FINA

OPĆA PRAVILA PRUŽANJA USLUGA CERTIFICIRANJA ZA CERTIFIKATE ZA AUTENTIKACIJU MREŽNIH STRANICA

Verzija 1.6

Datum stupanja na snagu: 25.09.2020.

OID Dokumenta: 1.3.124.1104.5.0.5.1.1.6

Informacije o dokumentu

Ime dokumenta:	Opća pravila pružanja usluga certificiranja za certifikate za autentikaciju mrežnih stranica
OID dokumenta:	1.3.124.1104.5.0.5.1.1.6
Tip dokumenta:	Opća pravila pružanja usluga certificiranja (*Certificate Policy*, CP)
Oznaka distribucije	Javno
Vlasnik dokumenta	Financijska agencija, Fina
Kontakt	pma@fina.hr

Povijest izmjena

Verzija	Datum	Razlog izmjene
1.0	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, dodana izjava o provjeri CAA zapisa i ispravak tipografskih grešaka.
1.2	27.07.2018.	Dodavanje odredbi za provjeru zemlje povezane sa Subjektom te 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.
1.4	27.05.2019.	Uklonjen profil certifikata „SSL certifikat razine 3 (OVCP)“ zajedno s opisima pripadajućih postupaka zbog prestanka njegova izdavanja, dodana pravila i kontakt podaci za prijavu problema s certifikatom, u točki 3.1.4. dodane informacije o ograničenjima skupa znakova, u poglavljima 3. i 4. dodana pojašnjenja u postupcima registracije i provjere podataka te dodane specifikacije razina elektroničkih potpisa koje Fina prihvaća na korisničkim zahtjevima i ugovorima o obavljanju usluga certificiranja, u točkama 4.6. i 4.7. dodana pojašnjenja za dostavu javnog ključa kod obnove certifikata, u točki 4.9. poboljšan opis razloga za opoziv certifikata te dodatno specificirani vremenski periodi vezani uz opoziv, u točki 5.2.4. dopunjeno je pravilo za odvajanje dužnosti, u točki 6.1.7. proširen je opis namjena ključeva, u točki 9.4. dodana su proširenja u opisu zaštite osobnih podataka, u točki 9.6.1. dopunjen je opis odgovornosti Fine, u točkama 9.7. i 9.9. ispravljen tekst odricanja odgovornosti Fine te su ispravljene prepoznate greške u dokumentu.

1.5	30.04.2020.	Ažurirana referenta lista zakonske regulative te su ispravljene prepoznate manje greške u dokumentu.
1.6	22.09.2020.	Dodane su odredbe za podršku Transparentnosti certifikata (*Certificate Transparency*) u točkama 2.2, 4.3.1, 4.4.2, i 4.4.3 te je u točki 6.3.2 skraćen vremenski period važenja novih SSL certifikata razine 2 (OVCP) na 12 mjeseci.

SADRŽAJ

REFERENTNE DOKUMENTIRANE INFORMACIJE 11

Temeljni zakon 11
Ostali zakoni 11
Normizacijski dokumenti 11
Finini dokumenti 12
1 UVOD 13

1.1 Pregled 13
1.1.1 Opseg i namjena 14
1.1.2 Tipovi certifikata 14

1.2 Naziv dokumenta i identifikacijski podaci 15
1.3 Sudionici u PKI 15
1.3.1 Certifikacijska tijela 16
1.3.2 Registracijski uredi 17
1.3.3 Korisnici 17
1.3.4 Pouzdajuće strane 18
1.3.5 Ostali sudionici 18

1.4 Uporaba certifikata 18
1.4.1 Primjerena uporaba certifikata 18
1.4.2 Zabrane uporabe certifikata 18

1.5 Administracija dokumenta 18
1.5.1 Organizacija odgovorna za održavanje dokumenta 18
1.5.2 Kontakt podaci 19
1.5.3 Tijelo koje utvrđuje uskladivost CPS-a s Općim pravilima 19
1.5.4 Procedure odobravanja CPS-a 19

1.6 Definicije i kratice 19
1.6.1 Definicije 19
1.6.2 Kratice 26
2 OBJAVE I ODGOVORNOSTI ZA REPOZITORIJ 27

2.1 Identifikacija tijela koje vodi repozitorij 27
2.2 Objava informacija o certificiranju 27
2.3 Vrijeme ili učestalost objavljivanja 28
2.4 Kontrole pristupa repozitoriju 28
3 IDENTIFIKACIJA I POTVRĐIVANJE IDENTITETA SUBJEKTA 29

3.1 Određivanje imena 29
3.1.1 Tipovi imena 29
3.1.2 Smislenost imena 29
3.1.3 Anonimnost korisnika ili pseudonimi 29
3.1.4 Pravila tumačenja raznih oblika imena 29
3.1.5 Jedinstvenost imena 30
3.1.6 Prepoznavanje, potvrđivanje identiteta i uloga zaštitnog znaka 30

3.2 Inicijalno utvrđivanje identiteta 31
3.2.1 Metoda dokazivanja posjeda privatnog ključa 31
3.2.2 Potvrda identiteta poslovnog subjekta i domene 31
3.2.3 Potvrda identiteta fizičke osobe 32
3.2.4 Informacije o korisniku koje se ne provjeravaju 33
3.2.5 Kriteriji interoperabilnosti 33

3.3 Identifikacija i potvrđivanje identiteta kod podnošenja zahtjeva za obnovu certifikata 33
3.3.1 Identifikacija i potvrđivanje identiteta kod redovne obnove certifikata 33
3.3.2 Identifikacija i potvrđivanje identiteta korisnika za ponovno izdavanje certifikata nakon opoziva 34
3.3.3 Identifikacija i potvrđivanje identiteta korisnika za ponovno izdavanje certifikata nakon isteka 34
3.3.4 Identifikacija i potvrđivanje identiteta korisnika za oporavak certifikata 34
3.4 Identifikacija i potvrđivanje identiteta kod zahtjeva za opoziv certifikata 34
4 OPERATIVNI ZAHTJEVI NA ŽIVOTNI CIKLUS CERTIFIKATA 36
4.1 Podnošenje zahtjeva za izdavanje certifikata 36
4.1.1 Tko može podnijeti zahtjev za izdavanje certifikata 36
4.1.2 Postupak prijave korisnika s podnošenjem zahtjeva za izdavanje certifikata i odgovornosti 36
4.2 Obrada zahtjeva za izdavanje certifikata 37
4.2.1 Obavljanje identifikacije i potvrđivanje identiteta 37
4.2.2 Odobravanje ili odbijanje zahtjeva za izdavanje certifikata 37
4.2.3 Vrijeme obrade zahtjeva za izdavanje certifikata 37
4.3 Izdavanje certifikata 37
4.3.1 Postupci CA tijekom izdavanja certifikata 37
4.3.2 Obavještavanje korisnika od strane CA o izdavanju certifikata 38
4.4 Prihvaćanje certifikata 38
4.4.1 Provedba prihvaćanja certifikata 38
4.4.2 Objava izdanog certifikata od strane CA 38
4.4.3 Obavještavanje drugih strana od strane CA o izdavanju certifikata 39
4.5 Par ključeva i korištenje certifikata 39
4.5.1 Korištenje privatnog ključa i certifikata od strane korisnika 39
4.5.2 Korištenje javnog ključa i certifikata od strane pouzdajuće strane 39
4.6 Obnova certifikata 40
4.6.1 Razlozi za obnovu certifikata 40
4.6.2 Tko može tražiti obnovu certifikata 40
4.6.3 Obrada zahtjeva za obnovu certifikata 40
4.6.4 Obavještavanje korisnika o obnovi certifikata 40
4.6.5 Provedba prihvaćanja obnovljenog certifikata 40
4.6.6 Objava obnovljenog certifikata od strane CA 40
4.6.7 Obavještavanje drugih strana o obnovi certifikata 40
4.7 Obnova certifikata uz generiranje novog para ključeva 40
4.7.1 Razlozi za obnovu certifikata uz generiranje novog para ključeva 41
4.7.2 Tko može zatražiti certificiranje novog javnog ključa 41
4.7.3 Obrada zahtjeva za obnovu certifikata uz generiranje novog para ključeva 41
4.7.4 Obavještavanje korisnika o obnovi certifikata uz generiranje novog para ključeva 42
4.7.5 Provedba prihvaćanja obnovljenog certifikata s generiranim novim parom ključeva 42
4.7.6 Objavljivanje certifikata po obnovi s generiranjem novog para ključeva 42
4.7.7 Obavještavanje drugih strana o obnovi certifikata s generiranim parom ključeva 42
4.8 Izmjene u certifikatu 42
4.8.1 Razlozi za izmjene u certifikatu 42
4.8.2 Tko može zatražiti izmjene u certifikatu 43
4.8.3 Obrada zahtjeva za izmjenama u certifikatu 43
4.8.4 Obavještavanje korisnika o izdavanju izmijenjenog certifikata 43
4.8.5 Provedba prihvaćanja izmijenjenog certifikata 43
4.8.6 Objavljivanje izmijenjenog certifikata od strane CA 43

4.8.7 Obavještavanje drugih strana o izdavanju izmijenjenog certifikata 43
4.9 Opoziv i suspenzija certifikata 43
4.9.1 Razlozi za opoziv 43
4.9.2 Tko može tražiti opoziv 45
4.9.3 Procedura za zahtjev za opozivom 45
4.9.4 Poček zahtjeva za opozivom 46
4.9.5 Vremenski period u kojem CA mora obraditi zahtjev za opozivom 46
4.9.6 Zahtjevi pouzdajućim stranama za provjeru opoziva 46
4.9.7 Učestalost izdavanja CRL 46
4.9.8 Maksimalno kašnjenje za CRL 46
4.9.9 *Raspoloživost online* provjere statusa opozvanosti certifikata 47
4.9.10 Zahtjevi na online provjeru statusa opozvanosti certifikata 47
4.9.11 Ostali načini objave statusa opozvanosti certifikata 47
4.9.12 Posebni zahtjevi vezani uz kompromitiranje privatnog ključa 47
4.9.13 Razlozi za suspenziju 47
4.9.14 Tko može tražiti suspenziju 47
4.9.15 Procedura za zahtjev za suspenziju i reaktivaciju 47
4.9.16 Ograničenje na trajanje suspenzije 47
4.10 Usluge statusa certifikata 48
4.10.1 Operativna svojstva 48
4.10.2 Dostupnost usluga 48
4.10.3 Opcionalna svojstva 48
4.11 Kraj korištenja 49
4.12 Sigurno skladištenje i oporavak privatnog ključa 49
5 PROVJERA SUSTAVA, UPRAVLJANJA I RADNIH POSTUPAKA 50
5.1 Mjere fizičke zaštite 50
5.1.1 Lokacija objekta i konstrukcija 50
5.1.2 Fizički pristup 50
5.1.3 Sustavi za napajanje i klimatizaciju 51
5.1.4 Opasnost od poplave 51
5.1.5 Protupožarna zaštita 51
5.1.6 Pohrana medija 51
5.1.7 Zbrinjavanje otpada 51
5.1.8 Sigurnosne kopije na drugoj lokaciji 51
5.2 Organizacijske mjere zaštite 52
5.2.1 Povjerljive uloge 52
5.2.2 Broj osoba potrebnih za obavljanje zadataka 52
5.2.3 Identifikacija i potvrđivanje identiteta za svaku ulogu 52
5.2.4 Uloge koje zahtijevaju odvajanje dužnosti 52
5.3 Osoblje 53
5.3.1 Kvalifikacije, radno iskustvo i zahtjevi za provjerom osoblja 53
5.3.2 Procedure provjere primjerenosti osoblja 53
5.3.3 Zahtjevi za školovanjem 53
5.3.4 Periodičko obavljanje znanja i osvješćivanje 53
5.3.5 Učestalost i slijed izmjene zaposlenika 53
5.3.6 Kazne za neovlaštene radnje 54
5.3.7 Zahtjevi na vanjske suradnike 54
5.3.8 Dokumentacija koja je dostupna osoblju 54
5.4 Postupci upravljanja revizijskim zapisima 54
5.4.1 Tipovi događaja koji se zapisuju 54
5.4.2 Učestalost obrade revizijskih zapisa 54
5.4.3 Vremenski period pohrane revizijskih zapisa 55

5.4.4 Zaštita revizijskih zapisa 55
5.4.5 Postupci izrade sigurnosnih kopija revizijskih zapisa 55
5.4.6 Sustav prikupljanja revizijskih zapisa (unutarnji ili vanjski) 55
5.4.7 Obavještavanje subjekta uzročnika događaja 55
5.4.8 Procjena ranjivosti 55
5.5 Arhiviranje zapisa 56
5.5.1 Tipovi arhiviranih zapisa 56
5.5.2 Vremenski period arhiviranja 56
5.5.3 Zaštita arhive 56
5.5.4 Postupci izrade sigurnosnih kopija arhive 56
5.5.5 Zahtjevi na zaštitu zapisa vremenskim žigom 56
5.5.6 Sustav prikupljanja arhiva (unutarnji ili vanjski) 56
5.5.7 Postupci dobivanja i provjere arhiviranih zapisa 57
5.6 Promjena CA ključa 57
5.7 Oporavak od kompromitiranja ili nepogode 57
5.7.1 Postupci u slučaju incidenta ili kompromitiranja 57
5.7.2 Postupci u slučaju oštećenja u računalnim resursima, programima i/ili podacima 57
5.7.3 Postupci u slučaju kompromitiranja privatnog ključa 57
5.7.4 Mogućnost nastavka poslovanja nakon nepogode 58
5.8 Prestanak rada CA ili RA 58
6 TEHNIČKE MJERE ZAŠTITE 60
6.1 Generiranje i instalacija para ključeva 60
6.1.1 Generiranje para ključeva 60
6.1.2 Dostava privatnog ključa korisniku 61
6.1.3 Dostava javnog ključa CA-u 61
6.1.4 Dostava javnog ključa CA pouzdajućim stranama 61
6.1.5 Duljine ključeva 62
6.1.6 Generiranje i provjera kvalitete parametara javnog ključa 62
6.1.7 Namjene ključeva (po X.509 v3 polju uporabe ključa) 62
6.2 Zaštita privatnog ključa i tehnike upravljanja kriptografskim modulom 63
6.2.1 Norme i tehničke mjere zaštite kriptografskog modula 63
6.2.2 Upravljanje privatnim ključem od strane više osoba (n od m) 63
6.2.3 Sigurno skladištenje privatnog ključa (*key escrow*) 63
6.2.4 Sigurnosno kopiranje privatnog ključa 63
6.2.5 Arhiviranje privatnog ključa 63
6.2.6 Prijenos privatnog ključa 64
6.2.7 Spremanje privatnog ključa u kriptografskom modulu 64
6.2.8 Metoda aktivacije privatnog ključa 64
6.2.9 Metoda deaktivacije privatnog ključa 64
6.2.10 Metoda uništavanja privatnog ključa 65
6.2.11 Ocjena kriptografskog modula 65
6.3 Ostali vidovi upravljanja parom ključeva 65
6.3.1 Arhiviranje javnog ključa 65
6.3.2 Vremenski period važenja certifikata i korištenja para ključeva 65
6.4 Aktivacijski podaci 66
6.4.1 Generiranje i instalacija aktivacijskih podataka 66
6.4.2 Zaštita aktivacijskih podataka 66
6.4.3 Ostale odredbe o aktivacijskim podacima 66
6.5 Upravljanje računalnom sigurnošću 66
6.5.1 Posebni tehnički zahtjevi na računalnu sigurnost 66
6.5.2 Ocjena računalne sigurnosti 67

6.6 Tehničke kontrole životnog ciklusa 67
6.6.1 Kontrole razvoja sustava 67
6.6.2 Kontrole upravljanja sigurnošću 67
6.6.3 Sigurnosne kontrole životnog ciklusa 67
6.7 Provjera mrežne sigurnosti 68
6.8 Uporaba vremenskog žiga 68
7 SADRŽAJ CERTIFIKATA, LISTA OPOZVANIH CERTIFIKATA I OCSP PROFILI 69
7.1 Profil certifikata 69
7.1.1 Broj(evi) verzije 69
7.1.2 Ekstenzije certifikata 69
7.1.3 Identifikator objekta (OID) algoritama 69
7.1.4 Oblici naziva 69
7.1.5 Ograničenja u nazivima 69
7.1.6 Identifikator objekta (OID) općih pravila certificiranja 70
7.1.7 Uporaba ekstenzije *Policy Constraints* 70
7.1.8 Sintaksa i semantika kvalifikatora općih pravila 70
7.1.9 Procesne semantike za kritičnu ekstenziju *Certificate Policies* 70
7.2 Profil CRL 70
7.2.1 Broj(evi) verzije 70
7.2.2 CRL i ekstenzije unosa u CRL 70
7.3 OCSP profil 71
7.3.1 Broj(evi) verzije 71
7.3.2 OCSP ekstenzije 71
8 PROVJERA SUKLADNOSTI 72
8.1 Učestalost ili okolnosti ocjene sukladnosti 72
8.1.1 Vanjska provjera sukladnosti 72
8.1.2 Interna provjera sukladnosti 72
8.2 Identitet/kvalifikacije ocjenitelja 72
8.3 Odnos ocjenitelja s predmetom ocjenjivanja sukladnosti 73
8.4 Predmeti ocjenjivanja sukladnosti 73
8.5 Mjere u slučaju nesukladnosti 73
8.6 Priopćavanje rezultata 73
9 OSTALE POSLOVNE I PRAVNE ODREDBE 74
9.1 Naknade za usluge 74
9.1.1 Naknade za izdavanje ili obnovu certifikata 74
9.1.2 Naknade za pristup certifikatu 74
9.1.3 Naknade za opoziv i pristup informacijama o statusu certifikata 74
9.1.4 Naknade za ostale usluge 74
9.1.5 Povrat naknada 74
9.2 Financijska odgovornost 74
9.2.1 Pokrivenost osiguranjem 75
9.2.2 Druga sredstva 75
9.2.3 Osiguranje ili garancije krajnjim korisnicima 75
9.3 Povjerljivost poslovnih podataka 75
9.3.1 Opseg povjerljivih poslovnih podataka 75
9.3.2 Podaci koji se ne smatraju povjerljivim poslovnim podacima 75
9.3.3 Odgovornost za zaštitu povjerljivih poslovnih podataka 75
9.4 Zaštita osobnih podataka 75
9.4.1 Plan zaštite osobnih podataka 76

9.4.2 Povjerljivi osobni podaci....76
9.4.3 Osobni podaci koji nisu povjerljivi....76
9.4.4 Odgovornost za zaštitu osobnih podataka....76
9.4.5 Ovlaštenje za korištenje osobnih podataka....76
9.4.6 Dostupnost podataka mjerodavnim tijelima....77
9.4.7 Ostale okolnosti objave podataka....77
9.5 Prava intelektualnog vlasništva....77
9.6 Obveze i odgovornosti....77
9.6.1 Obveze i odgovornosti CA....77
9.6.2 Obveze i odgovornosti RA....79
9.6.3 Obveze i odgovornosti korisnika....79
9.6.4 Obveze i odgovornosti pouzdajuće strane....80
9.6.5 Obveze i odgovornosti ostalih sudionika....81
9.7 Odricanje od odgovornosti....81
9.8 Ograničenja odgovornosti....81
9.9 Naknada štete....82
9.10 Trajanje i prestanak važenja....82
9.10.1 Trajanje....82
9.10.2 Prestanak važenja....83
9.10.3 Posljedice prestanka važenja i nastavak djelovanja....83
9.11 Individualne obavijesti i komunikacija sa sudionicima....83
9.12 Izmjene i dopune....83
9.12.1 Procedure izmjena i dopuna....83
9.12.2 Mehanizmi obavještavanja i vremenski periodi....84
9.12.3 Okolnosti pod kojima se mora mijenjati OID....84
9.13 Postupak rješavanja sporova....84
9.14 Važeći propisi....84
9.15 Usklađenost s primjenjivim propisima....84
9.16 Razne odredbe....85
9.17 Ostale odredbe....85

AUTORSKA PRAVA

REFERENTNE DOKUMENTIRANE INFORMACIJE

Temeljni zakon

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

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

Podzakonski akti

[3] Pravilnik o pružanju i korištenju usluga povjerenja (NN 60/2019)

Ostali zakoni

[4] Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka)

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

Normizacijski dokumenti

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

[7] ETSI EN 319 401 V2.2.1. (2018-04) – Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

[8] ETSI EN 319 411-1 V1.2.2. (2018-04) – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements

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

[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 V1.3.1 (2019-02) – Electronic Signatures and Infrastructures (ESI); Cryptographic Suites

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

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

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

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

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

[18] IETF RFC 6962 – Certificate Transparency

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

Finini dokumenti

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

[21] Pravilnik o postupcima certificiranja za certifikate za autentikaciju mrežnih stranica, $CPS_{WSA\text{-}eIDAS}$

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

1 UVOD

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

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

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

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

Kao treća strana od povjerenja, Fina svoje usluge certificiranja pruža od 2003. godine. Usluge povjerenja koje pruža Fina usklađene su sa zakonskom regulativom [1] – [5] te s mjerodavnim međunarodnim normama iz djelokruga pružanja usluga povjerenja. Fina neprekidno prati potrebe korisnika, razvoj tehnologije i promjene u normama iz područja pružanja usluga povjerenja te sukladno tome unapređuje i usklađuje svoj PKI.

Certifikati za autentikaciju mrežnih stranica koje izdaje Fina izdaju se sukladno ovim Općim pravilima.

1.1 Pregled

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

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

Dvorazinsku arhitekturu produkcijskih certifikacijskih tijela Fine čine:

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

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

Opća pravila koja se odnose se na Fina Root CA i Fina PKI hijerarhiju zasnovanu na Fina Root CA opisana su u dokumentu Opća pravila pružanja usluga certificiranja i Pravilnik o postupcima certificiranja za Fina Root CA (CP/CPS_{ROOT}) [20].

Fina RDC 2015 i Fina RDC-TDU 2015 su CA-ovi koji izdaju certifikate za krajnje korisnike.

1.1.1 Opseg i namjena

Ova Opća pravila pružanja usluga certificiranja za certifikate za autentikaciju mrežnih stranica (engl. *Certificate Policy for Certificates for Website Authentication* – $CP_{WSA\text{-}eIDAS}$, u daljnjem tekstu: Opća pravila) sadrže temeljna pravila i skup načela pružanja usluga certificiranja kojim Fina kao pružatelj usluga povjerenja pruža usluge izdavanja (nekvalificiranih) certifikata za autentikaciju mrežnih stranica, poznatih pod nazivom TLS/SSL certifikati, a koji uključuju validirane podatke o identitetu organizacije *Subjekta* (u daljnjem tekstu: OVCP certifikat ili certifikat).

Opseg ovih Općih pravila 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.

Produkcijski certifikati iz opsega ovih Općih pravila sastavni su dio Registra digitalnih certifikata (Fina RDC).

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

Struktura ovog dokumenta temelji se na normizacijskom dokumentu IETF RFC 3647 [14].

1.1.2 Tipovi certifikata

Ovim Općim pravilima definirana su pravila certificiranja za certifikate za autentikaciju mrežnih stranica koje izdaje Fina RDC 2015 CA, 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).

Fina je sukladna s aktualnom verzijom dokumenta Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates objavljenog na mrežnim stranicama http://www.cabforum.org. Ako postoji bilo kakvo neslaganje između odredbi ovog dokumenta i odredbi dokumenta Baseline Requirements, prednost nad ovim dokumentom imaju odredbe dokumenta Baseline Requirements.

U Tablici 1.1. prikazan je tip certifikata za autentikaciju mrežnih stranica iz opsega ovih Općih pravila, njegov nazivi i pripadajući Finini, ETSI i CAB Forum OID općih pravila certificiranja (u daljnjem tekstu: CP OID).

Fina RDC 2015 certifikat 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

Tablica 1.1. Certifikat za autentikaciju mrežnih stranica

Ovim Općim pravilima definiran je certifikat za autentikaciju mrežnih stranica s nazivom SSL certifikat razine 2 (OVCP) (u daljnjem tekstu: certifikat):

- ***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. ovih Općih pravila. Ovaj tip certifikata sukladan je s „OVCP“ općim pravilima za certifikate iz norme ETSI EN 319 411-1 [8].

SSL certifikat razine 2 (OVCP) se u daljnjem tekstu naziva Korisnički certifikat.

Certifikat za autentikaciju mrežnih stranica Fina izdaje za poslužitelje povezane s pravnim osobama koje imaju sjedište u Republici Hrvatskoj.

1.2 Naziv dokumenta i identifikacijski podaci

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

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

- Naziv: Opća pravila pružanja usluga certificiranja za certifikate za autentikaciju mrežnih stranica
- Verzija: 1.6
- Datum stupanja na snagu: 25.09.2020.
- OID: 1.3.124.1104.5.0.5.1.1.6
- Internetska adresa na kojoj je dokument objavljen: https://rdc.fina.hr/RDC2015/FinaRDC2015-CPWSA1-6-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

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*
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 ne izdaje certifikate Korisnicima.

Fina Root CA certifikat dostupan je na internetskoj adresi navedenoj u točki 6.1.4. ovog dokumenta.

1.3.1.2 Fina RDC 2015 CA

Certifikacijsko tijelo u Fina PKI iz opsega ovih Općih pravila je Fina RDC 2015. Fina kao pružatelj usluga povjerenja preko tog CA obavlja usluge izdavanja certifikata za javnost te upravljanje životnim ciklusom tih certifikata sukladno ovim Općim pravilima.

Fina RDC 2015 CA po istim pravilima izdaje certifikate i za potrebe Fine.

Fina RDC 2015 CA se u izdanim certifikatima identificira kao izdavatelj (eng. *Issuer*) te ih potpisuje koristeći svoj privatni ključ

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

Polje	Atribut	Vrijednost
Issuer	commonName	Fina Root CA
	organizationName	Financijska agencija
	countryName	HR
Validity	notBefore	*Vrijeme izdavanja certifikata*
	notAfter	*Vrijeme izdavanja certifikata + 10 godina*
Subject	commonName	Fina RDC 2015
	organizationName	Financijska agencija
	countryName	HR
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 internetskoj adresi navedenoj u točki 6.1.4. ovog dokumenta.

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. Registraciju korisnika u Fina RA mreži provodi Fina LRA zajedno sa Središnjim RA Fine.

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

Poslovima registracije u Fina RA mreži koordinira Središnji RA Fine.

1.3.3 Korisnici

Korisnik 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 su u točki 9.6.3. ovih Općih pravila. Korisnici s Finom sklapaju ugovor o obavljanju usluga certificiranja.

1.3.3.1 Subjekti certificiranja

Subjekt certificiranja je web poslužitelj koji je identificiran nazivom domene ili IP adresom i koji je pod nadzorom i radom Korisnika.

1.3.4 Pouzdajuće strane

Pouzdajuće strane su fizičke osobe ili poslovni subjekti koji se oslanjaju na uslugu povjerenja. Certifikat omogućuje Pouzdajućoj strani provjeru identiteta Subjekta.

1.3.5 Ostali sudionici

Nema odredbi.

1.4 Uporaba certifikata

Na temelju namjene, dozvoljene uporabe te 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.

U Tablici 1.4. opisana je razina sigurnosti za certifikat te je prikazan pripadajući opis područja primjene i preporučeni financijski limit.

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

Tablica 1.4. Razina sigurnosti za certifikat

1.4.1 Primjerena uporaba certifikata

Certifikati navedeni u Tablici 1.1. ovih Općih pravila i pripadajući privatni ključevi upotrebljavaju se samo za autentikaciju mrežnih stranica.

1.4.2 Zabrane uporabe certifikata

Osim uporabe za autentikaciju mrežnih stranica, sve ostale uporabe certifikata navedenih u Tablici 1.1. te njihovih privatnih ključeva su zabranjene.

1.5 Administracija dokumenta

1.5.1 Organizacija odgovorna za održavanje dokumenta

Za izradu i održavanje ovog dokumenta Općih pravila ovlaštena je i odgovorna Fina.

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

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

1.5.2 Kontakt podaci

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

- Poštanska adresa:

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

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

1.5.3 Tijelo koje utvrđuje uskladivost CPS-a s Općim pravilima

Uskladivost $CPS_{WSA\text{-}eIDAS}$ [21] s ovim Općim pravilima utvrđuje Fina PMA.

1.5.4 Procedure odobravanja CPS-a

Procedura odobravanja $CPS_{WSA\text{-}eIDAS}$ [21] dokumenta opisana je u $CPS_{WSA\text{-}eIDAS}$ [21] dokumentu.

1.6 Definicije i kratice

1.6.1 Definicije

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

POJAM	ZNAČENJE
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.
CT log	Javni mrežni servis koji pruža zapis o svakom dostavljenom valjanom TLS certifikatu. Takav zapis je kriptografski provjerljiv i omogućeno je samo dodavanje zapisa.
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.
Internacionalizirani naziv domene	Naziv internetske domene čiji se barem jedan dio u softverskim aplikacijama, u cijelosti ili djelomično, prikazuje u posebnom jezičnom pismu ili alfabetu.

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.
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 CT log	CT log servis koji djeluje u skladu s pravilima Isporučitelja aplikacijskog softvera.
Kvalificirani ocjenitelj	Fizička ili pravna osoba koja zadovoljava zahtjeve navedene u dokumentu CA/Browser Forum BRG [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 je opozvao izdavatelj certifikata.

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	Trajni prestanak valjanosti certifikata prije isteka roka važenja navedenog u certifikatu.
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 validaciju	Podaci koji se koriste za validaciju elektroničkog potpisa ili elektroničkog pečata.
Podaci za verifikaciju potpisa	Podaci, poput kodova ili javnih kriptografskih ključeva koji se koriste u svrhu verificiranja potpisa.

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.
Precertifikat	Podatkovni objekt izrađen od certifikata koji će biti izdan, dodavanjem posebne kritične „*poison*“ ekstenzije u Korisnički TBSCertificat. Precertifikat koji je opisan u IETF RFC 6962 [18] se ne smatra „certifikatom“ na kojeg se primjenjuju zahtjevi iz IETF RFC 5280 [15].
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.

POJAM	ZNAČENJE
RA mreža	Cjelokupna mreža registracijskih tijela, a sastoji se od Fina RA mreže te od vanjskih ugovorenih RA s kojima Fina ima sklopljen ugovor o obavljanju poslova registracije.
Razlikovno ime 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 važenja i novim potpisom istog CA, a provodi se u definiranom periodu prije datuma isteka važenja certifikata.
Registracijski ured (RA)	Tijelo odgovorno za identifikaciju i autentikaciju subjekata certificiranja, kao i drugih osoba ili organizacija.
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.
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.
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

POJAM	ZNAČENJE
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*)
Transparentnost certifikata	Otvoreni okvir za praćenje i nadziranje certifikata za autentikaciju mrežnih stranica (*Certificate Transparency*).
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.
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*
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
$CPS_{WSA-eIDAS}$	*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
CT	*Certificate Transparency*	Transparentnost 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
IDN	*Internationalized Domain Name*	Internacionalizirani 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
PKI	*Public Key Infrastructure*	Infrastruktura javnog ključa
PMA	*Policy Management Authority*	Tijelo za upravljanje pravilima certificiranja
RA	*Registration Authority*	Registracijski ured
SCT	*Signed Certificate Timestamp*	Potpisani vremenski žig certifikata
TDU	Tijelo (ili tijela) državne uprave	Tijelo (ili tijela) državne uprave
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 mrežnim stranicama i dijela dostupnog preko javnog LDAP imenika.

Na mrežnim stranicama Fina PKI repozitorija objavljuju se:

- dokumenti općih pravila pružanja usluga certificiranja,
- pravilnik o postupcima certificiranja,
- uvjeti i izjave o pružanju usluga izdavanja certifikata (engl. *Terms and conditions* i *PKI disclosure statement*),
- cjenik usluga certificiranja,
- obrasci za korisnike,
- Fina Root CA certifikat i subordinirani Fina RDC 2015 CA,
- CRL Fina Root CA i CRL subordiniranog Fina RDC 2015 CA,
- certifikati namijenjeni za provjeru i testiranje,
- obavijesti korisnicima i Pouzdajućim stranama vezane uz pružanje usluga certificiranja,
- rezultati vanjske provjere sukladnosti,
- ostale informacije vezane uz rad Fina RDC 2015 CA.

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

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

U dijelu Fina PKI repozitorija dostupnog preko javnog LDAP imenika dostupni su certifikati subordiniranog Fina RDC 2015 CA te CRL-ovi koje izdaje Fina RDC 2015 CA. Adresa javnog LDAP imenika 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.

U Fina PKI repozitoriju ne objavljuju se povjerljivi podaci.

Fina objavljuje precertificat na CT log servise ako je osoba ovlaštena za zastupanje pravne osobe za ovu objavu dala suglasnost.

2.3 Vrijeme ili učestalost objavljivanja

Fina na godišnjoj razini održava i ažurira Opća pravila i Pravilnik o postupcima certificiranja [21] te ih odobrava, objavljuje i primjenjuje. Drugi Fina PKI dokumenti i ostale relevantne informacije objavljuju se po potrebi, nakon odobrenja.

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

Učestalost objave CRL za certifikate koje izdaje Fina RDC 2015 CA definirana je u točki 4.9.7. ovih Općih pravila.

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

2.4 Kontrole pristupa repozitoriju

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

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

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

3 IDENTIFIKACIJA I POTVRĐIVANJE IDENTITETA SUBJEKTA

3.1 Određivanje imena

3.1.1 Tipovi imena

U svaki certifikat upisuju se podaci o Subjektu certificiranja te podatak o mjestu sjedišta pravne osobe. Podaci o subjektu koji se upisuju u certifikat odnose se na autentični naziv Subjekta. Polje „*Subject*“ u certifikatu usklađeno je s dokumentom IETF RFC 5280 [15].

Polje *Subject* i ekstenzija *Subject Alternative Name* u certifikatima sadrže puni kvalificirani naziv poslužitelja (u daljnjem tekstu: FQDN) ili IP adresu poslužitelja.

3.1.2 Smislenost imena

Za atribute u polju *Subject* u Fina PKI primjenjuju se sljedeća pravila:

- puni registrirani naziv pravne osobe mora biti kako je naveden u službenim nadležnim nacionalnim registrima,
- mjesto sjedišta mora biti kako je navedeno u službenim nadležnim nacionalnim registrima,
- FQDN ili IP adresa mora biti kako je navedeno u zahtjevu za izdavanje certifikata.

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 u Fina PKI određeno je na sljedeći način:

- Serial Number

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

U OVCP certifikatima polje *Serial Number* sadrži 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, npr. VATHR-12345678901.1. Za pravne osobe registrirane u Republici Hrvatskoj jedinstveni identifikator pravne osobe je OIB.

- Common Name

U OVCP certifikatima ovaj atribut sadrži FQDN ili IP adresu poslužitelja.

U atributu *Common Name* upisuje se jedan FQDN ili IP adresa nad kojima podnositelj zahtjeva ima kontrolu ili isključivo pravo na korištenje.

FQDN ili IP adresa mora biti sadržana i u ekstenziji *Subject Alternative Name* OVCP certifikata.

- Organization Name

Atribut *organizationName* sadrži puni registrirani skraćeni naziv pravne osobe.

- Locality

Atribut *Locality Name* sadrži naziv mjesta u kojem je sjedište pravne osobe.

- Country

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

- Subject Alternative Name

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

Fina ne podržava uporabu internacionaliziranih naziva domena (IDN).

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

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

Ekstenzija *Subject Alternative Name* u polju *dNSName* ne sadrži znak za podvlaku (engl. Underscore, „_“).

3.1.5 Jedinstvenost imena

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

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 Fina 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

Putem Fina RA mreža Fina prikuplja osobne podatke fizičkih osoba i podatke pravne osobe isključivo za potrebe registracije u cilju izdavanja certifikata.

Provjeru podataka iz zahtijeva za izdavanje certifikata Fina preko Fina RA mreže provodi njihovom usporedbom s podacima iz dostavljene ili samostalno prikupljene dokumentacije iz mjerodavnog i nadležnog izvora sukladno važećim nacionalnim zakonima i propisima.

3.2.1 Metoda dokazivanja posjeda privatnog ključa

Privatni ključ koji odgovara javnom ključu koji se dostavlja Fina RDC 2015 CA za izradu OVCP certifikata generira Skrbnik ili ga generira Fina, sukladno točki 6.1.1.2. ovih Općih pravila.

U slučaju kad Fina generira par korisničkih ključeva tehnološkim procesima i metodama provjere osigurava se povezanost pravne osobe s privatnim ključem, koji odgovara javnom ključu za koji Fina izdaje certifikat, kao i kontrola Skrbnika nad privatnim ključem.

U slučaju kad Skrbnik generira par ključeva Fina tehnološkim procesom i metodom zahtijevanja certifikata obuhvaća provjeru posjeduje li, ili kontrolira li Skrbnik privatni ključ koji je povezan s javnim ključem koji se na zaštićeni način dostavlja Fina RDC 2015 CA za izradu certifikata.

3.2.2 Potvrda identiteta poslovnog subjekta i domene

3.2.2.1 Potvrda identiteta poslovnog subjekta

Provjera i potvrda identiteta pravne osobe provodi se provjerom:

- registriranog naziva pravne osobe,
- pravnog postojanja pravne osobe,
- upisa u nadležni registar,
- identifikatora iz nadležnog registra,
- OIB-a pravne osobe,
- adrese sjedišta pravne osobe.

Pravna osoba odgovara za točnost, potpunost i ispravnost dostavljenih podataka.

3.2.2.2 Provjera države povezane sa Subjektom

Fina obavlja provjeru je li država koja će u certifikatu biti navedena u polju *countryName* povezana sa Subjektom koji će biti naveden u certifikatu. Država navedena u atributu *countryName* unutar polja Subject je Republika Hrvatska

Ova provjera obavlja se sukladno metodama navedenim u dokumentu CA/Browser Forum BRG [19].

3.2.2.3 Provjera prava korištenja domene

Fina za svaki FQDN naveden u zahtjevu za izdavanje certifikata provjerava ima li pravna osoba koja podnosi zahtjev vlasništvo ili pravo korištenja naziva domene navedene u zahtjevu.

Ova provjera obavlja se sukladno metodama navedenim u dokumentu CA/Browser Forum BRG [19].

3.2.2.4 Provjera i potvrđivanje IP adrese

Fina za svaku IP adresu navedenu u zahtjevu za izdavanje certifikata obavlja provjeru ima li pravna osoba koja podnosi zahtjev pravo upravljanja i korištenja IP adrese u vrijeme izdavanja certifikata.

Ova provjera obavlja se sukladno metodama navedenim u dokumentu CA/Browser Forum BRG [19].

3.2.3 Potvrda identiteta fizičke osobe

Inicijalna identifikacija i potvrđivanje identiteta Skrbnika provodi se postupcima neposredne ili posredne identifikacije.

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

- ime i prezime,
- datum, mjesto i država rođenja,
- OIB (ako je OIB dodijeljen),
- podatke sadržane na identifikacijskoj ispravi iz točke 3.2.3.3. ovih Općih pravila,
- kontakt podatke.

Za izdavanje certifikata Fina prikuplja i dokaz o povezanosti Skrbnika s pravnom osobom.

3.2.3.1 Postupak neposredne identifikacije

Neposredna identifikacija fizičke osobe provodi se u njenoj fizičkoj prisutnosti temeljem važeće identifikacijske isprave iz točke 3.2.3.3. ovih Općih pravila.

3.2.3.2 Postupak posredne identifikacije

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

a) validacijom kvalificiranog ili naprednog elektroničkog potpisa zasnovanog na kvalificiranom certifikatu, ili
b) provjerom podataka iz preslika dviju različitih identifikacijskih isprava, definiranih u točki 3.2.3.3. ovih Općih pravila.

3.2.3.3 Prihvatljive vrste identifikacijskih isprava

Fizičke osobe u postupku neposredne identifikacije dokazuju svoj identitet valjanom osobnom iskaznicom, putovnicom ili vozačkom dozvolom.

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

3.2.4 Informacije o korisniku koje se ne provjeravaju

Svi podaci o pravnoj osobi, domeni i IP adresi koji se upisuju u Korisnički certifikat prethodno su provjereni od strane Fine. Korisnik izjavljuje da su svi podaci navedeni u zahtjevu za izdavanje certifikata točni i cjeloviti.

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., i usporedbom s podacima iz preslike važeće identifikacijske isprave osobe ovlaštene za zastupanje.

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

3.2.6 Kriteriji interoperabilnosti

Nema odredbi.

3.3 Identifikacija i potvrđivanje identiteta kod podnošenja zahtjeva za obnovu certifikata

Fina provodi postupke identifikacije i potvrde identiteta podnositelja zahtjeva za:

- redovnu obnovu certifikata,
- izdavanje certifikata nakon isteka,
- ponovno izdavanje certifikata nakon opoziva, i
- oporavak certifikata.

Prilikom obnove ili ponovnog izdavanja certifikata Skrbniku se komuniciraju aktualni uvjeti pružanja usluga certificiranja iz točke 9.17. ovog dokumenta te ih on prihvaća prije izdavanja certifikata.

3.3.1 Identifikacija i potvrđivanje identiteta kod redovne obnove certifikata

Redovna obnova certifikata obavlja se pred kraj životnog vijeka certifikata.

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

Postupak identifikacije i potvrđivanja identiteta Skrbnika provodi se sukladno odredbama točke 3.2.3. ovog dokumenta.

Postupak identifikacije i potvrđivanja identiteta pravne osobe obavlja se provjerom podataka iz dostavljenog zahtjeva s dostavljenim i prikupljenim podacima te upitom na nacionalni OIB sustav.

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

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

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

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

3.3.4 Identifikacija i potvrđivanje identiteta korisnika za oporavak certifikata

Oporavak certifikata provodi se iz razloga i uz uvjete navedene u točki 4.7.1. ovih Općih pravila.

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

3.4 Identifikacija i potvrđivanje identiteta kod zahtjeva za opoziv 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 opoziv certifikata ovisno o načinu dostave zahtjeva:

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

  Identifikacija i potvrđivanje identiteta provodi se neposrednom identifikacijom podnositelja zahtjeva temeljem njegove identifikacijske isprave 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 najmanje razinom naprednog elektroničkog potpisa ili pečatiranog najmanje razinom naprednog elektroničkog pečata.

- Podnošenje zahtjeva za opoziv telefonskim putem

  Identifikacija podnositelja zahtjeva provodi se predstavljanjem podnositelja svojim imenom i prezimenom te navođenjem naziva pravne osobe. Potvrđivanje identiteta podnositelja zahtjeva provodi se dokazivanjem njegovog poznavanja zaporke za opoziv certifikata.

Fina provodi identifikaciju i potvrđivanje identiteta podnositelja prijave problema vezanih uz korištenje certifikata na način kao i pri podnošenju zahtjeva za opoziv certifikata. Ukoliko to nije izvedivo, Fina identifikaciju i potvrđivanje identiteta provodi na druge odgovarajuće načine.

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 Postupak prijave korisnika s podnošenjem zahtjeva za izdavanje certifikata i odgovornosti

Za izdavanje certifikata obvezno je podnošenje zahtjeva za izdavanje certifikata.

Prije inicijalnog izdavanja certifikata Korisnik sklapa s Finom ugovor o obavljanju usluga certificiranja.

4.1.2.1 Proces podnošenja zahtjeva za izdavanje certifikata

Zahtjev za izdavanje certifikata podnosi Skrbnik.

Zahtjev za izdavanje certifikata potpisuju Skrbnik i osoba ovlaštena za zastupanje pravne osobe.

Ovlaštenje Skrbnika za podnošenje zahtjeva za izdavanje certifikata potvrđuje osoba ovlaštena za zastupanje svojim potpisom zahtjeva za izdavanje certifikata.

U slučaju predaje zahtjeva u elektroničkom obliku zahtjev se potpisuje kvalificiranim elektroničkim potpisom ili naprednim elektroničkim potpisom koji se temelji na kvalificiranom certifikatu kojeg je izdao kvalificirani pružatelj usluga povjerenja ili na certifikatu kojeg je izdao Fina CA.

4.1.2.2 Odgovornosti i obveze u procesu podnošenja zahtjeva za izdavanje certifikata

Korisnici s Finom sklapaju ugovor o obavljanju usluga certificiranja kojim prihvaćaju ova Opća pravila, $CPS_{WSA\text{-}eIDAS}$ [21] dokument i uvjete pružanja usluga certificiranja.

Prije početka pružanja usluga certificiranja 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 zahtjev za izdavanje certifikata, sukladno opisu iz točke 4.1.2.1. ovih Općih pravila, a dokumentacija koju prilažu ili dostavljaju treba biti točna i cjelovita te valjana u trenutku podnošenja zahtjeva.

Obaveze i odgovornosti Korisnika navedene su u Poglavlju 9.6.3. ovih Općih pravila.

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

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

4.2 Obrada zahtjeva za izdavanje certifikata

4.2.1 Obavljanje identifikacije i potvrđivanje identiteta

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

4.2.2 Odobravanje ili odbijanje zahtjeva za izdavanje certifikata

Službenik za registraciju u Fina RA mreži provjerava podatke iz dokumenata koje prilaže podnositelj zahtjeva i potvrđuje točnost i cjelovitost informacija vezanih uz fizičku i pravnu osobu iz zahtjeva za izdavanje certifikata ili odbija zahtjev u slučaju neuspješne identifikacije ili netočnosti dostavljenih informacija.

Službenik za validaciju u Središnjem Fina RA provodi postupak validacije dokumentacije koji se odnosi na provjeru vlasništva ili kontrole pravne osobe nad FQDN ili IP adresom koji su navedeni u zahtjevu za izdavanje certifikata.

Središnji RA Fine provodi i postupak provjere CAA zapisa za svaki *dNSName* u *subjectAltName* ekstenziji certifikata prije njegovog izdavanja sukladno postupku iz dokumenta RFC 6844 – DNS Certification Authority Authorization (CAA) Resource Record [16] i slijedi upute za obradu iz pronađenih zapisa. CAA identifikacijska domena Fina CA-ova je ‘fina.hr’.

Ukoliko Fina RA mreža odbije zahtjev za izdavanje certifikata, o odbijanju i razlozima odbijanja zahtjeva obavještava korisnika.

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.

4.3 Izdavanje certifikata

Fina RDC 2015 CA izdaje certifikat nakon, provedenih svih procesa provjere podataka, odobrenja zahtjeva za izdavanje certifikata 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.

4.3.1 Postupci CA tijekom izdavanja certifikata

Fina RDC 2015 CA tijekom procesa izdavanja certifikata:

- provjerava je li zahtjev za izdavanje certifikata odobren od strane Službenika za registraciju i Službenika za validaciju,
- par Korisničkih ključeva za certifikate generira se sukladno točki 6.1.1.2. ovih Općih pravila,
- ako je osoba ovlaštena za zastupanje pravne osobe dala suglasnost Fina RDC 2015 CA upisuje precertifikat u kvalificirane CT log servise te SCT-ove dobivene od tih log servisa dodaje u Korisnički certifikat koji će se izdati,
- izdaje zahtijevani certifikat za javni ključ Subjekta dostavljen sukladno točki 6.1.3. ovih Općih pravila,
- čini certifikat dostupnim Skrbniku u svrhu njegova preuzimanja,
- čini certifikat javno dostupnim na Fina PKI repozitoriju.

4.3.2 Obavještavanje korisnika od strane CA o izdavanju certifikata

Skrbnik preuzima certifikat *online* te je obaviješten o izdavanju certifikata u tijeku 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 sve informacije koje će biti sadržane u certifikatu točne u trenutku njegova prihvaćanja.

4.4.1 Provedba prihvaćanja certifikata

Skrbnik neposredno prije izdavanja certifikata provodi provjeru sadržaja certifikata.

Skrbnik prihvaća certifikat označavanjem prihvaćanja certifikata na ekranu CMS sučelja.

Nakon prihvaćanja certifikata Fina Skrbniku izdaje traženi certifikat.

Fina primjenjuje sigurnosne mjere kako bi osigurala da izdani certifikat sadrži iste informacije koje je Skrbnik prije izdavanja tog certifikata prihvatio.

Ukoliko Skrbnik ne prihvaća certifikat, razloge neprihvaćanja može javiti na usmeni ili pisani način. Neprihvaćanjem certifikata Skrbnik odustaje od zahtjeva za izdavanjem certifikata, a Fina 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 Korisničkog certifikata Fina RDC 2015 CA čini pripadajući precertifikat dostupnim na kvalificiranim CT log servisima te Korisnički certifikat čini dostupnim na Fina PKI repozitoriju.

Suglasnost za javnu objavu certifikata u Fina PKI repozitoriju daje se prilikom podnošenja zahtjeva za izdavanje certifikata.

4.4.3 Obavještavanje drugih strana od strane CA o izdavanju certifikata

Podrazumijeva se da su druge strane obaviještene o izdavanju certifikata njegovom javnom objavom u Fina PKI repozitoriju i objavom pripadajućeg precertifikata u kvalificiranim CT log servisima, sukladno točki 4.4.2. ovog dokumenta.

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. ovih Općih pravila,
- koristiti certifikat i pripadajući privatni ključ samo u svrhe propisane ovim Općim pravilima 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. ovih Općih pravila,
- koristiti i čuvati privatni ključ na način koji onemogućuje njegovo neovlašteno korištenje,
- koristiti certifikat i pripadajući privatni ključ samo na poslužiteljima dostupnim preko FQDN-a ili IP adrese navedenim u *Subject Alternative Name* ekstenziji certifikata,
- štititi privatni ključ od krađe, gubitka, izmjena, kompromitiranja i neovlaštene uporabe,
- na čuvanje aktivacijskih podatka privatnog ključa na zaštićenom mjestu odvojenom od privatnog ključa,
- na obavještavanje Fine kao pružatelja usluga povjerenja i zahtijevanje opoziva certifikata,
- nakon kompromitiranja privatnog ključa prestati s njegovom uporabom i uporabom pripadajućeg certifikata,
- nakon saznanja o opozivu certifikata ili saznanja o kompromitiranju Fina RDC 2015 CA osigurati da se pripadajući privatni ključ certifikata od tada više ne koristi.

4.5.2 Korištenje javnog ključa i certifikata od strane pouzdajuće strane

Pouzdajućoj strani koja namjerava ostvariti pouzdanje u certifikat izdan prema ovim Općim pravilima preporučuje se:

- voditi računa o primjerenoj uporabi i zabrani uporabe javnog ključa i certifikata,
- obaviti provjeru roka važenja svih certifikata u certifikacijskom lancu,

- obaviti provjeru statusa opozvanosti certifikata uporabom aktualnih informacija o statusu opozvanosti certifikata.

4.6 Obnova certifikata

Fina provodi obnovu certifikata na način da za postojećeg Korisnika čiji je certifikat pred istekom, generira novi par ključeva i izdaje novi certifikat.

Ukoliko se ključevi generiraju na lokaciji Korisnika Fina preporuča generiranje novog para ključeva. Fina prihvaća ponovnu dostavu postojećeg javnog ključa Korisničkog certifikata ako javni ključ zadovoljava zahtjeve iz točki 6.1.5. i 6.1.6.ovog dokumenta.

Postupak obnove certifikata opisan je u točki 4.7. ovih Općih pravila.

4.6.1 Razlozi za obnovu certifikata

Vidi točku 4.7.1.

4.6.2 Tko može tražiti obnovu certifikata

Vidi točku 4.7.2.

4.6.3 Obrada zahtjeva za obnovu certifikata

Vidi točku 4.7.3.

4.6.4 Obavještavanje korisnika o obnovi certifikata

Vidi točku 4.7.4.

4.6.5 Provedba prihvaćanja obnovljenog certifikata

Vidi točku 4.7.5.

4.6.6 Objava obnovljenog certifikata od strane CA

Vidi točku 4.7.6.

4.6.7 Obavještavanje drugih strana o obnovi certifikata

Vidi točku 4.7.7.

4.7 Obnova certifikata uz generiranje novog para ključeva

Fina provodi obnovu certifikata na način da za postojećeg Korisnika čiji je certifikat pred istekom, generira novi par ključeva i izdaje novi certifikat.

Ukoliko se ključevi generiraju na lokaciji Korisnika Fina preporuča generiranje novog para ključeva. Fina prihvaća ponovnu dostavu postojećeg javnog ključa Korisničkog certifikata ako javni ključ zadovoljava zahtjeve iz točki 6.1.5. i 6.1.6.ovog dokumenta.

Nakon provedene identifikacije i potvrde identiteta podnositelja zahtjeva za:

- redovnu obnovu certifikata,
- izdavanje certifikata nakon isteka,
- ponovno izdavanje certifikata nakon opoziva, i
- oporavak certifikata.

Fina izdaje certifikat čiji su parametri jednaki kao i parametri certifikata na koji se zahtjev odnosi, ali s novim serijskim brojem certifikata, novim vremenskim periodom važenja i novim potpisom Fina RDC 2015 CA.

4.7.1 Razlozi za obnovu certifikata uz generiranje novog para ključeva

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

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

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

4.7.2 Tko može zatražiti certificiranje novog javnog ključa

Zahtjev za obnovu, oporavak, odnosno izdavanje certifikata nakon isteka mogu podnijeti 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 podnosi se u papirnatom ili elektroničkom obliku, sukladno točki 4.1.2.1.ovog dokumenta te se identifikacija i potvrđivanje identiteta fizičkih osoba i pravne osobe iz zahtjeva provodi sukladno točki 3.3.1. ovih Općih pravila. Službenik za registraciju u

Fina RA mreži provjerava podatke iz zahtjeva i potvrđuje točnost i cjelovitost informacija u zahtjevu. Odobravanje ili odbijanje zahtjeva provodi Središnji Fina RA.

Nakon provjere autentičnosti i valjanosti zahtjeva Fina RDC 2015 CA izdaje certifikat sukladno točki 4.3.1. ovih Općih pravila.

4.7.4 Obavještavanje korisnika o obnovi certifikata uz generiranje novog para ključeva

Fina obavještava Skrbnika o skorom isteku certifikata te ga poziva na redovnu obnovu certifikata.

Obavještavanje Skrbnika o obnovi certifikata provodi se sukladno točki 4.3.2. ovih Općih pravila.

4.7.5 Provedba prihvaćanja obnovljenog certifikata s generiranim novim parom ključeva

Provedba prihvaćanja certifikata izdanog sukladno točki 4.7.1. provodi se sukladno točki 4.4.1. ovih Općih pravila.

4.7.6 Objavljivanje certifikata po obnovi s generiranjem novog para ključeva

Objavljivanje certifikata izdanog sukladno točki 4.7.1. provodi se sukladno točki 4.4.2. ovih Općih pravila.

4.7.7 Obavještavanje drugih strana o obnovi certifikata s generiranim parom ključeva

Obavještavanje drugih strana o certifikatu izdanog sukladno točki 4.7.1. provodi se sukladno točki 4.4.3. ovih Općih pravila.

4.8 Izmjene u certifikatu

Pravne osobe imaju obvezu informiranja Fine o promjeni podataka koji ulaze u sadržaj certifikata 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 u certifikatu

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 u certifikatu

Zahtjev za izmjene u certifikatu može zatražiti Skrbnik ili osoba ovlaštena za zastupanje pravne osobe.

4.8.3 Obrada zahtjeva za izmjenama u certifikatu

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. ovih Općih pravila. Obrada zahtjeva i izdavanje certifikata provodi se sukladno točki 4.2., 4.3. i 4.4. ovih Općih pravila.

4.8.4 Obavještavanje korisnika o izdavanju izmijenjenog certifikata

Pri izdavanju certifikata u procesu izmjene certifikata obavještavanje korisnika provodi se sukladno točki 4.3.2. ovih Općih pravila.

4.8.5 Provedba prihvaćanja izmijenjenog certifikata

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

4.8.6 Objavljivanje izmijenjenog certifikata od strane CA

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

4.8.7 Obavještavanje drugih strana o izdavanju izmijenjenog certifikata

Obavještavanje drugih strana o izdavanju izmijenjenog certifikata provodi se na način opisan u točki 4.4.3. Općih pravila.

4.9 Opoziv i suspenzija certifikata

U sljedećim točkama opisana su pravila vezana uz opoziv Korisničkog certifikata.

Pravila vezana uz opoziv Fina RDC 2015 CA certifikata opisana su u točki 4.9. CP/CPS_{ROOT} [20] dokumenta.

4.9.1 Razlozi za opoziv

Fina RDC 2015 CA opoziva SSL certifikat razine 2 (OVCP) u roku od najdulje 24 sata:

- temeljem 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 odobren od strane Korisnika te da Korisnik retroaktivno nije dao takvo odobrenje,
- ako Fina zaprimi dokaz da je privatni ključ povezan s javnim ključem u certifikatu Korisnika kompromitiran ili ako privatni ključ ili aktivacijski podaci nisu više u jedinstvenom posjedu Skrbnika, odnosno pravne osobe,
- u slučaju da Skrbnik ili osoba ovlaštene za zastupanje prijave gubitak ili trajnu nedostupnost privatnog ključa povezanog s certifikatom,
- ako Fina zaprimi dokaz da se ne bi trebalo pouzdati u provjeru prava korištenja domene ili upravljanja bilo kojim FQDN-om ili IP adresom naznačene u certifikatu.

Fina RDC 2015 CA opoziva certifikat u planiranom roku od 24 sata, ali ne dulje od 5 dana od zaprimanja zahtjeva:

- ako certifikat više ne ispunjava zahtjeve za tip kriptografskog algoritma i pripadajuću duljinu ključa te ne zadovoljava zahtjeve za generiranje i provjeru kvalitete parametara javnog ključa propisane u ovom dokumentu i dokumentu CA/Browser Forum BRG [19],
- u slučaju da Fina zaprimi dokaz o zlouporabi certifikata ili zaprimi službenu obavijesti nadležnog tijela o korištenju certifikata u nezakonite svrhe,
- u slučaju da je Fina upoznata o Korisnikovom nepridržavanju preuzetih obveza i odgovornosti određenih ugovorom, Fininim uvjetima o pružanju usluga certificiranja, ovim Općim pravilima ili $CPS_{WSA\text{-}eIDAS}$ [21] dokumentom,
- u slučaju da je Fina upoznata s bilo kojom okolnošću koja ukazuju da korištenje FQDN-a ili IP adrese naznačene u certifikatu više nije zakonski dozvoljeno,
- ako Fina ima saznanja da certifikat nije izdan sukladno dokumentu CA/Browser Forum BRG [19], ovim Općim pravilima ili $CPS_{WSA\text{-}eIDAS}$ [21] dokumentu,
- u slučaju da Fina raspolaže saznanjima da informacije sadržane u certifikatu nisu točne ili da navode na pogrešne zaključke,
- u slučaju da certifikat više nije sukladan s općim pravilima prema kojima je bio izdan,
- u slučaju da opoziv nalaže ovaj dokument,
- u slučaju da je Fina upoznata s demonstriranom ili dokazanom metodom koja korisnički privatni ključ izlaže kompromitiranju, da je upoznata s razvijenom metodom kojom se na jednostavan način može iz javnog ključa izračunati privatni ključ, ili je upoznata s jasnim dokazom da je metoda koja se koristi za generiranje korisničkog privatnog ključa probijena,
- u slučaju da Fina prestaje s pružanjem usluga izdavanja 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 osigura nastavak pružanja usluge davanja informacije o statusu opozvanosti certifikata putem CRL ili OCSP servisa,
- ako Fina procjeni da certifikat svojim tehničkim karakteristikama, profilom ili sadržajem ne pruža prikladnu razinu povjerenja proizvođačima aplikacijskog softvera ili Pouzdajućim stranama,
- u slučaju da Korisnik otkaže ugovor o obavljanju usluge certificiranja,

- u slučajevima kada to nalaže zakon ili drugi propis.

Razlozi za opoziv Fina RDC 2015 CA certifikata dani su u točki 4.9.1. CP/CPS_{ROOT} [20] 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.

U točki 4.9.1. CP/CPS_{ROOT} [20] dokumenta navedeno je tko može tražiti opoziv Fina RDC 2015 CA certifikata.

4.9.3 Procedura za zahtjev za opozivom

Pisani zahtjev za opoziv certifikata dostavlja se 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.

Zahtjev za opoziv certifikata može se podnijeti i telefonskim putem pozivom Fini na telefonski broj koji je objavljen na mrežnim stranicama repozitorija iz točke 2.2. ovih Općih pravila. Ovaj Finin telefonski broj dostupan je od 0 do 24 sata, 7 dana u tjednu.

Fina na osnovu točnog i cjelovito ispunjenog i potpisanog zahtjeva za opoziv, odnosno provjerom poznavanja zaporke za opoziv certifikata kojom se potvrđuje identitet podnositelja zahtjeva u slučaju podnošenja zahtjeva putem telefona, opoziva certifikat i o tome obavještava Skrbnika te, ukoliko je to primjenjivo, pravnu osobu s kojom je Skrbnik povezan.

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

Prijava problema vezanih uz korištenje certifikata podnosi se inicijalno telefonskim putem pozivom Fini na telefonski broj koji je objavljen na mrežnim stranicama repozitorija iz točke 2.2.1. ovog dokumenta. Ovaj Finin telefonski broj dostupan je od 0 do 24 sata, 7 dana u tjednu. Po potrebi, nakon obavljene telefonske prijave dodatne potrebne informacije mogu se dostaviti e-mailom na adresu objavljenu na mrežnim stranicama repozitorija iz točke 2.2.1. ovog dokumenta

Nakon preispitivanja činjenica i okolnosti Fina će donijeti odluku vezanu uz opoziv certifikata.

Procedura za zahtjev za opozivom Fina RDC 2015 CA certifikata opisana je u točki 4.9.3. CP/CPS_{ROOT} [20] dokumenta.

4.9.4 Poček zahtjeva za opozivom

Podnositelji zahtjeva za opoziv certifikata iz točke 4.9.2. ovih Općih pravila trebaju u najkraćem razumnom roku od nastanka razloga za opoziv navedenih u točki 4.9.1. podnijeti zahtjev za opoziv certifikata.

4.9.5 Vremenski period u kojem CA mora obraditi zahtjev za opozivom

Fina obradu opoziva obavlja neposredno nakon zaprimanja zahtjeva za opoziv.

Fina u najkraćem razumnom roku, a najkasnije u roku koji ovisi o razlogu za opoziv, a koji je naveden u točki 4.9.1. ovog dokumenta i koji je umanjen za 60 minuta donosi odluku o opozivu certifikata. Vremenski period od donošenja odluke za provedu opoziva certifikata do trenutka kada je informacija opozvanosti certifikata preko nove CRL ili odgovora OCSP servisa dostupna svim pouzdajućim stranama iznosi najviše 60 minuta.

U slučaju obrade prijave problema vezanih uz korištenje certifikata istraživanje činjenice i okolnosti koje se odnose na prijavu obavlja se u roku od najviše 24 sata, a vremenski period od zaprimanja prijave do trenutka kada je informacija opozvanosti certifikata preko nove CRL ili odgovora OCSP servisa dostupna svim pouzdajućim stranama ne smije prijeći pripadajući rok naveden u točki 4.9.1. ovog dokumenta.

4.9.6 Zahtjevi pouzdajućim stranama za provjeru opoziva

Pouzdanje u opozvan certifikat može imati osobnu ili poslovnu štetu za Pouzdajuću stranu. Zbog toga, prije ostvarenja pouzdavanja u certifikat, Pouzdajuća strana bi trebala provesti provjeru statusa certifikata u cilju utvrđivanja njegove opozvanosti, a sukladno točkama 4.5.2., 4.9.9. i 4.9.10. ovih Općih pravila. Ako Pouzdajućoj strani u danom trenutku nije moguće dobiti informacije o statusu certifikata, ona se ne bi trebala 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 6 sati od prethodnog izdavanja CRL. CRL liste koje izdaje Fina RDC 2015 CA sadrže informacije o statusima opozvanosti certifikata minimalno do njihova isteka perioda važenja.

4.9.8 Maksimalno kašnjenje za CRL

Maksimalno kašnjenje CRL od trenutka njenog izdavanja do trenutka objave u redovitim uvjetima iznosi manje od 30 sekundi.

4.9.9 *Raspoloživost online* provjere statusa opozvanosti certifikata

Fina RDC 2015 CA podržava *online* provjeru statusa opozvanosti izdanih certifikata putem Fina OCSP servisa čiji je rad usklađen s dokumentom 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. ovih Općih pravila. Podaci o pristupnim točkama za dohvat CRL sadržani su u svakom izdanom certifikatu.

4.9.10 Zahtjevi na online provjeru statusa opozvanosti certifikata

Pouzdajuća strana treba imati aplikacijsko rješenje koje može koristiti OCSP servis iz točke 4.10.1. ovih Općih pravila.

4.9.11 Ostali načini objave statusa opozvanosti certifikata

Nema odredbi.

4.9.12 Posebni zahtjevi vezani uz kompromitiranje privatnog ključa

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 izdaje 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.

4.10.2 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.

Vrijeme odziva na zahtjev za dohvat CRL ili dobivanje OCSP odgovora u normalnim radnim uvjetima je manje od 10 sekundi.

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 nije dozvoljeno.

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 izdavanja certifikata primjenjuje mjere fizičke zaštite sustava certificiranja s ciljem minimiziranja rizika vezanih uz fizički zaštitu i u skladu s poslovnom politikom Fine i važećom zakonskom regulativom.

5.1.1 Lokacija objekta i konstrukcija

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

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

Sigurni prostori u kojima se nalaze komponente Fininog 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 podprostorima unutar tog prostora ostvaruje se uz dualnu kontrolu prolaza ovlaštenih osoba Fina PKI, a u skladu s njihovim ulogama i ovlastima.

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

O svakom pristupu sustavima certificiranja vodi se evidencija.

Oprema, informacije, mediji i softver iz Fina PKI štićenog prostora iznosi se isključivo uz minimalno dualnu kontrolu ovlaštenih osoba u Fina PKI kojima su dodijeljene odgovarajuće povjerljive uloge, i uz prethodno ovlaštenje.

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

5.1.3 Sustavi za napajanje i klimatizaciju

Uređaji i prostor u kojem se nalazi 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.

5.1.4 Opasnost od poplave

Lokacija na kojem se nalaze Fina RDC 2015 CA, Fina RA sustav i repozitorij zaštićena je od poplave.

5.1.5 Protupožarna zaštita

Fina RDC 2015 CA, Fina RA sustav i repozitorij zaštićeni su sustavom za detekciju požara i sustavom za automatski gašenje požara sukladno važećoj zakonskoj regulativi.

5.1.6 Pohrana medija

Mediji na kojima se nalaze arhivske i sigurnosne kopije Fina PKI podataka u elektroničkom obliku, kopije sadržaja repozitorija te sigurnosne kopije programske opreme pohranjuju se na dvije odvojene štićene lokacije s uspostavljenom protupožarnom zaštitom i koje su osigurane od poplave. Ovi mediji zaštićeni su od oštećenja, krađe i neovlaštenog pristupa.

5.1.7 Zbrinjavanje otpada

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

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

5.1.8 Sigurnosne kopije na drugoj lokaciji

Sigurnosne kopije Fina RDC 2015 CA i RA sustava, arhivske ili sigurnosne kopije podataka, kopije sadržaja repozitorija te sigurnosne kopije programske opreme pohranjuju se na lokaciji sekundarnog sustava certificiranja koji je izdvojen od primarnog produkcijskog sustava

certificiranja. Ove su sigurnosne kopije u odnosu na njihove originale zaštićene jednakom ili višom razinom mjera fizičke zaštite.

5.2 Organizacijske mjere zaštite

5.2.1 Povjerljive uloge

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

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

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

5.2.2 Broj osoba potrebnih za obavljanje zadataka

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

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

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

5.2.3 Identifikacija i potvrđivanje identiteta za svaku ulogu

Prilikom prijave na kritične aplikacije i servise unutar Fina PKI provodi se identifikacija i potvrda identiteta osobe koja pristupa aplikaciji ili servisu. Identifikacija i potvrda identiteta osobe provodi se odgovarajućom metodom autentikacije. Pristup i korištenje aplikacija i servisa unutar Fina PKI omogućen je samo ovlaštenim osobama sukladno povjerljivoj ulozi koju obnaša Tijekom korištenja kritičnih aplikacija i servisa aktivnosti prijavljene osobe propisno se bilježe, spremaju i čuvaju.

5.2.4 Uloge koje zahtijevaju odvajanje dužnosti

Zbog sigurnosnih zahtjeva izdavanja certifikata provodi se odvajanje sljedećih dužnosti:

- osobi kojoj je dodijeljena povjerljiva uloga Službenik za sigurnost, Službenik za registraciju, Službenik za validaciju ili Službenik za opoziv certifikata ne dodjeljuje se povjerljiva uloga Službenik za nadzor sustava,
- osobi kojoj je dodijeljena povjerljiva uloga Administrator sustava ne dodjeljuje se povjerljiva uloga Službenik za sigurnost ili Službenik za nadzor sustava.

5.3 Osoblje

5.3.1 Kvalifikacije, radno iskustvo i zahtjevi za provjerom osoblja

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

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

5.3.2 Procedure provjere primjerenosti osoblja

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

5.3.3 Zahtjevi za školovanjem

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

5.3.4 Periodičko obavljanje znanja i osvješćivanje

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

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

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

5.3.5 Učestalost i slijed izmjene zaposlenika

Nema odredbi.

5.3.6 Kazne za neovlaštene radnje

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

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

5.3.7 Zahtjevi na vanjske suradnike

Fina nema ugovorene vanjske suradnike za obavljanje dijela usluga iz opsega ovog dokumenta.

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

5.3.8 Dokumentacija koja je dostupna osoblju

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

5.4 Postupci upravljanja revizijskim zapisima

5.4.1 Tipovi događaja koji se zapisuju

U Fina PKI zapisuju se revizijski zapisi o svim događajima vezanim uz:

- upravljanje životnim ciklusom CA ključeva Fina RDC 2015 CA,
- registraciju fizičke osobe, pravne osobe i poslužitelja,
- životni ciklus ključeva i upravljanje ključevima koje generira Fina RDC 2015 CA,
- životni ciklus certifikata koje izdaje Fina RDC 2015 CA,
- zahtjeve za opoziv certifikata te pripadajuće provedene radnje.

U revizijskim zapisima zapisuju se i sigurnosni događaji u Fina PKI vezani uz promjene sigurnosnih politika, fizičku i tehničku zaštitu Fina PKI prostora, pokretanje i zaustavljanje rada sustava, sistemske greške i kvarove hardvera, aktivnosti vatrozida i usmjerivača te pokušaja pristupa sustavu.

5.4.2 Učestalost obrade revizijskih zapisa

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

5.4.3 Vremenski period pohrane revizijskih zapisa

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

5.4.4 Zaštita revizijskih zapisa

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

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

5.4.5 Postupci izrade sigurnosnih kopija revizijskih zapisa

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

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

5.4.6 Sustav prikupljanja revizijskih zapisa (unutarnji ili vanjski)

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

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

5.4.7 Obavještavanje subjekta uzročnika događaja

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

5.4.8 Procjena ranjivosti

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

Procjena rizika informacijske imovine provodi se jednom godišnje. Procjena ranjivosti sustava za prepoznate javne i privatne adrese Fina PKI provodi se kvartalno. Penetracijski test provodi se jednom godišnje.

Svaku novu kritičnu ranjivost Fina će od njezina saznanja razmotriti u roku od 48 sati te će postupiti sukladno utvrđenim postupcima.

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:

- dokumenti Fina PKI općih pravila i pravilnika o postupcima certificiranja,
- uvjeti pružanja usluga certificiranja,
- ugovori povezani s pružanjem usluga certificiranja,
- podaci i dokumentacija prikupljena postupkom registracije,
- certifikati i podaci vezani uz životni ciklus pojedinog certifikata,
- podaci i dokumentacija vezana uz promjenu statusa certifikata,
- revizijski zapisi iz točke 5.4.1. ovih Općih pravila,
- drugi Finini interni dokumenti.

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

5.5.2 Vremenski period arhiviranja

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

5.5.3 Zaštita arhive

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

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

5.5.4 Postupci izrade sigurnosnih kopija arhive

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

5.5.5 Zahtjevi na zaštitu zapisa vremenskim žigom

Nema odredbi.

5.5.6 Sustav prikupljanja arhiva (unutarnji ili vanjski)

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

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

5.5.7 Postupci dobivanja i provjere arhiviranih zapisa

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

Verifikacija podataka iz arhive obavlja se provjerom njihove cjelovitosti.

5.6 Promjena CA ključa

Fina osigurava da Fina RDC 2015 CA kontinuirano pruža uslugu povjerenja sa svojim validnim parom ključeva i pripadajućim CA certifikatom. Iz tog razloga Fina RDC 2015 CA će dovoljno vremena prije isteka CA certifikata, generirati novi par CA ključeva. 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. U oba slučaja za novi javni CA ključ Finin Root CA izdati će CA certifikat.

Fina RDC 2015 CA će o promjeni svojeg javnog ključa i o svojem novom CA certifikatu pravodobno obavijestiti sudionike Fina PKI.

Novi pripadajući javni ključ biti će dostupan sudionicima Fina PKI na način na koji je to bio i prethodni Fina RDC 2015 CA javni ključ, a sukladno opisu u točki 2.2 ovih Općih pravila.

5.7 Oporavak od kompromitiranja ili nepogode

5.7.1 Postupci u slučaju incidenta ili kompromitiranja

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

Plan kontinuiteta poslovanja revidira se jednom godišnje.

5.7.2 Postupci u slučaju oštećenja u računalnim resursima, programima i/ili podacima

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

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

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

5.7.3 Postupci u slučaju kompromitiranja privatnog ključa

U slučaju kompromitiranja ili sumnje u kompromitiranost privatnog ključa Fina RDC 2015 CA će odmah prekinuti s uporabom tog kompromitiranog privatnog ključa.

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

O opozivu 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 primjenljivo, poduzeti mjere za sprječavanje ponavljanja takvog događaja. Fina CA čiji je certifikat opozvan generirati će novi par CA ključeva. Fina Root CA će za novi javni CA ključ izdati novi CA certifikat.

Novi CA će uporabom novog privatnog CA ključa izdati certifikate postojećim registriranim subjektima te će sve naredne informacije o opozvanosti certifikata potpisivati uporabom novog ključa. Novi CA certifikat biti će dostupan sudionicima Fina PKI na način na koji je bio dostupan i prethodni CA certifikat, a sukladno opisu u točki 2.2 ovih Općih pravila.

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

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

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

5.7.4 Mogućnost nastavka poslovanja nakon nepogode

U planu kontinuiteta poslovanja 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 iz točke 5.1.1. ovih Općih pravila do oporavka svojeg primarnog produkcijskog sustava.

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,
- 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. ovih Opći pravila kako bi ti zapisi bili raspoloživi za pružanje dokaza u sudskim, upravnim i drugim postupcima u skladu s važećim odredbama zakonske regulative, ili će Fina s drugim poslovnim subjektom ugovoriti takvo arhiviranje, zaštitu i čuvanje zapisa.

6 TEHNIČKE MJERE ZAŠTITE

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

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.

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 [8] i sa zahtjevima dokumenta CA/Browser Forum BRG [19].

Par ključeva za Fina RDC 2015 CA generira se, uz minimalno dualnu kontrolu ovlaštenih osoba s povjerljivim ulogama u Fina PKI, u HSM modulima koji zadovoljavaju zahtjeve iz točke 6.2.1. ovih Općih pravila.

Fina RDC 2015 CA nalazi se tijekom i nakon ceremonije generiranja parova ključeva u Fina PKI štićenom prostoru iz točke 5.1.1. ovih Općih pravila, a pristup Fina 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 ocjenitelja koje 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 para ključeva za *SSL certifikat razine 2 (OVCP)* može provoditi Fina ili 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 [8] 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. ovih Općih pravila.

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. ovih Općih pravila.

6.1.2 Dostava privatnog ključa korisniku

Ako Fina generira privatni ključ, Fina osigurava sigurnu *online* dostavu privatnog ključa i pripadajućeg certifikata u softverskom zaštićenom tokenu Skrbniku te nakon dostave uništava korisnički privatni ključ.

U slučaju da Fina ima saznanja da je privatni ključ certifikata Korisnika 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, smatra se Korisnik već posjeduje privatni ključ.

6.1.3 Dostava javnog ključa CA-u

Korisnički javni ključ dostavlja se na certificiranje u Fina RDC 2015 CA na način koji osigurava provjeru cjelovitosti i izvornosti javnog ključa te na način koji sigurno povezuje potvrđeni identitet Subjekta i pripadajući javni ključ koji se dostavlja.

Ako par korisničkih ključeva generira Fina, dostava javnog ključa u Fina RDC 2015 CA obavlja se sigurnim internim elektroničkim komunikacijskim kanalom.

Ako par korisničkih ključeva generira Skrbnik proces zahtijevanja certifikata obuhvaća autentikaciju Subjekta i provjeru posjeduje li ili kontrolira li Skrbnik privatni ključ koji je povezan s javnim ključem koji se dostavlja za izradu certifikata.

6.1.4 Dostava javnog ključa CA pouzdajućim stranama

Javni ključ Fina RDC 2015 CA dostupan je Pouzdajućim stranama u Fina RDC 2015 CA certifikatu koje je izdao Fina Root CA.

Internetske adrese za izravno preuzimanje Fina Root CA i Fina RDC 2015 CA certifikata su:

- Fina Root CA: https://rdc.fina.hr/Root/FinaRootCA.cer
- Fina RDC 2015 CA: https://rdc.fina.hr/RDC2015/FinaRDCCA2015.cer

6.1.5 Duljine ključeva

Duljine ključeva u Fina PKI su sljedeće:

- Fina Root CA upotrebljava sha256WithRSA algoritam s ključem duljine 4096 bita,
- Subordinirani Fina 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, a sukladno točki 6.2.1. ovih Općih pravila te strogim pridržavanjem zahtjeva navedenih u dokumentaciji kriptografskih modula.

Ako Skrbnik generira par ključeva sukladno točki 6.1.1.2. ovih Općih pravila, generiranje ključeva se provodi korištenjem parametara za generiranje koji su sukladni s normizacijskim dokumentom ETSI TS 119 312 [12] i dokumentom CA/Browser Forum BRG [19]. Fina sukladno tim dokumentima provjerava kvalitetu parametara javnog ključa koje je generirao Skrbnik.

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

Fina RDC 2015 CA certifikat u ekstenziji *KeyUsage* ima postavljene vrijednosti *keyCertSign, 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 Finin servis izdavanja kvalificiranih vremenskih žigova,
- potpisivanje pripadajuće CRL.

SSL certifikat razine 2 (OVCP) u ekstenziji *Key Usage* ima postavljene vrijednosti *digitalSignature i keyEncipherment*. Pripadajući privatni ključ koristi se samo za autentikaciju mrežnih stranica.

6.2 Zaštita privatnog ključa i tehnike upravljanja kriptografskim modulom

6.2.1 Norme i tehničke mjere zaštite kriptografskog modula

Privatni ključ za Fina RDC 2015 CA generira se i štiti HSM modulom koji zadovoljava zahtjeve prema FIPS 140-2 [13] 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.

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

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

HSM modul kojim se štite privatni ključ Fina RDC 2015 CA smješten je u prostoru najviše razine sigurnosti unutar Fina PKI štićenog prostora. Fizički pristup ovim HSM modulima provodi se uz dualnu kontrolu ovlaštenih osoba s povjerljivim ulogama u Fina PKI.

Upravljanje privatnim ključem Fina RDC 2015 CA provodi se fizičkim pristupom HSM modulu, uz autorizaciju dvije ovlaštene osobe s povjerljivim ulogama u Fina PKI.

6.2.3 Sigurno skladištenje privatnog ključa (*key escrow*)

Sigurno skladištenje privatnog ključa Fina RDC 2015 CA se ne primjenjuje.

Sigurno skladištenje privatnih korisničkih ključeva povezanih s OVCP certifikatima se ne primjenjuje.

6.2.4 Sigurnosno kopiranje privatnog ključa

Sigurnosno kopiranje privatnog ključa Fina RDC 2015 CA provodi se u prostoru najviše razine sigurnosti unutar Fina PKI štićenog prostora pod dualnom kontrolom ovlaštenih osoba s povjerljivim ulogama u Fina PKI. Privatni ključ Fina RDC 2015 CA kopira se i dohvaća iz kriptografskog modula isključivo u enkriptiranom obliku i čuva u sigurnim prostorima najviše razine sigurnosti unutar Fina PKI štićenih prostora na odvojenim lokacijama.

Fizički pristup sigurnosnim kopijama privatnih ključeva 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.

6.2.5 Arhiviranje privatnog ključa

Fina ne arhivira privatne ključeve Fina PKI i ne arhivira korisničke privatne ključeve.

6.2.6 Prijenos privatnog ključa

Ako se privatni ključ Fina RDC 2015 CA prenosi iz ili u HSM modul, za vrijeme dok je izvan HSM modula privatni ključ je zaštićen enkriptiranjem na način koji osigurava jednaku razinu sigurnosti kao i kad se ključ nalazi u HSM modulu. Prijenos privatnog ključa provode samo ovlaštene osobe s povjerljivim ulogama u Fina PKI, uz dualnu kontrolu. Privatni ključ Fina RDC 2015 CA prenosi se iz HSM modula isključivo u svrhe izrade sigurnosne kopije.

Kod prijenosa privatnog ključa iz jednog HSM modula u drugi HSM modul privatni ključ se prenosi samo u HSM modul jednake ili više razine sigurnosti u odnosu na HSM modul iz kojega se privatni ključ prenosi.

Prijenos privatnih ključeva za *SSL certifikat razine 2 (OVCP)* u drugi sigurnosni spremnik privatnog ključa provodi Skrbnik na način da se privatni ključ prenosi samo u sigurnosni spremnik privatnog ključa jednake ili više razine sigurnosti u odnosu na sigurnosni spremnik iz kojega se privatni ključ prenosi.

Privatni ključ se prije prijenosa enkriptira kako bi tijekom prijenosa bio adekvatno zaštićen.

6.2.7 Spremanje privatnog ključa u kriptografskom modulu

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

Nema ograničenja obzirom na format u kojem je privatni ključ spremljen u HSM modulu.

6.2.8 Metoda aktivacije privatnog ključa

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

Aktivaciju privatnog ključa certifikata provodi samo pripadajući Skrbnik korištenjem odgovarajućih aktivacijskih podataka. Aktivacija privatnog ključa obavlja se na siguran način.

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.

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

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 važenja privatnog ključa, zbog kompromitiranja ili sumnje u kompromitiranost privatnog ključa, ili zbog prestanka njegova korištenja, a izvodi se od strane ovlaštenih osoba s povjerljivim ulogama u Fina PKI uz minimalno dualnu kontrolu. Postupak uništavanja privatnog Fina RDC 2015 CA ključa uključuje i uništavanje svih sigurnosnih kopija tog privatnog ključa.

Uništavanje privatnog Fina RDC 2015 CA ključa provodi se način određen internim Fininim dokumentima, a koji osigurava da se nakon uništenja privatni ključ ni na koji način ne može oporaviti ili ponovno koristiti.

O uništenju privatnog Fina RDC 2015 CA ključa vodi se zapisnik.

Preporuka je da Korisnik uništi svaki privatni ključ *SSL certifikata razine 2 (OVCP)* koji je trajno stavljen izvan uporabe.

Uništenje privatnih ključeva certifikata odgovornost je Korisnika.

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. ovih Općih pravila.

6.3 Ostali vidovi upravljanja parom ključeva

6.3.1 Arhiviranje javnog ključa

Javni ključ Fina RDC 2015 CA sastavni je dio pripadajućeg CA certifikata koji se arhivira sukladno točkama 5.5.3. i 5.5.4. ovih Općih pravila, a u arhivi se čuva na rok iz točke 5.5.2. ovih Općih pravila.

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

6.3.2 Vremenski period važenja certifikata i korištenja para ključeva

Predviđeni 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)	1 godina

Tablica 6.1. Rokovi uporabe certifikata

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

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

Aktivacijske podatke za privatne ključeve Korisnika generira Skrbnik. Korisnik je odgovoran za sigurnost i zadovoljenje propisane kvalitete aktivacijskih podataka.

6.4.2 Zaštita aktivacijskih podataka

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

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

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.

Ova Opća pravila ne postavljaju dodatne zahtjeve na životni ciklus aktivacijskih podataka za privatne ključeve Korisničkih certifikata.

Dodatna pravila o uvjetima i životnom ciklusu aktivacijskih podataka za privatne ključeve Korisničkih certifikata mogu biti određena u ugovoru o obavljanju usluga certificiranja.

6.5 Upravljanje računalnom sigurnošću

6.5.1 Posebni tehnički zahtjevi na računalnu sigurnost

Pristup IT sustavu i aplikacijama u Fina PKI imaju isključivo ovlaštene osobe nakon autentikacije.

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

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

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

6.5.2 Ocjena računalne sigurnosti

U cilju sigurnosti i kvalitete pružanja usluga povjerenja Fina ima uspostavljen sustav upravljanja informacijskom sigurnošću sukladan normi ISO/IEC 27001 [5].

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 certifikata potječe iz pouzdanog izvora. Nove verzije softvera testiraju se u testnom okruženju. Implementacija softvera u produkciju provodi se u skladu s dokumentiranim postupcima upravljanja promjenama.

6.6.2 Kontrole upravljanja sigurnošću

Fina provodi provjeru svih dijelova sustava certificiranja u Fina PKI produkcijskoj hijerarhiji zasnovanoj na Fina Root CA u odnosu na sigurnost, pouzdanost i kvalitetu djelovanja, a u skladu s važećim propisima iz točke 9.14. ovih Općih pravila.

U slučaju povrede sigurnosti sustava certificiranja ili gubitka njegovog integriteta koji može imati značajan utjecaj na pružanje usluge povjerenja ili na zaštitu osobnih podataka Fina će u roku od 24 sata o istome obavijestiti središnje tijelo državne uprave nadležno za poslove gospodarstva kao tijelo nadležno za nadzor 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.

Pristup i komunikacija između zona je ograničen na autorizirano osoblje s povjerljivim ulogama nužno za pružanje usluge. Nepotrebne komunikacije, računi, portovi, protokoli i servisi su eksplicitno zabranjeni ili deaktivirani.

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

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

CA sustavi posebno su sigurnosno podešeni i očvršćeni.

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

6.8 Uporaba vremenskog žiga

Vremenski žig se ne upotrebljava u opsegu usluga certificiranja iz ovih Općih pravila.

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

7 SADRŽAJ CERTIFIKATA, LISTA OPOZVANIH CERTIFIKATA I OCSP PROFILI

7.1 Profil certifikata

Profili certifikata koje izdaje Fina RDC 2015 CA usklađeni su s normama ETSI EN 319 411-1 [8], ETSI EN 319 412 [9] i [10] i dokumentom CA/Browser Forum BRG [19].

Fina RDC 2015 CA izdaje SSL certifikat razine 2 (OVCP) prema definiranom profilu. Ovim Općim pravilima za SSL certifikat razine 2 (OVCP) dodijeljen je jedinstveni OID općih pravila certificiranja (CP OID) naveden u Tablici 1.1. točke 1.1.2.

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 mrežnim stranicama Fina repozitorija iz točke 2.2. ovih Općih pravila.

7.1.3 Identifikator objekta (OID) algoritama

Algoritmi s pripadajućim OID identifikatorima za certifikate koje izdaje 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 Root CA i njemu subordiniranog Fina RDC 2015 CA opisani su u točkama 1.3.1.1. i 1.3.1.2. ovih Općih pravila.

Oblici naziva za SSL certifikat razine 2 (OVCP) opisani su u točkama 3.1.1. i 3.1.4. ovih Općih pravila.

7.1.5 Ograničenja u nazivima

Ekstenzija *Name Constraints* se ne koristi.

7.1.6 Identifikator objekta (OID) općih pravila certificiranja

Ekstenzija *Certificate Policies* certifikata sadrži odgovarajuće OID-ove općih pravila certificiranja koji su navedeni u Tablici 1.1. u točki 1.1.2. ovih Općih pravila.

7.1.7 Uporaba ekstenzije *Policy Constraints*

Ekstenzija *Policy Constraints* se ne koristi.

7.1.8 Sintaksa i semantika kvalifikatora općih pravila

Kvalifikator općih pravila u ekstenziji *Certificate Policies* sadrži dva pokazivača u URI formatu koji sadrže internetsku adresu $CPS_{WSA\text{-}eIDAS}$ dokumenta [21] 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 s dokumentom IETF RFC 5280 [15].

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 2015CA definirane su u tablici 7.2.

Ekstenzije	Kritično	Vrijednost
crlExtensions		
cRLNumber	NE	Jednolično rastući serijski broj CRL duljine do 20 okteta.
AuthorityKeyIdentifier	NE	SHA-1 hash vrijednost duljine 160 bita
ExpiredCertsOnCRL	NE	Datum i vrijeme od kojeg se u CRL počinje čuvati informacije o statusu opoziva za istekle certifikate.
crlEntryExtensions		
reasonCode	NE	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 dokumentom IETF RFC 6960 [17].

7.3.1 Broj(evi) verzije

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

7.3.2 OCSP ekstenzije

U odgovor Fina OCSP servisa uključene su slijedeće ekstenzije:

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

8 PROVJERA SUKLADNOSTI

Nadzor nad radom Fine kao 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 Fine kao pružatelja usluga povjerenja u području praćenja provedbe propisa o zaštititi osobnih podataka provodi Agencija za 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 [8].

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 norme EN 319 403 [11] i prema zahtjevima norme ETSI EN 319 411-1 [8] i ETSI EN 319 401 [7].

8.1.2 Interna provjera sukladnosti

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

Kvartalno se provodi provjera sukladnosti certifikata s ovim Općim pravilima, $CPS_{WSA\text{-}eIDAS}$ [21] dokumentom te u skladu sa zahtjevima iz dokumenta CA/Browser Forum, BRG [17]) na slučajnom uzorku više od jednog i najmanje 3% certifikata izdanih nakon prethodne provjere.

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 [8],
- PKI područja te područja informacijske sigurnosti,
- zakonske regulative iz područja pružanja usluga povjerenja.

8.3 Odnos ocjenitelja s predmetom ocjenjivanja sukladnosti

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

Interni ocjenitelji sukladnosti ne ocjenjuju sukladnost iz vlastitog djelokruga odgovornosti.

8.4 Predmeti ocjenjivanja sukladnosti

Predmeti ocjenjivanja sukladnosti obuhvaćaju slijedeća područja pružanja 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.

8.5 Mjere u slučaju nesukladnosti

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

Za vrijeme prekida izdavanja 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.

Fina javno objavljuje sažetak izvješća i potvrdu o provedenoj vanjskoj provjeri sukladnost. Nesukladnosti utvrđene tijekom vanjske provjere sukladnosti se smatraju povjerljivim informacijama i one se ne objavljuju.

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 mrežnim stranicama repozitorija iz točke 2.2. ovih Općih pravila.

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

9.1.1 Naknade za izdavanje ili obnovu certifikata

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

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 rokovima navedenim u točki 4.9.1. 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, i sl.

Za pristup ovim Općim pravilima i $CPS_{WSA\text{-}eIDAS}$ [21] dokumentu ne naplaćuju se naknade.

9.1.5 Povrat naknada

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

9.2 Financijska odgovornost

Fina kao pružatelj usluga povjerenja posjeduje financijsku stabilnost te raspolaže dostatnim financijskim sredstvima koja osiguravaju nesmetano pružanje usluga certificiranja u skladu s ovim Općim pravilima.

9.2.1 Pokrivenost osiguranjem

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

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

9.2.2 Druga sredstva

Nema odredbi.

9.2.3 Osiguranje ili garancije krajnjim korisnicima

Vidi točku 9.2.1.

9.3 Povjerljivost poslovnih podataka

9.3.1 Opseg povjerljivih poslovnih podataka

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

9.3.2 Podaci koji se ne smatraju povjerljivim poslovnim podacima

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

9.3.3 Odgovornost za zaštitu povjerljivih poslovnih podataka

Svaki sudionik obvezan je štititi povjerljive poslovne podatke iz točke 9.3.1. ovih Općih pravila, koje je saznao na bilo koji način, sukladno propisima koji uređuju zaštitu podataka prema vrsti podatka, odnosno vrsti i stupnju tajnosti podataka. U protivnom odgovara za nastalu štetu.

9.4 Zaštita osobnih podataka

Fina posvećuje pažnju zaštiti osobnih podataka koje prikuplja, pohranjuje i upotrebljava u svrhu pružanja usluge certificiranja iz opsega ovog dokumenta te s osobnim podacima postupa sukladno Uredbi (EU) 2016/679 [4] i Zakonu o provedbi Opće uredbe o zaštiti podataka [5]

Podnošenjem zahtjeva za izdavanje certifikata fizičke osobe daju Fini suglasnost za korištenje i obradu osobnih podataka fizičkih osoba prikupljene u postupku registracije sukladno važećoj zakonskoj regulativi te za čuvanje tih podataka u trajanju od najmanje 10 godina od prestanka valjanosti certifikata na kojeg se podaci odnose.

9.4.1 Plan zaštite osobnih podataka

Fina ima i provodi Politiku zaštite osobnih podataka kojom se utvrđuju načela obrade osobnih podataka fizičkih osoba te kojom se izražava svijest, znanje i predanost za poštivanje prava i sloboda pojedinaca pri obradi osobnih podataka, a kojih se Fina mora pridržavati u svojem poslovanju. Osobne podatke prikupljene za potrebe pružanja usluga certificiranja Fina obrađuje u opsegu koji je primjeren, relevantan i ograničen samo za pružanje te usluge.

Fina stručnim znanjem, pouzdanošću, resursima, poštivanjem propisanih tehničkih, organizacijskih i sigurnosnih mjera jamči obradu osobnih podataka sukladno Uredbi (EU) 2016/679 [4] i Zakonu o provedbi Opće uredbe o zaštiti podataka [5].

Mjere zaštite povjerljivosti i cjelovitosti 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

Svi osobni podaci koje u postupku registracije Korisnika i nakon toga prikupi Fina smatraju se povjerljivim.

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 na koje se ti podaci odnose.

9.4.6 Dostupnost podataka mjerodavnim tijelima

Fina neće činiti dostupnima podatke iz točaka 9.3.1. i 9.4.2. ovih Općih pravila osim u slučajevima propisanim zakonom ili kada to pisano zahtjeva mjerodavni sud, upravno ili neko drugo mjerodavno državno tijelo.

9.4.7 Ostale okolnosti objave podataka

Nema odredbi.

9.5 Prava intelektualnog vlasništva

Ovaj dokument Općih pravila kao i druga Finina dokumentacija objavljena na mrežnim stranicama repozitorija iz točke 2.2. je intelektualno vlasništvo Fine.

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

Vlasnik privatnog i javnog ključa je Korisnik 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.

9.6 Obveze i odgovornosti

9.6.1 Obveze i odgovornosti CA

Fina je odgovorna za usklađenost ovih Općih pravila sa zakonskom regulativom te za provođenje odredbi propisanih ovim Općim pravilima, $CPS_{WSA\text{-}eIDAS}$ [21] dokumentom, Uvjetima pružanja usluga certificiranja i sukladno obvezama u ugovoru o obavljanju usluga certificiranja sklopljenim s Korisnikom.

Fina na mrežnim stranicama repozitorija iz točke 2.2. ovih Općih pravila objavljuje uvjete pružanja usluga certificiranja, ova Opća pravila, $CPS_{WSA\text{-}eIDAS}$ [21] dokument 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 kao kvalificirani pružatelj usluga povjerenja odgovorna za:

- za usklađenost pružanja usluga certificiranja s odredbama svoje politike informacijske sigurnosti, odredbama Pravilnika o postupcima certificiranja [21] i odredbama ovog dokumenta, uključivši i kada je dio svoje usluge certificiranja ugovorom povjerila drugom poslovnom subjektu,

- 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 ima li podnositelj zahtjeva za izdavanje certifikata kontrolu i isključivo pravo korištenja naziva domene ili IP adrese sadržane u certifikatu (ili, mu je to pravo ili kontrola, u slučaju naziva domene, delegirana od subjekta koji to pravo ima),
- prije izdavanja certifikata provjerava je li Korisnik odobrio izdavanje certifikata te je li 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 svim slučajevima kad CA i Korisnik nisu povezani niti su isti entitet,
- u slučajevima kad su 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. ovih Općih pravila, 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 ovim Općim pravilima,
- osigurava provjeru da Korisnik posjeduje privatni ključ čiji se pripadajući javni ključ dostavlja na certificiranje,
- izdani certifikat čini dostupnim sukladno točki 4.4.2. ovih Općih pravila,
- temeljem autenticiranog i autoriziranog zahtjeva, po provedenom propisanom postupku, opoziva certifikat iz razloga navedenih u točki 4.9.1. ovih Općih pravila,
- osigurava da je repozitorij javno dostupan 24 sata na dan, 7 dana u tjednu te da pruža informacije o aktualnim statusima opozvanosti svih certifikata kojima nije istekao period važenja,
- pri pružanju usluge certificiranja primjenjuje odredbe važećih propisa iz točke 9.14. ovih Općih pravila,
- provodi zahtijevane sigurnosne mjere za zaštitu prostora i opreme sustava certificiranja,
- primjenjuje organizacijske i tehničke mjere zaštite ključeva i certifikata sukladno ovim Općim pravilima,
- sukladno planu kontinuiteta poslovanja osigurava nesmetan rad i maksimalnu raspoloživost usluga certificiranja,

- prati raspoloživost kapaciteta, planira održavanje i daljnji razvoj sustava certificiranja sukladno budućim potrebama, zahtjevima normi i razvoju tehnologije,
- podatke koji se sukladno točkama 9.3. i 9.4. ovih Općih pravila smatraju povjerljivima štiti i te podatke koristiti isključivo za potrebe usluga certificiranja iz opsega ovih Općih pravila,
- osigurava da se interne i vanjske provjere sukladnosti Fine kao pružatelja usluga povjerenja provode sukladno točki 8.1. ovih Općih pravila.

U slučaju prestanka pružanja usluga izdavanja certifikata Fina će postupiti sukladno točki 5.8. ovih Općih pravila.

9.6.2 Obveze i odgovornosti RA

Obveze i odgovornosti Fina RA mreže su:

- provođenje postupka registracije i identifikacije fizičkih osoba i pravnih osoba te provjeru podataka na način propisan ovim Općim pravilima,
- 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 prestanka valjanosti certifikata na kojeg se odnose,
- osiguravanje od gubitka ili povrede povjerljivosti, cjelovitosti i dostupnosti arhiviranih podataka Korisnika, na način propisan ovim Općim pravilima,
- obavještavanje podnositelja zahtjeva za izdavanje certifikata o javno objavljenim i dostupnim uvjetima pružanja usluga certificiranja i ovim Općim pravilima.

9.6.3 Obveze i odgovornosti korisnika

Prije inicijalnog izdavanja certifikata Korisnik s Finom sklapa ugovor o obavljanju usluga certificiranja kojim prihvaća ova Opća pravila i uvjete pružanja usluga certificiranja.

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

Korisnik je, kao pravna osoba, odgovoran je 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. ovih Općih pravila,
- pažljivo koristiti i čuvati privatne ključeve i aktivacijske podatke sukladno ovim Općim pravilima,
- poduzeti odgovarajuće mjere zaštite privatnog ključa i aktivacijskih podataka od neovlaštenog pristupa i uporabe u skladu s poglavljem 6. ovih Općih pravila,
- pregledati i provjeriti točnost sadržaja certifikata te prihvatiti taj certifikat prije njegova izdavanja,

- 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. ovih Općih pravila,
- ako je certifikat opozvan iz razloga kompromitiranja privatnog ključa, u najkraćem mogućem roku prekinuti svaku uporabu privatnog ključa povezanog s javnim ključem u certifikatu,
- odgovarati na 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. ovih Općih pravila, ugovora i uvjetima pružanja usluge,
- koristiti certifikat i pripadajući privatni ključ u skladu s odredbama iz točke 4.5.1. ovih Općih pravila,
- djelovati u skladu sa svim ostalim odredbama iz ovih Općih pravila koje se odnose na obveze Korisnika.

Obveze i odgovornosti Korisnika vezane uz korištenje privatnog ključa i certifikata opisane su u točki 4.5.1. ovih Općih pravila.

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 zloćudnog koda.

U slučaju promjene kontakt podataka nastale promjene Korisnik je dužan dostaviti Fini na kontakt podatke navedene u točki 9.11. ovih Općih pravila.

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

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

9.6.4 Obveze i odgovornosti pouzdajuće strane

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

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

- poduzela potrebne mjere opreza i koristiti certifikat u svrhe propisane ovim Općim pravilima, odnosno uvjetima pružanja usluge, pod okolnostima u kojima je pouzdanje razumno i u dobroj namjeri te pod okolnostima koje su poznate ili bi trebale biti poznate Pouzdajućoj strani prije ostvarenja pouzdanja,

- koristila aplikacijsko rješenje i IT okolinu u koju se može pouzdati,
- provjerila period važenja certifikata,
- provjerila status opozvanosti certifikata, a što Pouzdajuća strana utvrđuje provodeći provjeru statusa certifikata putem OCSP servisa ili temeljem zadnje izdane CRL, kako je propisano ovim Općim pravilima,
- 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 ovih Općih pravila.

Pouzdajuća strana koja nije poštovala propise i ova Opća pravila te nije postupala sukladno obvezama i odgovornostima iz ove točke sama snosi sve rizike pouzdanja u takav certifikat.

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

9.6.5 Obveze i odgovornosti ostalih sudionika

Nema odredbi.

9.7 Odricanje od odgovornosti

Fina nije odgovorna za štete, uključujući i indirektne štete, kao i za bilo koji gubitak dobiti, gubitak podataka ili druge indirektne štete u sljedećim slučajevima:

- kad je šteta nastala zbog neautorizirane uporabe korisničkih ključeva i certifikata,
- kad je šteta nastala uporabom certifikata koja nije dopuštena ovim dokumentom,
- kad je šteta prouzročena prijevarnom ili nemarnom uporabom certifikata, CRL ili OCSP servisa,
- kad je šteta nastala kao rezultat neispravnosti i pogrešaka u softveru i hardveru Korisnika i Pouzdajuće strane,
- kad je šteta nastala kao rezultat prijevarnog davanja podataka i prijevarnog predstavljanja pravne osobe ili fizičke osobe tijekom procesa identifikacije i potvrde identiteta, ako je identifikaciju i provjeru podataka RA mreža provodila u skladu sa zahtjevima iz ovog dokumenta i radnim uputama.

9.8 Ograničenja odgovornosti

Finina ukupna financijska odgovornost za nekvalificirane certifikate izdane prema ovim Općim pravilima i $CPS_{NQC\text{-}eIDAS}$ dokumentu [22] 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 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

Tablica 9.1. Maksimalna Finina financijska odgovornost

9.9 Naknada štete

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

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 ostvaruju Pouzdajuće ili druge strane.

Gore navedeno se,međutim, ne odnosi na bilo koje potraživanje, štetu ili gubitak kojeg Isporučitelj aplikacijskog softvera pretrpi u svezi s certifikatom kojeg je izdala Fina, a kada je to potraživanje, šteta ili gubitak izravno uzrokovao softver tog Isporučitelja aplikacijskog softvera u slučaju da je nepovjerljivi certifikat prikazao još uvijek validnim ili je prikazao povjerljivim certifikat:

- koji je tada već bio istekao, ili
- koji je tada već bio opozvan (ali samo u slučaju kada je informacija o aktualnom statusu opozvanosti certifikata u tom trenutku od strane Fine bila raspoloživa online, a pri tom aplikacijski softver je nije ispravno provjerio status opozvanosti ili je zanemario oznaku statusa opozvanosti).

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

9.10 Trajanje i prestanak važenja

9.10.1 Trajanje

Ovaj dokument Općih pravila važi do stupanja na snagu novog dokumenta Općih pravila ili do objave prestanka njegovog važenja. Nova verzija dokumenta ili objava prestanka važenja biti će objavljena na mrežnim stranicama repozitorija iz točke 2.2. ovih Općih pravila s naznačenim danom stupanja na snagu. Novom dokumentu biti će dodijeljena nova verzija i novi OID te će u njemu biti naznačene obavljene izmjene.

9.10.2 Prestanak važenja

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

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

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

9.10.3 Posljedice prestanka važenja i nastavak djelovanja

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

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

9.11 Individualne obavijesti i komunikacija sa sudionicima

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

- besplatni telefon: 0800 0080

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

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

9.12 Izmjene i dopune

9.12.1 Procedure izmjena i dopuna

Ova Opća pravila revidiraju se po potrebi.

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

Svi sudionici mogu na kontakt adresu Fina PMA iz točke 1.5. ovih Općih pravila poslati dopis s prijedlogom za ispravke pogrešaka, prijedlog nadopuna ili izmjenu ovog dokumenta. U dopisu se navode kontakt podaci osobe koja je poslala prijedlog promjene. Fina PMA može prihvatiti, prilagoditi ili odbiti predložene promjene nakon razmatranja istih.

9.12.2 Mehanizmi obavještavanja i vremenski periodi

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

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

Datum stupanja na snagu izmjena i dopuna ili novoobjavljenog dokumenta Općih pravila naznačeni su na njegovoj naslovnoj strani kao i na mrežnim stranicama na kojima je objavljen.

9.12.3 Okolnosti pod kojima se mora mijenjati OID

Veće izmjene u dokumentu Općih pravila koje mogu utjecati na sudionike zahtijevaju i izmjenu OID-a Općih pravila. Novi OID za novu verziju dokumenta određuje Fina PMA.

9.13 Postupak rješavanja sporova

U slučaju spora ili neslaganja između Fine i drugih sudionika povodom radnji i/ili postupaka glede pružanja usluge certificiranja uređene ovim Općim pravilima, isti će se nastojati razriješiti sporazumno. Ako sporazumno razrješenje spora nije moguće, isti će se razriješiti pred mjerodavnim sudom u Zagrebu uz primjenu hrvatskog prava.

Sudionici mogu Fini uputiti prigovor ako smatraju 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. ovih Općih pravila.

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 319 411-1 [8], ETSI EN 319 401 [7] i CA/Browser Forum BRG [19].

9.15 Usklađenost s primjenjivim propisima

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

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

9.16 Razne odredbe

Nema odredbi.

9.17 Ostale odredbe

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

Fina RDC 2015 CA izdaje testne certifikate. Testni certifikati se prvenstveno izdaju Fini za potrebe testiranja Fina PKI sustava, a mogu se izdati i drugoj pravnoj osobi u svrhu testiranja sustava. Testni certifikati izdaju se isključivo u svrhu testiranja i nemaju nikakav pravni učinak. Fina ne preuzima nikakvu odgovornost za izdavanje i korištenje testnih certifikata.

Fina javno objavljuje ova Opća pravila, $CPS_{WSA\text{-}eIDAS}$ [21] dokument i uvjete pružanja usluga certificiranja.

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