FINA

PRAVILNIK O POSTUPCIMA CERTIFICIRANJA ZA CERTIFIKATE ZA AUTENTIKACIJU MREŽNIH STRANICA

Verzija 1.3

Datum stupanja na snagu: 12.09.2018.

OID Dokumenta: 1.3.124.1104.5.0.5.2.1.3

Informacije o dokumentu

Ime dokumenta:	Pravilnik o postupcima certificiranja za certifikate za autentikaciju mrežnih stranica
OID dokumenta:	1.3.124.1104.5.0.5.2.1.3
Tip dokumenta:	Pravilnik o postupcima certificiranja (*Certification Practice Statement*, CPS)
Oznaka distribucije	Javno
Vlasnik dokumenta	Financijska agencija, Fina
Kontakt	pma@fina.hr

Povijest izmjena

Verzija	Datum	Razlog izmjene
1.0	22.05.2017.	Inicijalna verzija
1.1	21.03.2018.	Ažuriranje referente liste zakonske regulative, dopuna postupka registracije korisnika u točki 3.2.2., izmjena u periodu važenja certifikata i dodana provjera CAA zapisa u točki 4.2.2.
1.2	27.07.2018.	Dodavanje opisa podržanih metoda za provjeru prava korištenja domene i IP adrese, ažuriranje referente liste zakonske regulative, dodavanje odredbe o izdavanju certifikata za pravne osobe sa sjedištem u Republici Hrvatskoj, dodavanje izjave o usklađenosti dokumenta s RFC 3647.
1.3	11.09.2018.	Dodavanje SHA-256 *fingerprinta* CA certifikata, dopuna odredbi vezanih uz prestanak pružanja usluga povjerenja, poboljšanja u postupcima prihvaćanja certifikata, reduciranje potrebnih podataka koji se prikupljaju prilikom opoziva certifikata, dodavanje izjave o postupcima vezanim za upravljanje kritičnim ranjivostima, dodavanje izjave o obavljanju opoziva i suspenzije certifikata bez obzira na status naplate i dodavanje izjave o dostupnosti usluga osobama s invaliditetom.

SADRŽAJ

AUTORSKA PRAVA

REFERENTNE DOKUMENTIRANE INFORMACIJE

Temeljni zakon

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

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

Ostali zakoni

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

Normizacijski dokumenti

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

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

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

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

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

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

[10] ETSI EN 319 412-4 V1.1.1. (2016-02) – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates

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

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

[13] NIST FIPS PUB 140-1 (1994) – Security Requirements for Cryptographic Modules

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

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

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

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

[18] HRN ISO/IEC 9594-8:2015 - Informacijska tehnologija – Međusobno povezivanje otvorenih sustava – Imenik – 8. dio: Okviri certifikata javnog ključa i atributnog certifikata (ISO/IEC 9594-8:2014); Information technology – Open Systems Interconnection – The Directory – Part 8: Public-key and attribute certificate frameworks (ISO/IEC 9594-8:2014)

[19] CA/Browser Forum - Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (aktualna verzija)

[20] IETF RFC 6844 – DNS Certification Authority Authorization (CAA) Resource Record (2013)

Finini dokumenti

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

[22] Opća pravila pružanja usluga certificiranja za certifikate za autentikaciju mrežnih stranica, $CP_{WSA\text{-}eIDAS}$

[23] Pravilnik o postupcima certificiranja za nekvalificirane certifikate, $CPS_{NQC\text{-}eIDAS}$

1 UVOD

Kao treća strana od povjerenja, Fina svoje usluge certificiranja pruža od 2003. godine. Usluge povjerenja koje pruža Fina usklađene su sa zakonskom regulativom [1], [2] i [3] te s mjerodavnim međunarodnim normama iz djelokruga pružanja usluga povjerenja. Fina neprekidno prati potrebe korisnika, razvoj tehnologije i promjene u normama iz područja pružanja usluga povjerenja te sukladno tome unapređuje i usklađuje svoj PKI sustav kako bi svoje proizvode i usluge prilagodila zahtjevima za prekograničnu interoperabilnost.

1.1 Pregled

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

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

Dvorazinsku arhitekturu produkcijskih certifikacijskih tijela Fine čine:

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

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

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

Opća pravila i postupci koji se odnose na Fina Root CA i Fina PKI hijerarhiju zasnovanu na Fina Root CA opisana su u dokumentu Opća pravila pružanja usluga certificiranja i Pravilnik o postupcima certificiranja za Fina Root CA [21].

1.1.1 Opseg i namjena

Ovaj Pravilnik o postupcima certificiranja za certifikate za autentikaciju mrežnih stranica (engl. C*ertification Practice Statement for Certificates for Website Authentication*, u daljnjem tekstu: $CPS_{WSA\text{-}eIDAS}$) opisuje postupke i procedure koje primjenjuje Fina PKI na izdavanje i upravljanje životnim ciklusom produkcijskih digitalnih (nekvalificiranih) certifikata za autentikaciju mrežnih stranica (poznatih i pod nazivom TLS/SSL certifikati), a koji su usklađeni sa zahtjevima Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ [1] (u daljem tekstu: Uredbe (EU) br. 910/2014). Ovi certifikati za autentikaciju mrežnih stranica uključuju

validirane podatke o identitetu organizacije Subjekta (u daljnjem tekstu: OVCP certifikat ili certifikat), sukladno zahtjevima iz Opća pravila pružanja usluga certificiranja za certifikate za autentikaciju mrežnih stranica (u daljnjem tekstu: Opća pravila) [22].

Opseg ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta su usluge povjerenja koje pruža Fina, a koje se odnose na izdavanje i upravljanje životnom ciklusom produkcijskih certifikata za autentikaciju mrežnih stranica (engl. *certificate for website authentication*), a čiji je privatni ključ zaštićen softverskim tokenom, ili se izdaju za korištenje u HSM modulima.

Produkcijski certifikati iz opsega ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta sastavni su dio Registra digitalnih certifikata (Fina RDC). Certifikacijska tijelo (CA) iz opsega ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta to je Fina RDC 2015.

Ovaj $CPS_{WSA\text{-}eIDAS}$ dokument usklađen je s dokumentom Opća pravila [22], a koji je objavljen na internetskim stranicama http://www.fina.hr/finadigicert.

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

Struktura ovog dokumenta temelji se na normizacijskom dokumentu IETF RFC 3647 [15].

1.1.2 Tipovi certifikata

Fina kao pružatelj usluga povjerenja izdaje tipove certifikata za autentikaciju mrežnih stranica koji su obuhvaćeni opsegom ovog dokumenta i koji su prikazani u Tablici 1.1. Prikazani su nazivi tipova certifikata te OID-ovi općih pravila certificiranja (u daljnjem tekstu: CP OID) dodijeljeni od strane Fine, ETSI i CAB Foruma.

Fina RDC 2015 certifikati za autentikaciju mrežnih stranica			
Naziv grupe certifikata	**Naziv tipa certifikata**	**CP OID**	**Razina sigurnosti**
Fina RDC 2015 certifikati za autentikaciju mrežnih stranica	SSL certifikat razine 2 (OVCP)	Fina CP OID: 1.3.124.1104.5.12.14.2 ETSI CP OID: 0.4.0.2042.1.7 CAB Forum CP OID: 2.23.140.1.2.2	Srednja
	SSL certifikat razine 3 (OVCP)	Fina CP OID: 1.3.124.1104.5.12.14.3 ETSI CP OID: 0.4.0.2042.1.7 CAB Forum CP OID: 2.23.140.1.2.2	Visoka

Tablica 1.1. Tipovi certifikata za autentikaciju mrežnih stranica

Fina RDC 2015 certifikati za autentikaciju mrežnih stranica izdaju se za poslužitelje povezane s pravnim osobama koje imaju sjedište u Republici Hrvatskoj. Fina RDC 2015 CA izdaje sljedeće tipove certifikata za autentikaciju mrežnih stranice:

- ***SSL certifikat razine 2 (OVCP)*** – Certifikat za autentikaciju mrežnih stranica, srednje razine sigurnosti, čiji se pripadajući privatni ključ čuva u softverskom zaštićenom tokenu, sukladno točki 6.2.1. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta. Ovaj tip certifikata sukladan je s „OVCP“ općim pravilima za certifikate iz norme ETSI EN 319 411-1 [7].

- ***SSL certifikat razine 3 (OVCP)*** – Certifikat za autentikaciju mrežnih stranica, visoke razine sigurnosti, čiji se pripadajući privatni ključ čuva u HSM modulu, sukladno točki 6.2.1. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta. Ovaj tip certifikata sukladan je s „OVCP“ općim pravilima za certifikate iz norme ETSI EN 319 411-1 [7].

1.2 Naziv dokumenta i identifikacijski podaci

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

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

- Naziv: Pravilnik o postupcima certificiranja za certifikate za autentikaciju mrežnih stranica
- Verzija: 1.3
- Datum stupanja na snagu: 12.09.2018.
- OID: 1.3.124.1104.5.0.5.2.1.3
- Internetska adresa na kojoj je objavljen ovaj $CPS_{WSA\text{-}eIDAS}$ dokument: http://rdc.fina.hr/RDC2015/FinaRDC2015-CPSWSA1-3-hr.pdf

1.3 Sudionici u PKI

Sudionici unutar Fina PKI su:

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

1.3.1 Certifikacijska tijela

1.3.1.1 Fina Root CA

Fina Root CA je izdao samopotpisani Fina Root CA certifikat te CA certifikat za njemu subordinirani Fina RDC 2015 CA. Fina Root CA ne izdaje certifikate Korisnicima.

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

Polje	Atribut	Vrijednost
Issuer	commonName	Fina Root CA
	organizationName	Financijska agencija
	countryName	HR
Validity	notBefore	*Vrijeme izdavanja certifikata*
	notAfter	*Vrijeme izdavanja certifikata + 20 godina*

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

Tablica 1.2. Osnovni podaci o Fina Root CA certifikatu

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

1.3.1.2 Fina RDC 2015 CA

Certifikacijsko tijelo u Fina PKI iz opsega ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta je Fina RDC 2015 CA.

Fina RDC 2015 CA se u izdanom certifikatu identificira kao izdavatelj (eng. *Issuer*) certifikata te ga potpisuje koristeći svoj privatni ključ.

Fina RDC 2015 CA izdaje za javnost certifikate koji su navedeni u Tablici 1.1 u točki 1.1.2. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta. Prema istim pravilima Fina RDC 2015 CA izdaje certifikate i za potrebe Fine

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

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

Tablica 1.3. Osnovni podaci o Fina RDC 2015 CA certifikatu

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

1.3.2 Registracijski uredi

Poslovi registracije korisnika za Fina RDC 2015 CA obavljaju se u registracijskim uredima Fine.

Fina RA mrežu čini mreža lokalnih registracijskih ureda (u daljnjem tekstu: Fina LRA) u poslovnoj mreži Fine te Središnji RA Fine. Središnji RA Fine čine ovlaštene osobe Odjela RDC. Registraciju korisnika u Fina RA mreži provodi Fina LRA zajedno sa Središnji RA Fine. Poslovima registracije u Fina RA mreži koordinira Središnji RA Fine koji je središnja komunikacijska točka Fina RA mreže. Popis aktualnih registracijskih ureda Fina LRA nalazi se na internetskoj adresi http://www.fina.hr/finadigicert.

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

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

1.3.3 Korisnici

Korisnik iz opsega ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta je pravna osoba sa sjedištem u Republici Hrvatskoj koja je sklapanjem ugovora s Finom kao pružateljem usluga povjerenja preuzela ugovorne obveze Korisnika.

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

1.3.3.1 Subjekti certificiranja

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

1.3.4 Pouzdajuće strane

Pouzdajuće strane su fizičke osobe - građani ili poslovni subjekti koje se oslanjaju na uslugu povjerenja. Certifikat omogućuje pouzdajućoj strani provjeru identiteta Subjekta.

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

1.3.5 Ostali sudionici

Nema odredbi.

1.4 Uporaba certifikata

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

- sve podatke koji se nalaze u certifikatu ili činjenice o kojima je pouzdajuća strana obaviještena, uključujući i ovaj $CPS_{WSA\text{-}eIDAS}$ dokument,
- ekonomsku vrijednost transakcije ili podataka, ako je to primjenjivo,
- potencijalne gubitke ili štetu koja može biti uzrokovana pogrešnom identifikacijom Subjekta certificiranja od strane Pouzdajuće strane,
- primjenjivost zakonske regulative,
- bilo koji pokazatelj prikladnosti ili neprikladnosti, ili druge činjenice koje Pouzdajuća strana zna, a odnose se na Subjekt certificiranja, primijenjeno rješenje ili transakciju,
- preporučeni financijski limit povezan s razinom sigurnosti certifikata.

U Tablici 1.3. opisane su razine sigurnosti za certifikate. Za pojedinu razinu sigurnosti u tablici je prikazan pripadajući opis područja primjene i preporučeni financijski limit.

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

Tablica 1.4. Razine sigurnosti za certifikate

1.4.1 Primjerena uporaba certifikata

Certifikati navedeni u Tablici 1.1. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta i pripadajući privatni ključevi upotrebljavaju se samo za autentikaciju mrežnih stranica, tj. za autentikaciju web poslužitelja kojima se pristupa putem TLS ili SSL protokola.

1.4.2 Zabrane uporabe certifikata

Osim uporabe navedene u točki 1.4.1. ovog $CPC_{WSA\text{-}eIDAS}$ dokumenta, sve ostale uporabe certifikata navedenih u Tablici 1.1. te njihovih privatnih ključeva su zabranjene.

1.5 Administracija dokumenta Opća pravila

1.5.1 Organizacija odgovorna za održavanje dokumenta Opća pravila

Za izradu i održavanje dokumenta Općih pravila [34] i ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta ovlaštena je i odgovorna Fina.

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

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

1.5.2 Kontakt podaci

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

Poštanska adresa:

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

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

1.5.3 Tijelo koje utvrđuje usklađenost CPS-a s Općim pravilima

Usklađenost ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta s Općim pravilima utvrđuje Fina PMA.

Fina PMA odgovoran je za usklađenost ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta s Općim pravilima [22].

1.5.4 Procedure odobravanja CPS-a

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

1.6 Definicije i kratice

1.6.1 Definicije

POJAM	ZNAČENJE
Aktivacijski podaci	Tajni podaci potrebni za pristup ili aktivaciju kriptografskog modula. Aktivacijski podatak može biti PIN, zaporka ili elektronički ključ kojeg osoba zna ili posjeduje.
Autentikacija	Elektronički postupak koji omogućava da elektronička identifikacija fizičke ili pravne osobe, ili izvornost i cjelovitost podataka u elektroničkom obliku budu potvrđeni.

POJAM	ZNAČENJE
CA certifikat	Certifikat javnog ključa za CA kojeg je izdao drugi CA ili kojeg je izdao isti CA.
Certifikacijsko tijelo (CA)	Tijelo koje izrađuje i dodjeljuje certifikate javnog ključa, a kojem vjeruje jedan ili više korisnika. Certifikacijsko tijelo može biti: • pružatelj usluga povjerenja koji izrađuje i dodjeljuje certifikate javnog ključa, ili • tehnički servis izrade certifikata kojeg upotrebljava pružatelj usluga certificiranja koji izrađuje i dodjeljuje certifikate javnog ključa.
Certifikat	Vidi pojam „certifikat javnog ključa“.
Certifikat javnog ključa	Javni ključ Subjekta koji je zajedno s drugim informacijama zaštićen od krivotvorenja digitalnim potpisom izrađenim privatnim ključem certifikacijskog tijela koje je izdalo certifikat.
Certifikat za autentikaciju mrežnih stranica	Potvrda pomoću koje je moguće izvršiti autentikaciju mrežnih stranica te kojom se mrežne stranice povezuju s fizičkom ili pravnom osobom kojoj je izdan certifikat.
Certifikat za elektronički potpis	Elektronička potvrda koja povezuje podatke za validaciju elektroničkog potpisa s fizičkom osobom i potvrđuje barem ime ili pseudonim te osobe.
Elektronički potpis	Podaci u elektroničkom obliku koji su pridruženi ili su logički povezani s drugim podacima u elektroničkom obliku i koje Potpisnik koristi za potpisivanje.
Elektronički vremenski žig	Podaci u elektroničkom obliku koji povezuju druge podatke u elektroničkom obliku s određenim vremenom i na taj način dokazuju da su ti podaci postojali u to vrijeme.
Fina LRA	Lokalni registracijski ured u Fina poslovnoj mreži.
Fina PKI	Infrastruktura javnog ključa (PKI) uspostavljena u Fini koja je namijenjena za pružanje usluga certificiranja fizičkim osobama – građanima, poslovnim subjektima i tijelima državne uprave, a koja je uspostavljena kao treća strana od povjerenja (engl. *Trusted Third Party*).
Fina RA mreža	Mreža registracijskih ureda u Fini, a sastoji se od Središnjeg RA Fine i Fina LRA ureda.
Infrastruktura javnog ključa (PKI)	Infrastruktura za upravljanje javnim ključevima koji podržavaju usluge autentikacije, enkripcije, cjelovitosti i neporecivosti.

POJAM	ZNAČENJE
Interni naziv	Niz znakova (koji ne predstavlja IP adresu) u polju *Common Name* ili *Subject Alternative Name* certifikata. Interni naziv se ne može verificirati kao jedinstven na globalnoj razini u javnom DNS-u u vrijeme izdavanja certifikata jer ne završava s vršnom domenom (engl. *Top Level Domain*) koja je registrirana u *Root Zone Database* IANA-e.
Isporučitelj aplikacijskog softvera	Isporučitelj internetskog preglednika ili druge softverske aplikacije koja prikazuje ili upotrebljava certifikate i ugrađuje root certifikate.
Javni imenik	Informatički sustav koji služi za *online* objavu informacija vezanih uz certifikate, uključujući i informacije o opozvanosti certifikata.
Javni ključ	U kriptografskom sustavu javnog ključa, javno poznati ključ iz Subjektovog para ključeva.
Kontakt za domenu	Tehnički ili administrativni (ili istovrijedan prema ccTLD) kontakt registriranog nositelja naziva domene koji je naveden u WHOIS zapisu osnovnog naziva domene (*Base Domain Name*), DNS SOA zapisu ili je dobiven direktnim kontaktom registratora naziva domene.
Koordinirano svjetsko vrijeme (UTC)	Vremenska ljestvica koja se temelji na sekundi kako je definirana ITU-R preporukom TF.460-5. Za većinu primjena u praksi UTC je ekvivalentan srednjem sunčevom vremenu na nultom meridijanu (0°). Točnije, UTC je kompromis između vrlo stabilnog atomskog vremena (*Temps Atomique International* - TAI) i sunčevog vremena koje se izvodi iz nepravilne rotacije Zemlje (u odnosu na dogovoreno Greenwich srednje zvjezdano vrijeme (GMST).
Korisnik	Pravna osoba koja je sklapanjem ugovora s pružateljem usluga povjerenja preuzela ugovorne obveze Korisnika.
Kriptografski modul	Softver ili uređaj određene razine sigurnosti koji: ▪ generira par ključeva i/ili, ▪ štiti kriptografske informacije i/ili, ▪ obavlja kriptografske funkcije.
Kvalificirani ocjenitelj	Fizička ili pravna osoba koja zadovoljava zahtjeve navedene u dokumentu Baseline Requirements [19] kojeg objavljuje CA/Browser Forum.
Kvalificirani pružatelj usluga povjerenja	Pružatelj usluga povjerenja koji pruža jednu ili više kvalificiranih usluga povjerenja i kojemu je nadzorno tijelo odobrilo kvalificirani status.
Lista opozvanih certifikata (CRL)	Potpisana lista u kojoj su naznačeni certifikati koje izdavatelj certifikata više ne smatra valjanim.

POJAM	ZNAČENJE
Napredan elektronički potpis	Elektronički potpis koji ispunjava sljedeće zahtjeve: (a) na nedvojben način je povezan s Potpisnikom, (b) omogućava identificiranje Potpisnika, (c) izrađen je korištenjem podacima za izradu elektroničkog potpisa koje Potpisnik može, uz visoku razinu pouzdanja, koristiti pod svojom isključivom kontrolom, i (d) povezan je s njime potpisanim podacima na način da se može otkriti bilo koja naknadna izmjena podataka.
Opća pravila pružanja usluge certificiranja - Certificate Policy (CP)	Imenovani skup pravila koji ukazuje na primjenjivost certifikata za određenu skupinu i/ili klasu primjena sa zajedničkim zahtjevima na sigurnost.
Opoziv certifikata	Radnja koja certifikat nepovratno čini nevažećim od trenutka opoziva.
Osoba ovlaštena za zastupanje	Osoba koja je po zakonu ovlaštena zastupati Korisnika koji je pravna osoba.
OVCP certifikati	Certifikat koji uključuje provjerene informacije o identitetu organizacije povezane sa subjektom.
Par ključeva	Dva jedinstveno povezana kriptografska ključa, od kojih je jedan privatni ključ, a drugi javni ključ.
Podaci za izradu elektroničkog potpisa	Jedinstveni podaci koje Potpisnik koristi za izradu elektroničkog potpisa
Podaci za verifikaciju potpisa	Podaci, poput kodova ili javnih kriptografskih ključeva koji se koriste u svrhu verificiranja potpisa.

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

POJAM	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.
Redovna obnova certifikata	Obnova certifikata u FINA PKI podrazumijeva izdavanje novog certifikata čiji su parametri jednaki kao i parametri certifikata na koji se zahtjev odnosi, ali s novim javnim ključem, novim serijskim brojem certifikata, novim vremenskim periodom valjanosti i novim potpisom istog CA, a provodi se u definiranom periodu prije datuma isteka valjanosti certifikata.
Registracijski ured (RA)	Tijelo odgovorno za identifikaciju i autentikaciju subjekata certificiranja, kao i drugih osoba ili organizacija.
Registrirani nositelj naziva domene	Jedna ili više osoba, ili jedan ili više subjekata registriranih kod registratora naziva domene, koji time imaju pravo upravljanja uporabom naziva domene. Najčešće označava fizičku ili pravnu osobu „vlasnika“ naziva domene, a koja je u WHOIS zapisu ili registru naziva domene navedena kao korisnik (*registrant*).
Rezervirana IP adresa	IPv4 ili IPv6 adresa koju je IANA označila kao rezerviranu.
Root CA	Certifikacijsko tijelo najviše razine unutar domene pružatelja usluga povjerenja i koje potpisuje certifikate subordiniranih CA-ova.
Root CA certifikat	CA certifikat kojeg je samom sebi izdao root CA.
Siguran kriptografski uređaj	Uređaj koji čuva privatni korisnički ključ, štiti ga protiv kompromitiranja i obavlja potpisne ili dekripcijske funkcije u ime korisnika.
Skrbnik	Fizička osoba zaposlena u poslovnom subjektu ili na drugi način povezana s poslovnim subjektom, a koja je od strane istog poslovnog subjekta ovlaštena za podnošenje zahtjeva za izdavanje poslovnih certifikata za sustave, uređaje i autentikaciju mrežnih stranica te za preuzimanje certifikata i pripadajućih aktivacijskih podataka. Skrbnik je ovlašten za podnošenje zahtjeva za upravljanje životnim ciklusom certifikata. Skrbnik je kontakt osoba poslovnog subjekta prema pružatelju usluge povjerenja za predmetni certifikat.
Slučajna vrijednost	Vrijednost koju Fina kao pružatelj usluga povjerenja generira podnositelju zahtjeva za izdavanja certifikata i koja pokazuje najmanje 112 bitova entropije.
Službenik za opoziv certifikata	Osoba koja je odgovorna za promjenu operativnog statusa certifikata.
Službenik za registraciju	Osoba odgovorna za potvrđivanje podataka koji su potrebni za izdavanje certifikata i za odobravanje zahtjeva za izdavanje certifikata.

POJAM	ZNAČENJE
Službenik za validaciju	Osoba odgovorna za provjeru podataka vezanih uz izdavanje certifikata koji se izdaju sukladno zahtjevima dokumenta CA/Browser Forum BRG [19].
Središnji RA	Središnji registracijski ured koji je primarno je zadužen za koordiniranje cjelokupne RA mreže, ali može i izravno obavljati registriranje korisnika
Sredstvo za izradu elektroničkog potpisa	Konfigurirani softver ili hardver koji se koristi za izradu elektroničkog potpisa.
Subjekt	Entitet identificiran u certifikatu kao nositelj privatnog ključa koji je povezan s javnim ključem sadržanim u certifikatu.
Sustav certificiranja	Sustav IT proizvoda i komponenti organiziranih za pružanje usluga certificiranja.
Tijelo državne uprave (TDU)	Tijelo državne vlasti nadležno za obavljanje poslova državne uprave u upravnom području za koje je nadležno. Tijela državne uprave su ministarstva, državni uredi, državne upravne organizacije i uredi državne uprave u županijama ili druga tijela državne uprave utvrđena mjerodavnim važećim zakonom.
Tijelo za ocjenjivanje sukladnosti	Tijelo u smislu članka 2. točke 13. Uredbe (EZ) br. 765/2008 koje je u skladu s tom Uredbom ovlašteno kao nadležno za provedbu ocjenjivanja sukladnosti kvalificiranog pružatelja usluga povjerenja i kvalificiranih usluga povjerenja koje on pruža.
Tijelo za upravljanje pravilima certificiranja (PMA)	Tijelo s konačnom ovlašću i odgovornošću za određivanje i odobravanje pravila pružanja usluga povjerenja (engl. *Policy Management Authority*)
Usluga povjerenja	Elektronička usluga koja se u pravilu pruža uz naknadu i koja se sastoji od: (a) izrade, verifikacije i validacije elektroničkih potpisa, elektroničkih pečata ili elektroničkih vremenskih žigova, usluge elektroničke preporučene dostave i certifikata koji se odnose na te usluge, ili (b) izrade, verifikacije i validacije certifikata za autentikaciju mrežnih stranica, ili (c) čuvanja elektroničkih potpisa, pečata ili certifikata koji se odnose na te usluge.
Usluge certificiranja	Usluge izdavanje i upravljanje životnom ciklusom certifikata.
Validacija	Postupak verifikacije i potvrđivanja da su elektronički potpis ili pečat valjani.
Validacija certifikata	Postupak verificiranja i potvrđivanja da je certifikat valjan.

POJAM	ZNAČENJE
Verifikacija potpisa	Proces provjere kriptografske vrijednosti potpisa korištenjem podataka za verifikaciju potpisa.

Tablica 1.5. Definicije

1.6.2 Kratice

KRATICA	PUNI NAZIV	ZNAČENJE
CA	*Certification Authority*	Certifikacijsko tijelo
CAA	*Certification Authority Authorization*	Autorizacija ovlaštenja za izdavanje certifikata
CAB Forum	*CA/Browser Forum*	*CA/Browser Forum*
ccTLD	*Country Code Top-Level Domain*	Vršna internetska domena za države
CP	*Certificate Policy*	Opća pravila pružanja usluga certificiranja
$CP_{WSA-eIDAS}$	*Certificate Policy for Certificates for Website Authentication*	Opća pravila pružanja usluga certificiranja za certifikate za autentikaciju mrežnih stranica
CPS	*Certification Practice Statement*	Pravilnik o postupcima certificiranja
$CPS_{NQC-eIDAS}$	*Certification Practice Statement for Non-Qualified Certificates*	Pravilnik o postupcima certificiranja za nekvalificirane certifikate
$CPS_{WSA-eIDAS}$	*Certification Practice Statement for certificates for website authentication*	Pravilnik o postupcima certificiranja za certifikate za autentikaciju mrežnih stranica
CRL	*Certificate Revocation List*	Lista opozvanih certifikata
DN	*Distinguished Name*	Razlikovno ime
DNS	*Domain Name System*	Sustav za prevođenje naziva računala u odgovarajuće IP adrese
FQDN	*Fully Qualified Domain Name*	Potpuni kvalificirani naziv domene
LDAP	*Lightweight Directory Access Protocol*	Protokol za pristup informacijskim direktorijima
LRA	*Local Registration Authority*	Lokalni registracijski ured
OCSP	*Online Certificate Status Protocol*	Protokol *on-line* provjere statusa certifikata
OVCP	*Organizational Validation Certificate Policy*	Opća pravila certificiranja za certifikate validacije organizacije
OID	*Object Identifier*	Identifikator objekta
PIN	*Personal Identification Number*	Osobni tajni broj za aktivaciju smart kartice,

KRATICA	PUNI NAZIV	ZNAČENJE
		USB 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
SOA	*Start of Authority*	Početni autoritet
TDU	Tijelo (ili tijela) državne uprave	Tijelo (ili tijela) državne uprave
TLD	Top-Level Domain	Vršna internetska domena
UTC	*Coordinated Universal Time*	Koordinirano svjetsko vrijeme

Tablica 1.6. Kratice

2 OBJAVE I ODGOVORNOSTI ZA REPOZITORIJ

2.1 Identifikacija tijela koje vodi repozitorij

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

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

2.2 Objava informacija o certificiranju

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

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

2.2.1 Sadržaji repozitorija

Na internetskim stranicama Fina PKI repozitorija objavljuju se:

- aktualna opća pravila pružanja usluga certificiranja,
- pravilnik o postupcima certificiranja,
- prijašnje verzije općih pravila pružanja usluga certificiranja i pravilnika o postupcima certificiranja,
- uvjeti i izjave o pružanju usluga izdavanja certifikata (engl. *Terms and conditions* i *PKI disclosure statement*),
- opis važećih profila certifikata,
- cjenik usluga certificiranja,
- obrasci zahtjeva za izdavanje certifikata,
- obrasci ugovora o obavljanju usluga certificiranja,
- obrasci zahtjeva za opoziv ili oporavak certifikata,
- obrasci punomoći,
- Fina Root CA certifikat i Fina RDC 2015 CA certifikat,
- objedinjena CRL Fina RDC 2015 CA,
- informacije o zakonskoj regulativi iz područja pružanja usluga certificiranja,
- informacije o postojanju dokumenata važnim za poslovanje koji ne mogu biti u cijelosti ili uopće objavljeni zbog osjetljivosti ili tajnosti sadržaja,
- aktualne lokacije Fina LRA ureda,
- korisničke upute,
- certifikati namijenjeni za provjeru i testiranje,
- obavijesti korisnicima i pouzdajućim stranama vezane uz davanje usluga certificiranja,
- ostale informacije vezane uz rad Fina RDC 2015 CA.

Preko internetske stranice repozitorija moguće je pretraživanje javnog imenika i preuzimanje certifikata koje je izdao Fina RDC 2015 CA. Za pronalaženje traženog certifikata potrebno je poznavanje i upis osnovnih podataka o subjektu.

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

U strukturi javnog imenika javno se objavljuju:

- certifikat Fina RDC 2015 CA,
- objedinjena CRL i segmentirana CRL za Fina RDC 2015 CA.

Adresa javnog LDAP imenika za Fina RDC 2015 je ldap://rdc-ldap2.fina.hr.

Putem Fina OCSP servisa dostupne su informacije o statusu izdanih certifikata koje izdaje Fina RDC 2015 CA. Adresa Fina OCSP servisa je http://ocsp.fina.hr.

Adrese na kojima se objavljuju CRL Fina RDC 2015 CA navedene su u točki 4.10.1 ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta.

U Fina PKI repozitoriju ne objavljuju se povjerljivi podaci.

Fina posjeduje i održava testne web stranice koje omogućuju Isporučiteljima aplikacijskih softvera testiranje vlastitog softvera s korisničkim certifikatima ulančanim do Fina Root CA certifikata. U tu svrhu Fina održava zasebne web stranice koje upotrebljavaju valjan, istekli i opozvani korisnički certifikat, a koje se nalaze na sljedećim web adresama:

- https://testsslvalid.fina.hr,
- https://testsslexpired.fina.hr,
- https://testsslrevoked.fina.hr.

2.2.2 Postupci objave sadržaja i upravljanja repozitorijem

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

Izdani certifikati i pripadajuće informacije objavljuju se po njihovu izdavanju.

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

Fina RDC 2015 CA automatski objavljuje pripadajuće CRL na javnom imeniku i na internetskim stranicama repozitorija nakon njihova izdavanja.

Objavu nove verzije cjenika odobrava voditelj Centra elektroničkog poslovanja.

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

2.3 Vrijeme ili učestalost objavljivanja

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

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

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

Učestalost objave CRL za certifikate koje izdaje Fina RDC 2015 CA definirana je u točki 4.9.7 ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta.

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

2.4 Kontrole pristupa repozitoriju

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

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

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

3 IDENTIFIKACIJA I POTVRĐIVANJE IDENTITETA SUBJEKTA

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

3.1 Određivanje imena

3.1.1 Tipovi imena

Podaci o Subjektu koji se upisuju u certifikat odnose se na autentični naziv Subjekta. Polje „*Subject*“ u certifikatu usklađeno je s preporukom IETF RFC 5280 [16].

Polje *Subject* u OVCP certifikatima sadrži puni kvalificirani naziv poslužitelja (u daljnjem tekstu: FQDN) ili IP adresu poslužitelja.

Ukoliko bilo koji podatak koji se unosi u atribute *localityName* i *organizationName* polja „*Subject*“ sadrži posebne znakove ili slova koja nisu sadržana u engleskoj ili hrvatskoj abecedi, takvi znakovi se zamjenjuju najbližim znakom engleske abecede sukladno Fininim pravilima korištenja zamjenskih znakova.

3.1.2 Smislenost imena

Vrijednosti u atributima polja *Subject* određuju se na sljedeći način:

- serialNumber: Identifikator pravne osobe sastavljen na način koji pokazuje značenje njegovog sadržaja: VAT, dvoslovčani ISO kod države sjedišta pravne osobe, „-„, OIB pravne osobe te točkom odijeljeni broj W koji predstavlja Fininu internu oznaku,
- commonName: FQDN ili IP adresa poslužitelja,
- localityName: Mjesto sjedišta pravne osobe,
- organizationName: Naziv pravne osobe,
- countryName: HR.

Ekstenzija *Subject Alternative Name* sadrži FQDN ili IP adresu poslužitelja.

3.1.3 Anonimnost korisnika ili pseudonimi

Anonimnost i pseudonimi korisnika nisu podržani.

3.1.4 Pravila tumačenja raznih oblika imena

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

Tumačenje oblika imena za certifikate		
Atribut po X.520	**Fina RDC 2015**	**Pojašnjenje**
serialNumber	VAT, dvoslovčani ISO kod države prebivališta pravne osobe, „-„, OIB pravne osobe, „.“,W (interni broj Fine)	Npr. VATHR-12345678901.1
commonName (CN)	Puni kvalificirani naziv poslužitelja (FQDN) ili IP adresa poslužitelja	Samo jedan puni kvalificirani naziv poslužitelja (FQDN) ili samo jedna IP adresa poslužitelja
localityName (L)	Mjesto sjedišta pravne osobe	Mjesto sjedišta pravne osobe
organizationName (O)	Puni registrirani skraćeni naziv pravne osobe	Puni registrirani skraćeni naziv pravne osobe ili naziv pravne osobe ako skraćeni naziv nije registriran.
countryName (C)	HR	Dvoslovčani ISO kod Republike Hrvatske

Tablica 3.1. Tumačenje oblika imena za certifikate po X.520 normi

Ekstenzija *Subject Alternative Name* sadrži barem jedan FQDN ili jednu IP adresu poslužitelja od kojih je jedan FQDN ili IP adresa upisana u atributu *Common Name.*

Uporaba zamjenskog znaka (engl. *Wildcard*) u nazivu FQDN ili IP adrese nije dopuštena.

Ekstenzija *Subject Alternative Name* ne smije sadržavati Rezerviranu IP adrese ili Interni naziv.

3.1.5 Jedinstvenost imena

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

Jedinstvenost imena u OVCP certifikatima osigurana je vrijednošću atributa *Serial Number* i *Common Name* u polju *Subject* certifikata na način da se u ovaj atribut razlikovnog imena certifikata upisuje jedinstveni FQDN poslužitelja ili IP adresa.

3.1.6 Prepoznavanje, potvrđivanje identiteta i uloga zaštitnog znaka

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

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

3.2 Inicijalno utvrđivanje identiteta

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

Pri izdavanju certifikata iz opsega ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta Fina provjerava i potvrđuje identitet Skrbnika temeljem neposredne fizičke identifikacije ili korištenjem metoda koje pružaju odgovarajuću razinu sigurnosti utvrđivanja identiteta.

3.2.1 Metoda dokazivanja posjeda privatnog ključa

3.2.1.1 Dokazivanje posjeda privatnog ključa za SSL certifikat razine 2 (OVCP)

Par ključeva za *SSL certifikat razine 2 (OVCP)* može generirati Fina na svojoj lokaciji ili ga može generirati Skrbnik na lokaciji Korisnika, sukladno točki 6.1.1.2. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta.

a) Par ključeva generira Fina

Ukoliko generiranje para ključeva za *SSL certifikat razine 2 (OVCP)* obavlja Fina dokazivanje da Skrbnik posjeduje privatni ključ čiji je javni ključ dostavljen na certificiranje osigurava se sljedećim postupkom:

- Generiranje para ključeva putem Fina CMS-a pokreće registrirani i autenticirani Skrbnik, sukladno postupku opisanom u točki 4.3.1.1.a) ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta,
- Generiranje para ključeva u Fini provodi se sukladno točki 6.1.1.2. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta,
- Izdavanje certifikata *SSL certifikat razine 2 (OVCP)* obavlja se sukladno točki 4.3.1.1.a) ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta,
- Skrbnik uporabom Fina CMS-a i sigurnog TLS kanala preuzima izdani par ključeva i certifikat u PKCS#12 datoteci zaštićenoj svojim aktivacijskim podatkom i time dolazi u posjed privatnog ključa.

b) Par ključeva generira Skrbnik na lokaciji Korisnika

Ukoliko par ključeva *SSL certifikat razine 2 (OVCP)* generira Skrbnik na lokaciji Korisnika dokazivanje da Skrbnik posjeduje privatni ključ čiji je javni ključ dostavljen na certificiranje osigurava se sljedećim postupkom:

- Skrbnik na lokaciji Korisnika provodi generiranje para ključeva za *SSL certifikat razine 2 (OVCP)* sukladno točki 6.1.1.2. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta.
- Skrbnik na lokaciji Korisnika izrađuje PKCS#10 zahtjev u kojem se nalazi javni ključ iz generiranog para ključeva, a zahtjev potpisuje privatnim ključem iz istog generiranog para ključeva.

- Registrirani i autenticirani Skrbnik uporabom Fina CMS-a i sigurnog TLS kanala u Fina RDC 2015 CA šalje PKCS#10 zahtjev za izdavanje certifikata.
- Fina RDC 2015 CA prije izdavanja certifikata verifikacijom potpisa u PKCS#10 zahtjevu utvrđuje da Skrbnik posjeduje pripadajući privatni ključ.

3.2.1.2 Dokazivanje posjeda privatnog ključa za SSL certifikat razine 3 (OVCP)

Par ključeva za *SSL certifikat razine 3 (OVCP)* uvijek generira Skrbnik unutar HSM modula na lokaciji Korisnika, sukladno točki 6.1.1.2. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta. Dokazivanje da Skrbnik posjeduje privatni ključ čiji je javni ključ dostavljen na certificiranje osigurava se sljedećim postupkom:

- Generiranje para ključeva provodi Skrbnik uvijek unutar HSM modula, sukladno certifikacijskoj dokumentaciji HSM modula na lokaciji Korisnika,
- Javni ključ se PKCS#10 zahtjevom koji je potpisan pripadajućim privatnim ključem iz generiranog para ključeva uporabom sigurnog TLS kanala prosljeđuje u Fina RDC 2015 CA na certificiranje. Odgovornost je Skrbnika da je javni ključ koji se dostavlja na certificiranje iz para ključeva generiranog unutar HSM modula.
- Fina RDC 2015 CA prije izdavanja certifikata verifikacijom potpisa u PKCS#10 zahtjevu utvrđuje da Skrbnik posjeduje pripadajući privatni ključ.

3.2.2 Potvrda identiteta poslovnog subjekta i domene

3.2.2.1 Potvrda identiteta poslovnog subjekta

Podnositelj zahtjeva u zahtjevu za izdavanje certifikata navodi točno i cjelovito popunjene podatke o pravnoj osobi. Zahtjev potpisuje osoba ovlaštene za zastupanje.

Dodatno, pravna osoba, ovisno o važećim zakonima i propisima Republike Hrvatske koji reguliraju obavljanje aktivnosti pravne osobe, prilaže sljedeću dokumentaciju za utvrđivanje pravnog subjektiviteta i identiteta:

- izvornik ili presliku, uz predočenje izvornika, važećeg izvatka, ne starijeg od šest mjeseci, iz nadležnog registra, sukladno zakonima i propisima Republike Hrvatske, zbog dokaza upisa u nadležni registar poslovne djelatnosti ili zakon, odnosno drugi propis temeljem kojeg je pravna osoba osnovana ako nije određeno da se pravna osoba upisuje u registar,
- presliku identifikacijske isprave fizičke osobe ovlaštene za zastupanje pravne osobe.

Po inicijalnom prikupljanju podataka iz zahtjeva i zaprimanju priložene dokumentacije obavlja se identifikacija i potvrda identiteta pravne osobe na sljedeći način:

- Provjerava se cjelovitost, autentičnost i valjanost dokumentacije za registriranje pravne osobe.
- Provjerava se je li pravna osoba upisana u nadležni registar ako je po propisima dužna upisati se u isti, odnosno akt nadležnog organa ili propis o osnivanju pravne osobe, ako pravna osoba nije dužna upisati se u registar.

Fina RA mreža dodatno provjerava točnost provjerljivih podataka upisanih u zahtjevu. Provjera se provodi temeljem upita na nacionalni OIB sustav kroz Fina RA aplikaciju za podatke koji su dohvatljivi iz OIB sustava.

Provjerava se ovlaštenje osobe ovlaštene za zastupanje pravne osobe 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 pravne osobe.

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

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

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

3.2.2.2 Provjera zemlje povezane sa Subjektom

Središnji Fina RA prije odobrenja zahtjeva za izdavanje certifikata provjerava da je zemlja navedena u polju *countryName* certifikata povezana sa Subjektom navedenim u polju *commonName* certifikata.

Ovu provjeru obavlja Službenik za validaciju na jedan od sljedeća dva načina:

- Provjerava se da je adresno područje IP adrese Subjekta dodijeljeno od zemlje navedene u polju *countryName* certifikata. Povezanost IP adrese i FQDN-a dostavljenog u zahtjevu za izdavanje certifikata provjerava se usporedbom s pripadajućim DNS zapisom kojeg vodi nadležno tijelo.
- Provjeravaju se informacije koje pruža registrator naziva domene.

3.2.2.3 Provjera prava korištenja domene

Prije odobravanja izdavanja certifikata Službenik za validaciju u Središnjem Fina RA za svaki FQDN naveden u zahtjevu za izdavanje certifikata provjerava izvornost i točnost naziva

domene te također provjerava vlasništvo ili pravo korištenja naziva domene od strane pravne osobe koja podnosi zahtjev.

3.2.2.3.1 E-mail, telefaks ili dopis upućen poštom na Kontakt za domenu

Ova metoda provjere se temelji na točki 3.2.2.4.2 dokumenta CA/Browser Forum BRG [19].

Provjera se obavlja slanjem poruke koja sadrži Slučajnu vrijednosti na e-mail adresu, telefaks ili poštansku adresu te zaprimanjem odgovora s potvrdom u kojoj je korištena ista Slučajna vrijednost. Poruka sa Slučajnom vrijednošću šalje se na e-mail adresu, broj telefaksa ili dopisom na poštansku adresu Kontakta za domenu.

Pojedinom e-mail porukom, telefaksom i dopisom upućenim poštom može se potvrditi vlasništvo ili pravo korištenja nad više domena za autorizaciju.

Središnji Fina RA može poslati ovaj e-mail, telefaks ili dopis na više primatelja, od kojih je svaki primatelj identificiran od strane registratora naziva domene koji predstavlja registratora naziva domene za svaki pojedini FQDN koji se provjerava uporabom e-maila, telefaksa ili dopisa upućenog poštom.

Slučajna vrijednost predstavlja jedinstveni podatak u svakom e-mailu, telefaksu ili dopisu upućenog poštom.

Središnji Fina RA može ponovno u cijelosti poslati e-mail, telefaks ili dopis upućen poštom, uključujući i ponovnu uporabu iste Slučajne vrijednosti, uz uvjet da cjelokupni kontekst komunikacije i primatelji ostanu nepromijenjeni.

Slučajna vrijednost ostaje važeća za uporabu u odgovoru za potvrdu najviše 30 dana od njenog kreiranja.

3.2.2.3.2 Konstruirana e-mail adresa kontakta za domenu

Ova metoda provjere se temelji na točki 3.2.2.4.4 dokumenta CA/Browser Forum BRG [19].

Provjera se obavlja:

- slanjem e-mail poruke na jednu ili više e-mail adresa izrađenih uporabom riječi „admin“, „administrator“, „webmaster“, „hostmaster“, ili „postmaster“ koje se koriste za lokalni dio e-mail adrese, a nakon čega se dodaje znak „@“ iza kojeg slijedi naziv domene za autorizaciju,
- e-mail poruka sadrži Slučajnu vrijednost,
- zaprimanjem odgovora s potvrdom u kojoj je korištena ista Slučajna vrijednost.

Pojedinom e-mail porukom može se potvrditi vlasništvo ili pravo korištenja nad više FQDN-ova osiguravajući da je domena za autorizaciju upotrjebljena u e-mail adresi domena za autorizaciju svakog pojedinog FQDN-a koji se potvrđuje.

Slučajna vrijednost predstavlja jedinstveni podatak u svakom e-mailu.

E-mail može ponovno u cijelosti biti poslan uključujući i ponovnu uporabu iste Slučajne vrijednosti, uz uvjet da cjelokupni kontekst komunikacije i primatelj ostane nepromijenjen.

Slučajna vrijednost ostaje važeća za uporabu u odgovoru za potvrdu najviše 30 dana od njenog kreiranja.

3.2.2.4 Provjera i potvrđivanje IP adrese

Prije odobravanja izdavanja certifikata Službenik za validaciju u Središnjem Fina RA za svaku IP adresu navedenu u zahtjevu za izdavanje certifikata provjerava izvornost i točnost IP adrese, te također provjerava pravo korištenja i upravljanja IP adresom u vrijeme izdavanja certifikata od strane pravne osobe koja podnosi zahtjev.

Provjera se obavlja na jedan od sljedećih načina:

- pribavljanjem dokumentacije o dodjeli IP adrese od strane Internet Assigned Numbers Authority-a (IANA) ili regionalnog Internet registra (RIPE, APNIC, ARIN, AfriNIC, LACNIC),
- provođenjem pretraživanja pomoću *reverse-IP address lookup* metode te nakon toga provjerom vlasništva ili prava korištenja naziva domene dobivenog ovim pretraživanjem, na način opisan u točki 3.2.2.3 ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta,
- uporabom druge metode provjere koja osigurava da Fina kao pružatelj usluga povjerenja vodi dokumentiranu evidenciju kojom se dokazuje da korištena metoda provjere prava upravljanja i korištenja IP adrese od strane podnositelja zahtjeva osigurava razinu pouzdanja koja je jednaka ili veća od razine pouzdanja prethodno opisanih metoda iz ove točke.

3.2.3 Potvrda identiteta fizičke osobe

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

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

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

- ime i prezime,
- OIB (ako je OIB dodijeljen),
- datum, mjesto i zemlja rođenja,
- podatke o identifikacijskoj ispravi iz točke 3.2.3.3. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta,
- poštansku adresu,
- e-mail adresu,
- broj telefona.

Za izdavanje certifikata Fina prikuplja i dokaz o povezanosti Skrbnika s pravnom osobom kojoj se izdaje certifikat.

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

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

Identifikacija fizičkih osoba koji su strani državljani se može provesti na dva načina, ovisno o tome je li stranom državljaninu dodijeljen OIB u Republici Hrvatskoj. U slučaju da strani državljanin ima dodijeljen OIB, identifikacija se obavlja na način identičan identifikaciji hrvatskih građana. U slučaju da stranom državljaninu nije dodijeljen OIB prikupljaju se podaci o datumu i mjestu rođenja, te mjestu prebivališta. Ove dodatne podatke Fina RA mreža prikuplja i provjerava njihovu točnost usporedbom istih u priloženoj dokumentaciji.

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

3.2.3.1 Postupak neposredne identifikacije

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

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

- provjerava se cjelovitost, autentičnost i važenje identifikacijske isprave,
- provjerava se točnost podataka o fizičkoj osobi te njen potpis u zahtjevu za izdavanje certifikata s podacima i potpisom iz identifikacijske isprave. Dodatno se obavlja provjera podataka iz važeće identifikacijske isprave upitom na nacionalni OIB sustav, osim za strane državljane koji nemaju dodijeljen OIB u Republici Hrvatskoj.

3.2.3.2 Postupak posredne identifikacije

Postupak posredne identifikacije fizičke osobe provodi se na način koji pruža primjerenu razinu sigurnosti utvrđivanja identiteta fizičke osobe.

a) Fina provodi postupak posredne identifikacije fizičke osobe pomoću certifikata kvalificiranog elektroničkog potpisa izdanog temeljem neposredne identifikacije fizičke osobe.

b) Postupak posredne identifikacije fizičke osobe Fina može provoditi i provjerom podataka iz preslika dviju različitih identifikacijskih isprava, definiranih u točki 3.2.3.3. b) ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta.

3.2.3.3 Prihvatljive vrste identifikacijskih isprava

Fizičke osobe dokazuju svoj identitet:

a) u postupku neposredne identifikacije valjanom osobnom iskaznicom ili putovnicom,
b) u postupku posredne identifikacije iz točke 3.2.3.2. b) ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta preslikom dviju različitih identifikacijskih isprava s fotografijom izdanim od nadležnog nacionalnog tijela. Prihvatljive identifikacijske isprave u ovom slučaju su osobna iskaznica, putovnica ili vozačka dozvola.

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

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

3.2.4 Informacije o korisniku koje se ne provjeravaju

Certifikati iz opsega ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta sadrže samo podatke koje je Fina provjerila.

3.2.5 Provjera identiteta ovlaštenih osoba

Prije izdavanja certifikata Fina provodi utvrđivanje identiteta osobe ovlaštene za zastupanje provjerom podataka iz dostavljene dokumentacije za utvrđivanje pravnog subjektiviteta pravne osobe navedene u točki 3.2.2. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta i usporedbom s podacima iz preslike važeće identifikacijske isprave osobe ovlaštene za zastupanje.

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

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

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

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

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

3.2.6 Kriteriji interoperabilnosti

Nema odredbi.

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

Fina provodi postupke identifikacije i potvrde identiteta podnositelja zahtjeva za:

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

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

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

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

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

Postupak identifikacije i potvrđivanja identiteta podnositelja zahtjeva kod obnove certifikata provodi se na lokaciji Fina RA mreže. Postupak identifikacije i potvrđivanja identiteta Skrbnika provodi se sukladno odredbama točke 3.2.3. $CPS_{WSA\text{-}eIDAS}$ dokumenta.

Provjera pravne osobe provodi se utvrđivanjem je li došlo do promjena u podacima pravne osobe u odnosu na podatke kojima trenutno raspolaže Fina RA sustav. Ova provjera se obavlja uvidom u podatke iz dostavljenog zahtjeva za izdavanje certifikata i upitom na nacionalni OIB sustav te po potrebi uvidom u podatke koje na pouzdan način objavljuje nadležno tijelo. Ukoliko se podaci o pravnoj osobi koji su sadržani u certifikatu razlikuju od važećih podataka u Fina RA sustavu, provodi se postupak izmjene podataka u certifikatu sukladno točki 4.8. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta.

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

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

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

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

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

3.3.4 Identifikacija i potvrđivanje identiteta korisnika za oporavak certifikata

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

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

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

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

Fina provodi identifikaciju i potvrđivanje identiteta podnositelja zahtjeva za certifikata ovisno o načinu dostave zahtjeva:

- Osobno podnošenje zahtjeva za opoziv u registracijskom uredu Fina RA mreže

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

- postupkom neposredne identifikacije podnositelja zahtjeva uz predočenje identifikacijske isprave podnositelja zahtjeva iz točke 3.2.3.3. a) ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta, ili
- usporedbom potpisa podnositelja zahtjeva i podataka na zahtjevu s potpisom i podacima prikupljenih prilikom registracije.

- Podnošenje zahtjeva za opoziv poštanskom dostavom ili dostavom preko dostavljača

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

- Elektronička dostava zahtjeva za opoziv na e-mail adresu

  Identifikacija i potvrđivanje identiteta podnositelja zahtjeva provodi se verifikacijom i validacijom zahtjeva potpisanog naprednim elektroničkim potpisom, odnosno naprednim elektroničkim pečatom.

- Podnošenje zahtjeva za opoziv telefonskim putem

  Identifikacija podnositelja zahtjeva provodi se predstavljanjem podnositelja svojim imenom i prezimenom te navođenjem naziva poslovnog subjekta. Potvrđivanje identiteta podnositelja zahtjeva provodi se dokazivanjem njegovog poznavanja zaporke za opoziv certifikata. Ovlašteni službenik koji je zaprimio telefonski poziv provjerava istovjetnost zaporke koju izgovara podnositelj zahtjeva i zaporke koja je predana u RA mrežu prilikom podnošenja zahtjeva za izdavanje tog certifikata.

4 OPERATIVNI ZAHTJEVI NA ŽIVOTNI CIKLUS CERTIFIKATA

4.1 Podnošenje zahtjeva za izdavanje certifikata

4.1.1 Tko može podnijeti zahtjev za izdavanje certifikata

Zahtjev za izdavanje certifikata podnose pravne osobe, 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

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

Prije inicijalnog izdavanja svakog certifikata Korisnik sklapa s Finom ugovor o obavljanju usluga certificiranja kojeg potpisuje osoba ovlaštena za zastupanje pravne osobe.

Zahtjev za izdavanje certifikata podnosi se u registracijskim uredima Fina RA mreže.

Zahtjev za izdavanje certifikata može se podnijeti i u elektroničkom obliku.

4.1.2.1 Proces podnošenja zahtjeva za izdavanje certifikata

Zahtjev za izdavanje certifikata podnosi Skrbnik.

U slučaju predaje zahtjeva i ugovora u elektroničkom obliku zahtjev i ugovor se potpisuju naprednim elektroničkim potpisom.

Zahtjev za izdavanje certifikata dodatno potpisuje osoba ovlaštena za zastupanje pravne osobe.

Ako je rješenjem o upisu pravne osobe 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 $CPS_{WSA\text{-}eIDAS}$ dokumenta.

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

U slučaju da je zahtjev za izdavanje certifikata predan u elektroničkom obliku, Finin servis za zaprimanje elektroničkih obrazaca zahtjeva provjerava zahtjev i dodaje vremenski žig s

vremenom zaprimanja zahtjeva. Službenik za registraciju u Fina RA mreži provjerava podatke iz zahtjeva, te provodi validaciju svih naprednih elektroničkih potpisa na zahtjevu. Po pozitivnoj provjeri elektroničkog zahtjeva, isti se upisuje u RA aplikaciju.

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

4.1.2.2 Odgovornosti i obveze u procesu podnošenja zahtjeva za izdavanje certifikata

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

Ugovor na strani Korisnika potpisuje osoba ovlaštena za zastupanje pravne osobe.

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

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

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

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

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

4.2 Obrada zahtjeva za izdavanje certifikata

4.2.1 Obavljanje identifikacije i potvrđivanje identiteta

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

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

- Nakon zaprimanja zahtjeva za izdavanje certifikata na kojem je označeno izdavanje certifikata, Službenik za registraciju pregledava zaprimljeni zahtjev zbog kontrole, sukladno postupcima opisanim u točkama 3.2.2., 3.2.3. i 3.2.5. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta.
- Ako zahtjev nije točno i u cijelosti popunjen te pravilno potpisan Službenik za registraciju mora odbiti takav zahtjev sukladno točki 4.2.2. ovog $CPS_{WSA\text{-}eIDAS}$

dokumenta i podnositelju zahtjeva pojasniti način ispravnog i točnog popunjavanja i potpisivanja zahtjeva.

- Službenik za registraciju provjerava je li pravna osoba već registrirana. Ako zapis o registraciji pravne osobe ne postoji u Fina RA sustavu, upisom podataka iz zahtjeva i dostavljene dokumentacije uporabom Fina RA aplikacije i provjerom podataka upitom na nacionalni OIB sustav (ukoliko je primjenjivo), izrađuju se zapisi o registraciji pravne osobe,
- Službenik za registraciju provjerava je li Skrbnik naveden u zahtjevu već registriran. Ako zapis o registraciji Skrbnika ne postoji u Fina RA sustavu, upisom podataka iz zahtjeva i dostavljene dokumentacije uporabom Fina RA aplikacije i provjerom podataka upitom na nacionalni OIB sustav (ukoliko je primjenjivo), izrađuju se zapisi o registraciji Skrbnika.
- Službenik u Fina RA mreži postavlja status zahtjeva na „pripremljeno“ čime se u Fina RA aplikaciji naznačuje odobrenje zahtjeva. Tom prilikom generira se i razlikovno ime (*Distinguished Name*, DN) subjekta.
- Službenik za registraciju putem Fina RA aplikacije svojim certifikatom elektronički potpisuje narudžbu koja sadrži provjerene podatke iz zahtjeva te narudžbu prosljeđuje na daljnju obradu u Fina RDC 2015 CA.

4.2.2 Odobravanje ili odbijanje zahtjeva za izdavanje certifikata

Službenik za registraciju u Fina RA mreži provjerava podatke iz dokumenata koje prilaže podnositelj zahtjeva i potvrđuje točnost i cjelovitost informacija u zahtjevu za izdavanje certifikata. Službenik za registraciju u Fina LRA potpisom ovjerava uspješnu i pravilnu identifikaciju podnositelja zahtjeva te zaštićenim putem dostavlja podatke u Središnji Fina RA ili odbija zahtjev u slučaju neuspješne identifikacije ili netočnosti dostavljenih informacija

Službenik za validaciju u Središnjem Fina RA provodi provjeru podataka sukladno točki 3.2.2.1. i točki 3.2.2.2.ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta te provodi postupak provjere CAA zapisa za svaki dNSName u subjectAltName ekstenziji certifikata prije njegovog izdavanja sukladno postupku iz RFC 6844 – DNS Certification Authority Authorization (CAA) Resource Record [20] i slijedi upute za obradu iz pronađenih zapisa. CAA identifikacijska domena Fina CA-ova je „fina.hr“.

Ukoliko Službenik za registraciju ili Službenik za validaciju odbije zahtjev za izdavanje certifikata, pismenim ili usmenim putem obavještava podnositelja o odbijanju zahtjeva i razlozima odbijanja istog.

Zahtjev za izdavanje certifikata može se odbiti zbog:

- netočnih ili nepotpunih podataka,
- nepravilno potpisanog zahtjeva, odnosno ugovora,
- nepotpune ili neispravne priložene dokumentacije,
- neispunjenja zahtjeva za vlasništvo ili pravo korištenja naziva domene, odnosno IP adrese poslužitelja navedene u zahtjevu za izdavanje certifikata,
- prethodnih neodgovarajućih postupaka i nepoštivanja ugovornih obveza korisnika,

- zakonske zabrane,
- neispunjenja ograničenja iz CAA zapisa,
- sumnje na pokušaj prijevare.

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 Fina RA mreži.

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

4.3 Izdavanje certifikata

Fina RDC 2015 CA izdaje certifikat nakon provedenih svih procesa provjere podataka, odobrenja zahtjeva za izdavanje certifikata od strane Službenika za registraciju te prihvaćanja certifikata od strane Skrbnika. Izdavanje certifikata provodi se na siguran način kako bi se osigurala autentičnost certifikata. Iz tog razloga Fina ima implementirane mjere kojima se sprječava krivotvorenje certifikata.

Mjere protiv krivotvorenja certifikata uključuju:

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

4.3.1 Radnje CA tijekom izdavanja certifikata

4.3.1.1 Izdavanje SSL certifikata razine 2 (OVCP)

a) Par ključeva generira Fina

Izdavanje *SSL certifikata razine 2 (OVCP)* kada par ključeva generira Fina provodi se sljedećim postupkom:

- nakon potvrde narudžbe za izdavanje certifikata iz RA aplikacije od strane Službenika za registraciju Fina CMS sustav generira i dostavlja autentikacijske podatke za prijavu Skrbnika na Fina CMS,
- autentikacijski podaci za prijavu Skrbniku se dostavljaju elektronički korištenjem dva odvojena kanala ili ove podatke Skrbniku uručuje Službenik za registraciju osobno, uz prethodnu neposrednu identifikaciju,

- po udaljenom pristupu Fina CMS-u s korisničke lokacije, autentikaciji Skrbnika te iniciranju postupka uporabom Fina CMS sustava, Fina CMS sustav generira par korisničkih ključeva te se zahtjev za izdavanje certifikata dostavlja u Fina RDC 2015 CA,
- Fina RDC 2015 CA certificira javni ključ izdajući certifikat prema profilu za tip certifikata *SSL certifikata razine 2 (OVCP)*,
- Skrbnik uporabom Fina CMS-a upisuje aktivacijski podatak za zaštitu privatnog ključa,
- Fina CMS Skrbniku dostavlja privatni ključ i certifikat u PKCS#12 datoteci zaštićenoj aktivacijskim podatkom putem sigurnog TLS kanala.

b) Par ključeva generira Skrbnik na lokaciji Korisnika

Izdavanje *SSL certifikata razine 2 (OVCP)* kada par ključeva generira Skrbnik na lokaciji Korisnika provodi se sljedećim postupkom:

- nakon potvrde narudžbe za izdavanje certifikata iz RA aplikacije od strane Službenika za registraciju Fina CMS sustav generira i dostavlja autentikacijske podatke za prijavu Skrbnika na Fina CMS,
- autentikacijski podaci za prijavu Skrbnika dostavljaju se elektronički korištenjem dva odvojena kanala ili ove podatke Skrbniku Službenik za registraciju uručuje osobno, uz prethodnu neposrednu identifikaciju,
- Skrbnik na lokaciji Korisnija provodi generiranje para ključeva sukladno točki 6.1.1.2. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta,
- Skrbnik na lokaciji Korisnika izrađuje PKCS#10 zahtjev u kojem se nalazi javni ključ iz generiranog para ključeva, a zahtjev potpisuje privatnim ključem iz istog generiranog para ključeva,
- Skrbnik uporabom Fina CMS-a i sigurnog TLS kanala u određeni Fina RDC 2015 CA šalje PKCS#10 zahtjev za izdavanje certifikata,
- Fina RDC 2015 CA certificira javni ključ izdajući korisniku certifikat prema profilu za tip certifikata *SSL certifikata razine 2 (OVCP)*,
- Skrbnik preuzima izdani certifikat putem Fina CMS sustava.

4.3.1.2 Izdavanje SSL certifikat razine 3 (OVCP)

Izdavanje certifikata tipa *SSL certifikat razine 3 (OVCP)* provodi se sljedećim postupkom:

- nakon potvrde narudžbe za izdavanje certifikata iz RA aplikacije od strane Službenika za registraciju Fina CMS sustav generira i dostavlja autentikacijske podatke za prijavu Skrbnika na Fina CMS,
- autentikacijski podaci za prijavu Skrbnika dostavljaju se elektronički korištenjem dva odvojena kanala ili ove podatke Skrbniku Službenik za registraciju uručuje osobno, uz prethodnu neposrednu identifikaciju,
- Skrbnik na lokaciji Korisnika provodi generiranje para ključeva unutar HSM modula, sukladno točki 6.1.1.2. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta,

- Skrbnik na lokaciji Korisnika izrađuje PKCS#10 zahtjev u kojem se nalazi javni ključ iz generiranog para ključeva, a zahtjev potpisuje privatnim ključem u HSM modulu iz istog generiranog para ključeva,
- Skrbnik uporabom TLS kanala u Fina RDC 2015 CA šalje PKCS#10 zahtjev za izdavanje certifikata,
- Fina RDC 2015 CA certificira javni ključ izdajući korisniku certifikat prema profilu za tip certifikata *SSL certifikata razine 3 (OVCP)*,
- Skrbnik preuzima izdani certifikat putem Fina CMS sustava.

4.3.2 Obavještavanje korisnika od strane CA o izdavanju certifikata

Skrbnik se obavještava o mogućnosti preuzimanja certifikata putem e-maila.

Skrbnik preuzima certifikat *online*, te je o izdavanju certifikata obaviješten tijekom samog *online* postupka preuzimanja certifikata.

4.4 Prihvaćanje certifikata

Prihvaćanje certifikata od strane Skrbnika preduvjet je za izdavanje i korištenje certifikata.

Prihvaćajući certifikat Skrbnik prihvaća da su svi sve informacije koje će biti sadržane u certifikatu točne u trenutku njegova prihvaćanja.

4.4.1 Provedba prihvaćanja certifikata

Skrbnik je dužan neposredno prije izdavanja certifikata provesti provjeru sadržaja certifikata. Provjera sadržaja certifikata obavlja se uvidom u sadržaje polja *Subject* i *Issuer*, uvidom u sadržaj ekstenzije *Subject Alternative Name* te uvidom u detaljan opis profila tipa certifikata čije se izdavanje traži. Ukoliko Skrbnik prihvaća prikazani sadržaj certifikata, svoje prihvaćanje potvrđuje označavanjem prihvaćanja certifikata na ekranu CMS sučelja, uz prethodnu autentikaciju na CMS sustav.

Nakon prihvaćanja certifikata Fina RDC 2015 CA Skrbniku izdaje traženi certifikat.

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

- ispisivanjem, odnosno prikazivanjem podataka certifikata izravnim dohvatom prethodno provjerenih podataka korisnika iz Finine baze registriranih korisnika,
- korištenjem sigurnih komunikacijskih kanala za dohvat korisničkih podataka za njihov ispis i prikaz Skrbniku te za dohvat javno objavljenog dokumenta s detaljnim opisom odobrenih profila certifikata,
- izdavanjem certifikata isključivo prema odobrenom profilu certifikata koji je naveden u izjavi o prihvaćanju, a koji je kao odobreni profil certifikata definiran i podešen u sustavu Fina RDC 2015 CA,
- primjenom mjera protiv krivotvorenja certifikata iz točke 4.3.

Ukoliko Skrbnik ne prihvaća certifikat, razloge svog neprihvaćanja može obrazložiti u registracijskom uredu RA mreže ili ih pismeno navesti i poslati u Finu na e-mail adresu info.rdc@fina.hr. Fina RA mreža pri tome prosljeđuje obavijest o neprihvaćanju i eventualnim razlozima neprihvaćanja u Središnji RA. Neprihvaćanjem certifikata Skrbnik odustaje od zahtjeva za izdavanjem certifikata, a Fina RDC 2015 CA ne izdaje certifikat koji se odnosi na taj zahtjev.

Fina Skrbniku omogućuje podnošenja novog zahtjeva za izdavanje certifikata u kojem su, po potrebi, uneseni korigirani podaci u odnosu na prethodni zahtjev.

4.4.2 Objava izdanog certifikata od strane CA

Ukoliko je osoba ovlaštena za zastupanje pravne osobe odobrila javnu objavu certifikata Fina RDC 2015 CA čini certifikat dostupnim na Fina PKI repozitoriju.

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

Certifikat je pouzdajućim stranama dostupan preko sučelja na internetskoj stranici repozitorija iz točke 2.2. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta.

4.4.3 Obavještavanje drugih strana od strane CA o izdavanju certifikata

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

4.5 Par ključeva i korištenje certifikata

4.5.1 Korištenje privatnog ključa i certifikata od strane korisnika

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

- pri generiranju parova ključeva, koristiti algoritme propisane normizacijskim dokumentom ETSI TS 119 312 [12] te duljine ključeva sukladno točke 6.1.5. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta,
- koristiti certifikat i pripadajući privatni ključ samo u svrhe propisane ovim $CPS_{WSA\text{-}eIDAS}$ dokumentom i uvjetima pružanja usluga certificiranja,
- koristiti certifikat i pripadajući privatni ključ u skladu sa zakonima i drugim propisima Republike Hrvatske te sukladno odredbama iz točke 1.4.1. i 1.4.2. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta,
- da od trenutka kad je privatni ključ u jedinstvenom posjedu Korisnika štiti privatni ključ od krađe, gubitka, izmjena i kompromitiranja,
- koristiti i čuvati privatni ključ na način koji onemogućuje njegovo neovlašteno korištenje,

- kod korištenja privatnog ključa povezanog s *SSL certifikatom razine 3 (OVCP)* privatni ključ koristiti uporabom HSM modula, sukladno točki 6.2.1.,
- kod korištenja privatnog ključa povezanog s *SSL certifikatom razine 2 (OVCP)* provoditi aktiviranje privatnog ključa prikladnim aktivacijskim podacima,
- kod korištenja privatnog ključa povezanog s *SSL certifikatom razine 2 (OVCP)* provoditi aktiviranje privatnog ključa prikladnim aktivacijskim podacima,
- koristiti certifikat i pripadajući privatni ključ samo na poslužiteljima dostupnim preko FQDN-a ili IP adrese navedenim u *Subject Alternative Name* ekstenziji certifikata,
- na čuvanje aktivacijskih podatka privatnog ključa na zaštićenom mjestu odvojenom od privatnog ključa,
- na obavještavanje Fine kao pružatelja usluga povjerenja i zahtijevanje opoziva certifikata u svim primjenjivim slučajevima navedenim u točki 4.9.1 ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta,
- nakon kompromitiranja privatnog ključa odmah i trajno prestati s njegovom uporabom i uporabom pripadajućeg certifikata.

4.5.2 Korištenje javnog ključa i certifikata od strane pouzdajuće strane

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

- voditi računa o primjerenoj uporabi i ograničenjima uporabe certifikata koja su naznačena u certifikatu ili na njih upućuju reference u certifikatu,
- voditi računa o primjerenoj uporabi i zabrani uporabe javnog ključa i certifikata opisanim u točki 1.4. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta,
- obaviti provjeru roka važenja svih certifikata u certifikacijskom lancu te provesti provjeru certifikata prema postupcima za validaciju certifikacijske staze, sukladno dokumentu IETF RFC 5280 [16],
- obaviti provjeru statusa opozvanosti certifikata putem OCSP servisa ili temeljem zadnje izdane CRL, kako je propisano ovim $CPS_{WSA\text{-}eIDAS}$ dokumentom.

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

4.6 Obnova certifikata

Fina provodi obnovu certifikata na način da za postojeću pravnu osobu čiji je certifikat pred istekom, na zahtjev pravne osobe generira novi par ključeva i izdaje novi certifikat. Razlikovno ime (DN) subjekta novog certifikata jednako je razlikovnom imenu (DN-u) Subjekta certifikata koji je pred istekom.

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

4.6.1 Razlozi za obnovu certifikata

Vidi točku 4.7.1.

4.6.2 Tko može tražiti obnovu certifikata

Vidi točku 4.7.2.

4.6.3 Obrada zahtjeva za obnovu certifikata

Vidi točku 4.7.3.

4.6.4 Obavještavanje korisnika o obnovi certifikata

Vidi točku 4.7.4.

4.6.5 Provedba prihvaćanja obnovljenog certifikata

Vidi točku 4.7.5.

4.6.6 Objava obnovljenog certifikata od strane CA

Vidi točku 4.7.6.

4.6.7 Obavještavanje drugih strana o obnovi certifikata

Vidi točku 4.7.7.

4.7 Obnova certifikata uz generiranje novog para ključeva

Nakon provedene identifikacije i potvrde identiteta podnositelja zahtjeva za:

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

Fina izdaje certifikat čiji je razlikovno ime (DN) i drugi parametri jednaki kao i parametri certifikata na koji se zahtjev odnosi, ali s novim javnim ključem, novim serijskim brojem certifikata, novim vremenskim periodom valjanosti i novim potpisom Fina RDC 2015 CA.

4.7.1 Razlozi za obnovu certifikata uz generiranje novog para ključeva

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

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

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

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

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

U postupku oporavka Fina RDC 2015 CA će opozvati certifikat čiji se oporavak traži te će izdati novi certifikat.

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

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

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

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

4.7.2 Tko može zatražiti certificiranje novog javnog ključa

Zahtjev za obnovu, oporavak, odnosno izdavanje certifikata nakon isteka mogu podnijeti Skrbnik ili osoba ovlaštena za zastupanje pravne osobe.

4.7.3 Obrada zahtjeva za obnovu certifikata uz generiranje novog para ključeva

Zahtjev za obnovu certifikata uz generiranje novog para ključeva podnosi se u Fina RA mreži te se identifikacija i potvrđivanje identiteta fizičkih osoba i pravne osobe iz zahtjeva provodi sukladno točki 3.3.1. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta. Službenik za registraciju u Fina RA mreži provjerava podatke iz zahtjeva i potvrđuje točnost i cjelovitost informacija u zahtjevu. Odobravanje ili odbijanje zahtjeva provodi registracijski ured Fina RA mreže u kojem je zahtjev podnesen.

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

Nakon provjere autentičnosti i valjanosti zahtjeva Fina RDC 2015 CA izdaje certifikat sukladno točki 4.3.1. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta.

4.7.4 Obavještavanje korisnika o obnovi certifikata uz generiranje novog para ključeva

Fina tijekom mjeseca koji prethodi mjesecu u kojem ističe certifikat obavještava Skrbnika o skorom isteku certifikata te ga poziva na redovnu obnovu certifikata uz generiranje novog para ključeva.

Obavještavanje Skrbnika o obnovi certifikata provodi se sukladno točki 4.3.2. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta.

4.7.5 Provedba prihvaćanja obnovljenog certifikata s generiranim novim parom ključeva

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

4.7.6 Objavljivanje certifikata po obnovi s generiranjem novog para ključeva

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

4.7.7 Obavještavanje drugih strana o obnovi certifikata s generiranim parom ključeva

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

4.8 Izmjene unutar certifikata

Pravne osobe imaju obvezu informiranja Fine o promjeni podataka koji ulaze u sadržaj certifikata u roku od sedam dana te zatražiti izmjene podataka u certifikatu.

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

4.8.1 Razlozi za izmjene unutar certifikata

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

- promjene FQDN-a ili IP adrese,
- naziva ili mjesta sjedišta pravne osobe.

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

4.8.2 Tko može zatražiti izmjene unutar certifikata

Izmjene unutar OVCP certifikata može zatražiti Skrbnik ili osoba ovlaštena za zastupanje pravne osobe.

4.8.3 Obrada zahtjeva za izmjenama unutar certifikata

Zahtjev za izmjene podataka podnosi se u registracijski ured Fina RA mreže. Identifikacija i potvrđivanje identiteta podnositelja zahtjeva provodi se sukladno proceduri inicijalnog utvrđivanja identiteta iz točke 3.2. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta. Obrada zahtjeva i izdavanje certifikata provodi se sukladno točki 4.2., 4.3. i 4.4. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta.

Nakon provjere autentičnosti i valjanosti zahtjeva Fina RDC 2015 CA izdaje certifikat sukladno točki 4.3.1. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta.

4.8.4 Obavještavanje korisnika o izdavanju izmijenjenog certifikata

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

4.8.5 Provedba prihvaćanja izmijenjenog certifikata

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

4.8.6 Objavljivanje izmijenjenog certifikata od strane CA

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

4.8.7 Obavještavanje drugih strana o izdavanju izmijenjenog certifikata

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

4.9 Opoziv i suspenzija certifikata

4.9.1 Razlozi za opoziv

Fina opoziva certifikat:

- temeljem potpisanog zahtjeva Skrbnika ili osobe ovlaštene za zastupanje pravne osobe,
- u slučaju da Skrbnik ili osoba ovlaštena za zastupanje pravne osobe obavijesti Finu da zahtjev za izdavanjem certifikata nije autoriziran od strane Korisnika te da Korisnik retroaktivno ne odobrava izdavanje predmetnog certifikata,
- u slučaju da Korisnik otkaže ugovor o obavljanju usluge certificiranja,
- ako se pojavi osnovana sumnja da je privatni ključ Korisnika kompromitiran ili ako privatni ključ ili aktivacijski podaci nisu više u jedinstvenom posjedu Skrbnika, odnosno pravne osobe,
- u slučaju gubitka ili trajne nedostupnosti privatnog ključa,

- u slučaju da Fina raspolaže dokazom o zlouporabi certifikata ili temeljem službene obavijesti nadležnog tijela o korištenju certifikata u nezakonite svrhe,
- u slučaju da se Korisnik ne pridržava preuzetih obveza i odgovornosti određenih ugovorom, Fininim uvjetima o pružanju usluga certificiranja, Općim pravilima [22] ili ovim $CPS_{WSA\text{-}eIDAS}$ dokumentom,
- u slučaju da Fina raspolaže saznanjima da korištenje FQDN ili IP adrese naznačene u certifikatu Korisniku više nije pravno dopušteno,
- u slučaju promjene podataka sadržanih u certifikatu,
- ako certifikat nije izdan sukladno Općim pravilima [22] ili ovom $CPS_{WSA\text{-}eIDAS}$ dokumentu,
- u slučaju da Fina raspolaže saznanjima da informacije sadržane u certifikatu nisu točne ili da navode na pogrešne zaključke,
- u slučaju da Fina prestaje s pružanjem usluga izdavanja certifikata, a nije kod drugog pružatelja usluga povjerenja osigurala nastavak pružanja usluge opoziva certifikata,
- u slučaju da Fina iz bilo kojeg razloga više nema pravo izdavanja certifikata sukladno zahtjevima dokumenta CA/Browser Forum BRG [19], osim u slučaju ako Fina s nadležnim tijelima dogovori nastavak pružanja usluge davanja informacije o statusu opozvanosti certifikata putem CRL ili OCSP servisa,
- ako se pojavi osnovana sumnja u kompromitiranost privatnog Fina CA ključa kojim se potpisuje certifikat Korisnika,
- ako Fina procjeni da certifikat svojim tehničkim karakteristikama, profilom ili sadržajem ne pruža prikladnu razinu povjerenja proizvođačima aplikacijskog softvera ili Pouzdajućim stranama,
- u slučajevima kada to nalaže zakon ili drugi propis,
- u slučajevima kad je opoziv certifikata opravdan zahtjevima Općih pravila [22] ili ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta.

4.9.2 Tko može tražiti opoziv

Zahtjev za opoziv certifikata podnosi Skrbnik ili osoba ovlaštena za zastupanje pravne osobe.

Zahtjev za opoziv certifikata može uputiti Fina RA mreža.

Fina može opozvati certifikat temeljem autenticirane službene obavijesti nadležnog tijela.

Korisnici, Pouzdajuće strane, Isporučitelji aplikacijskog softvera i ostale treće strane mogu Fini prijaviti probleme vezane uz korištenje certifikata kao što su kompromitiranje privatnog ključa, zlouporaba certifikata, korištenje certifikata u nezakonite svrhe, neprimjerena uporaba certifikata te druge prijevarne radnje.

4.9.3 Procedura za zahtjev za opozivom

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

- osobnom dostavom u registracijski ured Fina RA mreže u uredovno vrijeme,
- poštanskom dostavom ili preko dostavljača na adresu registracijskog ureda u Fina RA mreži,
- elektroničkom dostavom na e-mail adresu navedenu u točki 9.11. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta, 24 sata na dan, 7 dana u tjednu,

Zahtjev za opoziv certifikata može se podnijeti i telefonskim putem pozivom Fini na telefonski broj koji je objavljen na internetskim stranicama repozitorija iz točke 2.2.1. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta. Ovaj Finin telefonski broj dostupan je od 0 do 24 sata, 7 dana u tjednu.

Ako se zahtjev za opoziv podnosi telefonskim putem, nakon pozitivne potvrde identiteta podnositelja zahtjeva prema točki 3.4 ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta ovlašteni službenik od podnositelja dobiva informacije o certifikatu za kojeg se podnosi zahtjev za opoziv, poput serijskog broja certifikata, ili ukoliko ta informacija podnositelju nije dostupna, koriste se i druge informacije poput tipa certifikata i približnog datuma njegovog izdavanja. Nakon identificiranja certifikata podnositelj potvrđuje svoj zahtjev za opozivanje identificiranog certifikata.

Fina na osnovu točnog i cjelovito podnesenog zahtjeva za opoziv, nakon identifikacije i potvrđivanja identiteta podnositelja opoziva certifikat i o tome obavještava Skrbnika te, ukoliko je to primjenjivo, pravnu osobu s kojom je Skrbnik povezan.

Nakon opoziva certifikata Fina RDC 2015 CA izdaje i objavljuje CRL, a informacija o statusu opozvanosti certifikata postaje dostupna i preko OCSP servisa.

U slučaju prijave problema vezanih uz korištenje certifikata temeljem dojave treće strane Fina će provjeriti utemeljenost prijave problema vezanih uz korištenje certifikata te će donijeti odluku o koracima koje je potrebno provesti vezano uz dostavljenu prijavu.

Prijava problema vezanih uz korištenje certifikata dostavlja se na e-mail adresu iz točke 9.11. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta.

4.9.4 Poček zahtjeva za opozivom

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

4.9.5 Vremenski period u kojem CA mora obraditi zahtjev za opozivom

Službenik za opoziv certifikata i Službenik za registraciju mogu, ako je potrebno zatražiti i prikupiti dodatne podatke koji mogu utjecati na odluku o opozivu certifikata. Ako Službenik za opoziv certifikata na osnovu prikupljenih podataka ne može donijeti odluku o opozivu certifikata dužan je o tome obavijestiti PMA koji u tom slučaju donosi odluku o opozivu certifikata.

Službenik za opoziv certifikata u najkraćem razumnom roku, a najkasnije u roku od 24 sata od donošenja odluke o opozivu certifikata opoziva certifikat ili provodi druge potrebne korake.

Neposredno nakon opoziva certifikata, Fina RDC 2015 CA promptno ažurira podatkovnu osnovicu certifikata i izdaje novu CRL.

4.9.6 Zahtjevi za provjeru opoziva za pouzdajuće strane

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

4.9.7 Učestalost izdavanja CRL

Fina RDC 2015 CA izdaje i potpisuje Fina RDC 2015 CRL. CRL se objavljuje odmah po opozivu certifikata te svakih šest sati od prethodnog izdavanja CRL. CRL liste koje izdaju Fina CA-ovi sadrže informacije o statusima opozvanosti certifikata minimalno do njihova isteka perioda važenja.

Vrijeme u kojem najkasnije mora biti izdana sljedeća CRL (vrijednost polja *Next Update*) je 24 sata od zadnjeg prethodnog izdavanja CRL.

4.9.8 Maksimalno kašnjenje za CRL

Neposredno nakon opoziva certifikata, Fina RDC 2015 CA promptno ažurira podatkovnu osnovicu certifikata i izdaje novu CRL. Maksimalno kašnjenje CRL od trenutka njenog izdavanja do trenutka objave u redovitim uvjetima iznosi dvije minute.

4.9.9 *Online* dostupnost provjere opozvanih certifikata/statusa certifikata

Fina RDC 2015 CA podržava *online* provjeru statusa opozvanosti izdanih certifikata putem Fina OCSP servisa čiji je rad usklađen s preporukom IETF RFC 6960 [17].

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

Adresa Fina OCSP servisa je http://ocsp.fina.hr, a upisuje se u ekstenziji *Authority Information Access* svakog certifikata.

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

4.9.10 Zahtjevi na *online* provjeru opozvanih certifikata

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

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

4.9.11 Drugi dostupni načini objave opozvanih certifikata

Nema odredbi.

4.9.12 Posebni zahtjevi vezani uz kompromitiranje privatnog ključa

U slučaju zaprimanja zahtjeva za opoziv certifikata ili zaprimanja prijave problema vezanih uz korištenje certifikata Fina će biti u stanju opozvati predmetni certifikat te će informacija o kompromitiranju privatnog ključa kao razloga za opoziv biti sadržana u informaciji o statusu opozvanosti certifikata.

4.9.13 Razlozi za suspenziju

Fina ne provodi suspenziju OVCP certifikata.

4.9.14 Tko može tražiti suspenziju

Ne primjenjuje se.

4.9.15 Procedura za zahtjev za suspenziju i reaktivaciju

Ne primjenjuje se.

4.9.16 Ograničenje na trajanje suspenzije

Ne primjenjuje se.

4.10 Usluge statusa certifikata

4.10.1 Operativna svojstva

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

Preporuka je Pouzdajućim stranama da za provjeru statusa certifikata koriste Fina OCSP servis te da se provjera statusa dohvatom CRL koristiti kao alternativna metoda provjere u

slučaju nedostupnosti OCSP servisa ili u slučaju da aplikacija Pouzdajuće strane podržava provjeru statusa certifikata samo putem CRL.

Adresa Fina OCSP servisa je http://ocsp.fina.hr, a upisuje se u ekstenziji *Authority Information Access* svih certifikata koje izdaju Fina RDC 2015 CA.

CRL se objavljuju se na internetskom poslužitelju i na javnom imeniku repozitorija Fina RDC 2015 CA. Na internetskom poslužitelju objavljuje se objedinjena CRL, a na javnom imeniku objavljuju se objedinjena i segmentirana CRL.

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

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

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

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

4.10.1.1 Adrese za dohvat CRL Fina RDC 2015 certifikata

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

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

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

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

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

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

Oznaka x u cn=CRLx označava segment CRL.

4.10.2 Dostupnost usluga

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

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

4.10.3 Opcionalna svojstva

Nema odredbi.

4.11 Kraj korištenja

Ako Korisnik otkaže ugovor prije isteka certifikata, Fina RDC 2015 CA će opozvati sve certifikate na koje se odnosi taj ugovor.

4.12 Sigurno skladištenje i oporavak privatnog ključa

Sigurno skladištenje privatnih korisničkih ključeva za OVCP certifikate se ne primjenjuje.

5 PROVJERA SUSTAVA, UPRAVLJANJA I RADNIH POSTUPAKA

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

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

5.1 Mjere fizičke zaštite

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

5.1.1 Lokacija objekta i konstrukcija

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

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

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

Fina PKI štićeni prostor interno je podijeljen na sigurnosne zone.

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

5.1.2 Fizički pristup

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

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

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

O svakom pristupu sustavima certificiranja vodi se evidencija.

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

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

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

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

5.1.3 Sustavi za napajanje i klimatizaciju

Uređaji i prostor u kojem se nalaze Fina RDC 2015 CA, Fina RA sustav i repozitorij te sustavi tehničke zaštite opskrbljeni su neprekidnim napajanjem električnom energijom i klimatizacijom koja je dimenzionirana na način koji osigurava odgovarajuće radne uvjete i u slučaju prekida vanjskog napajanja.

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

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

5.1.4 Opasnost od poplave

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

Papirnata arhiva Fina PKI pohranjena je u prostoru koji fizičkom konstrukcijom objekta i povišenim podom, te smještajem arhivske građe u metalne regale, štiti arhivirani materijal od poplave te puknuća vodovodnih i odvodnih cijevi.

5.1.5 Protupožarna zaštita

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

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

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

5.1.6 Pohrana medija

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

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

5.1.7 Zbrinjavanje otpada

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

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

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

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

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

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

5.1.8 Sigurnosne kopije na drugoj lokaciji

Sigurnosne kopije Fina RDC 2015 CA, središnjeg Fina RA sustava, sadržaja repozitorija i arhive u elektroničkom obliku, sigurnosne kopije programske opreme pohranjuju se u Fina PKI štićenom prostoru na pričuvnoj lokaciji.

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

5.2 Organizacijske mjere zaštite

5.2.1 Povjerljive uloge

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

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

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

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

5.2.2 Broj osoba potrebnih za obavljanje zadataka

Fina ima stalno zaposlen dovoljan broj stručnih osoba sa znanjem, iskustvom i kvalifikacijama koji je potreban u Fina PKI za davanje usluga iz opsega ovog $CPS_{WSA\text{-}eIDAS}$ Pristup i rad u štićenom Fina PKI prostoru provodi se isključivo uz istovremenu prisutnost najmanje dvije ovlaštene osobe Fina PKI koje imaju dozvole pristupa sustavu smještenom u štićenom Fina PKI prostoru.

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

5.2.3 Identifikacija i potvrđivanje identiteta za svaku ulogu

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

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

Ovlaštene osobe s povjerljivim ulogama u Fina PKI moraju se autenticirati prije bilo kojeg pristupa Fina RDC 2015 CA, odnosno Fina RA sustavu. U tu svrhu ovlaštene osobe Fina PKI dobivaju odgovarajuća sredstva za autentikaciju. Prije dobivanja sredstva za autentikaciju navedeno osoblje mora zadovoljiti zahtjeve navedene u točki 5.3. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta.

Sredstva za autentikaciju su:

- kartice kontrole s prolaza za ulazak u Fina PKI štićene sigurnosne zone, a dozvolu pristupa smiju dobiti samo ovlaštene osobe s povjerljivim ulogama u Fina PKI,
- certifikati na sigurnim kriptografskim uređajima koje smiju dobiti samo ovlaštene osobe u Fini s povjerljivim ulogama u Fina PKI,
- korisničko ime i zaporka ili certifikat na sigurnom kriptografskom uređaju koje smiju dobiti samo ovlaštene osobe u Fini s povjerljivim ulogama u Fina PKI,
- upravljačke kartice kriptografskog modula koje smiju dobiti samo ovlaštene osobe u Fini s povjerljivim ulogama u Fina PKI.

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

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

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

5.2.4 Uloge koje zahtijevaju odvajanje dužnosti

Opis poslova ovlaštenog osoblja s povjerljivim ulogama na Fina RDC 2015 CA sustavu temelji se na načelu odvajanja dužnosti i dodjele minimalnih korisničkih prava koja omogućuju nesmetano obavljanje dodijeljenih poslova. Kod odvajanja uloga primjenjuju se sljedeća pravila:

- Službeniku za sigurnost, Službeniku za registraciju i Službeniku za validaciju ne smije biti dodijeljena uloga Službenika za nadzor sustava,
- Administratoru sustava ne smije biti dodijeljena uloga Službenika za sigurnost ili uloga Službenika za nadzor sustava.

5.3 Provjere osoblja

5.3.1 Kvalifikacije, radno iskustvo i zahtjevi za provjerom osoblja

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

Prije početka rada u Fina PKI kandidati moraju posjedovati odgovarajuća stručna znanja, iskustvo, kvalifikacije i edukacije u radu s kriptografskim tehnologijama, zaštitom računalnih sustava, informacijskom sigurnošću te zaštitom osobnih podataka u domeni vlastitog djelokruga rada u okviru poslova Fina PKI.

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

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

5.3.2 Procedure provjere primjerenosti osoblja

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

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

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

5.3.3 Zahtjevi za školovanjem

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

Fina PKI osoblju s povjerljivim ulogama u radu na Fina RDC 2015 CA sustavu osigurava se edukacija i usavršavanje sukladno njihovim povjerljivim ulogama.

Edukacija i usavršavanje osoblja s povjerljivim ulogama u radu na Fina RDC 2015 CA sustavu obuhvaća:

- Fina RDC 2015 CA i Fina RA sigurnosni principi i mehanizmi,
- svjesnost o sigurnosti,
- CA softver koji je u uporabi u Fina RDC 2015 CA sustavu,
- zadaci povezani s povjerljivim ulogama koje će obavljati na Fina RDC 2015 CA sustavu,

- postupci oporavka od nezgode i nastavka poslovanja.

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

- osnovno o certifikatima,
- tipovi certifikata koje izdaje Fina RDC 2015 CA i područja njihove uporabe,
- načini registracije korisnika te rad u Fina RA i Fina CMS aplikacijama,
- svjesnost o sigurnosti,
- informacije s kojima je potrebno upoznati korisnike.

5.3.4 Učestalost i uvjeti za obnovu znanja

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

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

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

5.3.5 Učestalost i slijed izmjene zaposlenika

Ne primjenjuje se

5.3.6 Kazne za neovlaštene radnje

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

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

5.3.7 Zahtjevi na vanjske suradnike

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

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

5.3.8 Dokumentacija koja je dostupna osoblju

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

5.4 Postupci upravljanja revizijskim zapisima

5.4.1 Tipovi događaja koji se zapisuju

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

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

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

U revizijskim zapisima zapisuju se u elektroničkom ili papirnatom obliku zapisi o svim događaji u Fina PKI vezani uz:

- upravljanje životnim ciklusom CA ključeva Fina RDC 2015 CA,
- upravljanje životnim ciklusom HSM modula kojim je zaštićen privatni ključ Fina RDC 2015 CA,
- upravljanje životnim ciklusom korisničkih ključeva koje generira Fina,
- upravljanje životnim ciklusom certifikata koje izdaje Fina RDC 2015 CA,
- registraciju fizičke i pravne osobe,
- sigurnosne događaje, uključujući događaje podizanja i spuštanja sustava, ispada sustava i kvara hardvera, aktivnosti vatrozidova i usmjernika te izmjene sigurnosnih postavki sustava.

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

5.4.2 Učestalost obrade revizijskih zapisa

Postupak pregleda revizijskih zapisa obuhvaća:

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

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

Preglede revizijskih zapisa Fina RDC 2015 CA i pripadajućih HSM modula obavlja Službenik za nadzor sustava. Pregledi revizijskih zapisa Fina RDC 2015 CA i pripadajućih HSM modula obavljaju se redovito, jednom dnevno radnim danima, te u slučaju izvanrednih situacija. O obavljenom pregledu ovih revizijskih zapisa vodi se evidencija u papirnatom ili elektroničkom obliku, a vodi je osoba s povjerljivom ulogom Službenik za nadzor sustava.

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

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

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

5.4.3 Vremenski period pohrane revizijskih zapisa

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

5.4.4 Zaštita revizijskih zapisa

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

Zaštita cjelovitosti kritičnih revizijskih zapisa Fina RDC 2015 CA sustava za izdavanje certifikata osigurana je pri generiranju zapisa.

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

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

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

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

5.4.5 Postupci izrade sigurnosnih kopija revizijskih zapisa

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

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

5.4.6 Sustav prikupljanja revizijskih zapisa (unutarnji ili vanjski)

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

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

5.4.7 Obavještavanje subjekta uzročnika događaja

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

5.4.8 Procjena ranjivosti

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

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

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

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

5.5 Arhiviranje zapisa

5.5.1 Tipovi arhiviranih zapisa

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

- opća pravila pružanja usluga certificiranja,
- pravilnici o postupcima certificiranja,
- uvjeti pružanja usluga certificiranja,
- ugovori povezani s pružanjem usluga certificiranja,
- podaci vezani uz generiranje Fina RDC 2015 CA para ključeva i izdavanju pripadajućih certifikata,
- podaci i pripadajuća dokumentacija prikupljena postupkom registracije fizičkih i pravnih osoba,
- podaci iz zahtjeva za izdavanje certifikata dostavljeni od strane korisnika,
- certifikati i podaci vezani uz životni ciklus pojedinog certifikata, uključujući sve zahtjeve i obavijesti za opoziv certifikata te pripadajuće provedene radnje,
- evidencija opozvanih certifikata, podaci o opozivu certifikata te pripadajuća dokumentacija,
- revizijski zapisi iz točke 5.4.1. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta,
- drugi Fininі interni dokumenti.

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

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

5.5.2 Vremenski period arhiviranja

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

5.5.3 Zaštita arhive

Arhivirana dokumentacija Fina RDC 2015 CA sustava u papirnatom obliku čuva se u Fina PKI štićenom prostoru koji je opisan u točki 5.1.1. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta. Arhivirani zapisi su na zahtjev raspoloživi ovlaštenim osobama Fina PKI, uz dualnu kontrolu.

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

Arhivirani zapisi u elektroničkom obliku iz točke 5.5.1. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta čuvaju na odgovarajućim medijima za arhiviranje podataka u Fina PKI štićenom prostoru. Arhivirani

zapisi štite se mehanizmima i postupcima koji osiguravaju povjerljivost i cjelovitost zapisa te ne dozvoljavaju izmjenu zapisa, kao ni jednostavno brisanje ili uništenje zapisa. Povjerljivost arhiviranih zapisa u elektroničkom obliku štiti se enkripcijom, a cjelovitost zapisa digitalnim potpisom. Arhivirani zapisi su na zahtjev raspoloživi ovlaštenim osobama Fina PKI, uz dualnu kontrolu. Minimalno jednom godišnje Fina PKI osoblje provjerava integritet arhive, te ako je arhiva oštećena, ona se obnavlja pomoću sigurnosne kopije.

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

5.5.4 Postupci izrade sigurnosnih kopija arhive

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

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

5.5.5 Zahtjevi na zaštitu zapisa vremenskim žigom

Nema odredbi.

5.5.6 Sustav prikupljanja arhiva (unutarnji ili vanjski)

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

Dokumentacija Fina RDC 2015 CA sustava u papirnatom obliku prikuplja se manualno i arhivira se interno u Fina PKI štićenom prostoru.

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

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

5.5.7 Postupci pristupa i verifikacije podataka iz arhiva

Pristup zapisima iz arhive imaju samo osobe ovlaštene za pristup podacima iz arhive. Pristup podacima arhiviranim u štićenim prostorima imaju samo ovlaštene osobe Fina PKI, uz dualnu kontrolu.

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

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

5.6 Promjena CA ključa

Radi potrebe osiguranja kontinuiteta pružanja usluge izdavanja certifikata Fina će dovoljno vremena prije isteka CA certifikata, generirati novi par ključeva za Fina RDC 2015 CA. Također, Fina RDC 2015 CA će dovoljno vremena ranije generirati novi par CA ključeva i u slučaju kada tu promjenu zahtjeva razina sigurnosti kriptografskog algoritma privatnog CA ključa u uporabi.

Fina RDC 2015 CA par potpisnih ključeva generira se na način opisan u točki 6.1 ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta. Novi certifikat Fina RDC 2015 CA s novo generiranim javnim ključem potpisuje se privatnim ključem Fina Root CA.

O planiranoj promjeni ključa Fina RDC 2015 CA, Fina će pravovremeno obavijestiti sudionike Fina PKI objavom informacija na stranicama Fina PKI repozitorija iz točke 2.2. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta. Novi certifikat Fina RDC 2015 CA biti će dostupan je sudionicima Fina PKI putem javnog imenika i internetskih stranica repozitorija.

Novi certifikat Fina RDC 2015 CA dostavit će se Korisnicima i Pouzdajućim stranama na način na koji se dostavlja postojeći Fina RDC 2015 CA certifikat, sukladno točki 6.1.4. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta.

5.7 Oporavak od kompromitiranja ili nepogode

5.7.1 Postupci u slučaju incidenta ili kompromitiranja

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

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

- prirodnih katastrofa,
- napada, pljački ili blokade zgrade,
- uništenja IT infrastrukture na primarnoj produkcijskoj lokaciji,
- nedostupnost IT infrastrukture na primarnoj produkcijskoj lokaciji uslijed kvara hardvera ili softvera većih razmjera,
- nedostupnosti radnika,
- prekida usluga dobavljača,
- za događaje gubitka ili kompromitiranja ili sumnje u kompromitiranost privatnog ključa Fina RDC 2015 CA.

U slučaju prirodnih ili drugih nepogoda primjenjuju se odgovarajuće odredbe Pravilnika zaštite na radu.

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

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

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

Obavještavanje u slučaju kompromitiranja ili sumnje u kompromitiranost privatnog ključa Fina RDC 2015 CA opisano je u točki 5.7.3. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta.

Plan kontinuiteta poslovanja revidira se jednom godišnje.

5.7.2 Oštećenja u računalnim resursima, programima i/ili podacima

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

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

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

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

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

5.7.3 Postupci u slučaju kompromitiranja privatnog ključa

U slučaju kompromitiranja privatnog ključa Fina RDC 2015 CA Fina će odmah po saznanju prekinuti s uporabom kompromitiranog privatnog ključa Fina RDC 2015 CA te će ispitati okolnosti kompromitiranja ključa. Ako se potvrdi kompromitiranje ključa Fina donosi odluku o opozivu CA certifikata povezanog s kompromitiranim ključem te Fina Root CA opoziva taj CA certifikat.

O opozivu Fina RDC 2015 CA certifikata Fina će obavijestiti sljedeće sudionike Fina PKI:

- Fina RA mrežu,
- Korisnike,
- Pouzdajuće strane.

Nakon ustanovljavanja i otklanjanja uzroka koji su prouzročili kompromitiranje CA ključa, Fina će, ako je primjenjivo, poduzeti mjere za sprječavanje ponavljanja takvog događaja. Ovisno o utvrđenim uzrocima kompromitiranja ključa Fina može donijeti odluku o privremenom prelasku na produkciju sa sekundarne lokacije.

Fina će za Fina RDC 2015 CA čiji je certifikat opozvan organizirati ceremoniju generiranja novog para CA ključeva te će Fina Root CA će za novi javni CA ključ izdati novi CA certifikat.

Fina RDC 2015 CA će uporabom novog privatnog CA ključa izdati certifikate postojećim registriranim Subjektima te će sve naredne informacije o opozvanosti certifikata potpisivati uporabom novog ključa. Novi CA certifikat biti će dostupan sudionicima Fina PKI na način na koji je bio dostupan i prethodni CA certifikat, a sukladno opisu u točki 2.2. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta.

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

- Fina RA mrežu,
- Korisnike,
- Pouzdajuće strane.

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

5.7.4 Mogućnost nastavka poslovanja nakon nepogode

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

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

5.8 Prestanak rada CA ili RA

O planiranom prestanku pružanja usluga izdavanja certifikata Fina će:

- obavijestiti sve Korisnike usluge, Pouzdajuće strane i središnje tijelo državne uprave nadležno za poslove gospodarstva najmanje tri mjeseca prije planiranog prestanka pružanja usluga izdavanja certifikata,
- uložiti sav napor da kod drugog pružatelja usluga povjerenja osigura nastavak pružanja usluga izdavanja certifikata te će tom pružatelju usluga dostaviti svu dokumentaciju prikupljenu u postupku registracije Korisnika kao i svu dokumentaciju o izdanim certifikatima,

- na tog pružatelja usluga prenijeti svoju obavezu da pouzdajućim stranama tijekom razumnog vremena omogući raspoloživost Fina CA certifikata u kojima su javni ključevi Fina CA-ova, kao i raspoloživost drugih certifikata s javnim ključevima Fininih usluga povjerenja,
- na tog pružatelja usluga prenijeti svoju obavezu omogućavanja raspoloživosti CRL za sve opozvane Korisničke certifikate i certifikate Fina CA-ova koji prestaju s radom,
- na tog pružatelja usluga prenijeti svoju obavezu pružanja informacija putem OCSP servisa o opozvanim Korisničkim i Fina CA certifikatima,
- opozvati sve izdane certifikate,
- opozvati certifikate Fina CA-ova koji prestaju s radom te uništiti pripadajuće privatne ključeva tih CA-ova.

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

6 TEHNIČKE MJERE ZAŠTITE

Ovo poglavlje opisuje mjere zaštite koje se poduzimaju u cilju postizanja zahtijevane razine sigurnosti kriptografskih ključeva, aktivacijskih podataka, kritičnih sigurnosnih parametara, upravljanja ključevima i drugih mjera tehničke sigurnosti za Fina RDC 2015 CA i za izdavanje korisničkih certifikata.

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

6.1 Generiranje i instalacija para ključeva

6.1.1 Generiranje para ključeva

Fina provodi generiranje para ključeva Fina RDC 2015 CA koristeći algoritme za generiranje ključeva koji su sukladni s normizacijskim dokumentom ETSI TS 119 312 [12].

6.1.1.1 Generiranje para Fina CA ključeva

Postupak generiranja para Fina RDC 2015 CA ključeva provodi se formalnom ceremonijom generiranja para ključeva za subordinirane Fina CA-ove kojoj prisustvuju ovlaštene osobe Fina PKI.

Ceremonija generiranja para ključeva za Fina RDC 2015 CA provodi se prema protokolu za generiranje ključeva u kojem su dokumentirani koraci koji se izvode za vrijeme ceremonije. Protokol za generiranje ključeva sukladan je s mjerama tehničke sigurnosti prema normi ETSI EN 319 411-1[7] i sa zahtjevima CA/Browser Forum BRG [19].

Kriptografski algoritmi koji se koristi za generiranje ključeva kao i duljina ključeva za Fina RDC 2015 CA odabrani su sukladno normizacijskom dokumentu ETSI TS 119 312 [12] tako da budu prikladni za cijelo vrijeme važenja CA certifikata.

Par ključeva za FINA RDC 2015 CA generira se, uz minimalno dualnu kontrolu ovlaštenih osoba s povjerljivim ulogama u Fina PKI, u HSM modulu koji zadovoljava zahtjeve iz točke 6.2.1. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta.

FINA RDC 2015 CA nalazi se tijekom i nakon ceremonije generiranja parova ključeva u Fina PKI štićenom prostoru, a pristup Fina RDC 2015 CA dopušten je ovlaštenim osobama Fina PKI s povjerljivim ulogama, uz minimalno dualnu kontrolu.

Provođenje postupka ceremonije generiranja para ključeva za Fina RDC 2015 CA snima se video kamerom ili provođenju postupka svjedoči Kvalificirani ocjenitelj.

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

Fina posjeduje izvješće Kvalificiranog auditora koji svjedoči da je postupak generiranja parova ključeva za Fina RDC 2015 CA proveden sukladno protokolu i zahtjevima za generiranje ključeva.

6.1.1.2 Generiranje para ključeva za certifikate korisnika

Generiranje korisničkog para ključeva za *SSL certifikat razine 2 (OVCP)* može provoditi pripadajući Skrbnik ili Fina.

Generiranja korisničkog para ključeva za *SSL certifikat razine 3 (OVCP)* provodi samo pripadajući Skrbnik.

Ukoliko generiranje para ključeva za *SSL certifikat razine 2 (OVCP)* provodi Fina, generiranje se provodi u kriptografskom modulu u Fina PKI štićenom prostoru. Generiranje korisničkog para ključeva za *SSL certifikat razine 2 (OVCP)* usklađeno je s normom ETSI EN 319 411-1 [7] i sa zahtjevima CA/Browser Forum BRG [19].

Ukoliko generiranje para ključeva *SSL certifikat razine 2 (OVCP)* provodi Skrbnik, generiranje se provodi u kontroliranoj okolini na lokaciji Korisnika. Privatni ključevi štite se u softverskom zaštićenom tokenu na način opisan u točki 6.2.1. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta.

Generiranje korisničkog para ključeva za *SSL certifikat razine 3 (OVCP)* provodi Skrbnik u kontroliranoj okolini na lokaciji Korisnika, u HSM modulu koji zadovoljava zahtjeve iz točke 6.2.1. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta.

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

6.1.2 Dostava privatnog ključa korisniku

Ako Fina generira privatni ključ koji će biti povezan sa *SSL certifikatom razine 2 (OVCP)*, tada se privatni ključ i pripadajući certifikat dostavljaju registriranom Skrbniku u obliku zaštićene PKCS#12 datoteke. Zaštita PKCS#12 datoteke provodi se temeljem aktivacijskog podatka kojeg postavlja Skrbnik prije njene dostave Dostava PKCS#12 datoteke obavlja se *online* TLS kanalom korištenjem Fina CMS sustava, uz prethodnu uspješnu autentikaciju Skrbnika. Nakon dostave PKCS#12 datoteke Skrbniku Fina uništava pripadajući privatni ključ i PKCS#12 datoteku.

U slučaju da Fina ima saznanja da je privatni ključ koji je povezan sa *SSL certifikatom razine 2 (OVCP)* dostavljen neovlaštenoj osobi ili poslovnom subjektu koji nisu povezana s tim privatnim ključem, Fina će opozvati sve certifikate koji sadrže javni ključ povezan s tim privatnim ključem.

Ako Skrbnik na svojoj lokaciji generira privatni ključ u HSM modulu ili softverskom modulu, smatra se da Korisnik već posjeduje privatni ključ.

6.1.3 Dostava javnog ključa CA-u

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

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

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

6.1.4 Dostava CA javnog ključa pouzdajućim stranama

Javni ključevi Fina RDC 2015 CA dostupan je Pouzdajućim stranama u Fina RDC 2015 CA certifikatu kojeg je izdao Fina Root CA te je tako osigurana cjelovitost i omogućena provjera izvornosti javnog ključa Fina RDC 2015 CA.

Provjera izvornosti javnih ključeva Fina RDC 2015 CA osigurava se:

- objavom Fina Root CA certifikata i certifikata Fina RDC 2015 CA na internetskim stranicama Fina PKI repozitorija iz točke 2.2. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta, te dostavom sažetka Fina Root CA certifikata pouzdanim kanalom na zahtjev.
- objavom certifikata Fina RDC 2015 CA na nacionalnom pouzdanom popisu kvalificiranih pružatelja usluga povjerenja (*Trusted* lista) koje na svojim internetskim stranicama objavljuje središnje tijelo državne uprave nadležno za poslove gospodarstva kao tijelo odgovorno za pouzdani popis kvalificiranih pružatelja usluga povjerenja u Republici Hrvatskoj.

6.1.5 Duljine ključeva

Duljine ključeva u Fina PKI su sljedeće:

- Fina Root CA upotrebljava *sha256WithRSA* algoritam s ključem duljine 4096 bita,
- Fina RDC 2015 CA upotrebljava *sha256WithRSA* algoritam s ključem duljine 4096 bita,
- Fina OCSP servis upotrebljava RSA ključeve duljine 2048 bita,
- Korisnici upotrebljavaju RSA par ključeva duljine 2048 bita.

6.1.6 Generiranje i provjera kvalitete parametara javnog ključa

Fina RDC 2015 CA provodi generiranje para ključeva koristeći parametre za generiranje koji su sukladni s normizacijskim dokumentom ETSI TS 119 312 [12].

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

Kad Skrbnik generira par ključeva, Skrbnik je dužan generiranje para ključeva provesti na način koji osigurava korištenjem parametara sukladno normizacijskim dokumentima ETSI TS 119 312 [12] i CA/Browser Forum BRG [19]. Pri zaprimanju javnog ključa generiranog od strane Skrbnika Fina provjerava da li javni ključ zadovoljava kvalitetu sukladnu tim dokumentima te odbacuje javni ključ koji ne zadovoljava ove zahtjeve kvalitete i za njega ne izdaje certifikat.

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

Certifikat Fina RDC 2015 CA u ekstenziji *Key Usage* ima postavljene vrijednosti *keyCertSign* i *cRLSign*. Fina RDC 2015 CA pripadajući privatni ključ koristi samo za:

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

Certifikati iz Tablice 1.1. iz točke 1.1.2. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta namijenjeni su za autentikaciju mrežnih stranica. Ekstenzija *Key Usage* ovih certifikata označena je kritičnom (*critical*) i ima postavljene vrijednosti *digitalSignature* i *keyEncipherment*.

6.2 Zaštita privatnog ključa i tehnike upravljanja kriptografskim modulom

6.2.1 Norme i upravljačke funkcije kriptografskog modula

Privatni ključ za Fina RDC 2015 CA generira se i štiti HSM modulom koji zadovoljava zahtjeve prema FIPS 140-2 [14] razina 3.

Privatni ključevi za Fina OCSP servise generiraju se i štite HSM modulima koji zadovoljavaju zahtjeve norme FIPS 140-2 [14] razina 3.

Zaštita privatnog ključa *SSL certifikata razine 2 (OVCP)* provodi se u softverskom zaštićenom tokenu u kontroliranoj okolini na lokaciji Korisnika. Za način zaštite privatnih ključeva *SSL certifikata razine 2 (OVCP)* na lokaciji Korisnika zadužen je Korisnik.

Zaštita privatnih ključeva *SSL certifikata razine 3 (OVCP)* provodi se HSM modulom koji zadovoljava zahtjeve norme FIPS 140-1 [13] ili 140-2 [14] razina 3 ili više, ili zahtjeve primijenjenih jednako vrijednih sigurnosnih kriterija, uz primjenu dodatnih mjera fizičke i ICT zaštite na lokaciji Korisnika.

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

HSM moduli kojim se štite privatni ključevi Fina RDC 2015 CA i OCSP servisa smješteni su u prostoru najviše razine sigurnosti unutar Fina PKI štićenog prostora. Fizički pristup ovim HSM modulima provodi se uz dualnu kontrolu ovlaštenih osoba s povjerljivim ulogama u Fina PKI.

Upravljanje Fina RDC 2015 CA privatnim potpisnim ključem provodi se uz najmanje dualnu kontrolu osoba s povjerljivim ulogama u Fina PKI. Pri upravljanju privatnim ključem Fina RDC 2015 CA osobe s povjerljivim ulogama koriste pripadajuće upravljačke kartice kriptografskog modula na principu n od m.

6.2.3 Sigurno skladištenje privatnog ključa (*key escrow*)

Nije dozvoljeno skladištenje privatnog ključa Fina RDC 2015 CA.

Nije dozvoljeno skladištenje privatnih korisničkih ključeva povezanih s OVCP certifikatima.

6.2.4 Sigurnosno kopiranje privatnog ključa

Sigurnosno kopiranje privatnog ključa Fina RDC 2015 CA provodi se uz dualnu kontrolu ovlaštenih osoba s povjerljivim ulogama u Fina PKI, u prostoru najviše razine sigurnosti unutar Fina PKI štićenog prostora. Privatni Fina RDC 2015 CA ključ se izvan HSM modula nalazi isključivo u enkriptiranom obliku te se u tom obliku kopira i čuva u sigurnom prostoru najviše razine sigurnosti unutar Fina PKI štićenih prostora na odvojenim lokacijama.

Fizički pristup sigurnosnim kopijama privatnog ključa Fina RDC 2015 CA imaju isključivo ovlaštene osobe s povjerljivim ulogama u Fina PKI uz dualnu kontrolu.

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

Korisnik je odgovoran za zaštitu kopija privatnih ključeva za *SSL certifikat razine 2 (OVCP)* te je odgovoran u slučaju njihovog neovlaštenog korištenja na isti način kao i originala, a sukladno točki 9.6.3. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta.

6.2.5 Arhiviranje privatnog ključa

Nije dozvoljeno arhiviranje privatnog ključa Fina RDC 2015 CA te se on uništava sukladno točki 6.2.10. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta.

Nije dozvoljeno arhiviranje privatnih ključeva Korisnika.

6.2.6 Prijenos privatnog ključa

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

Prijenos privatnog ključa Fina RDC 2015 iz HSM modula autoriziraju ovlaštene osobe s povjerljivim ulogama u Fina PKI, uz dualnu kontrolu, u Fina PKI štićenom prostoru.

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

Prijenos privatnih ključeva za *SSL certifikat razine 2 (OVCP)* u drugi spremnik privatnog ključa smije provoditi Skrbnik na način da se privatni ključ prenositi samo u kriptografski modul jednake ili više razine sigurnosti u odnosu na kriptografski modul iz kojega se privatni ključ prenosi. Privatni ključ se prije prijenosa enkriptira kako bi tijekom prijenosa bio adekvatno zaštićen.

6.2.7 Spremanje privatnog ključa u kriptografskom modulu

Privatni ključ Fina RDC 2015 CA zaštićen je HSM modulom i može se koristiti jedino ako je propisno aktiviran.

Privatni ključ za *SSL certifikat razine 3 (OVCP)* zaštićen je HSM modulom i može se koristiti jedino ako je propisno aktiviran.

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

6.2.8 Metoda aktivacije privatnog ključa

Pokretanje Fina RDC 2015 CA servisa za izradu certifikata te aktivacija privatnog Fina RDC 2015 CA ključa u hardverskom kriptografskom modulu provodi se pod dualnom kontrolom ovlaštenih osoba Fina RDC 2015 CA korištenjem upravljačkih kartica kriptografskog modula.

Jednom aktiviran, privatni ključ ostaje aktiviran bez vremenskog ograničenja.

Aktivaciju privatnih ključeva certifikata smije provoditi pripadajući Skrbnik korištenjem svojeg PIN-a ili odgovarajućih aktivacijskih podataka. Aktivacija privatnog ključa obavlja se na siguran način.

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

6.2.9 Metoda deaktivacije privatnog ključa

Deaktivacija privatnog ključa Fina RDC 2015 CA provodi se prema postupcima i uz zadovoljenje zahtjeva određenih u certifikacijskom dokumentu upotrijebljenog HSM modula, uz dualnu kontrolu ovlaštenih osoba s povjerljivim ulogama u Fina PKI.

Deaktivacija privatnog ključa Fina RDC 2015 CA, provodi se kada postoji neposredan zahtjev za privremenim obustavljanjem aktivnosti sustava, u slučajevima isteka perioda valjanosti privatnog ključa te u slučaju opoziva pripadajućeg certifikata.

Privatni ključ Fina RDC 2015 CA deaktivira se:

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

Za propisnu deaktivaciju i uporabu privatnih ključeva certifikata odgovoran je Skrbnik.

Privatni ključevi certifikata zaštićeni HSM modulom deaktiviraju se prestankom napajanja uređaja ili naredbom iz korisničke aplikacije za deaktivaciju uređaja.

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

6.2.10 Metoda uništavanja privatnog ključa

Postupak uništavanja privatnog Fina RDC 2015 CA ključa provodi se nakon isteka perioda valjanosti privatnog ključa, zbog kompromitiranja ili sumnje u kompromitiranost privatnog ključa, ili zbog prestanka njegova korištenja, a provode ga ovlaštene osobe s povjerljivim ulogama u Fina PKI uz minimalno dualnu kontrolu. Postupkom uništavanja privatnog Fina RDC 2015 CA ključa trajno su onesposobljene sve sigurnosne kopije tog privatnog ključa te ih više nije moguće upotrijebiti.

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

Uništavanje privatnog Fina RDC 2015 CA ključa provodi se sukladno Fininim internim procedurama uz prisutnost osoba s povjerljivim ulogama u Fina PKI.

Preporuka je da Korisnik uništi svaki privatni ključ certifikata koji je trajno stavljen izvan uporabe.

Uništenje privatnih ključeva certifikata provodi Skrbnik.

Skrbnik je odgovoran za uništenje privatnih ključeva certifikata.

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

6.2.11 Ocjena kriptografskog modula

Ocjena HSM modula i drugih kriptografskih modula provodi se prema normama za kriptografske module navedenim u točki 6.2.1. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta.

6.3 Ostali vidovi upravljanja parom ključeva

6.3.1 Arhiviranje javnog ključa

Javni ključ Fina RDC 2015 CA i korisnički javni ključevi certifikata arhiviraju se u svrhu pružanja dokaza o certifikatima u sudskim, upravnim i drugim postupcima.

Javni ključ Fina RDC 2015 CA sastavni je dio pripadajućeg CA certifikata koji se arhivira sukladno točkama 5.5.3. i 5.5.4. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta, a u arhivi se čuva na rok iz točke 5.5.2. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta.

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

6.3.2 Periodi važenja certifikata i korištenja para ključeva

Rok važenja certifikata po vrstama je definiran u Tablici 6.1.

Certifikat	Rok
Fina RDC 2015 CA certifikat	10 godina
Certifikati za potpis odgovora Fina OCSP servisa	1 godina
SSL certifikat razine 2 (OVCP)	2 godine
SSL certifikat razine 3 (OVCP)	1 godina

Tablica 6.1. Periodi važenja certifikata

Period važenja Fina RDC 2015 CA certifikata ne smije biti izvan perioda važenja Fina Root CA certifikata.

Vremenski period valjanosti privatnog ključa jednak je vremenskom periodu valjanosti pripadajućeg certifikata. Certifikati i pripadajući ključevi ne smiju se upotrebljavati nakon isteka roka valjanosti certifikata i nakon njegova opoziva.

6.4 Aktivacijski podaci

6.4.1 Generiranje i instalacija aktivacijskih podataka

Aktivacijski podaci povezani s privatnim ključevima za Fina RDC 2015 CA generiraju se i instaliraju prilikom provođenja formalne ceremonije generiranja para ključeva za subordinirane Fina CA-ove. Aktivacijski podaci instaliraju se na pripadajuće upravljačke kartice kriptografskog modula koje se koriste za aktivaciju privatnog ključa Fina RDC 2015 CA na principu n od m.

Ako privatne ključeve za certifikate generira Fina tada Fina prethodno generira i pripadajuće autentikacijske podatke kojima se Skrbnik prijavljuje na Fina CMS. Aktivacijske podatke kojima se štiti privatni ključ u PKCS#12 datoteci generira i upisuje autenticirani Skrbnik koristeći Fina CMS i TLS komunikacijski kanal.

Aktivacijske podatke za *SSL certifikat razine 3 (OVCP)* certifikate generira Skrbnik.

Ako aktivacijske podatke generira Skrbnik, za sigurnost i zadovoljenje propisane kvalitete aktivacijskih podataka odgovoran je pripadajući Korisnik.

6.4.2 Zaštita aktivacijskih podataka

Aktivacijski podaci povezani s privatnim ključem Fina RDC 2015 CA čuvaju se na siguran način.

Aktivacijski podaci za privatni ključ Fina RDC 2015 CA koji su smješteni na pripadajuće upravljačke kartice kriptografskog modula zaštićeni su pripadajućim zaporkama koje su generirane u Fina PKI štićenom prostoru. Upravljačke kartice kriptografskog modula dodjeljuju se ovlaštenim osobama s povjerljivim ulogama u Fina PKI. Upravljačke kartice kriptografskog modula i pripadajuće zaporke čuvaju se u odvojenim sigurnosnim spremnicima pojedinog Fina PKI štićenog prostora.

Ako privatne ključeve za certifikate generira Fina tada Fina Skrbniku dostavlja autentikacijske podatke kojima će se Skrbnik prijaviti na Fina CMS pomoću dva odvojena kanala.

Skrbnici su zaduženi za zaštitu i čuvanje aktivacijskih podataka pripadajućih privatnih ključeva.

Aktivacijski podaci ne smiju se čuvati zajedno s HSM odnosno kriptografskim modulom na kojeg se odnose.

Za zaštitu aktivacijskih podataka privatnih ključeva povezanih s certifikatima odgovoran je Korisnik.

6.4.3 Ostale odredbe o aktivacijskim podacima

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

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

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

6.5 Upravljanje računalnom sigurnošću

6.5.1 Posebni tehnički zahtjevi na računalnu sigurnost

HSM kojim se štiti privatni ključ Fina Root CA izoliran je od svih ostalih redovnih operacija na način da se nalazi na dediciranom hardveru i namijenjen je isključivo za zaštitu Fina Root CA privatnog ključa. Računalo koje obavlja funkciju Fina Root CA u istom je smislu izolirano od svih ostalih redovnih operacija. Fina Root CA s pripadajućim HSM-om cijelo je vrijeme izdvojen od računalne mreže (*offline*) te je u redovnom stanju uvijek ugašen. Ovlaštenje za uključivanje Fina Root CA s pripadajućim HSM-om imaju samo osobe s povjerljivim ulogama u Fina PKI. Pristup privatnom ključu Fina Root CA imaju samo ovlaštene osobe s povjerljivim ulogama u Fina PKI sukladno točki 6.2.2. CP/CPS_{ROOT} [21] dokumenta.

Pristup IT sustavu i aplikacijama u Fina PKI imaju isključivo ovlaštene osobe nakon autentikacije. Kontrola pristupa operacijskom sustavu Fina RDC 2015 CA poslužitelja dopušta pristup samo ovlaštenom osoblju s povjerljivim ulogama u Fina PKI.

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

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

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

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

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

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

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

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

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

6.5.2 Ocjena računalne sigurnosti

U cilju sigurnosti i kvalitete pružanja usluga povjerenja Fina ima uspostavljen sustav upravljanja informacijskom sigurnošću sukladan normi ISO/IEC 27001 [4]. Sukladnost se potvrđuje certifikatom izdanim od strane neovisnog certifikacijskog tijela.

6.6 Tehničke kontrole životnog ciklusa

6.6.1 Kontrole razvoja sustava

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

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

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

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

6.6.2 Kontrole upravljanja sigurnošću

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

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

Pri pokretanju HSM modula provodi se automatska provjera njihovog integriteta.

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

Razlozi zbog kojih se pojedina zakrpa ne primjenjuje se dokumentiraju kroz sustav upravljanja promjenama.

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

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

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

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

6.6.3 Sigurnosne kontrole životnog ciklusa

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

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

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

6.7 Provjera mrežne sigurnosti

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

Mrežni segment na kojem se nalaze radne stanice za administraciju Fina RDC 2015 CA vatrozidom je odvojen od ostalih mrežnih segmenata i računala koja se nalaze u tim mrežnim segmentima.

Oprema za zaštitu računalne mreže bilježi tok prometa i pokušaje pristupa Fina RDC 2015 CA servisima te LDAP servisu javnog imenika. Informacije koje se bilježe definirane su u točki 5.4.1. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta. Samo ovlašteno osoblje u Fina PKI ima administratorske ovlasti za podešavanje i upravljanje opremom za zaštitu računalne mreže. Udaljeno podešavanje opreme za zaštitu računalne mreže nije dozvoljeno.

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

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

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

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

CA sustavi posebno su sigurnosno podešeni i očvršćeni.

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

6.8 Uporaba vremenskog žiga

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

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

7 SADRŽAJ CERTIFIKATA, LISTA OPOZVANIH CERTIFIKATA I OCSP PROFILI

7.1 Profil certifikata

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

Profili certifikata iz opsega ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta koje izdaje Fina RDC 2015 CA usklađeni su s normama ETSI EN 319 411-1 [7] i ETSI EN 319 412 [8], [9] i [10].

Subordinirani Fina RDC 2015 CA izdaju certifikate prema profilima koji su određeni ovim $CPS_{WSA\text{-}eIDAS}$ dokumentom. Ovisno o namjeni certifikata, pravilima prema kojima je certifikat izdan, razini sigurnosti i načinu čuvanja pripadajućih privatnih ključeva, svaki tip certifikata ima definiran jedinstveni Finin OID općih pravila certificiranja (CP OID), a pored tog OID-a sadrži i odgovarajući ETSI OID općih pravila certificiranja.

7.1.1 Broj(evi) verzije

Certifikati su sukladni verziji 3 prema X.509 specifikaciji.

7.1.2 Ekstenzije certifikata

Dokument s opisom profila certifikata dostupan je na internetskim stranicama Fina repozitorija iz točke 2.2. ovih Općih pravila.

7.1.3 Identifikator objekta (OID) algoritama

Algoritmi s pripadajućim OID identifikatorima za sve certifikate koje izdaje subordinirani Fina RDC 2015 CA prikazani su u Tablici 7.1.

Algoritam	OID
sha256WithRSAEncryption	1.2.840.113549.1.1.11
rsaEncryption	1.2.840.113549.1.1.1

Tablica 7.1. Algoritmi s pripadajućim OID identifikatorima

7.1.4 Oblici naziva

Oblici naziva za Fina RDC 2015 CA opisan je u točki 1.3.2. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta.

Oblici naziva za OVCP certifikate koje izdaje Fina RDC 2015 CA opisani su u točkama 3.1.1. i 3.1.4. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta.

7.1.5 Ograničenja u nazivima

Ekstenzija *Name Constraints* se ne koristi.

7.1.6 Identifikator objekta (OID) općih pravila certificiranja

Ekstenzija *Certificate Policies* certifikata sadrži odgovarajuće Finine i ETSI OID-ove. U tablici 1.1. točke 1.1.2. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta naveden je popis tipova certifikata te pripadajući Finini i ETSI OID-ovi općih pravila certificiranja u ekstenziji *Certificate Policies*.

7.1.7 Uporaba ekstenzije *Policy Constraints*

Ekstenzija *Policy Constraints* se ne koristi.

7.1.8 Sintaksa i semantika kvalifikatora općih pravila

Kvalifikator općih pravila u ekstenziji *Certificate Policies* sadrži dva pokazivača u URI formatu koji sadrže internetsku adresu ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta na hrvatskom i engleskom jeziku.

7.1.9 Procesne semantike za kritičnu ekstenziju *Certificate Policies*

Nema odredbi.

7.2 Profil CRL

Profil CRL koje izdaje Fina RDC 2015 CA sukladan je preporuci IETF RFC 5280 [16].

7.2.1 Broj(evi) verzije

CRL su sukladne verziji 2 prema X.509 specifikaciji.

7.2.2 CRL i ekstenzije unosa u CRL

Ekstenzije CRL koje se koriste u CRL listama i u elementima unosa CRL lista koje izdaje Fina RDC 2015 CA definirane su u tablici 7.2.

Ekstenzije	Kritično	Vrijednost
crlExtensions		
cRLNumber	NO	Jednolično rastući serijski broj CRL duljine do 20 okteta.
AuthorityKeyIdentifier	NO	SHA-1 hash vrijednost duljine 160 bita
crlEntryExtensions		
reasonCode	NO	Kod razloga opoziva certifikata

Tablica 7.2. Ekstenzije CRL liste i elemenata unosa CRL listi koje izdaje Fina RDC 2015 CA

7.3 OCSP profil

Profil odgovora Fina OCSP servisa usklađen je s preporukom IETF RFC 6960 [17].

7.3.1 Broj(evi) verzije

Profil odgovora Fina OCSP servisa sukladan je verziji 1 prema IETF RFC 6960 [17].

7.3.2 OCSP ekstenzije

Ekstenzije odgovora Fina OCSP servisa prikazane su u tablici 7.3.

Ekstenzije	Kritično	Vrijednost
Nonce	NO	Vrijednost Nonce iz zahtijeva za status certifikata.
Extended Revoked Definition	NO	Kod razloga opoziva certifikata (*Reason code*)

Tablica 7.3. Ekstenzije odgovoraFina OCSP servis

8 PROVJERA SUKLADNOSTI

Nadzor nad radom Fine kao pružatelja usluga povjerenja reguliran je Uredbom (EU) br. 910/2014 [1] i Zakonom o provedbi Uredbe (EU) br. 910/2014 [2], a provodi ga središnje tijelo državne uprave nadležno za poslove gospodarstva.

Nadzor nad radom pružatelja usluga povjerenja u području prikupljanja, uporabe i zaštite osobnih podataka mogu provoditi i državna te druga tijela određena zakonom i drugim propisima koji uređuju zaštitu osobnih podataka.

Provjera sukladnosti obavlja se u cilju potvrđivanja da Fina kao pružatelj usluga povjerenja i usluga izdavanja certifikata koju Fina pruža ispunjavaju zahtjeve utvrđene Uredbom (EU) br. 910/2014 [1], Zakonom o provedbi Uredbe (EU) br. 910/2014 [2] te normom ETSI EN 319 411-1 [7].

Fina ima implementiran sustav upravljanja kvalitetom prema normi ISO 9001 i već se godinama nalazi u certifikacijskom ciklusu čime dokazuje da ispunjava zahtjeve te norme, da ima dokumentiran sustav, definirane ovlasti i odgovornosti te opisane procese.

Također, Fina ima uspostavljen, kontinuirano nadziran, certificiran i prema poslovnim potrebama unaprjeđivan vlastiti sustav informacijske sigurnosti u skladu sa normom ISO/IEC 27001 [4].

8.1 Učestalost ili okolnosti ocjene sukladnosti

Provjere sukladnosti u radu Fina PKI su vanjske provjere sukladnosti i interne provjere sukladnosti.

8.1.1 Vanjska provjera sukladnosti

Vanjska provjera sukladnosti provodi se najmanje svakih 12 mjeseci, sukladno zahtjevima normi ETSI EN 319 411-1 [7] i ETSI EN 319 403 [11].

8.1.2 Interna provjera sukladnosti

Interna provjera sukladnosti provodi se prije početka pružanja nove usluge, periodično najmanje svakih 12 mjeseci te nakon značajnijih promjena u radu Fina PKI.

Kvartalno se provodi provjera sukladnosti certifikata s ovim $CPS_{WSA\text{-}eIDAS}$ dokumentom, Općim pravilima [22] te u skladu sa zahtjevima iz CA/Browser Forum, BRG [19], na slučajnom uzorku od najmanje 3% certifikata izdanih nakon prethodne provjere.

Internom provjerom sukladnosti provodi se provjera usklađenosti sustava sa zahtjevima norme ETSI EN 319 411-1 [7] i sa zahtjevima iz CA/Browser Forum, BRG [19].

8.2 Identitet/kvalifikacije ocjenitelja

Vanjsku provjeru sukladnosti provodi tijelo za ocjenjivanje sukladnosti. Osposobljenost tijela za ocjenjivanje sukladnosti i osposobljenost pripadajućih ocjenitelja osigurana je akreditacijom tijela za ocjenjivanje sukladnosti prema normi ETSI EN 319 403 [11].

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

- odredbi norme ETSI EN 319 411-1 [7],
- PKI područja te područja informacijske sigurnosti,
- zakonske regulative iz područja pružanja usluga povjerenja.

Interni ocjenitelji sukladnosti provode interne provjere sukladnosti uz pomoć zaposlenika kojima je dodijeljena uloga Službenik za nadzor sustava.

8.3 Odnos ocjenitelja s tijelom koje se ocjenjuje

Tijelo za ocjenjivanje sukladnosti i pripadajući ocjenitelji neovisni su od Fine i Fininih sustava ocjenjivanja.

Interni ocjenitelji sukladnosti ne ocjenjuju sukladnost iz vlastitog djelokruga odgovornosti.

8.4 Predmeti ocjenjivanja sukladnosti

Predmeti ocjenjivanja sukladnosti obuhvaćaju slijedeća područja pružanja usluga povjerenja:

- cjelovitost i točnost dokumentacije,
- implementiranost zahtjeva za usluge povjerenja,
- organizacijski procesi i procedure,
- tehničke procese i procedure,
- implementirane mjere informacijske sigurnosti,
- vjerodostojne sustave,
- fizičku sigurnost predmetnih lokacija.

Opis predmetnog ocjenjivanja sukladnosti definiran je planom ocjenjivanja sukladnosti.

Fina će ocjenitelju sukladnosti na zahtjev omogućiti pristup svim prostorima Fina PKI sustava, pristup izvješćima internih i vanjskih provjera sukladnosti te drugim izvješćima i zapisima iz djelokruga pružanja usluga povjerenja. Fina će također ocjenitelju sukladnosti omogućiti pristup zapisima i ugovorima vezanim uz treće strane, interna, vanjska i upravljačka izvješća i sl. iz djelokruga pružanja usluga povjerenja.

8.5 Mjere u slučaju nesukladnosti

U ovisnosti o značaju otkrivene nesukladnosti vanjski ocjenitelj sukladnosti može u izvješću navesti koju nesukladnost Fina mora otkloniti.

U slučaju značajne nesukladnosti Fina će što prije formirati plan otklanjanja značajne nesukladnosti i uz konzultaciju sa vanjskim ocjeniteljem sukladnosti što prije otkloniti značajne nesukladnosti.

Ako je u pružanju usluga povjerenja utvrđena značajna nesukladnost koja kroz kraći vremenski rok nije otklonjiva Fina će poduzeti potrebne korake kako bi otklonila nesukladnost i ako je moguće u roku koji je odredilo nadzorno tijelo.

Manje nesukladnosti, uz konzultaciju sa vanjskim ocjeniteljem, Fina će otkloniti do slijedeće ocjene sukladnosti.

Vanjski ocjenitelj može predložiti i savjetovati izmjenu koja utječe na pružanje usluga povjerenja u cilju podizanja efikasnosti ili poboljšanja pružanja usluge povjerenja. U tom slučaju Fina zadržava pravo prihvaćanja prijedloga.

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

8.6 Priopćavanje rezultata

Rezultati interne provjere sukladnosti povjerljive su prirode i Fina ih ne objavljuje javno.

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

Rezultate vanjske provjere sukladnosti Fina javno objavljuje na internetskim stranicama repozitorija iz točke 2.2 ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta najkasnije tri mjeseca po završetku vanjske provjere sukladnosti. Nesukladnosti utvrđene tijekom provjere sukladnosti se ne objavljuju jer one mogu sadržavati povjerljive informacije.

9 OSTALE POSLOVNE I PRAVNE ODREDBE

9.1 Naknade za usluge

Fina obavještava Korisnike i Pouzdajuće strane o svim uslugama koje se naplaćuju. Ukoliko posebnim ugovorom nije drugačije određeno, usluge se naplaćuju sukladno cjeniku Fine. Cjenik svih usluga koje se naplaćuju objavljen je na internetskim stranicama repozitorija iz točke 2.2. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta.

Fina zadržava pravo izmjene cjenika. Izmjene cjenika objavljuju se na internetskim stranicama repozitorija iz točke 2.2. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta.

9.1.1 Naknade za izdavanje ili obnovu certifikata

Fina sukladno objavljenom cjeniku naplaćuje naknadu za usluge izdavanja i obnove 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 naplaćuje naknadu za uslugu opoziva certifikata.

Fina uvijek po svakom zaprimljenom zahtjevu u roku od 24 sata provodi opoziv i suspenziju certifikata, neovisno o statusu plaćanja pojedinog zahtjeva.

Fina ne naplaćuje uslugu davanja informacija o statusu opozvanosti certifikata koju pruža u vidu OCSP servisa ili objave CRL.

9.1.4 Naknade za ostale usluge

Fina može odrediti i naplaćivati primjerene naknade i za ostale usluge kao što su registracija Korisnika, promjena podataka u certifikatu, isporuka certifikata i opreme na lokaciju Korisnika i sl.

Za pristup Općim pravilima i ovom $CPS_{WSA\text{-}eIDAS}$ dokumentu ne naplaćuju se naknade.

9.1.5 Povrat naknada

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

9.2 Financijska odgovornost

Fina kao pružatelj usluga povjerenja posjeduje financijsku stabilnost te raspolaže dostatnim financijskim sredstvima koja osiguravaju nesmetano pružanje usluga certificiranja u skladu s ovim $CPS_{WSA\text{-}eIDAS}$ dokumentom.

9.2.1 Pokrivenost osiguranjem

Fina kao pružatelj usluga povjerenja ima osiguran rizik od odgovornosti za štete koje nastanu obavljanjem usluga certificiranja.

Fina dodatno osigurava imovinu policom osiguranja koja pokriva osiguranje od rizika požara, vremenskih nepogoda, poplava, eksplozija, udar vozila, pad ili udar letjelice, demonstracija, osiguranje opreme, strojne opreme, elektroničkih i komunikacijskih uređaja, instalacija i sl.

9.2.2 Druga sredstva

Nema odredbi.

9.2.3 Osiguranje ili garancije krajnjim korisnicima

Vidi točku 9.2.1.

9.3 Povjerljivost poslovnih podataka

9.3.1 Opseg povjerljivih poslovnih podataka

Povjerljivi poslovni podaci su svi podaci, u bilo kojem obliku, koje na bilo koji način između sebe razmjene sudionici u svezi s uspostavom i pružanjem usluga certificiranja, a koje sudionici označe povjerljivim, ili određenom vrstom ili stupnjem tajnosti, ili koji su po prirodi povjerljivi jer bi njihovo neovlašteno otkrivanje moglo prouzročiti štetu sudioniku.

9.3.2 Podaci koji se ne smatraju povjerljivim poslovnim podacima

Podaci koji se ugrađuju u sadržaj certifikata, podaci o statusu certifikata te podaci i dokumenti javno objavljeni u Fina PKI repozitoriju ne smatraju se povjerljivim poslovnim podacima.

9.3.3 Odgovornost za zaštitu povjerljivih poslovnih podataka

Svaki sudionik obvezan je štititi povjerljive poslovne podatke iz točke 9.3.1. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta, koje je saznao na bilo koji način, sukladno propisima koji uređuju zaštitu podataka prema vrsti podatka, odnosno vrsti i stupnju tajnosti podataka. U protivnom odgovara za nastalu štetu.

9.4 Zaštita osobnih podataka

Fina koristi i obrađuje podatke fizičkih osoba prikupljene u postupku registracije sukladno važećoj zakonskoj regulativi te ih Fina čuva u trajanju od najmanje 10 godina od isteka certifikata na kojeg se zapisi odnose.

9.4.1 Plan zaštite osobnih podataka

Fina provodi tehničke, kadrovske i organizacijske mjere zaštite osobnih podataka sukladno Zakon o provedbi Opće uredbe o zaštiti podataka [3] u svrhu zaštite privatnosti osoba i zaštite podataka od moguće zlouporabe te očuvanja točnosti, potpunosti i ažurnosti osobnih podataka.

Mjere zaštite osobnih podataka primjenjuju se prilikom razmjene osobnih podataka fizičkih osoba između Fina RA mreže i sustava certificiranja te prilikom čuvanja i arhiviranja osobnih podataka do njihovog izlučivanja iz arhive i uništavanja.

9.4.2 Povjerljivi osobni podaci

U postupku registracije te nakon toga, a u cilju izdavanja certifikata Fina je ovlaštena prikupljati osobne podatke koji su potrebni za valjano utvrđivanje identiteta Skrbnika i osoba ovlaštenih za zastupanje pravnih osoba te druge podatke potrebne za valjano pružanje usluga certificiranja. Svi ovi osobni podaci smatraju se povjerljivima i Fina ih propisno štiti.

9.4.3 Osobni podaci koji nisu povjerljivi

Osobni podaci koje u postupku registracije Korisnika i nakon toga prikupi Fina i koji su sadržaj certifikata su osobni podaci koji zbog dostupnosti svima zainteresiranima nisu povjerljivi.

9.4.4 Odgovornost za zaštitu osobnih podataka

Fina je odgovorna za zaštitu osobnih podataka prikupljenih u svrhu pružanja usluga certificiranja.

9.4.5 Ovlaštenje za korištenje osobnih podataka

Fina je ovlaštena, osim za potrebe ispunjenja zakonskih obveza, odnosno ugovornih obveza po ugovoru o certificiranju, koristiti ili objavljivati osobne podatke samo temeljem pisane suglasnosti fizičkih osoba i pravnih osoba iskazane u potpisanom zahtjevu za izdavanje certifikata ili ugovoru.

9.4.6 Dostupnost podataka mjerodavnim tijelima

Fina neće činiti dostupnima podatke iz točaka 9.3.1. i 9.4.2. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta osim u slučajevima propisanim zakonom ili kada to pisano zahtjeva mjerodavni sud, upravno ili neko drugo mjerodavno državno tijelo.

9.4.7 Ostale okolnosti objave podataka

Nema odredbi.

9.5 Prava intelektualnog vlasništva

Ovaj $CPS_{WSA\text{-}eIDAS}$ dokument kao i druga Finina dokumentacija objavljena na internetskim stranicama repozitorija iz točke 2.2. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta je intelektualno vlasništvo Fine.

Fina ne polaže pravo intelektualnog vlasništva na softver koji se koriste u Fina PKI, a koji je u vlasništvu trećih osoba

Vlasnik privatnog i javnog ključa je Korisnik te je ovlašten za uporabu privatnog ključa bez obzira generira li par ključeva Skrbnik, ili ga generira Fina kao pružatelj usluga povjerenja te bez obzira na način na koji je privatni ključ zaštićen.

Fina kao pružatelj usluga certificiranja vlasnik je certifikata koje izdaje.

9.6 Obveze i odgovornosti

9.6.1 Obveze i odgovornosti CA

Fina je odgovorna je za usklađenost ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta s Općim pravilima [22], njegovu usklađenost sa zakonskom regulativom te za provođenje odredbi propisanih ovim $CPS_{WSA\text{-}eIDAS}$ dokumentom, Uvjetima pružanja usluga certificiranja i sukladno obvezama u ugovoru o obavljanju usluga certificiranja sklopljenim s Korisnikom.

Fina na internetskim stranicama repozitorija iz točke 2.2. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta objavljuje uvjete pružanja usluga certificiranja, ovaj $CPS_{WSA\text{-}eIDAS}$ dokument, Opća pravila [22] te sve obavijesti i informacije o promjenama u radu koje na bilo koji način mogu utjecati na sudionike Fina PKI.

Fina je kao pružatelj usluga povjerenja odgovorna za štetu nastalu tijekom pružanja usluge prouzročene od strane poslovnog subjekta s kojim je Fina podugovorila dio usluge certificiranja. Ova odgovornost između Fine i poslovnog subjekta uređuje se posebnim ugovorom.

Fina je odgovorna za:

- ispravnu provjeru identiteta, podataka i ovlaštenja podnositelja zahtjeva u cilju prikupljanja podataka za izdavanja certifikata,
- izdavanje certifikata na siguran način radi očuvanja njegove autentičnosti i točnosti,
- usklađenost sa svojim obvezama.

Sukladno obvezama i odgovornostima Fina:

- provjerava kontrolu i isključivo pravo korištenja podnositelja zahtjeva nad domenskim imenom ili IP adresom sadržanom u certifikatu,
- prije izdavanja certifikata provjerava da je Korisnik odobrio izdavanje certifikata te da je podnositelj zahtjeva od Korisnika ovlašten za podnošenje zahtjeva za izdavanje certifikata,
- ima uspostavljene procedure kojima se osigurava provjera točnosti svih podataka sadržanih u certifikatu prije njegovog izdavanja,
- ima uspostavljene procedure kojima se osigurava smanjenje mogućnosti pogrešnog razumijevanja podataka sadržanih u certifikatu,
- ima uspostavljene procedure za provjeru identiteta podnositelja zahtjeva te procedure za izdavanje certifikata,
- sklapa ugovor o obavljanju usluga certificiranja s Korisnikom u slučajevima kad CA i Korisnik nisu povezani niti su isti entitet,
- u slučajevima kad Fina RDC 2015 CA izdaje certifikat za potrebe Fine, tada je Fina kao podnositelj zahtjeva upoznata s uvjetima pružanja usluga certificiranja,
- izdaje certifikat s profilom sukladnim poglavlju 7.1. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta, a prema tipu certifikata navedenom u zahtjevu za izdavanje certifikata,
- ako generira parove korisničkih ključeva, generira ih na siguran način i uz osiguranje tajnosti privatnog ključa, sukladno ovom $CPS_{WSA\text{-}eIDAS}$ dokumentu,
- osigurava provjeru da Korisnik posjeduje privatni ključ čiji se pripadajući javni ključ dostavlja na certificiranje,
- izdani certifikat čini dostupnim sukladno točki 4.4.2. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta,
- temeljem autenticiranog i autoriziranog zahtjeva, po provedenom propisanom postupku, opoziva certifikat iz razloga navedenih u točki 4.9.1. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta,
- pruža ažurnu informaciju o statusu opozvanosti certifikata,
- osigurava javnu dostupnost repozitorija na principu 24x7 s aktualnim statusima opozvanosti svih certifikata kojima nije istekao period važenja,
- pri pružanju usluge certificiranja primjenjuje odredbe važećih propisa iz točke 9.14. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta,
- provodi zahtijevane sigurnosne mjere za zaštitu prostora i opreme sustava certificiranja,
- primjenjuje organizacijske i tehničke mjere zaštite ključeva i certifikata sukladno ovom $CPS_{WSA\text{-}eIDAS}$ dokumentu,
- sukladno Planu kontinuiteta poslovanja osigurava nesmetan rad i maksimalnu raspoloživost usluga certificiranja,
- prati raspoloživost kapaciteta, planira održavanje i daljnji razvoj sustava certificiranja sukladno budućim potrebama, zahtjevima normi i razvoju tehnologije,
- podatke koji se sukladno točkama 9.3. i 9.4. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta smatraju povjerljivima štiti i te podatke koristiti isključivo za potrebe usluga certificiranja iz opsega ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta,
- osigurava da se interne i vanjske provjere sukladnosti Fine kao pružatelja usluga povjerenja provode sukladno točki 8.1. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta.

U slučaju prekida poslovanja Fina će postupiti sukladno točki 5.8. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta.

Ograničenja odgovornosti Fine kao davatelja usluga certificiranja opisana su u točki 9.8. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta.

9.6.2 Obveze i odgovornosti RA

Obveze i odgovornosti Fina RA mreže su:

- provođenje postupka registracije i identifikacije fizičkih osoba i pravnih osoba na način propisan ovim $CPS_{WSA\text{-}eIDAS}$ dokumentom,
- prosljeđivanje cjelovitih, točnih i provjerenih podataka o Subjektima na daljnju obradu u Fina RDC 2015 CA,
- čuvanje, arhiviranje i zaštita podataka i dokumentacije na period od najmanje 10 godina od isteka certifikata na kojeg se odnose,
- osiguravanje od gubitka ili povrede povjerljivosti, cjelovitosti i dostupnosti arhiviranih podataka Korisnika, na način propisan ovim $CPS_{WSA\text{-}eIDAS}$ dokumentom,
- obavještavanje podnositelja zahtjeva za izdavanje certifikata o javno objavljenim i dostupnim uvjetima pružanja usluga certificiranja, Općim pravilima [22] i ovim $CPS_{WSA\text{-}eIDAS}$ dokumentom.

9.6.3 Obveze i odgovornosti korisnika

Prije inicijalnog izdavanja certifikata Korisnik s Finom sklapa ugovor o obavljanju usluga certificiranja kojim prihvaća Opća pravila [22], ovaj $CPS_{WSA\text{-}eIDAS}$ dokument i uvjete pružanja usluga certificiranja.

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

Korisnik je, kao pravna osoba, odgovoran za točnost, cjelovitost i ispravnost podataka dostavljenih u postupku registracije i predaje zahtjeva za izdavanje certifikata te naknadno po zahtjevu Fine, a povezano uz izdavanje certifikata.

Korisnik je dužan:

- u procesu registracije predstaviti se na način propisan u poglavlju 3. i u točki 4.1.2.2. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta,
- pažljivo koristiti i čuvati privatne ključeve i aktivacijske podatke sukladno ovom $CPS_{WSA\text{-}eIDAS}$ dokumentu,
- poduzeti odgovarajuće mjere zaštite privatnog ključa i aktivacijskih podataka od neovlaštenog pristupa i uporabe u skladu s poglavljem 6. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta,
- pregledati i provjeriti točnost sadržaja izdanog certifikata prije njegova prihvaćanja,
- u najkraćem mogućem roku zatražiti opoziv certifikata i prekinuti uporabu pripadajućeg privatnog ključa u slučaju sumnje ili stvarne pogrešne uporabe ili kompromitiranja privatnog ključa, te ako neka od informacija sadržanih u certifikatu postane netočna, sukladno točki 4.9. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta,

- ako je certifikat opozvan iz razloga kompromitiranja privatnog ključa, u najkraćem mogućem roku prekinuti svaku uporabu privatnog ključa povezanog s javnim ključem u certifikatu,
- slijediti upute Fine povezane s kompromitiranjem ključa ili pogrešne uporabe certifikata,
- koristiti certifikat i pripadajući privatni ključ samo na poslužiteljima dostupnim preko FQDN-a ili IP adrese navedenim u *Subject Alternative Name* ekstenziji certifikata, a u skladu sa zakonima i drugim propisima Republike Hrvatske te sukladno odredbama iz točke 1.4.1. i 1.4.2. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta, ugovora i uvjetima pružanja usluge,
- koristiti certifikat i pripadajući privatni ključ u skladu s odredbama iz točke 4.5.1. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta,
- djelovati u skladu sa svim ostalim odredbama iz ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta koje se odnose na obveze Korisnika.

Obveze i odgovornosti Korisnika vezane uz korištenje privatnog ključa i certifikata opisane su u točki 4.5.1. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta.

Korisnik, kao pravna osoba, sklapanjem ugovora o obavljanju usluga certificiranja s Finom prihvaća da Fina kao pružatelj usluga povjerenja ima pravo trenutno opozvati certifikat u slučaju da Korisnik krši uvjete Ugovora ili uvjeta pružanja usluga certificiranja, ili u slučaju da Fina otkrije da se certifikat koristi kako bi se omogućilo obavljanje kriminalnih aktivnosti, kao što su primjerice *phishing* napadi, prijevarne radnje ili distribucija zlođudnog koda.

U slučaju promjene kontakt podataka nastale promjene Korisnik je dužan dostaviti Fini na kontakt podatke navedene u točki 9.11. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta.

Korisnik odgovara za nepravilnosti koje su nastale zbog neispunjavanja obveza utvrđenih gore navedenim odredbama iz ove točke.

Korisniku koji ne postupa u skladu s preuzetim obvezama može biti opozvan certifikat te će izgubiti sva prava proizašla iz ugovora o obavljanju usluga certificiranja.

9.6.4 Obveze i odgovornosti pouzdajuće strane

Pouzdajuća strana dužna je samostalno i svjesno donijeti odluku o razumnom pouzdanju u certifikat.

Razumnim pouzdanjem smatra se odluka Pouzdajuće strane da se pouzda u certifikat ako je u vrijeme ostvarenja pouzdanja:

- poduzela potrebne mjere opreza i koristiti certifikat u svrhe propisane ovim $CPS_{WSA\text{-}eIDAS}$ dokumentom, odnosno uvjetima pružanja usluge, pod okolnostima u kojima je pouzdanje razumno i u dobroj namjeri te pod okolnostima koje su poznate ili bi trebale biti poznate Pouzdajućoj strani prije ostvarenja pouzdanja,
- koristila aplikacijsko rješenje i IT okolinu u koju se može pouzdati,
- provjerila period važenja certifikata,

- provjerila status opozvanosti certifikata, a što Pouzdajuća strana utvrđuje provodeći provjeru statusa certifikata putem OCSP servisa ili temeljem zadnje izdane CRL, kako je propisano ovim $CPS_{WSA\text{-}eIDAS}$ dokumentom,
- provjerila da privatni ključ koji se koristi za autentikaciju odgovara javnom ključu u certifikatu za vrijeme perioda važenja certifikata.

Korištenje javnog ključa i certifikata od strane Pouzdajuće strane opisano je u točki 4.5.2., a zahtjevi za provjeru opoziva certifikata navedeni su u točki 4.9.6. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta.

Pouzdajuća strana koja nije poštovala propise i ovaj $CPS_{WSA\text{-}eIDAS}$ dokument te nije postupala sukladno obvezama i odgovornostima iz ove točke sama snosi sve rizike pouzdanja u takav certifikat.

Pouzdajuća strana snosi sve rizike pouzdanja u certifikat ako zna ili ima razloga smatrati da postoje činjenice koje mogu uzrokovati osobnu ili poslovnu štetu prouzročenu ostvarenjem pouzdanja u certifikat.

9.6.5 Obveze i odgovornosti ostalih sudionika

Nema odredbi.

9.7 Odricanje od odgovornosti

Fina nije odgovorna za štete, uključujući i indirektne, štete za slučaj nezgode, štete za slučaj nepogode s posljedicama ili za bilo koji gubitak dobiti, gubitak podataka ili druge indirektne štete koje su proizašle iz veze s uslugama certificiranja.

Fina nije odgovorna za štete:

- štete pretrpljene u vremenu od opoziva certifikata do izdavanja nove CRL,
- štete zbog neautorizirane uporabe korisničkih ključeva i certifikata,
- štete nastale uporabom certifikata koja nije dopuštena ovim $CPS_{WSA\text{-}eIDAS}$ dokumentom,
- štete prouzročene prijevarnom ili nemarnom uporabom certifikata, CRL ili OCSP servisa,
- štete nastale kao rezultat neispravnosti i pogrešaka u softveru i hardveru Subjekta i Pouzdajuće strane.

Fina nije odgovorna za štete, uključujući i indirektne štete, štete za slučaj nezgode, štete za slučaj nepogode s posljedicama ili za bilo koji gubitak dobiti, gubitak podataka ili druge indirektne štete koje su nastale kao rezultat prijevarnog davanja podataka i prijevarnog predstavljanja korisnika tijekom procesa identifikacije i potvrde identiteta ako je provjeru podataka ured Fina RA mreže provodio u skladu sa zahtjevima iz ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta i $CPS_{NQC\text{-}eIDAS}$ dokumenta [23].

9.8 Ograničenja odgovornosti

Finina ukupna financijska odgovornost za nekvalificirane certifikate izdane prema ovom $CPS_{WSA\text{-}eIDAS}$ dokumentu i $CPS_{NQC\text{-}eIDAS}$ dokumentu [23] te za transakcije obavljene na temelju pouzdavanja u tako izdane certifikate iznosi najviše 1.500.000 kuna.

Ako nije posebnim ugovorom ili na drugi način određeno, Finina maksimalna financijska odgovornost prema Korisniku i Pouzdajućoj strani koja se razumno pouzdaje u certifikat ograničava se sukladno preporučenim financijskim limitima određenim u Tablici 1.4. Finina maksimalna financijska odgovornost za nekvalificirane certifikate prikazana je Tablici 9.1.

Kategorija certifikata	Maksimalna Finina financijska odgovornost		
	Po kategoriji	Po transakciji	Ukupno
Certifikati srednje razine sigurnosti - *SSL certifikat razine 2 (OVCP)*	do 600.000 kn	do 80.000 kn	1.500.000 kn
Certifikati visoke razine sigurnosti - *SSL certifikat razine 3 (OVCP)*	do 800.000 kn	do 400.000 kn	

Tablica 9.1. Maksimalna Finina financijska odgovornost

9.9 Naknada štete

Svaki sudionik odgovara oštećenom za štetu koju je počinio zbog nepoštivanja odredbi ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta, Općih pravila i važećih relevantnih propisa.

Bez obzira na odricanje od odgovornosti i ograničenja odgovornosti prema Korisnicima i Pouzdajućim stranama koja su opisana Općim pravilima [21] i ovim $CPS_{WSA\text{-}eIDAS}$ dokumentom Fina prihvaća da ugovoreni Isporučitelji aplikacijskog softvera preko kojih se distribuira Finin Root CA ne preuzimaju nikakvu obvezu ili potencijalnu odgovornost Fine određenu ovim Općim pravilima ili drugim aktom zbog izdavanja ili održavanja certifikata ili zbog pouzdanja koje u certifikat ostvaruje Pouzdajuća strana, ili drugi. To se, međutim, ne odnosi na potraživanja, štete, odnosno pretrpjeli gubitak u slučajevima u kojima softver Isporučitelja aplikacijskog softvera nije obavio provjeru utemeljenosti ostvarenja pouzdanja u certifikat ili ju je pogrešno prikazao, a u trenutku kada je informacija o aktualnom statusu opozvanosti certifikata bila *online* dostupna putem OCSP servisa i CRL.

Korisnik odgovara oštećenom, odnosno svakom drugom sudioniku ako ishodi i koristi certifikat izdan od Fine temeljem prijevarno danih podataka u zahtjevu za izdavanje certifikata.

Pouzdajuća strana odgovara oštećenom, odnosno svakom drugom sudioniku ako se pouzda u izdani certifikat bez provjere njegove valjanosti opisane u točki 9.6.4. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta ili ga koristi protivno svrhama određenim ovim $CPS_{WSA\text{-}eIDAS}$ dokumentom.

9.10 Trajanje i prestanak važenja

9.10.1 Trajanje

Ovaj $CPS_{WSA\text{-}eIDAS}$ dokument važi do stupanja na snagu novog $CPS_{WSA\text{-}eIDAS}$ dokumenta ili do objave prestanka njegovog važenja. Nova verzija dokumenta ili objava prestanka važenja biti će objavljena na internetskim stranicama repozitorija iz točke 0. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta s naznačenim danom stupanja na snagu. Novom dokumentu biti će dodijeljena nova verzija i novi OID te će u njemu biti naznačene obavljene izmjene.

9.10.2 Prestanak važenja

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

Prestanak važenja ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta nije vezan i ne utječe na važenje certifikata izdanih primjenom ovog dokumenta.

Fina može za pojedine odredbe važećeg $CPS_{WSA\text{-}eIDAS}$ dokumenta izraditi izmjene i dopune kao što je to navedeno u točki 9.12. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta.

9.10.3 Posljedice prestanka važenja i nastavak djelovanja

Stupanjem na snagu nove verzije $CPS_{WSA\text{-}eIDAS}$ dokumenta na sve se certifikate izdane od tog dana primjenjuju odredbe iz tog dokumenta.

Certifikati izdani primjenom prethodnih $CPS_{WSA\text{-}eIDAS}$ dokumenata važe do njihova isteka pri čemu se mogu obnoviti primjenom pravila iz novog $CPS_{WSA\text{-}eIDAS}$ dokumenta.

9.11 Individualne obavijesti i komunikacija sa sudionicima

Individualna komunikacija sa sudionicima primarno se provodi preko Finine službe za odnose s korisnicima:

- besplatni telefon: 0800 0080

Individualne obavijesti i druga službena komunikacija u pisanom obliku provodi se korištenjem sljedećih kontaktnih podataka:

Kontaktni podaci za dostavu dopisa prema Fini	
Poštanska adresa:	Fina Centar elektroničkog poslovanja, Ulica grada Vukovara 70 10000 Zagreb Hrvatska
E-mail:	info.rdc@fina.hr
Telefaks:	+385-1-6304-081

9.12 Izmjene i dopune

9.12.1 Procedure izmjena i dopuna

Ovaj $CPS_{WSA\text{-}eIDAS}$ dokument revidira se po potrebi.

Fina može bez obavijesti unositi tipografske ispravke, promjene kontakt podataka te druge manje ispravke koje bitno ne utječu na sudionike.

Svi sudionici mogu na kontakt adresu Fina PMA iz točke 0. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta poslati dopis s prijedlogom za ispravke pogrešaka, prijedlog nadopuna ili izmjenu ovog dokumenta. U dopisu se navode kontakt podaci osobe koja je poslala prijedlog promjene. Fina PMA može prihvatiti, prilagoditi ili odbiti predložene promjene nakon razmatranja istih.

Izradu novog ili izmjenu i dopunu postojećeg $CPS_{WSA\text{-}eIDAS}$ dokumenta odobrava i provodi Fina PMA, a sukladno poslovnim zahtjevima Fine i zahtjevima zakonske regulative i propisa iz točke 9.14 ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta.

9.12.2 Mehanizmi obavještavanja i vremenski periodi

Sve izmjene i dopune $CPS_{WSA\text{-}eIDAS}$ dokumenta objavljuju se u elektroničkom obliku na internetskim stranicama repozitorija iz točke 2.2. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta.

Nove verzije Općih pravila s izmijenjenim OID-om Općih pravila objavljuju se u elektroničkom obliku na internetskim stranicama repozitorija iz točke 2.2. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta.

Datum stupanja na snagu izmjena i dopuna ili novoobjavljenog ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta naznačeni su na njegovoj naslovnoj strani kao i na internetskim stranicama na kojima je objavljen.

9.12.3 Okolnosti pod kojima se mora mijenjati OID

Veće izmjene u ovom $CPS_{WSA\text{-}eIDAS}$ dokumentu koje mogu utjecati na sudionike zahtijevaju i izmjenu OID-a Općih pravila. Novi OID za novu verziju dokumenta određuje Fina PMA.

9.13 Postupak rješavanja sporova

U slučaju spora ili neslaganja između Fine i drugih sudionika povodom radnji i/ili postupaka glede pružanja usluge certificiranja uređene ovim $CPS_{WSA\text{-}eIDAS}$ dokumentom, isti će se nastojati razriješiti sporazumno. Ako sporazumno razrješenje spora nije moguće, isti će se razriješiti pred mjerodavnim sudom u Zagrebu uz primjenu hrvatskog prava.

Sudionici mogu Fini uputiti prigovor ako smatraju postoji odstupanje sadržaja usluge u odnosu na objavljene uvjete pružanja usluga. Fina će povodom prigovora odgovoriti podnositelju prigovora. Prigovori se upućuju pisano u papirnatom ili elektroničkom obliku na adrese navedene u točki 9.11. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta.

9.14 Važeći propisi

Usluge povjerenja iz opsega ovih Općih pravila Fina pruža sukladno odredbama Uredbe (EU) br. 910/2014 [1], Zakona o provedbi Uredbe (EU) br. 910/2014 [2] te normizacijskih dokumenata ETSI EN 319 401 [6] i ETSI EN 319 411-1 [7] i CA/Browser Forum BRG [19].

9.15 Usklađenost s primjenjivim propisima

Ovaj $CPS_{WSA\text{-}eIDAS}$ dokument i pružanje usluga certificiranja koje su obuhvaćene ovim $CPS_{WSA\text{-}eIDAS}$ dokumentom usklađeni su s propisima iz točke 9.14. ovog $CPS_{WSA\text{-}eIDAS}$ dokumenta.
Svi sudionici suglasni su s primjenom hrvatskog prava u tumačenju primijenjenih odredbi.

9.16 Razne odredbe

Nema odredbi.

9.17 Ostale odredbe

Gdje je to moguće, Fina omogućuje da usluge certificiranja i proizvodi za krajnjeg korisnika koji se koriste pri pružanju tih usluga budu dostupni osobama s invaliditetom.

Ako podnositelj zahtjeva ima neku vrstu invaliditeta, Fina pomaže podnositelju pri predaji zahtjeva i registraciji. Pomoć podnositelju također je osigurana prilikom predaje zahtjeva za opoziv, suspenziju i reaktivaciju certifikata.

Fina javno objavljuje Opća pravila [22], ovaj $CPS_{WSA\text{-}eIDAS}$ dokument i uvjete pružanja usluga certificiranja.

Uvjeti pružanja usluga certificiranja komuniciraju se dokumentom u papirnatom obliku ili dokumentom u elektroničkom obliku čija je cjelovitost zaštićena.

Prije sklapanja ugovora o obavljanju usluga certificiranja Korisnici se informiraju o uvjetima pružanja usluga certificiranja. Prihvaćanje uvjeta pružanja usluga certificiranja preduvjet je za izdavanje certifikata.

U postupcima obnove certifikata, ponovnog izdavanja certifikata nakon isteka, opoziva ili izmjene podataka u certifikatu Fina obavještava Skrbnika te ukoliko je primjereno Korisnika o eventualnim izmjenama uvjeta o pružanju usluga certificiranja.