladno opisu za polje Organization (O) za poslovne FINA RDC certifikate u tablici 3.1. ovog CPS_{NQC} dokumenta.
	countryName	HR
subjectPublic KeyInfo	AlgorithmIdentifier	RSA 1024 bit
	subjectPublicKey	Javni ključ subjekta

Polje	Kritično	Atribut	Vrijednost
Ekstenzije			
subjectAltName	NE	rfc822Name	Opcionalno. Sadrži *e-mail* adresu potpisnika u IETF RFC 822 standardiziranom obliku.
CertificatePolicies	NE	policyIdentifier	Srednja razina sigurnosti OID: 1.3.124.1104.5.11.2.4.2
		policyQualifiers	CPS: http://rdc.fina.hr/cp/cp4-0.pdf
Key Usage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit

Tablica 7.6. Specifična osnovna polja i ekstenzije profila Poslovnog autentifikacijskog N2 certifikata (NCP+)

- **Poslovni autentifikacijski Win2 certifikat (NCP+)** - Poslovni autentifikacijski normalizirani certifikat za Windows srednje razine sigurnosti koji se koristi za jaku autentifikaciju na Windows domenu, za druge vidove jake autentifikacije, za elektronički potpis i enkripciju te ima definiran OID: **1.3.124.1104.5.11.21.4.2**. Izdavanje ovog certifikata je u skladu s normizacijskim dokumentom HRN ETSI/EN 319 411-3 (NCP+) [11] i izdaje ga FINA RCD CA. Certifikat vrijedi dvije godine.

Osnovna polja i ekstenzije profila certifikata specifične za Poslovni autentifikacijski Win2 certifikat (NCP+) definirane su u Tablici 7.7.

Polje	Atribut		Vrijednost
Osnovna polja			
Subject	commonName		Ime i prezime potpisnika
	serialNumber		Sukladno opisu za polje Serial Number (SN) za poslovne FINA RDC certifikate u tablici 3.1. ovog CPS_{NOC} dokumenta, Z=1.
	localityName		Mjesto sjedišta poslovnog subjekta
	organizationName		Sukladno opisu za polje Organization (O) za poslovne FINA RDC certifikate u tablici 3.1. ovog CPS_{NOC} dokumenta.
	countryName		HR
subjectPublic KeyInfo	AlgorithmIdentifier		RSA 1024 bit
	subjectPublicKey		Javni ključ subjekta
Polje	**Kritično**	**Atribut**	**Vrijednost**
Ekstenzije			
subjectAltName	NE	rfc822Name	Opcionalno. Sadrži *e-mail* adresu potpisnika u IETF RFC 822 standardiziranom obliku.
		otherName	User Principal Name (UPN) u obliku email adrese
CertificatePolicies	NE	policyIdentifier	Srednja razina sigurnosti OID: 1.3.124.1104.5.11.21.4.2
		policyQualifiers	CPS: http://rdc.fina.hr/cp/cp4-0.pdf
Key Usage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit
extKeyUsage	NE	Client Authentication	OID: 1.3.6.1.5.5.7.3.2
		Smart Card Logon	OID: 1.3.6.1.4.1.311.20.2.2
		Secure Email	OID: 1.3.6.1.5.5.7.3.4

Tablica 7.7. Specifična osnovna polja i ekstenzije profila Poslovnog autentifikacijskog Win2 certifikata (NCP+)

FINA e-kartica, odnosno FINA e-token, može sadržavati navedene tipove certifikata u kombinacijama K1 – K5 prikazanim Tablicom 7.8.

Certifikat	OID	K1	K2	K3	K4	K5
Poslovni potpisni Q2 (QCP+)	1.3.124.1104.5.11.2.2.2	X			X	X
Poslovni autentifikacijski N2 (NCP+)	1.3.124.1104.5.11.2.4.2		X		X	
Poslovni autentifikacijski Win2 (NCP+)	1.3.124.1104.5.11.21.4.2			X		X

Tablica 7.8. Kombinacije certifikata sadržanih na FINA e-kartici ili e-tokenu za poslovne subjekte

Postupci certificiranja za Osobni potpisni Q2 certifikat (QCP+) su opisani u CPS_{QC} dokumentu.

- **Poslovni soft certifikat (NCP) -** Poslovni autentifikacijski normalizirani certifikat standardne razine sigurnosti koji se izdaje u PKCS#12 formatu, a koristi se za jaku autentifikaciju, elektronički potpis i enkripciju te ima definiran OID: **1.3.124.1104.5.11.2.3.1**. Izdavanje ovog certifikata je u skladu s normizacijskim dokumentom HRN ETSI/EN 319 411-3 (NCP) [11] i izdaje se od strane FINA RCD CA. Certifikat vrijedi pet godina.

Osnovna polja i ekstenzije profila certifikata specifične za Poslovni soft certifikat (NCP) definirane su u Tablici 7.9.

Polje	Atribut		Vrijednost
Osnovna polja			
Subject	commonName		Ime i prezime potpisnika
	serialNumber		Sukladno opisu za polje Serial Number (SN) za poslovne FINA RDC certifikate u tablici 3.1. ovog CPS_{NOC} dokumenta, Z=10.
	localityName		Mjesto sjedišta poslovnog subjekta
	organizationName		Sukladno opisu za polje Organization (O) za poslovne FINA RDC certifikate u tablici 3.1. ovog CPS_{NOC} dokumenta.
	countryName		HR
subjectPublic KeyInfo	AlgorithmIdentifier		RSA 1024 bit
	subjectPublicKey		Javni ključ subjekta
subjectAltName	NE	rfc822Name	Opcionalno. Sadrži *e-mail* adresu potpisnika u IETF RFC 822 standardiziranom obliku.
CertificatePolicies	NE	policyIdentifier	Standardna razina sigurnosti OID: 1.3.124.1104.5.11.2.3.1
		policyQualifiers	CPS: http://rdc.fina.hr/cp/cp4-0.pdf
Key Usage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit

Tablica 7.9. Specifična osnovna polja i ekstenzije profila Poslovnog soft certifikata (NCP)

- **Poslovni soft certifikat (LCP) -** Poslovni autentifikacijski LCP certifikat standardne razine sigurnosti koji se izdaje u PKCS#12 formatu, a koristi se za jaku autentifikaciju, elektronički potpis i enkripciju te ima definiran OID: **1.3.124.1104.5.11.2.5.1**. Izdavanje ovog certifikata je u skladu s normizacijskim dokumentom HRN ETSI/EN 319 411-3 (LCP) [11] i izdaje se od strane FINA RCD CA. Certifikat vrijedi pet godina.

Osnovna polja i ekstenzije profila certifikata specifične za Poslovni soft certifikat (LCP) definirane su u Tablici 7.10.

Polje	Atribut		Vrijednost
Osnovna polja			
Validity	notBefore		Vrijeme izdavanja certifikata
	notAfter		Vrijeme izdavanja certifikata + 120 mjeseci (UTC format zapisa)
Subject	commonName		Ime i prezime potpisnika
	serialNumber		Sukladno opisu za polje Serial Number (SN) za poslovne FINA RDC certifikate u tablici 3.1. ovog CPS_{NOC} dokumenta, Z=8.
	localityName		Mjesto sjedišta poslovnog subjekta
	organizationName		Sukladno opisu za polje Organization (O) za poslovne FINA RDC certifikate u tablici 3.1. ovog CPS_{NOC} dokumenta.
	countryName		Država sjedišta poslovnog subjekta
subjectPublic KeyInfo	AlgorithmIdentifier		RSA 2048 bit
	subjectPublicKey		Javni ključ subjekta
CertificatePolicies	NE	policyIdentifier	Standardna razina sigurnosti OID: 1.3.124.1104.5.11.2.5.1
		policyQualifiers	CPS: http://rdc.fina.hr/cp/cp4-0.pdf
Key Usage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit
PrivateKeyUsagePeriod	NE	notBefore	Vrijeme izdavanja certifikata
		notAfter	Vrijeme izdavanja certifikata + 120 mjeseci (UTC format zapisa)
Polje	**Kritično**	**Atribut**	**Vrijednost**
Ekstenzije			
subjectAltName	NE	rfc822Name	Opcionalno. Sadrži *e-mail* adresu potpisnika u IETF RFC 822 standardiziranom obliku.

Tablica 7.10. Specifična osnovna polja i ekstenzije profila Poslovnog soft certifikata (LCP)

3. FINA RDC poslovni certifikati za IT opremu

Poslovne certifikate za IT opremu izdaje FINA RCD CA. Ovi certifikati se mogu izdati kao:

- certifikati za poslužitelje;
- certifikati za aplikacije;
- certifikati za potpis koda;
- certifikat za izradu vremenskog žiga.

Certifikati za poslužitelje se mogu izdati kao:

- **SSL certifikat razine 2 (NCP)** - Normalizirani certifikat za poslužitelje, srednje razine sigurnosti, uz korištenje softverskog spremnika ključa. Ovaj tip certifikata ima definiran OID: **1.3.124.1104.5.11.3.3.2.** Generiranje ključeva ovog certifikata obavlja skrbnik u softverskom kriptografskom modulu na svojoj udaljenoj lokaciji. Izdavanje ovog certifikata je u skladu s normizacijskim dokumentom HRN ETSI/EN 319 411-3 (NCP) [11] i izdaje ga FINA RCD CA. Certifikat vrijedi dvije godine.

Osnovna polja i ekstenzije profila certifikata specifične za SSL certifikat razine 2 (NCP) definirane su u Tablici 7.10.

Polje	Atribut	Vrijednost
Osnovna polja		
Subject	commonName	Puni kvalificirani naziv poslužitelja (FQDN)
	localityName	Mjesto sjedišta poslovnog subjekta
	organizationName	Sukladno opisu za polje Organization (O) za poslovne FINA RDC certifikate u tablici 3.1. ovog CPS_{NQC} dokumenta.
	countryName	HR
subjectPublic KeyInfo	AlgorithmIdentifier	RSA 1024 bit
	subjectPublicKey	Javni ključ subjekta

Polje	Kritično	Atribut	Vrijednost
Ekstenzije			
subjectAltName	NE	dNSName	Puni kvalificirani naziv poslužitelja (FQDN)
CertificatePolicies	NE	policyIdentifier	Srednja razina sigurnosti OID: 1.3.124.1104.5.11.3.3.2
		policyQualifiers	CPS: http://rdc.fina.hr/cp/cp4-0.pdf
Netscape Cert Type	NE		SSL server autentication
Key Usage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit

Tablica 7.10. Specifična osnovna polja i ekstenzije profila Poslovnog SSL certifikata razine 2 (NCP)

- **SSL certifikat razine 3 (NCP+)** - Normalizirani certifikat za poslužitelje, visoke razine sigurnosti, uz korištenje HSM modula. Ovaj tip certifikata ima definiran OID: **1.3.124.1104.5.11.3.4.3.** Generiranje ključeva ovog certifikata obavlja skrbnik u HSM modulu na svojoj udaljenoj lokaciji. Izdavanje ovog certifikata je u skladu s normizacijskim dokumentom HRN ETSI/EN 319 411-3 (NCP+) [11] i izdaje ga FINA RCD CA. Certifikat vrijedi jednu godinu.

Osnovna polja i ekstenzije profila certifikata specifične za SSL certifikat razine 3 (NCP+) definirane su u Tablici 7.11.

Polje	Atribut	Vrijednost
Osnovna polja		
Subject	commonName	Puni kvalificirani naziv poslužitelja (FQDN)
	localityName	Mjesto sjedišta poslovnog subjekta
	organizationName	Sukladno opisu za polje Organization (O) za poslovne FINA RDC certifikate u tablici 3.1. ovog CPS_{NQC} dokumenta.
	countryName	HR
subjectPublic KeyInfo	AlgorithmIdentifier	RSA 1024 bit
	subjectPublicKey	Javni ključ subjekta

Polje	Kritično	Atribut	Vrijednost
Ekstenzije			
subjectAltName	NE	dNSName	Puni kvalificirani naziv poslužitelja (FQDN)
CertificatePolicies	NE	policyIdentifier	Visoka razina sigurnosti OID: 1.3.124.1104.5.11.3.4.3
		policyQualifiers	CPS: http://rdc.fina.hr/cp/cp4-0.pdf
Netscape Cert Type	NE		SSL server autentication
Key Usage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit

Tablica 7.11. Specifična osnovna polja i ekstenzije profila Poslovnog SSL certifikata razine 3 (NCP+)

- **WinDC certifikat razine 2 (NCP)** - Normalizirani certifikat za Windows Domain Controler, srednje razine sigurnosti, uz korištenje softverskog spremnika ključa. Ovaj tip certifikata ima definiran OID: **1.3.124.1104.5.11.31.3.2.** Generiranje ključeva ovog certifikata obavlja skrbnik u softverskom kriptografskom modulu na svojoj udaljenoj lokaciji. Izdavanje ovog certifikata je u skladu s normizacijskim dokumentom HRN ETSI/EN 319 411-3 (NCP) [11] i izdaje ga FINA RCD CA. Certifikat vrijedi dvije godine.

Osnovna polja i ekstenzije profila certifikata specifične za WinDC certifikat razine 2 (NCP) definirane su u Tablici 7.12.

Polje	Atribut	Vrijednost
Osnovna polja		
Subject	commonName	Puni kvalificirani naziv poslužitelja (FQDN)
	localityName	Mjesto sjedišta poslovnog subjekta
	organizationName	Sukladno opisu za polje Organization (O) za poslovne FINA RDC certifikate u tablici 3.1. ovog CPS_{NOC} dokumenta.
	countryName	HR
subjectPublic KeyInfo	AlgorithmIdentifier	RSA 1024 bit
	subjectPublicKey	Javni ključ subjekta

Polje	Kritično	Atribut	Vrijednost
Ekstenzije			
subjectAltName	NE	dNSName	Puni kvalificirani naziv poslužitelja (FQDN)
		otherName	DS Object GUID
CertificatePolicies	NE	policyIdentifier	Srednja razina sigurnosti OID: 1.3.124.1104.5.11.31.3.2
		policyQualifiers	CPS: http://rdc.fina.hr/cp/cp4-0.pdf
Certificate Template Name	NE		DomainController
Key Usage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit
extKeyUsage	NE	Server Authentication	OID: 1.3.6.1.5.5.7.3.1
		Client Authentication	OID: 1.3.6.1.5.5.7.3.2

Tablica 7.12. Specifična osnovna polja i ekstenzije profila Poslovnog WinDC certifikata razine 2 (NCP)

- **WinDC certifikat razine 3 (NCP+)** - Normalizirani certifikat za Windows Domain Controler, visoke razine sigurnosti, uz korištenje HSM modula. Ovaj tip certifikata ima definiran OID: **1.3.124.1104.5.11.31.4.3.** Generiranje ključeva ovog certifikata obavlja skrbnik u HSM modulu na svojoj udaljenoj lokaciji. Izdavanje ovog certifikata je u skladu s normizacijskim dokumentom HRN ETSI/EN 319 411-3 (NCP+) [11] i izdaje se ga FINA RCD CA. Certifikat vrijedi jednu godinu.

Osnovna polja i ekstenzije profila certifikata specifične za WinDC certifikat razine 3 (NCP+) definirane su u Tablici 7.13.

Polje	Atribut		Vrijednost
Osnovna polja			
Subject	commonName		Puni kvalificirani naziv poslužitelja (FQDN)
	localityName		Mjesto sjedišta poslovnog subjekta
	organizationName		Sukladno opisu za polje Organization (O) za poslovne FINA RDC certifikate u tablici 3.1. ovog CPS_{NOC} dokumenta.
	countryName		HR
subjectPublic KeyInfo	AlgorithmIdentifier		RSA 1024 bit
	subjectPublicKey		Javni ključ subjekta
Polje	**Kritično**	**Atribut**	**Vrijednost**
Ekstenzije			
subjectAltName	NE	dNSName	Puni kvalificirani naziv poslužitelja (FQDN)
		otherName	DS Object GUID
CertificatePolicies	NE	policyIdentifier	Visoka razina sigurnosti OID: 1.3.124.1104.5.11.31.4.3
		policyQualifiers	CPS: http://rdc.fina.hr/cp/cp4-0.pdf
Certificate Template Name	NE		DomainController
Key Usage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit
extKeyUsage	NE	Server Authentication	OID: 1.3.6.1.5.5.7.3.1
		Client Authentication	OID: 1.3.6.1.5.5.7.3.2

Tablica 7.13. Specifična osnovna polja i ekstenzije profila Poslovnog WinDC certifikata razine 3 (NCP+)

Certifikati za aplikacije se mogu izdati kao:

- **Aplikacijski certifikat razine 1 (NCP)** - Normalizirani certifikat za aplikacije, standardne razine sigurnosti, uz korištenje softverskog spremnika ključa. Ovaj tip certifikata ima definiran OID: **1.3.124.1104.5.11.5.3.1.** Generiranje ključeva ovog certifikata obavlja FINA RDC CA te se certifikat izdaje u PKCS#12 formatu. Izdavanje ovog certifikata je u skladu s normizacijskim dokumentom HRN ETSI/EN 319 411-3 (NCP) [11] i izdaje ga FINA RCD CA. Certifikat vrijedi pet godina.

Osnovna polja i ekstenzije profila certifikata specifične za Aplikacijski certifikat razine 1 (NCP) definirane su Tablici 7.14.

Polje	Atribut		Vrijednost
Osnovna polja			
Subject	commonName		Naziv aplikacije
	localityName		Mjesto sjedišta poslovnog subjekta
	organizationName		Sukladno opisu za polje Organization (O) za poslovne FINA RDC certifikate u tablici 3.1. ovog CPS_{NOC} dokumenta.
	countryName		HR
subjectPublic KeyInfo	AlgorithmIdentifier		RSA 2048 bit
	subjectPublicKey		Javni ključ subjekta
Polje	**Kritično**	**Atribut**	**Vrijednost**
Ekstenzije			
subjectAltName	NE	rfc822Name	Opcionalno. Sadrži *e-mail* adresu subjekta u IETF RFC 822 standardiziranom obliku.
CertificatePolicies	NE	policyIdentifier	Standardna razina sigurnosti OID: 1.3.124.1104.5.11.5.3.1
		policyQualifiers	CPS: http://rdc.fina.hr/cp/cp4-0.pdf
Key Usage	NE	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit

Tablica 7.14. Specifična osnovna polja i ekstenzije profila Poslovnog aplikacijskog certifikata razine 1 (NCP)

- **Aplikacijski certifikat razine 2 (NCP)** - Normalizirani certifikat za aplikacije, srednje razine sigurnosti, uz korištenje softverskog spremnika ključa. Ovaj tip certifikata ima definiran OID: **1.3.124.1104.5.11.5.3.2.** Generiranje ključeva ovog certifikata obavlja skrbnik u softverskom kriptografskom modulu na svojoj udaljenoj lokaciji. Izdavanje ovog certifikata je u skladu s normizacijskim dokumentom HRN ETSI/EN 319 411-3 (NCP) [11] i izdaje ga FINA RCD CA. Certifikat vrijedi dvije godine.

Osnovna polja i ekstenzije profila certifikata specifične za Aplikacijski certifikat razine 2 (NCP) definirane su Tablici 7.15.

Polje	Atribut		Vrijednost
Osnovna polja			
Subject	commonName		Naziv aplikacije
	localityName		Mjesto sjedišta poslovnog subjekta
	organizationName		Sukladno opisu za polje Organization (O) za poslovne FINA RDC certifikate u tablici 3.1. ovog CPS_{NOC} dokumenta.
	countryName		HR
subjectPublic KeyInfo	AlgorithmIdentifier		RSA 1024 bit
	subjectPublicKey		Javni ključ subjekta
Polje	**Kritično**	**Atribut**	**Vrijednost**
Ekstenzije			
subjectAltName	NE	rfc822Name	Opcionalno. Sadrži *e-mail* adresu subjekta u IETF RFC 822 standardiziranom obliku.
CertificatePolicies	NE	policyIdentifier	Srednja razina sigurnosti OID: 1.3.124.1104.5.11.5.3.2
		policyQualifiers	CPS: http://rdc.fina.hr/cp/cp4-0.pdf

Polje	Kritično	Atribut	Vrijednost
Ekstenzije			
Key Usage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit

Tablica 7.15. Specifična osnovna polja i ekstenzije profila Poslovnog aplikacijskog certifikata razine 2 (NCP)

- **Aplikacijski certifikat razine 2 (NCP+)** - Normalizirani certifikat za aplikacije, srednje razine sigurnosti, uz korištenje SSCD uređaja. Ovaj tip certifikata ima definiran OID: **1.3.124.1104.5.11.5.4.2.** Generiranje ključeva ovog certifikata obavlja skrbnik na SSCD uređaju. Izdavanje ovog certifikata je u skladu s normizacijskim dokumentom HRN ETSI/EN 319 411-3 (NCP+) [11]. Ove certifikate izdaje FINA RCD CA. Certifikat vrijedi dvije godine.

Osnovna polja i ekstenzije profila certifikata specifične za Aplikacijski certifikat razine 2 (NCP+) definirane su u Tablici 7.16.

Polje	Atribut	Vrijednost
Osnovna polja		
Subject	commonName	Naziv aplikacije
	localityName	Mjesto sjedišta poslovnog subjekta
	organizationName	Sukladno opisu za polje Organization (O) za poslovne FINA RDC certifikate u tablici 3.1. ovog CPS_{NOC} dokumenta.
	countryName	HR
subjectPublic KeyInfo	AlgorithmIdentifier	RSA 1024 bit
	subjectPublicKey	Javni ključ subjekta

Polje	Kritično	Atribut	Vrijednost
Ekstenzije			
subjectAltName	NE	rfc822Name	Opcionalno. Sadrži *e-mail* adresu subjekta u IETF RFC 822 standardiziranom obliku.
CertificatePolicies	NE	policyIdentifier	Srednja razina sigurnosti OID: 1.3.124.1104.5.11.5.4.2
		policyQualifiers	CPS: http://rdc.fina.hr/cp/cp4-0.pdf
Key Usage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit

Tablica 7.16. Specifična osnovna polja i ekstenzije profila Poslovnog aplikacijskog certifikata razine 2 (NCP+)

- **Aplikacijski certifikat razine 3 (NCP+)** - Normalizirani certifikat za aplikacije, visoke razine sigurnosti, uz korištenje HSM modula. Ovaj tip certifikata ima definiran OID: **1.3.124.1104.5.11.5.4.3.** Generiranje ključeva ovog certifikata izvodi skrbnik u HSM modulu na svojoj udaljenoj lokaciji. Izdavanje ovog certifikata je u skladu s normizacijskim dokumentom HRN ETSI/EN 319 411-3 (NCP+) [11]. Ove certifikate izdaje FINA RCD CA. Certifikat vrijedi jednu godinu.

Osnovna polja i ekstenzije profila certifikata specifične za Aplikacijski certifikat razine 3 (NCP+) definirane su u Tablici 7.17.

Polje	Atribut	Vrijednost
Osnovna polja		
Subject	commonName	Naziv aplikacije
	localityName	Mjesto sjedišta poslovnog subjekta
	organizationName	Sukladno opisu za polje Organization (O) za poslovne FINA RDC certifikate u tablici 3.1. ovog CPS_{NOC} dokumenta.
	countryName	HR
subjectPublic KeyInfo	AlgorithmIdentifier	RSA 2048 bit
	subjectPublicKey	Javni ključ subjekta

Polje	Kritično	Atribut	Vrijednost
Ekstenzije			
subjectAltName	NE	rfc822Name	Opcionalno. Sadrži *e-mail* adresu subjekta u IETF RFC 822 standardiziranom obliku.
CertificatePolicies	NE	policyIdentifier	Visoka razina sigurnosti OID: 1.3.124.1104.5.11.5.4.3
		policyQualifiers	CPS: http://rdc.fina.hr/cp/cp4-0.pdf
Key Usage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit

Tablica 7.17. Specifična osnovna polja i ekstenzije profila Poslovnog aplikacijskog certifikata razine 3 (NCP+)

Certifikati za potpis koda su definirani kao:

- **Certifikat za potpis koda (NCP+)** - Normalizirani certifikat za potpis koda, srednje razine sigurnosti, uz korištenje SSCD uređaja. Ovaj tip certifikata ima definiran OID: **1.3.124.1104.5.11.7.4.2.** Ključevi ovog certifikata moraju biti od najmanje 1024-bita i njihovo generiranje izvodi CA u SSCD uređaju. Izdavanje ovog certifikata je u skladu s normizacijskim dokumentom HRN ETSI/EN 319 411-3 (NCP+) [11]. Ove certifikate izdaje FINA RCD CA. Certifikat vrijedi dvije godine.

Osnovna polja i ekstenzije profila certifikata specifične za certifikat za potpis koda (NCP+) definirane su u tablici 7.18.

Polje	Atribut	Vrijednost
Osnovna polja		
Subject	commonName	Skraćeni naziv poslovnog subjekta
	serialNumber	Identifikator poslovnog subjekta iz polja organizationName istog certifikata, cijeli broj W, Z=10.
	localityName	Mjesto sjedišta poslovnog subjekta
	organizationName	Sukladno opisu za polje Organization (O) za poslovne FINA RDC certifikate u tablici 3.1. ovog CPS_{NOC} dokumenta.
	countryName	HR
Polje	**Atribut**	**Vrijednost**
Osnovna polja		
subjectPublic KeyInfo	AlgorithmIdentifier	RSA 1024 bit
	subjectPublicKey	Javni ključ subjekta

Polje	Atribut		Vrijednost
Osnovna polja			
CertificatePolicies	NE	policyIdentifier	Srednja razina sigurnosti OID: 1.3.124.1104.5.11.7.4.2
		policyQualifiers	CPS: http://rdc.fina.hr/cp/cp4-0.pdf
Netscape Cert Type	NE	Signature	Netscape certifikat tip za potpis koda
Key Usage	DA	digitalSignature	Uključen digitalSignature bit
extKeyUsage	NE	codeSigning	OID: 1.3.6.1.5.5.7.3.3

Tablica 7.18. Specifična osnovna polja i ekstenzije profila Poslovnog certifikata za potpis koda (NCP+)

FINA RDC CA izdaje certifikate za izradu vremenskog žiga kao:

- **Certifikat za vremenski žig (NCP+)** - Normalizirani certifikat za izradu vremenskog žiga, visoke razine sigurnosti, uz korištenje HSM modula. Ovaj tip certifikata ima definiran OID: **1.3.124.1104.5.11.52.4.3.** Generiranje ključeva ovog certifikata obavlja se u HSM modulu uz nadzor ovlaštenih osoba davatelja usluge vremenskog žiga ili naprednog vremenskog žiga. Izdavanje ovog certifikata je u skladu s normizacijskim dokumentom HRN ETSI/EN 319 411-3 (NCP+) [11] i izdaje se od strane FINA RCD CA. Certifikat vrijedi deset godina.

Osnovna polja i ekstenzije profila certifikata specifične za certifikat za vremenski žig (NCP+) definirane su u Tablici 7.19.

Polje	Atribut		Vrijednost
Osnovna polja			
Subject	commonName		Naziv usluge izdavanja vremenskog žiga
	localityName		Mjesto sjedišta poslovnog subjekta
	organizationName		Sukladno opisu za polje Organization (O) za poslovne FINA RDC certifikate u tablici 3.1. ovog CPS_{NQC} dokumenta.
	countryName		HR
subjectPublic KeyInfo	AlgorithmIdentifier		RSA 2048 bit
	subjectPublicKey		Javni ključ subjekta
Polje	**Kritično**	**Atribut**	**Vrijednost**
Ekstenzije			
subjectAltName	NE	URIName	Opcionalno. Sadrži URL adresu TSA
CertificatePolicies	NE	policyIdentifier	Visoka razina sigurnosti OID: 1.3.124.1104.5.11.52.4.3
		policyQualifiers	CPS: http://rdc.fina.hr/cp/cp4-0.pdf
Key Usage	DA	digitalSignature	Uključen digitalSignature bit
		nonRepudiation	Uključen nonRepudiation bit
extKeyUsage	DA	timeStamping	OID: 1.3.6.1.5.5.7.3.8

Tablica 7.19. Specifična osnovna polja i ekstenzije profila Poslovnog certifikata za vremenski žig (NCP+)

7.1.1.2. FINA RDC-TDU certifikati za državne dužnosnike i zaposlenike u tijelima državne uprave

FINA e-kartica za TDU i **FINA e-token za TDU** na smart kartici, odnosno USB tokenu, sadrži normalizirani certifikat:

- **TDU autentifikacijski N2 certifikat (NCP+)** - Autentifikacijski normalizirani certifikat srednje razine sigurnosti za državne dužnosnike i zaposlenike u tijelima državne uprave koji se koristi za jaku autentifikaciju, elektronički potpis i enkripciju te ima definiran OID: **1.3.124.1104.5.21.2.4.2**. Izdaje na SSCD uređaju u skladu s normizacijskim dokumentom HRN ETSI/EN 319 411-3 (NCP+) [11] i izdaje se od strane FINA RCD-TDU CA. Certifikat vrijedi dvije godine.

Ekstenzije profila certifikata specifične za TDU autentifikacijski N2 certifikat (NCP+) definirane su u Tablici 7.21.

Polje	Atribut	Vrijednost
Osnovna polja		
Version	Version	V3, vrijednost="2"
serialNumber	CertificateSerialNumber	32-bitni neponovljivi cijeli broj
signatureAlgorithm	AlgorithmIdentifier	sha1RSA (sha1 sa RSA enkripcijom) OID: 1.2.840.113549.1.1.5
signatureValue		Vrijednost potpisa izdavatelja certifikata
Issuer	organizationalUnit	RDC-TDU
	organizationName	FINA
	countryName	HR
Validity	notBefore	Vrijeme izdavanja certifikata
	notAfter	Vrijeme izdavanja certifikata + vrijeme valjanosti certifikata (UTC format zapisa)
Subject	commonName	Ime i prezime potpisnika
	serialNumber	Sukladno opisu za polje Serial Number (SN) za FINA RDC-TDU certifikate u tablici 3.1. ovog CPS_{NQC} dokumenta, Z=1.
	localityName	Mjesto sjedišta TDU
	organizationalUnit	Opcionalno: org. jedinica TDU 2. razine
	organizationalUnit	Opcionalno: org. jedinica TDU 1. razine
	organizationName	Sukladno opisu za polje Organization (O) za FINA RDC-TDU certifikate u tablici 3.1. ovog CPS_{NQC} dokumenta.
	countryName	HR
SubjectPublicKeyInfo	AlgorithmIdentifier	RSA 1024 bit
	subjectPublicKey	Javni ključ subjekta

Polje	Kritično	Atribut	Vrijednost
Ekstenzije			
SubjectAltName	NE	rfc822Name	Opcionalno. Sadrži e-mail adresu potpisnika u IETF RFC 822 standardiziranom obliku.
PrivateKeyUsagePeriod	NE	notBefore	Vrijeme izdavanja certifikata
		notAfter	Vrijeme izdavanja certifikata + vrijeme valjanosti certifikata (UTC format zapisa)

Polje	Kritično	Atribut	Vrijednost
Ekstenzije			
CRLDistributionPoints	NE	DistributionPoint	[1]DirName:/C=HR/O=FINA/OU=RDC-TDU/CN=CRL(x) [2]URI:ldap://rdc-tdu-ldap.fina.hr/ou=RDC-TDU,o=FINA,c=HR?certificateRevocationList%3Bbinary [3]URI:http://rdc-tdu.fina.hr/crls/rdc-tdu.crl
CertificatePolicies	NE	policyIdentifier	Srednja razina sigurnosti OID: 1.3.124.1104.5.21.2.4.2
		policyQualifiers	CPS: http://rdc-tdu.fina.hr/cp4-0.pdf
AuthorityKeyIdentifier	NE	keyIdentifier	60-bitna SHA-1 hash vrijednost ključa s vodećim 0100 bitovima (po IETF RFC 5280)
SubjectKeyIdentifier	NE	keyIdentifier	60-bitna SHA-1 hash vrijednost ključa s vodećim 0100 bitovima (po IETF RFC 5280)
BasicConstraints	NE	cA	cA: FALSE
Key Usage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit

Tablica 7.21. Profil Normaliziranog TDU certifikata

FINA e-kartica za TDU, odnosno FINA e-token za TDU, može sadržavati navedene tipove certifikata u kombinacijama K1 – K3 prikazanim Tablicom 7.22.

Certifikat	OID	K1	K2	K3
TDU potpisni Q2 (QCP+)	1.3.124.1104.5.21.2.2.2	X		X
TDU autentifikacijski N2 (NCP+)	1.3.124.1104.5.21.2.4.2		X	X

Tablica 7.22. Kombinacije certifikata sadržanih na FINA e-kartici ili e-tokenu za državne dužnosnike i zaposlenike TDU

Postupci certificiranja za TDU potpisni Q2 certifikat (QCP+) su opisani u CPS_{QC} dokumentu.

7.1.2. Ekstenzije certifikata

Podržane i korištene ekstenzije X.509 v3 certifikata se trebaju koristiti na način opisan u profilima definiranim u ovom poglavlju. Korištene ekstenzije ne mijenjaju ili degradiraju uporabu X.509 osnovnih polja.

Programska podrška svih sudionika FINA PKI koja koristi certifikate mora korektno procesirati ekstenzije certifikata koje su u tablicama profila u točki 7.1.1. CPS_{NC} dokumenta označene kao kritične.

7.1.3. Identifikator objekta (OID) algoritama

OID-ovi podržanih algoritama su korišteni u skladu s odredbama IETF RFC 3279 [17] i IETF RFC 5280 [19].

7.1.4. Oblik naziva

Svaki DN nekvalificiranih certifikata je usklađen sa IETF RFC 5280 [19] preporukom.

7.1.5. Ograničenja u nazivima

Ograničenja u nazivima su usklađena sa pravilima definiranim u IETF RFC 5280 [19] preporuci.

7.1.6. Identifikator objekta (OID) općih pravila certificiranja

FINA CA-ovi osiguravaju da se OID općih pravila certificiranja nalazi u svim certifikatima koje oni izdaju. Oblik OID-a općih pravila certificiranja usklađen je s IETF RFC 5280 [19] preporukom.

7.1.7. Korištenje ekstenzija ograničenja općih pravila

Ekstenzije ograničenja općih pravila certificiranja se koriste u skladu s IETF RFC 5280 [19] preporukom.

7.1.8. Sintaksa i semantika označnih podataka općih pravila

Primjenjuju se pravila definirana u IETF RFC 5280 [19] preporuci.

7.1.9. Procesna semantika za kritične ekstenzije općih pravila certificiranja

Nije primjenjivo.

7.2. CRL profil

CRL se izdaje sukladno IETF RFC 5280 [19] preporuci.

Profil za CRL liste je definiran u Tablici 7.23.

Polje	Komentar/Sadržaj Polja
Version	v2
Signature	
signatureAlgorithm	sha1RSA (sha1 sa RSA enkripcijom)
signatureValue	Vrijednost potpisa kojim je potpisana CRL lista
Issuer	
organizationalUnit	Naziv FINA CA (RDC ili RDC-TDU)
organizationName	FINA
countryName	HR
thisUpdate	Vrijeme početka važenja CRL liste, format: YYMMDDhhmmssZ (UTCtime)
nextUpdate	Vrijeme početka važenja CRL liste + 24 sata, format: YYMMDDhhmmssZ (UTCtime)
revokedCertificates	
serialNumber	Serijski broj opozvanog korisničkog certifikata (32-bitni neponovljivi cijeli broj)
revocationDate	Datum opoziva, format: YYMMDDhhmmssZ (UTCtime)
IssuingDistributionPoint*	
commonName*	CRLx

Polje	Komentar/Sadržaj Polja
organizationalUnit*	Naziv FINA CA (RDC ili RDC-TDU)
organizationalName*	FINA
countryName*	HR
crlEntryExtensions	
reasonCode	Upisuje se kod razloga opoziva**
crlExtensions	
cRLNumber	Redni broj CRL liste, format: 24 bitni broj
AuthorityKeyIdentifier	60-bitna SHA-1 hash vrijednost ključa s vodećim 0100 bitovima (po IETF RFC 5280)

Tablica 7.23. Profil za CRL liste

* Polje se odnosi samo na segmentiranu CRL listu i nisu sadržana u kombiniranoj CRL listi.

** Razlozi opoziva (reasonCode) mogu biti:

- *keyCompromise* – ugroza privatnog ključa subjekta,
- *affiliationChanged* – promjena DN-a subjekta,
- *Superseded* – promjena ključa subjekta,
- *cessationOfOperation* – kraj životnog vijeka certifikata,
- *unspecified* – nije poznat razlog opoziva
- *certificateHold* - certifikat je suspendiran

7.2.1. Broj(evi) verzije

FINA CA-ovi podržavaju X.509 verzija 2 CRL liste.

7.2.2. CRL i ekstenzije unosa u CRL

Korištene ekstenzije su definirane u tablici profila u točki 7.2 CPS_{NQC} dokumenta.

7.3. OCSP profil

Nije podržano.

7.3.1. Broj(evi) verzije

Nije podržano.

7.3.2. OCSP ekstenzije

Nije podržano.

8. PROVJERA USKLAĐENOSTI

Inspekcijski nadzor nad radom FINA PKI reguliran je Zakonom o elektroničkom potpisu [1] i [2], 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 i FINA TSA sukladno pravilima definiranim u Općim pravilima [27] i postupcima iz CPS_{NQC} dokumenta provode interni ocjenitelji iz Odjela upravljanja politikom ePoslovanja.

Provjera usklađenosti izdavanja nekvalificiranih certifikata koje izdaju FINA CA-ovi provodi se sukladno normizacijskom dokumentu HRN ETSI/EN 319 411-3 [11] i sukladno razini kvalitete koja je za pojedine tipove nekvalificiranih certifikata opisana u ovom CPS_{NQC} dokumentu.

Provjera usklađenosti izdavanja vremenskog žiga se provodi sukladno normizacijskom dokumentu HRS ETSI/TS 102 023 [13].

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 i FINA TSA, te nakon znatnih promjena u radu FINA PKI sustava, odnosno nakon nepogode ili sumnje u kompromitiranje sustava.

8.2. Identitet/kvalifikacije ocjenitelja

Ocjenitelji moraju:

- raspolagati znanjima i razumijevanjem odredbi norme HRN ETSI/EN 319 411-3 [11] te normizacijskih dokumenata HRS ETSI/TS 102 023 [13] i CWA 14167-1 [14];
- 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 postupaju li FINA CA i FINA TSA prema pripadnim općim pravilima [27] i ovom CPS_{NQC} dokumentu.

Provjera usklađenosti sustava za izdavanje certifikata se provodi 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 319 411-3 [11].

Provjerom implementacije sustava provodi se provjera usklađenosti sustava sa zakonskom regulativom o elektroničkom potpisu, Općim pravilima [27], ovim CP_{NQC} dokumentom i normom HRN ETSI/EN 319 411-3 [11].

Provjera usklađenosti za uslugu izdavanja vremenskog žiga se provodi provjerom usklađenosti dokumentacije i provjerom implementacije sustava.

Provjera dokumentacije sustava za izdavanje vremenskog žiga obuhvaća provjeru usklađenosti dokumentacije sa zahtjevima zakonske regulative o elektroničkom potpisu i usklađenosti s normizacijskim dokumentom HRS ETSI/TS 102 023 [13].

Provjerom implementacije sustava za izdavanje vremenskog žiga provodi se provjera usklađenosti sustava sa zakonskom regulativom o elektroničkom potpisu, Općim pravilima davanja usluga izdavanja vremenskog žiga [28], ovim CP_{NQC} dokumentom i normizacijskim dokumentom HRS ETSI/TS 102 023 [13].

8.5. Mjere u slučaju neusklađenosti

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

Ukoliko je u radu FINA CA utvrđena značajna neusklađenost u odnosu na zahtjeve propisane ovim CPS_{NQC} dokumentom, FINA PMA će dati zahtjev za prekid izdavanja certifikata s CP OID-ovima iz opsega ovog CPS_{NQC} 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, FINA TSA i FINA RA/LRA vode interne dnevnike sustava s popisom vremenskih razdoblja u kojima nisu radili u skladu s CPS_{NQC} 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_{NQC} dokumenta objaviti sažetak provjere usklađenosti koji je relevantan korisnicima i ostalim sudionicima FINA PKI.

Svi dokumenti interne provjere usklađenosti su na zahtjev 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 povezanim s izdavanjem certifikata obavlja se objavom cjenika i drugih mjerodavnih informacija na internetskim stranicama FINA RDC i FINA RDC-TDU repozitorija iz točke 2.2. CPS_{NQC} dokumenta, a informiranje o cijenama i naplati usluga povezanim s izdavanjem vremenskog žiga na internetskim stranicama FINA TSA repozitorija iz točke 2.2.3. i FINA RDC repozitorija iz točke 2.2.1. ovog CPS_{NQC} 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 i FINA RDC-TDU nekvalificiranih 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 normaliziranih certifikata:

- usluga registriranja poslovnog subjekta i fizičke osobe – građanina;
- promjena podataka u certifikatu;
- čitač smart kartice;

- neposredna identifikacija potpisnika ili skrbnika te isporuka certifikata na SSCD uređaju na korisničkoj lokaciji;
- najam i održavanje opreme za elektronički potpis i enkripciju.

FINA, sukladno uvjetima iz sklopljenog ugovora o pružanju usluge izdavanja vremenskog žiga naplaćuje davanje usluge izdavanja vremenskog žiga. Ukoliko posebnim ugovorom nije drugačije određeno, usluge se naplaćuju sukladno cjeniku FINA TSA usluga.

Za pristup Općim pravilima [27], Općim pravila davanja usluga izdavanja vremenskog žiga [28] i drugoj javno objavljenoj dokumentaciji na web dijelu repozitorija iz točke 2.2. CPS_{NQC} 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_{NQC} dokumenta, neovisno o broju korisnika usluga i za cijelo vrijeme obavljanja usluga certificiranja.

9.2.1. Pokrivenost osiguranjem

FINA, kao davatelj usluga certificiranja ima osiguran rizik od odgovornosti za štete koje nastanu obavljanjem usluga izdavanja nekvalificiranih certifikata i vremenskih žigova.

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 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 te svi podaci koje se odnose na način i na sredstva kojim FINA TSA izdaje vremenske žigove.

Povjerljivi su i svi korisnički privatni ključevi koje generira FINA CA. Sukladno točkama 6.2.3. i 6.2.4. FINA CA skladišti samo privatne ključeve koje generira za pripadajuće NCP i LCP certifikate standardne razine sigurnosti. Privatne ključeve koje FINA CA ne skladišti, dostavlja korisniku, a najkasnije po dostavi njihove eventualne kopije na svojoj lokaciji FINA CA uništava na siguran način.

9.3.2. Podaci koji se ne smatraju povjerljivim poslovnim podacima

Poslovni podaci u bilo kojem obliku, koje na bilo koji način između sebe razmjene sudionici u svezi s uspostavom i pružanjem usluga certificiranja, a koje sudionici ne označe povjerljivim, ili određenom vrstom ili stupnjem tajnosti, ili koji po svojoj prirodi nisu povjerljivi jer njihovim neovlaštenim otkrivanje se 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 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 središta 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_{NQC} 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 štetu.

9.4. Zaštita osobnih podataka

FINA primjenjuje odredbe Zakona o zaštiti osobnih podataka [8] 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, skrbnika 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 su odgovorni za zaštitu osobnih podatka sukladno odredbama Zakona o zaštiti osobnih podataka [8] 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 je ovlaštena, osim za potrebe ispunjenja zakonskih, odnosno ugovornih obveza po ugovorima kojima se uređuju usluge certificiranja, koristiti osobne podatke samo temeljem pisane privole potpisnika, skrbnika ili korisnika usluge izdavanja vremenskog žiga. Potpisnik i skrbnik, odnosno korisnik usluge izdavanja vremenskog žiga, svoju privolu za korištenje osobnih podataka daju FINI u zahtjevu za izdavanje certifikata, odnosno u zahtjevu za korištenje usluge izdavanja vremenskog žiga.

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_{NQC} dokumenta, osim ako joj to nalažu zakonski propisi, Opća pravila [27] 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 [27], Opća pravila davanja usluga izdavanja vremenskog žiga [28], kao i druga FININA dokumentacija objavljena na internetskim stranicama RDC, RDC-TDU i FINA TSA repozitorija iz točke 2.2. CPS_{NQC} dokumenta je FININO vlasništvo i bez njena izričita ovlaštenja nije dozvoljeno njeno neovlašteno korištenje.

CPS_{NQC} dokument je interni dokument FINE, te se javno objavljuje na internetskim stranicama RDC i RDC-TDU repozitorija jedino u nepotpunom obliku koji sadrži samo informacije čija je javna objava dozvoljena.

Svaka stvar ili djelo koje je predmet nekog od prava intelektualnog vlasništva, vezano uz davanje usluga certificiranja koje su u opsegu Općih pravila [27] i Opća pravila davanja usluga izdavanja vremenskog žiga [28], neovisno pripada li FINI ili drugom sudioniku, zaštićeno je sukladno relevantnim propisima.

Sudionici PKI su dužni 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 nekvalificiranih certifikata primjenjuje Zakon [1] i [2], podzakonske propise [3], [4] i [5] donijete temeljem Zakona [1] i [2], obvezujuće međunarodne norme i preporuke, Opća pravila [27] i ovaj $CPS_{NQC.}$ Pri davanju usluga certificiranja iz opsega ovog CPS_{NQC} dokumenta FINA primjenjuje i druge akte navedene u ovom CPS_{NQC} dokumentu.

Akte koji su namijenjeni za javnu objavu FINA objavljuje na internetskim stranicama odgovarajućeg FINA CA repozitorija iz točke 2.2. CPS_{NQC} 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 nekvalificirane certifikate usklađene s X.509 v3 normom [25] i preporukom IETF RFC 5280 [19], a u skladu s odredbama normizacijskog dokumenta HRN ETSI/EN 319 411-3 [11].

Tijekom pružanja usluge izdavanja nekvalificiranih certifikata i upravljanja njihovim životnim ciklusom FINA CA-ovi poštuju sve zahtjeve i odredbe propisane Općim pravilima [27] i ovim CPS_{NQC} dokumentom.

FINA CA-ovi obavljaju usluge iz opsega ovog CPS_{NQC} 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 utvrđivanje identiteta potpisnika ili skrbnika, 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 FINE, a sukladno točki 2.2. CPS_{NQC} 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 ili skrbnika, poslovnog subjekta i osobe ovlaštene za zastupanje, a koji se smatraju povjerljivima sukladno točki 9.4. CPS_{NQC} dokumenta. Ove podatke FINA, kao davatelj usluga certificiranja, koristiti isključivo za potrebe usluga certificiranja iz opsega CPS_{NQC} dokumenta.

FINA, kao davatelj usluga certificiranja, osigurava rad RA mreže u skladu s odredbama Zakona [1] i [2], podzakonskih propisa donesenih temeljem Zakona [3], [4] i [5], Općih pravila [27], CPS_{NQC} 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 se dokazuje da subjekt certificiranja posjeduje privatni ključ čiji se pripadajući javni ključ dostavlja na certificiranje.

FINA CA osigurava uvjete da se par ključeva subjekta generira na siguran način i da je tajnost privatnog ključa osigurana sukladno odredbama norme HRN ETSI/EN 319 411-3 [11] za sve certifikate čiji se parovi ključeva generiraju u FINA CA, odnosno čije parove ključeva na korisničkoj lokaciji generiraj potpisnik, odnosno skrbnik, uz udaljeni nadzor FINA CA, odnosno ugovorenog RA. FINA CA propisuje uvjete generiranja para ključeva koje obavlja skrbnik na korisničkoj lokaciji uz osiguranje tajnosti privatnog ključa, sukladno odredbama norme HRN ETSI/EN 319 411-3 [11].

FINA CA osigurava da odgovarajući SSCD na siguran način bude dostavljen u RA mrežu u cilju njegove dostave potpisniku, odnosno skrbniku, u skladu s normom HRN ETSI/EN 319 411-3 [11] dokumentom, ukoliko je uporaba SSCD uređaja određena tipom traženog

certifikata. 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 nesmetani 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 i FINA TSA 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_{NQC} 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_{NQC} dokumenta;
- osigura da je potpisnik ili skrbnik u vrijeme izdavanja certifikata posjedovao privatni ključ čiji je pripadajući javni ključ ugrađen u certifikat, ili ukoliko se par ključeva generira na lokaciji CA, 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_{NQC} 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 ovim CPS_{NQC} dokumentom;
- čuvanje i zaštita prikupljenih podataka na način i u skladu sa zakonima na koje se poziva ovaj CPS_{NQC} dokument;
- prosljeđivanje cjelovitih, točnih i provjerenih podataka o korisnicima i subjektu certificiranja na daljnju obradu u FINA CA;
- arhiviranje zahtjeva i prikupljene dokumentacije na način propisan ovim CPS_{NQC} dokumentom;
- osiguravanje od gubitka ili povrede povjerljivosti, cjelovitosti i dostupnosti arhiviranih podataka korisnika, na način propisan ovim CPS_{NQC} dokumentom.
- osiguranje SSCD uređaja i njegova zaštićena dostava potpisniku, odnosno skrbniku, u skladu s ovim CPS_{NQC} dokumentom, ukoliko je uporaba SSCD uređaja određena tipom traženog certifikata.

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_{NQC} dokumenta;
- pažljivo koristiti i čuvati sredstvo za izradu elektroničkog potpisa, privatne ključeve i aktivacijske podatke, te ih koristiti u skladu s odredbama Zakona [1] i [2], odgovarajućim propisima i ovim CPS_{NQC} 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_{NQC} 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_{NQC} 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_{NQC} dokumenta;
- u slučaju korištenja usluge izdavanja vremenskog žiga, verificirati elektronički potpis FINA TSA na zaprimljenom vremenskom žigu i provjeriti valjanost FINA TSA certifikata.
- djelovati u skladu sa svim ostalim odredbama iz ovog CPS_{NQC} dokumenta koje se odnose na obveze korisnika.

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, odnosno onemogućeno korištenje usluge izdavanja vremenskog žiga, 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, odnosno vremenski žig.

Razumnim pouzdanjem smatra se odluka pouzdajuće strane da se pouzda u certifikat, odnosno vremenski žig, ako je u vrijeme ostvarenja pouzdanja:

- koristila certifikat u svrhe propisane Općim pravilima [27] i ovim CPS_{NQC} 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 liste kako je propisano u ovom CPS_{NQC} dokumentu;
- provjerila da su svi podaci o identitetu subjekta certifikata ispravno prikazani aplikacijom u koju se može pouzdati;
- u slučaju verificiranja elektroničkog potpisa, provjerila da je elektronički potpis izrađen privatnim ključem koji odgovara javnom ključu u certifikatu potpisnika za vrijeme perioda valjanosti certifikata;
- u slučaju korištenja vremenskog žiga, obavila verifikaciju potpisa vremenskog žiga te na zadnjoj izdanoj CRL listi provjerila opozvanost FINA TSA certifikata čijim je pripadnim privatnim ključem TSU potpisao vremenski žig.

Korištenje javnog ključa i certifikata od strane pouzdajuće strane opisano je u točki 4.5.2., a uvjeti za provjeru opoziva certifikata su navedeni u točki 4.9.6. ovog CPS_{NQC} dokumenta.

Pouzdajuća strana koja se, ne poštujući propise, Opća pravila [27], Opća pravila davanja usluga izdavanja vremenskog žiga [28] te protivno gore utvrđenim obvezama i odgovornostima iz ove točke CPS_{NQC} dokumenta , pouzdala u nevažeći (istekli, opozvani ili suspendirani) certifikat ili neispravan vremenski žig, sama snosi sve rizike pouzdanja u takav certifikat, odnosno vremenski žig.

Pouzdajuća strana snosi sve rizike pouzdanja u certifikat, odnosno vremenski žig, ako zna, ili ima razloga smatrati, da postoje činjenice koje mogu uzrokovati osobnu ili poslovnu štetu prouzročenu korištenjem certifikata, odnosno vremenskog žiga.

9.6.5. Obveze i odgovornosti ostalih sudionika

Nema odredbi.

9.6.6. Obveze i odgovornosti TSA

FINA, kao davatelj usluga izdavanja vremenskog žiga, pri izdavanju vremenskih žigova primjenjuje Zakon [1] i [2], podzakonske propise [3], [4] i [5] donijete temeljem Zakona [1] i [2], obvezujuće međunarodne norme i preporuke, Opća pravila davanja usluga izdavanja vremenskog žiga [28] i ovaj $CPS_{NQC.}$ Pri davanju usluga izdavanja vremenskog žga iz opsega ovog CPS_{NQC} dokumenta FINA primjenjuje i druge akte navedene u ovom CPS_{NQC} dokumentu.

FINA, kao davatelj usluga izdavanja vremenskog žiga, snosi punu odgovornost za davanje usluga izdavanja vremenskog žiga i odgovorna je za siguran i ispravan rad jedne ili više TSU jedinica koje izrađuju vremenski žig.

Akte koji su namijenjeni za javnu objavu FINA objavljuje na internetskim stranicama FINA TSA repozitorija iz točke 2.2.3. ovog CPS_{NQC} dokumenta.

FINA TSA 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 TSA izdaje vremenski žig usklađen s preporukom IETF RFC 3161 [16], a u skladu s odredbama normizacijskog dokumenta HRS ETSI/TS 102 023 [13].

FINA TSA ima obvezu osigurati točnost podataka o UTC vremenu kojeg ugrađuje u vremenski žig u granicama odstupanja navedenim u točki 1.2 Općih pravila davanja usluga izdavanja vremenskog žiga [28].

Tijekom pružanja usluge izdavanja vremenskog žiga FINA TSA poštuje sve zahtjeve i odredbe propisane Općim pravilima davanja usluga izdavanja vremenskog žiga [28] i ovim CPS_{NQC} dokumentom.

FINA TSA obavlja usluge iz opsega ovog CPS_{NQC} dokumenta s pažnjom dobrog stručnjaka.

FINA TSA u svom poslovanju primjenjuje organizacijske i tehničke mjere zaštite podataka korisnika, poslovnog subjekta i osobe ovlaštene za zastupanje, a koji se smatraju povjerljivima sukladno točki 9.4. CPS_{NQC} dokumenta. Ove podatke FINA, kao davatelj usluga izdavanja vremenskog žiga, koristiti isključivo za potrebe usluga certificiranja iz opsega CPS_{NQC} dokumenta.

FINA TSA provodi zahtijevane sigurnosne mjere za zaštitu prostora i opreme sustava izdavanja vremenskog žiga.

FINA TSA, sukladno najboljoj poslovnoj praksi, osigurava nesmetani rad i maksimalnu moguću raspoloživost usluge izdavanja vremenskih žigova, 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 TSA rješava zastoje i greške u radu sustava u najkraćem mogućem roku.

FINA, kao davatelj usluga izdavanja vremenskog žiga, planira održavanje i daljnji razvoj sustava za izdavanje vremenskih žigova sukladno priznatim normama i razvoju tehnologije.

U slučaju prekida poslovanja FINA TSA, FINA će postupiti sukladno točki 5.8. ovog CPS_{NQC} dokumenta.

FINA, kao davatelj usluga izdavanja vremenskog žiga, odgovara za štetu uzrokovanu nepoštivanjem mjerodavnih odredbi iz ovog CPS_{NQC} dokumenta u radu FINA RA mreže.

9.7. Odricanje od odgovornosti

Osim onog što je za FINU izričito navedeno u točki 9.6. ovog CPS_{NQC} 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_{NQC} dokumenta.

FINA ne odgovara za uporabu certifikata, odnosno vremenskog žiga, 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 zbog korištenja usluge vremenskog žiga u ime korisnika, kada korištenje usluge nije autorizirano od strane korisnika;
- za štete nastale uporabom certifikata u primjenama koje nisu dopuštene Općim pravilima i ovim CPS_{NQC} dokumentom;
- za štete prouzročene lažnom ili nemarnom uporabom certifikata ili CRL-a;
- 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_{NQC} dokumenta i zahtjevima iz Općih pravila [27].

9.8. Ograničenja odgovornosti

FININA ukupna financijska odgovornost za nekvalificirane certifikate izdane prema Općim pravilima i ovom CPS_{NQC} dokumentu i za transakcije obavljene na temelju pouzdavanja u tako izdane certifikate iznosi najviše 1.500.000 kuna.

Ako nije posebnim ugovorom ili na drugi način određeno, FININA maksimalna financijska odgovornost prema korisniku i pouzdajućoj strani koja se razumno pouzdaje u nekvalificirani certifikat ograničava se, sukladno preporučenim financijskim limitima određenim u Tablici 1.5 iz točke 1.4. ovog CPS_{NQC} dokumenta na način prikazan u Tablici 9.1.

Kategorija certifikata	Maksimalna FININA financijska odgovornost		
	Po kategoriji	Po transakciji	Ukupno
Nekvalificirani certifikati standardne razine sigurnosti	do 100.000 kn	do 8.000 kn	1.500.000 kn
Nekvalificirani certifikati srednje razine sigurnosti	do 600.000 kn	do 80.000 kn	
Nekvalificirani certifikati visoke razine sigurnosti	do 800.000 kn	do 400.000 kn	

Tablica 9.1. Maksimalna FININA financijska odgovornost za nekvalificirane certifikate

FININA maksimalna financijska odgovornost prema korisniku i pouzdajućoj strani koja se razumno pouzdaje u vremenski žig iznosi najviše 20.000,00 kuna po transakciji.

FININA ukupna financijska odgovornost za vremenske žigove izdane sukladno ovom CPS_{NQC} dokumentu i za transakcije obavljene na temelju pouzdavanja u tako izdane vremenske žigove iznosi najviše 100.000,00 kuna.

9.9. Naknada štete

Svaki sudionik odgovora oštećenom za štetu koju je počinio zbog nepoštovanja odredbi Općih pravila [27], ovog CPS_{NQC} 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_{NQC} dokumenta, ili ga koristi protivno svrhama određenim u Općim pravilima [27] i ovom CPS_{NQC} dokumentu.

FINA je odgovorna osobi koja se pouzdaje u certifikat samo ako je ta odgovornost jasno uspostavljena ugovorom, Općim pravilima [27], ovim CPS_{NQC} dokumentom ili hrvatskom zakonskom regulativom.

9.10. Trajanje i prestanak važenja

9.10.1. Trajanje

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

O potrebi izmjena i/ili dopunama CPS_{NQC} 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_{NQC} 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_{NQC} dokumenta.

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

FINA može za pojedine odredbe važećeg CPS_{NQC} dokumenta izraditi izmjene i dopune, kao što je to navedeno u točki 9.12. Općih pravila [27] i ovog CPS_{NQC} dokumenta.

9.10.3. Posljedice prestanka važenja i nastavak djelovanja

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

Novi CPS_{NQC} dokumenta ne utječe na važenje certifikata koji su izdani primjenom prethodnih CPS_{NQC} dokumenata. Certifikati izdani primjenom prethodnih CPS_{NQC} dokumenata važe do njihova isteka, pri čemu se mogu obnoviti samo primjenom odredbi iz novog CPS_{NQC} 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) Vrtni put 3 10000 Zagreb Hrvatska
e-mail:	info.rdc@fina.hr
Telefax:	385-1-6304-081

U slučaju dostave elektroničkom poštom dopis mora biti potpisan naprednim elektroničkim potpisom pošiljatelja.

9.12. Izmjene i dopune

9.12.1. Procedure izmjena i dopuna

CPS_{NQC} dokument revidira se po potrebi i nakon svake izmjene Općih pravila. 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_{NQC} dokumenta koje mogu bitno utjecati na sudionike zahtijevaju njihovo obavješćivanje. Takve izmjene uvjetuju i izmjenu OID-a CPS_{NQC} dokumenta.

Svi sudionici mogu na kontakt adresu FINA PMA iz točke 1.4 ovog CPS_{NQC} 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_{NQC} je interni dokument FINE i ne objavljuje se javno. Javno se može objaviti verzija CPS_{NQC} dokunmenta koja ne sadrži tajne podatke. Takav dokument objavljuje na internetskim stranicama repozitorija FINA CA iz točke 2.2. ovog CPS_{NQC} dokumenta.

9.12.3. Okolnosti pod kojima se mora mijenjati OID

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

Veće izmjene u CPS_{NQC} dokumentu koje mogu utjecati na sudionike zahtijevaju i izmjenu OID-a CPS_{NQC} 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_{NQC} 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_{NQC} dokumenta.

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

9.14. Važeći propisi

Za tumačenje odredbi ovog CPS_{NQC} dokumenta mjerodavne su odredbe Zakona o elektroničkom potpisu [1] i [2], podzakonskih akata [3], [4] donijetih temeljem tog zakona,

odredbe Općih pravila [27], odnosno Općih pravila davanja usluga izdavanja vremenskog žiga [28], te propisa, normi i preporuka na koje iste upućuju.

9.15. Usklađenost s važećim propisima

Ovaj CPS_{NQC} dokument i davanje usluga certificiranja koje su obuhvaćene ovim CPS_{NQC} dokumentom usklađeni su s propisima iz točke 9.14. ovog CPS_{NQC} 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_{NQC} dokumenta, Općih pravila [27], odnosno Općih pravila davanja usluga izdavanja vremenskog žiga [28], te da ti ugovori omogućuju ugovornim stranama zaštitu interesa sukladno Općim pravilima [27], odnosno Općim pravilima davanja usluga izdavanja vremenskog žiga [28].