FINA

OPĆA PRAVILA PRUŽANJA USLUGA CERTIFICIRANJA I PRAVILNIK O POSTUPCIMA CERTIFICIRANJA ZA

Fina Root CA

Verzija 2.4

Datum stupanja na snagu: 10.06.2019.

OID Dokumenta: 1.3.124.1104.5.0.2.2.2.4

Informacije o dokumentu

Ime dokumenta:	Opća pravila pružanja usluga certificiranja i Pravilnik o postupcima certificiranja za Fina Root CA
OID dokumenta:	1.3.124.1104.5.0.2.2.2.4
Tip dokumenta:	Opća pravila pružanja usluga certificiranja i Pravilnik o postupcima certificiranja (*Certificate Policy and Certification Practice Statement*, CP/CPS)
Oznaka distribucije	Javno
Vlasnik dokumenta	Financijska agencija, Fina
Kontakt	pma@fina.hr

Povijest izmjena

Verzija	Datum	Razlog izmjene
1.0	07.12.2015.	Inicijalna verzija
2.0	28.03.2017.	Usklađivanje Uredbom (EU) br. 910/2014 [1] i objedinjavanje dokumenata Opća pravila pružanja usluga certificiranja za Fina Root CA i Pravilnika o postupcima certificiranja za Fina Root CA
2.1	22.05.2017.	Promjene sukladno komentarima ocjenitelja
2.2	19.04.2018.	Ažuriranje referente liste zakonske regulative i ispravljanje prepoznatih grešaka.
2.3	12.09.2018.	Dodavanje osnovnih podataka o Fina Root CA certifikatu, dopuna odredbi vezanih uz prestanak pružanja usluga povjerenja, dodavanje izjave o postupcima vezanim za upravljanje kritičnim ranjivostima i dodavanje izjave o dostupnosti usluga osobama s invaliditetom.
2.4	22.05.2019.	Dodane reference na opća pravila i pravilnik o postupcima certificiranja za kvalificirane certifikate za autentikaciju mrežnih stranica, u točki 4.6. dodana pojašnjenja za dostavu javnog ključa kod obnove certifikata, u točki 4.9.1. dodani razlozi za opoziv subordiniranih Fina CA certifikata, u točki 4.10.2. navedeno je vrijeme odziva na zahtjev za dohvat CRL ili dobivanje OCSP odgovora, u točki 5.2.4. dopunjeno je pravilo za odvajanje dužnosti, u točki 5.4.1. proširena je specifikacija revizijskih zapisa, u točki 6.1.4. poboljšan je i prošireni opis dostave javnog ključa CA pouzdajućim stranama, u točki 9.4. dodana su proširenja u opisu zaštite osobnih podataka, u točki 9.7. ispravljen je tekst odricanja odgovornosti Fine te su ispravljene prepoznate greške u dokumentu.

SADRŽAJ

AUTORSKA PRAVA

REFERENCE

Temeljni zakon

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

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

Ostali zakoni

[3] 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)

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

Normizacijski dokumenti

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

[6] ISO 9001:2015 - Quality management systems - Requirements

[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 319 411-2 V2.2.2. (2018-04) - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates

[10] 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

[11] ETSI TS 119 312 V1.3.1. (2019-02) - Electronic Signatures and Infrastructures (ESI); Cryptographic Suites

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

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

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

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

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

[17] CA/Browser Forum - Guidelines for the Issuance and Management of Extended Validation Certificates

Finini dokumenti

[18] Opća pravila pružanja usluga certificiranja za kvalificirane certifikate za elektroničke potpise i pečate, $CP_{QC\text{-}eIDAS}$

[19] Pravilnik o postupcima certificiranja za kvalificirane certifikate za elektroničke potpise i pečate, $CPS_{QC\text{-}eIDAS}$

[20] Opća pravila pružanja usluga certificiranja za nekvalificirane certifikate, $CP_{NQC\text{-}eIDAS}$

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

[22] Opća pravila pružanja usluga certificiranja za kvalificirane certifikate za autentikaciju mrežnih stranica, CP_{QWAC}

[23] Pravilnik o postupcima certificiranja za kvalificirane certifikate za autentikaciju mrežnih stranica, CPS_{QWAC}

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

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

[26] Opća pravila davanja usluga certificiranja, $CP_{Non\text{-}eIDAS}$

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

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.

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

Kao treća strana od povjerenja, Fina svoje usluge certificiranja pruža od 2003. godine. Usluge povjerenja koje pruža Fina usklađene su sa zakonskom regulativom [1] – [4] te s mjerodavnim međunarodnim normama iz djelokruga pružanja usluga povjerenja. Fina neprekidno prati potrebe Korisnika, razvoj tehnologije i promjene u normama iz područja pružanja usluga povjerenja te sukladno tome unapređuje i usklađuje svoj PKI sustav.

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.

1.1.1. Hijerarhijska struktura Fina PKI zasnovana na Fina Root CA

Hijerarhijska struktura Fina PKI zasnovana na Fina Root CA temelji se na dvorazinskoj arhitekturi produkcijskih certifikacijskih tijela (engl. *Certification Authorities,* u daljem tekstu: CA ili CA-ovi). Sustav za izdavanje digitalnih certifikata (u daljnjem tekstu: certifikati) sastoji se od korijenskog certifikacijskog tijela (engl. *Root Certification Authority*, *Root* CA) koji izdaje certifikate za produkcijska Finina subordinirana certifikacijska tijela (engl. *Subordinate Certification Authority*, *Subordinate* CA). Subordinirani Fina CA-ovi izdaju certifikate krajnjim Korisnicima.

Dvorazinsku arhitekturu produkcijskih certifikacijskih tijela Fine čine:

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

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

Fina Root CA izdao je i certifikat za potpisivanje odgovora Fina OCSP servisa za status opozvanosti certifikata koje izdaje Fina Root CA.

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

1.1.2. Opseg i namjena

Opseg ovih Općih pravila pružanja usluga certificiranja i Pravilnika o postupcima certificiranja za Fina Root CA (engl. *Certificate Policy and Certification Practice Statement for Fina Root CA* – CP/CPS, u daljnjem tekstu: CP/CPS$_{ROOT}$) su usluge povjerenja koje pruža Fina, a koje se odnose na izdavanje i upravljanje životnom ciklusom u produkcijskoj hijerarhiji certifikata zasnovanoj na Fina Root CA.

Struktura ovog dokumenta temelji se na normizacijskom dokumentu IETF RFC 3647 [13].

Postupci koji se primjenjuju u izdavanju Korisničkih certifikata opisani su u pripadajućim pravilnicima o postupcima certificiranja [19], [21], [23] i [25], u daljnjem u tekstu: pripadajući CPS dokumenti.

1.1.3. Certifikati u Fina PKI hijerarhiji zasnovanoj na Fina Root CA

Certifikati koje izdaju Fina Root CA i njemu subordinirani Fina CA-ovi namijenjeni su za korištenje u elektroničkom poslovanju unutar i izvan Republike Hrvatske.

1.1.3.1. Certifikati koje izdaje Fina Root CA

Fina Root CA izdaje sljedeće certifikate:

Fina Root CA	
Fina Root CA certifikat	CP OID: 1.3.124.1104.5.2
Certifikati za subordinirane Fina CA-ove	CP OID: 1.3.124.1104.5.2.1
Certifikat za potpis odgovora OCSP servisa	CP OID: 1.3.124.1104.5.2.9.4.3

Tablica 1.1. Certifikati koje izdaje Fina Root CA

Fina Root CA ne izdaje Korisničke certifikate.

1.1.3.2. Korisnički Certifikati koje izdaje Fina RDC 2015 CA

Fina RDC 2015 CA izdaje sljedeće grupe certifikata:

- **Osobni certifikati** namijenjeni su fizičkim osobama – građanima.
- **Poslovni certifikati** namijenjeni su za poslovnu uporabu, a izdaju se fizičkim osobama povezanim s Poslovnim subjektom.
- **Certifikati za e-pečat** namijenjeni su za elektroničko pečatiranje, a izdaju se pravnim osobama.
- **Poslovni certifikati za IT opremu** izdaju se za IT sustave, aplikacije ili servise povezane s Poslovnim subjektom

- **Certifikati za autentikaciju mrežnih stranica** (TLS/SSL certifikati, poslužiteljski certifikati) izdaju se pravnim osobama i državnim tijelima za internetske poslužitelje (web serveri).

Certifikati koje izdaje Fina RDC 2015 CA i koji su usklađeni s Uredbom (EU) br. 910/2014 [1] opisani su u sljedećim dokumentima općih pravila:

- Opća pravila pružanja usluga certificiranja za kvalificirane certifikate za elektroničke potpise i pečate, $CP_{QC\text{-}eIDAS}$ [18],
- Opća pravila pružanja usluga certificiranja za nekvalificirane certifikate, $CP_{NQC\text{-}eIDAS}$ [20],
- Opća pravila pružanja usluga certificiranja za certifikate za autentikaciju mrežnih stranica, $CP_{WSA\text{-}eIDAS}$ [24],
- Opća pravila pružanja usluga certificiranja za kvalificirane certifikate za autentikaciju mrežnih stranica, CP_{QWAC} [22].

Certifikati koje izdaje Fina RDC 2015 CA, koji nisu usklađeni s Uredbom (EU) br. 910/2014 [1] opisani su u Općim pravilima davanja usluga certificiranja, $CP_{Non\text{-}eIDAS}$ [26].

1.1.3.3. Korisnički certifikati koje izdaje Fina RDC-TDU 2015 CA

Fina RDC-TDU 2015 CA izdaje sljedeće grupe certifikata:

- certifikati za državne dužnosnike i zaposlenike u tijelima državne uprave (TDU),
- certifikati za e-pečat za TDU.

Certifikati koje izdaje Fina RDC-TDU 2015 CA i koji su usklađeni s Uredbom (EU) br. 910/2014 [1] opisani su u sljedećim općim pravilima:

- Opća pravila pružanja usluga certificiranja za kvalificirane certifikate za elektroničke potpise i pečate, $CP_{QC\text{-}eIDAS}$ [18],
- Opća pravila pružanja usluga certificiranja za nekvalificirane certifikate, $CP_{NQC\text{-}eIDAS}$ [20].

1.2. Naziv dokumenta i identifikacijski podaci

British Standards Institution (BSI) *International Code Designator* (ICD) dodijelio je Fini sljedeći OID: 1.3.124.1104. Na temelju tog OID-a Fina je za područje 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 i Pravilnik o postupcima certificiranja za Fina Root CA
- Verzija: 2.4
- Datum stupanja na snagu: 10.06.2019.
- OID: 1.3.124.1104.5.0.2.2.2.4

Internetska adrese na kojoj je objavljena verzija dokumenta CP/CPS_{ROOT} za javnu objavu je: https://rdc.fina.hr/Root/FinaRootCA-CPCPS2-4-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

Certifikacijska tijela u Fina PKI iz opsega ovog CP/CPS_{ROOT} dokumenta su Fina Root CA te njemu subordinirani Fina RDC 2015 i Fina RDC-TDU 2015 CA-ovi.

Fina Root CA izdaje CA certifikate za njemu subordinirane Fina CA-ove i certifikat za potpis odgovora Fina OCSP servisa. Fina Root CA ne izdaje certifikate Korisnicima.

Fina RDC 2015 CA izdaje certifikate za javnost. Korisnici kojima Fina RDC 2015 CA izdaje certifikate su fizičke osobe - građani, pripadajuće osobe unutar Poslovnih subjekata i Poslovni subjekti, a sukladno opisu u točki 1.1.3.2. ovog dokumenta.

Fina RDC-TDU 2015 CA izdaje certifikate državnim dužnosnicima i zaposlenicima u tijelima državne uprave sukladno opisu u točki 1.1.3.3. ovog dokumenta.

Navedena tri CA čine hijerarhijsku strukturu koja je opisana u točki 1.1.1. ovog dokumenta.

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 certifikat dostupan je na internetskoj adresi navedenoj u točki 6.1.4.

1.3.2. Registracijski uredi

Poslovi registracije Korisnika za Fina CA-ove obavljaju se u registracijskim uredima Fine. Za potrebe registracije Korisnika za Fina CA-ove, Fina može s drugim Poslovnim subjektom ugovoriti obavljanje usluge registracije za određene tipove certifikata.

Mrežu registracijskih ureda (u daljnjem tekstu: RA mreža) čine Fina RA mreža i mreža pojedinog vanjskog ugovorenog RA.

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

Poslovima registracije u RA mreži koordinira Središnji RA Fine.

1.3.3. Korisnici

Korisnici Fina PKI u smislu ovog dokumenta su osobe koje s Finom ugovaraju korištenje usluga certificiranja.

Korisnici Fina PKI mogu biti:

- fizičke osobe – građani,
- pripadajuće osobe unutar Poslovnih subjekata,
- Poslovni subjekti, uključujući i tijela državne uprave.

Posebna kategorija Poslovnih subjekata u okviru Fina PKI su tijela državne uprave (u daljnjem tekstu: TDU). Certifikate za dužnosnike i zaposlenike TDU izdaje Fina RDC-TDU 2015 CA, a za sve druge Korisnike certifikate izdaje Fina RDC 2015 CA.

1.3.4. Pouzdajuće strane

Pouzdajuće strane su fizičke osobe ili Poslovni subjekti koji se oslanjaju na uslugu povjerenja te djeluju temeljem razumnog pouzdanja u certifikat.

1.3.5. Ostali sudionici

Nema odredbi.

1.4. Uporaba certifikata

1.4.1. Primjerena uporaba certifikata

Fina Root CA certifikat isključivo se koristi za izdavanje CA certifikata njemu subordiniranih Fina CA-ova, za izdavanje CRL te za izdavanje certifikata za Fina OCSP servis kojim ovaj OCSP servis potpisuje odgovore za status subordiniranih Fina CA certifikata.

Certifikati subordiniranih Fina CA-ova koriste se za izdavanje Korisničkih certifikata, izdavanje pripadajućih CRL, za izdavanje certifikata za Finin servis izdavanja kvalificiranih

elektroničkih vremenskih žigova (Fina QTSA servis), za izdavanje certifikata za Fina OCSP servis, a u skladu s vrijednostima u ekstenzijama *Basic Constraints* i *PathLengthConstraint* u CA certifikatima Fina CA-ova.

1.4.2. Zabrane uporabe certifikata

Sve uporabe Fina Root CA certifikata i certifikati subordiniranih Fina CA-ova različite od uporaba navedenih u točki 1.4.1. ovog dokumenta su zabranjene.

1.5. Administracija dokumenta

1.5.1. Organizacija odgovorna za održavanje dokumenta

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

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

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

1.5.2. Kontakt podaci

Kontakt podaci za administraciju i sadržaj ovog dokumenta dani su u nastavku.

Poštanska adresa:

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

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

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

Usklađenost Pravilnika o postupcima certificiranja s Općim pravilima pružanja usluga certificiranja kao i usklađenost CPS dokumenata s pripadajućim općim pravilima pružanja usluga certificiranja utvrđuje Fina PMA.

1.5.4. Procedure odobravanja CPS-a

Izrada, odobravanje i stupanje na snagu Pravilnika o postupcima certificiranja kojima se potvrđuje njegova sukladnost s Općim pravilima opisana je u točki 9.12.1 ovog dokumenta.

1.6. Definicije i kratice

1.6.1. Definicije

DEFINICIJA	ZNAČENJE
Aktivacijski podaci	Tajni podaci potrebni za pristup ili aktivaciju kriptografskog modula. Aktivacijski podatak može biti PIN, zaporka ili elektronički ključ kojeg osoba zna ili posjeduje.
CA certifikat	Certifikat javnog ključa za CA kojeg je izdao drugi CA ili kojeg je izdao isti CA.
Certifikacijsko tijelo (CA)	Tijelo koje izrađuje i dodjeljuje certifikate javnog ključa, a kojem vjeruje jedan ili više korisnika. Certifikacijsko tijelo može biti: 1. pružatelj usluga povjerenja koji izrađuje i dodjeljuje certifikate javnog ključa, ili 2. 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.
Elektronički potpis	Podaci u elektroničkom obliku koji su pridruženi drugim podacima u elektroničkom obliku ili su logički povezani s njima radi osiguravanja izvornosti i cjelovitosti tih podataka.
Fina LRA	Lokalni registracijski ured u Fina poslovnoj mreži.
Fina PKI	Infrastruktura javnog ključa (PKI) uspostavljena u Fini koja je namijenjena za 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
Identifikator objekta (OID)	Identifikator koji predstavlja specifičan objekt. OID se sastoji od brojeva odijeljenih točkama i navedenih u hijerarhijskom poretku. Svaki broj identificira poseban čvor u stablu čvorova, počevši od korijena tog stabla.
Infrastruktura javnog ključa (PKI)	Infrastruktura za upravljanje javnim ključevima koji podržavaju usluge autentikacije, enkripcije, cjelovitosti i neporecivosti.
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.
Korisnik	Poslovni subjekt ili fizička osoba koja je sklapanjem ugovora s pružateljem usluga povjerenja preuzela ugovorne obveze Korisnika.

DEFINICIJA	ZNAČENJE
Kriptografski modul	Softver ili uređaj određene razine sigurnosti koji: • generira par ključeva i/ili • štiti kriptografske informacije i/ili • obavlja kriptografske funkcije.
Kvalificirani ocjenitelj	Fizička ili pravna osoba koja zadovoljava zahtjeve za *Qualified Auditor* navedene u dokumentu CA/Browser Forum BRG [16].
Kvalificirano sredstvo za izradu elektroničkog potpisa	Sredstvo za izradu elektroničkog potpisa koje ispunjava zahtjeve utvrđene u Prilogu II Uredbe (EU) br. 910/2014 [1].
Lista opozvanih certifikata (CRL)	Potpisana lista u kojoj su naznačeni certifikati koje izdavatelj certifikata više ne smatra valjanim.
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.
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.
Pouzdajuća strana	Fizička osoba ili poslovni subjekt koji se oslanja na elektroničku identifikaciju ili uslugu povjerenja.
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.
Pripadajuća osoba	Fizička osoba zaposlena u poslovnom subjektu ili na drugi način povezana s Poslovnim subjektom, a koja je od strane istog poslovnog subjekta autorizirana za dobivanje certifikata. Takav certifikat identificira osobu i Poslovni subjekt te naznačuje da je ta osoba povezana s Poslovnim subjektom.
Privatni ključ	U kriptografskom sustavu javnog ključa, ključ iz Subjektovog para ključeva koji je poznat samo Subjektu.

DEFINICIJA	ZNAČENJE
QSCD uređaj	Kvalificirano sredstvo za izradu elektroničkog potpisa/pečata (vidi pojam „kvalificirano sredstvo za izradu elektroničkog potpisa“).
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.
Reaktivacija certifikata	Radnja koja suspendirani certifikat ponovno čini valjanim.
Registracijski ured (RA)	Tijelo odgovorno za identifikaciju i autentikaciju Subjekata certificiranja, kao i drugih osoba ili organizacija.
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.
Središnji RA	Središnji registracijski ured koji je primarno je zadužen za koordiniranje cjelokupne RA mreže, ali može i izravno obavljati registriranje Korisnika.
Sredstvo elektroničke identifikacije	Materijalna i/ili nematerijalna jedinica koja sadrži osobne identifikacijske podatke i koja se koristi za autentikaciju na *online* uslugu.
Subjekt	Entitet identificiran u certifikatu kao nositelj privatnog ključa koji je povezan s javnim ključem sadržanim u certifikatu.
Suspenzija certifikata	Privremeni prestanak valjanosti certifikata prije isteka roka važenja navedenog u certifikatu. Suspendirani certifikat se reaktivacijom može ponovno učiniti valjanim.
Sustav certificiranja	Sustav IT proizvoda i komponenti organiziranih za pružanje usluga certificiranja.
Tijelo (tijela) 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 upravljanje pravilima certificiranja (PMA)	Tijelo s konačnom ovlašću i odgovornošću za određivanje i odobravanje pravila pružanja usluga povjerenja (engl. *Policy Management Authority*).

1.6.2. Kratice

KRATICA	PUNI NAZIV	ZNAČENJE
CA	*Certification Authority*	Certifikacijsko tijelo
CP	*Certificate Policy*	Opća pravila pružanja usluga certificiranja
CP/CPS$_{ROOT}$	*Certificate Policy and Certification Practice Statement for Fina Root CA*	Opća pravila pružanja usluga certificiranja i Pravilnik o postupcima certificiranja za Fina Root CA
CP$_{QC\text{-}eIDAS}$	*Certificate Policy for Qualified Certificates for Electronic Signatures and Seals*	Opća pravila pružanja usluga certificiranja za kvalificirane certifikate za elektroničke potpise i pečate

KRATICA	PUNI NAZIV	ZNAČENJE
$CP_{NQC-eIDAS}$	*Certificate Policy for Non-qualified Certificates*	Opća pravila pružanja usluga certificiranja za nekvalificirane certifikate
$CP_{WSA-eIDAS}$	*Certificate Policy for Certificates for Website Authentication*	Opća pravila pružanja usluga certificiranja za certifikate za autentikaciju mrežnih stranica
CP_{QWAC}	*Certificate Policy for Qualified Certificates for Website Authentication*	Opća pravila pružanja usluga certificiranja za kvalificirane certifikate za autentikaciju mrežnih stranica
$CP_{Non-eIDAS}$	*Certification Policy*	Opća pravila pružanja usluga certificiranja
CPS	*Certification Practice Statement*	Pravilnik o postupcima certificiranja
$CPS_{QC-eIDAS}$	*Certification Practice Statement for Qualified Certificates for Electronic Signatures and Seals*	Pravilnik o postupcima certificiranja za kvalificirane certifikate za elektroničke potpise i pečate
$CPS_{NQC-eIDAS}$	*Certification Practice Statement for Non-Qualified Certificates*	Pravilnik o postupcima certificiranja za nekvalificirane certifikate
$CPS_{WSA-eIDAS}$	*Certification Practice Statement for Certificates for Website Authentication*	Pravilnik o postupcima certificiranja za certifikate za autentikaciju mrežnih stranica
CPS_{QWAC}	*Certification Practice Statement for Qualified Certificates for Website Authentication*	Pravilnik o postupcima certificiranja za kvalificirane certifikate za autentikaciju mrežnih stranica
$CPS_{NQC-Non-eIDAS}$	*Certification Practice Statement for Non-Qualified Certificates*	Pravilnik o postupcima certificiranja za nekvalificirane certifikate
CRL	*Certificate Revocation List*	Lista opozvanih certifikata
DN	*Distinguished Name*	Razlikovno ime
LDAP	*Lightweight Directory Access Protocol*	Protokol za pristup informacijskim direktorijima
LRA	*Local Registration Authority*	Lokalni registracijski ured
OCSP	*Online Certificate Status Protocol*	*Online* provjera statusa certifikata
OID	*Object Identifier*	Identifikator objekta
PIN	*Personal Identification Number*	Osobni tajni broj za aktivaciju *smart* kartice, USB tokena ili sličnog uređaja
PKI	*Public Key Infrastructure*	Infrastruktura javnog ključa
PMA	*Policy Management Authority*	Tijelo za upravljanje pravilima certificiranja
RA	*Registration Authority*	Registracijski ured
TDU	Tijelo (ili tijela) državne uprave	Tijelo (ili tijela) državne uprave
UTC	*Coordinated Universal Time*	Koordinirano svjetsko vrijeme

2. OBJAVE I ODGOVORNOSTI ZA REPOZITORIJ

2.1. Identifikacija tijela koje vodi repozitorij

Fina PKI repozitorij vodi Fina kao pružatelj usluga povjerenja. Fina je odgovorna za rad i za objavu dokumenata i informacija na Fina PKI 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.

Fina PKI repozitorij se sastoji od dijela dostupnog na internetskim stranicama i dijela dostupnog preko javnog LDAP imenika.

2.2.1. Sadržaji repozitorija

Na Fina PKI repozitoriju javno se objavljuju dokumenti i informacije o pružanja usluga certificiranja.

Na internetskim stranicama Fina PKI repozitorija objavljuju se:

- ova Opća pravila pružanja usluga certificiranja i Pravilnik o postupcima certificiranja za Fina Root CA,
- opća pravila pružanja usluga certificiranja,
- pravilnici o postupcima certificiranja,
- prijašnje verzije dokumenata općih pravila i pravilnika o postupcima certificiranja,
- uvjeti i izjave o pružanju usluga izdavanja certifikata (engl. *Terms and conditions* i *PKI disclosure statement*),
- opis važećih profila certifikata,
- cjenik usluga certificiranja,
- obrasci za Korisnike,
- Fina Root CA certifikat i certifikati subordiniranih Fina CA-ova,
- objedinjena CRL Fina Root CA i objedinjene CRL subordiniranih CA-ova,
- informacije o zakonskoj regulativi iz područja pružanja usluga certificiranja,
- aktualne lokacije Fina LRA ureda,
- Korisničke upute,
- obavijesti Korisnicima i Pouzdajućim stranama vezane uz pružanje usluga certificiranja,
- ostale informacije vezane uz Fina Root CA i njemu subordinirane Fina CA-ove.

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

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

U dijelu Fina PKI repozitorija dostupnog preko javnog LDAP imenika objavljuju se:

- objedinjene CRL koje izdaju Fina CA-ovi,
- segmentirane CRL koje izdaju Fina CA-ova.

LDAP imenik dostupan je s adrese: ldap://rdc-ldap2.fina.hr.

Putem Fina OCSP servisa dostupne su informacije o statusu izdanih certifikata. Fina OCSP servis je raspoloživ s adrese: http://ocsp.fina.hr.

Na Fina PKI repozitoriju nisu javno objavljeni povjerljivi dokumenti i informacije.

2.2.2. Postupci objave sadržaja i upravljanja repozitorijem

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

Objavu informacija i drugih dokumenata odobravaju, ovisno o njihovom području i vrsti, ovlaštene osobe Fina PKI za područje svoje nadležnosti.

Informacije o Fina Root CA certifikatu, certifikatima subordiniranih Fina CA-ova objavljuju se po njihovu izdavanju.

Subordinirani CA-ovi svoje CRL nakon izdavanja automatski objavljuju na javnom imeniku i na internetskim stranicama repozitorija.

2.3. Vrijeme ili učestalost objavljivanja

Fina na godišnjoj razini održava i ažurira ovaj dokument te ga odobrava, objavljuje i primjenjuje. Prijašnje verzije ovih dokumenata ostaju objavljene na repozitoriju najmanje do isteka certifikata izdanih sukladno tim dokumentima.

Dokumenti i ostale informacije iz točke 2.2. ovog dokumenta objavljuju se po potrebi nakon odobrenja odgovornog tijela unutar pružatelja usluga povjerenja.

Učestalost objave CRL za certifikate koje izdaju Fina Root CA i subordinirani Fina CA-ovi 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. ovog dokumenta.

2.4. Kontrole pristupa repozitoriju

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

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

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

3. IDENTIFIKACIJA I POTVRĐIVANJE IDENTITETA

Fina Root CA i njemu subordinirani Fina CA-ovi u certifikat upisuju podatke o imenu, odnosno nazivu Subjekta za kojeg se certifikat izdaje u polje *Subject* certifikata. Razlikovno ime (engl. *Distinguished Name*, DN) u polju *Subject* u certifikatima usklađeno je s preporukom IETF RFC 5280 [14] i normom X.520.

Razlikovno ime u polju *Subject* certifikata jedinstveno je unutar Fina PKI produkcijske hijerarhije zasnovane na Fina Root CA. Jedinstvenost razlikovnog imena u certifikatima osigurava se jedinstvenim skupom podataka u polju *Subject*.

Postupak identifikacije i autentikacije ovlaštenih osoba Fina PKI s povjerljivim ulogama za potrebe Fina Root CA te postupak identifikacije i autentikacije ovlaštenih osoba Fina PKI s povjerljivim ulogama za potrebe subordiniranih Fina CA-ova opisan je u internim Fininim dokumentima.

Postupak dokazivanja posjeda privatnog ključa za Fina Root CA te privatnih ključeva za njemu subordinirane Fina CA-ove osiguran je provođenjem procedure ceremonije generiranja para ključeva za Fina Root CA i za subordinirane Fina CA-ove.

Identifikacija i autentikacija Korisnika kojima subordinirani Fina CA-ovi izdaju certifikate te dokazivanje posjeda pripadajućih privatnih ključeva opisano je u pripadajućim CPS dokumentima.

4. OPERATIVNI ZAHTJEVI NA ŽIVOTNI CIKLUS CERTIFIKATA

4.1. Podnošenje zahtjeva za izdavanje certifikata

Zahtjev za izdavanje Fina Root CA certifikata i certifikata za njemu subordinirane Fina CA-ove odobrava Uprava Fine.

Zahtjev za izdavanje certifikata za Fina OCSP servis odobrava ovlaštena osoba Fina PMA.

4.2. Obrada zahtjeva za izdavanje certifikata

Nakon odobrenja zahtjeva za izdavanje certifikata za Fina Root CA ili izdavanja subordiniranog Fina CA iz točke 4.1. ovog dokumenta ovlaštene osobe s odgovarajućim povjerljivim ulogama u Fina PKI započinju provođenje ceremonije generiranja parova ključeva i izdavanja certifikata za Fina Root CA ili subordinirani Fina CA.

4.3. Izdavanje certifikata

4.3.1. Postupci CA tijekom izdavanja certifikata

Proces izdavanja certifikata Fina Root CA provodi se prema proceduri generiranja para ključeva Fina Root CA kojom se provodi ceremonija generiranja para ključeva za Fina Root CA.

Proces izdavanja certifikata subordiniranih Fina CA-ova provode se prema proceduri generiranja para ključeva Fina CA kojom se provodi ceremonija generiranja para ključeva za subordinirane Fina CA-ove.

Izdavanje Fina Root CA certifikata i certifikata subordiniranih Fina CA-ova provodi se u CA prostoru unutar Fina PKI štićenog prostora uz sudjelovanje ovlaštenih osoba Fina PKI s povjerljivim ulogama..

4.3.2. Obavještavanje korisnika od strane CA o izdavanju certifikata

Fina Root CA certifikat i certifikati subordiniranih Fina CA-ova objavljuju se na internetskim stranicama Fina PKI repozitorija iz točke 2.2.1. ovog dokumenta.

4.4. Prihvaćanje certifikata

4.4.1. Provedba prihvaćanja certifikata

Prihvaćanje Korisničkih certifikata od strane Korisnika opisano je u pripadajućim CPS dokumentima.

4.4.2. Objava certifikata od strane CA

Fina Root CA certifikat objavljuje se na internetskim stranicama Fina PKI repozitorija iz točke 2.2.1. ovog dokumenta.

Certifikati subordiniranih Fina CA-ova objavljuju se putem javnog LDAP imenika i na internetskim stranicama Fina PKI repozitorija iz točke 2.2.1. ovog dokumenta.

Certifikati za Fina OCSP servis objavljuju se putem javnog LDAP imenika Fina repozitorija iz točke 2.2.1. ovog dokumenta.

4.4.3. Obavještavanje drugih strana od strane CA o izdavanju certifikata

Podrazumijeva se da su druge strane obaviještene o izdavanju Fina Root CA certifikata njegovim objavljivanjem na internetskim stranicama Fina PKI repozitorija iz točke 2.2.1. ovog dokumenta.

Podrazumijeva se da su druge strane obaviještene o izdavanju certifikata subordiniranih Fina CA-ova njihovom objavom putem javnog LDAP imenika i na internetskim stranicama Fina PKI repozitorija iz točke 2.2.1. ovog dokumenta.

4.5. Par ključeva i korištenje certifikata

4.5.1. Korištenje privatnog ključa i certifikata od strane korisnika

Fina Root CA certifikat i certifikati njegovih subordiniranih Fina CA-ova u ekstenziji *Key Usage* imaju postavljenu vrijednost *keyCertSign* i *CRLSign*. Privatni ključevi tih CA-ova su jedini privatni ključevi u Fina PKI kojima je dopušteno potpisivanje certifikata i CRL.

Fina je odgovorna za:

- korištenje privatnih ključeva Fina Root CA i Fina CA-ova sukladno točki 1.4. kao i dugim odredbama iz ovog dokumenta,
- propisnu zaštitu privatnih ključeva Fina Root CA i Fina CA-ova,
- trenutni prekid uporabe privatnog ključa Fina CA i postupanje sukladno točki 5.7.3. ovog dokumenta u slučaju kompromitiranja privatnog ključa Fina Root CA ili subordiniranog Fina CA.

Korištenje privatnog ključa i pripadajućeg Korisničkog certifikata od strane Korisnika opisano je u pripadajućim CPS dokumentima.

4.5.2. Korištenje javnog ključa i certifikata od strane pouzdajuće strane

Pouzdajuća strana koja namjerava ostvariti pouzdanje u Fina Root CA certifikat ili u certifikat njegovog subordiniranog Fina CA treba:

- voditi računa o primjerenoj uporabi i zabrani uporabe javnog ključa i certifikata opisanim u točki 1.4. ovog dokumenta,

- obaviti provjeru roka važenja svih certifikata u certifikacijskom lancu te provesti provjeru certifikata prema postupcima za validaciju certifikacijske staze,
- obaviti provjeru statusa opozvanosti certifikata uporabom aktualnih informacija o tim statusima na način opisan u točki 4.10.1. ovog dokumenta.

Pouzdanjem istekli ili opozvani certifikat Pouzdajuća strana gubi jamstva dobivena od Fine kao pružatelja usluge certificiranja.

Korištenje javnog ključa i certifikata od strane Pouzdajuće strane opisano je u pripadajućim CPS dokumentima.

4.6. Obnova certifikata

Svaka obnova certifikata u Fina PKI pri kojoj Fina generira par ključeva podrazumijeva izdavanje certifikata s novim parom ključeva istom Subjektu certificiranja.

Za tipove korisničkih certifikata za koje je pripadajućim općim pravilima pružanja usluga certificiranja dozvoljeno generiranje parova ključeva na korisničkoj lokaciji Fina preporuča generiranje novog para ključeva. Fina za te certifikate prihvaća i ponovnu dostavu postojećeg javnog ključa 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. ovog dokumenta.

4.7. Obnova certifikata uz generiranje novog para ključeva

Obnovu certifikata uz generiranje novog para ključeva za Fina CA može zatražiti samo ovlaštena osoba u Fina PMA.

Obnovu certifikata uz generiranje novog para ključeva za Fina CA odobrava Uprava Fine.

Nakon odobrenja obnove certifikata uz generiranje novog para ključeva za subordinirani Fina CA ovlaštene osobe s odgovarajućim povjerljivim ulogama u Fina PKI započinju provođenje ceremonije generiranja parova ključeva i izdavanja certifikata za određeni subordinirani Fina CA.

Novi certifikat Fina CA objavljuju se na Fina PKI repozitoriju iz točke 2.2.1. ovog dokumenta.

Zahtjev za obnovu certifikata uz generiranje novog para ključeva za Fina OCSP servis odobrava ovlaštena osoba Fina PMA.

Generiranje para ključeva i izdavanje certifikat za Fina OCSP servis provode ovlaštene osobe s odgovarajućim povjerljivim ulogama u Fina PKI.

Postupak obnove za certifikate Korisnika opisan je u pripadajućim CPS dokumentima.

4.8. Izmjene u certifikatu

Izmjena podataka u certifikatu za Fina Root CA i u certifikatima za njemu subordinirane Fina CA-ove se ne provode.

Izmjena podataka u Korisničkim certifikatima je postupak u kojem Korisnici podnose zahtjev za promjenu podataka koji ulaze u sadržaj certifikata.

Korisnici imaju obvezu zatražiti izmjene podataka u certifikatu u roku od 7 dana od nastalih promjena.

Subordinirani Fina CA-ovi omogućuju izmjenu podataka u Korisničkim certifikatu samo za certifikat koji nije opozvan, suspendiran ili nije istekao.

Postupak izmjene podataka u Korisničkim certifikatima opisan je u pripadajućim CPS dokumentima.

4.9. Opoziv i suspenzija certifikata

Zahtjev za opoziv CA certifikata u Fina PKI odobrava Uprava Fine.

Suspenzija CA certifikata u Fina PKI nije dozvoljena.

Odredbe vezane uz opoziv i suspenziju Korisničkih certifikata navedene su u pripadajućim CPS dokumentima.

4.9.1. Razlozi za opoziv

Fina Root CA će opozvati Fina CA certifikat u roku od sedam (7) dana:

- temeljem pisanog zahtjeva ovlaštene osobe u Fina PMA za opoziv Fina CA certifikata,
- ako Fina PMA ima saznanja da zahtjev za izdavanje Fina CA certifikata nije bio odobren te da mu retroaktivno nije dano odobrenje,
- ako Fina PMA zaprimi dokaz da je privatni ključ povezan s javnim ključem u Fina CA certifikatu kompromitiran ili ako Fina CA 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 [16],
- u slučaju da Fina PMA zaprimi dokaz o zlouporabi Fina CA certifikata,
- ako Fina PMA ima saznanja da Fina RDC 2015 CA certifikat nije izdan sukladno dokumentu CA/Browser Forum BRG [16], ili da Fina CA certifikat nije izdan sukladno ovom dokumentu, ili da Fina RDC 2015 CA nije sukladan s tim dokumentima,
- ako Fina PMA utvrdi da informacije sadržane u CA certifikatu nisu točne ili da navode na pogrešne zaključke,
- u slučaju zabranjene uporabe privatnog ključa CA,
- ako Fina procjeni da CA certifikat svojim tehničkim karakteristikama, profilom ili sadržajem ne pruža prikladnu razinu povjerenja Pouzdajućim stranama,

- ako subordinirani Fina CA ili Fina Root CA prestaje s radom, a Fina nije kod drugog pružateljem usluga povjerenja osigurala pružanje usluge opoziva Fina CA certifikata,
- u slučaju da to nalaže ovaj dokument.
- u slučajevima kada to nalaže zakon ili drugi propis.

Razlozi za opoziv Korisničkih certifikata opisani su u pripadajućim CPS dokumentima.

4.9.2. Tko može tražiti opoziv

Opoziv Fina Root CA certifikata i certifikata subordiniranog Fina CA može zatražiti samo ovlaštena osoba u Fina PMA.

4.9.3. Procedura za zahtjev za opozivom

Ovlaštene osobe s povjerljivim ulogama Službenik za sigurnost i Službenik za nadzor sustava provjeravaju cjelovitost, autentičnost i odobrenje zahtjeva za opoziv certifikata. Opoziv certifikata provode ovlaštene osobe s povjerljivim ulogama u Fina PKI u CA prostoru Fina PKI štićenog prostora.

4.9.4. Poček zahtjeva za opozivom

Nakon donošenja odluke za opoziv certifikata, zahtjev za opoziv mora biti podnesen što je prije moguće.

4.9.5. Vremenski period u kojem CA mora obraditi zahtjev za opozivom

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

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 Fina Root CA i Fina CA certifikata Pouzdajuća strana provodi provjeru statusa certifikata u cilju utvrđivanja njihove opozvanosti, a sukladno točkama 4.5.2., 4.9.9. i 4.9.10. ovog dokumenta. Ako Pouzdajućoj strani u danom trenutku nije moguće dobiti informacije o statusu certifikata, ona se ne smije pouzdati u takav certifikat.

4.9.7. Učestalost izdavanja CRL

Fina Root CA objavljuje CRL u roku od 8 sati od opoziva certifikata kojeg je izdao Fina Root CA te u roku od najviše 12 mjeseci od prethodnog izdavanja CRL. Vrijeme u kojem najkasnije mora biti izdana sljedeća CRL (vrijednost polja *Next Update*) je 12 mjeseci od zadnjeg prethodnog izdavanja CRL.

Subordinirani Fina CA izdaje CRL odmah po opozivu, suspenziji ili reaktivaciji certifikata te svakih 6 sati od prethodnog izdavanja CRL. Vrijeme u kojem najkasnije mora biti izdana sljedeća CRL (vrijednost polja *Next Update*) je 24 sata od zadnjeg prethodnog izdavanja CRL.

4.9.8. Maksimalno kašnjenje za CRL

Maksimalno kašnjenje CRL koju izdaje Fina Root CA od trenutka njenog izdavanja do trenutka njene objave iznosi do 8 sati.

Maksimalno kašnjenje CRL koje izdaju Fina CA-ovi 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 Root CA i njemu subordinirani Fina CA-ovi podržavaju *online* provjeru statusa opozvanosti certifikata putem Fina OCSP servisa koji je usklađen s preporukom IETF RFC 6960 [15].

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

Adresa Fina OCSP servisa je http://ocsp.fina.hr, a sadržana je u ekstenziji *Authority Information Access* svakog certifikata koje izdaju Fina Root CA i subordinirani Fina CA-ovi.

Fina OCSP servis će potpisati odgovor onim OCSP certifikatom kojeg je izdao Fina CA koji je izdao i Korisnički certifikat čiji se status provjerava. Odgovor za status Fina CA certifikata bit će potpisan certifikatom kojeg je OCSP servisu izdao Fina Root CA.

4.9.10. Zahtjevi na *online* provjeru statusa opozvanosti certifikata

Za korištenje Fina OCSP servisa Pouzdajuća strana treba imati aplikacijsko rješenje koje može koristiti OCSP servis iz točke 4.10.1. ovog dokumenta uporabom GET ili POST metode.

4.9.11. Ostali načini objave statusa opozvanosti certifikata

Nema odredbi.

4.9.12. Posebni zahtjevi vezani uz kompromitiranje privatnog ključa

Nema odredbi.

4.9.13. Razlozi za suspenziju

Ne primjenjuje se.

4.9.14. Tko može tražiti suspenziju

Ne primjenjuje se.

4.9.15. Procedura za zahtjev za suspenziju i reaktivaciju certifikata

Ne primjenjuje se.

4.9.16. Ograničenje na trajanje suspenzije

Ne primjenjuje se.

4.10. Usluge statusa certifikata

4.10.1. Operativna svojstva

Provjera statusa certifikata obavlja se korištenjem CRL ili Fina OCSP servisa.

CRL Fina Root CA certifikata objavljuju se internetskim stranicama Fina PKI repozitorija iz točke 2.2.1. ovog dokumenta te je izravno dostupna s adrese https://rdc.fina.hr/Root/FinaRootCA.crl.

Na internetskim stranicama Fina PKI repozitorija objavljuju se objedinjene CRL subordiniranih Fina CA-ova. Na javnom LDAP imeniku Fina PKI repozitorija objavljuju se objedinjene i segmentirane CRL subordiniranih Fina CA-ova. Adrese na kojima je objavljena CRL sadržane su u ekstenziji *CRLDistributionPoints* u svakom izdanom certifikatu.

Adresa Fina OCSP servisa je http://ocsp.fina.hr i sadržana je u ekstenziji *Authority Information Access* u svakom izdanom certifikatu.

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, usluge 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

Odredbe vezane uz prekid korištenja usluge od strane Korisnika navedene su u pripadajućim CPS dokumentima.

4.12. Sigurno skladištenje i oporavak privatnog ključa

Odredbe vezane uz sigurno skladištenje i oporavak ključa za Korisničke certifikate koje izdaju subordinirani Fina CA-ovi navedene su u pripadajućim CPS dokumentima.

5. PROVJERA SUSTAVA, UPRAVLJANJA I RADNIH POSTUPAKA

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

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

5.1. Mjere fizičke zaštite

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

5.1.1. Lokacija objekta i konstrukcija

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

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

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

Fina PKI štićeni prostor interno je podijeljen na sigurnosne zone.

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

5.1.2. Fizički pristup

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

Osobama koje nemaju ovlaštenje fizičkog pristupa sustavu certificiranja pristup je dozvoljen samo u pratnji i uz cjelovremeni nadzor ovlaštenih osoba Fina PKI uz njihovu dualnu kontrolu, a u skladu s Fininim internim procedurama. Za vrijeme boravka osoba koje nemaju ovlaštenje fizičkog pristupa sustavima u Fina PKI štićenom prostoru ne provode se postupci koji bi tim osobama mogli otkriti povjerljive informacije.

O svakom pristupu sustavima certificiranja vodi se evidencija.

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

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

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

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

5.1.3. Sustavi za napajanje i klimatizaciju

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

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

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

5.1.4. Opasnost od poplave

Oprema Fina Root CA sustava i sustava njemu subordiniranih Fina CA-ova smještena je na lokacijama koje su osigurane od poplave i smještena je na povišenim podovima.

5.1.5. Protupožarna zaštita

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

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

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

5.1.6. Pohrana medija

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

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

5.1.7. Zbrinjavanje otpada

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

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

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

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

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

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

5.1.8. Sigurnosne kopije na drugoj lokaciji

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

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

5.2. Organizacijske mjere zaštite

5.2.1. Povjerljive uloge

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

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

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

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

5.2.2. Broj osoba potrebnih za obavljanje aktivnosti

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 ovog dokumenta.

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

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

5.2.3. Identifikacija i potvrđivanje identiteta za svaku ulogu

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

Ovlaštene osobe s povjerljivim ulogama u Fina PKI moraju se autenticirati prije bilo kojeg pristupa Fina Root CA. U tu svrhu ovlaštene osobe Fina PKI dobivaju odgovarajuća sredstva za autentikaciju. Prije dobivanja sredstva za autentikaciju navedeno osoblje mora zadovoljiti zahtjeve navedene u točki 5.3. ovog dokumenta.

Sredstva za autentikaciju su:

- kartice kontrole s prolaza za ulazak u Fina PKI štićene sigurnosne zone, a dozvolu pristupa smiju dobiti samo ovlaštene osobe s povjerljivim ulogama u Fina PKI,

- certifikati na sigurnim kriptografskim uređajima koje smiju dobiti samo ovlaštene osobe u Fini s povjerljivim ulogama u Fina PKI,
- korisničko ime i zaporka ili certifikat na sigurnom kriptografskom uređaju koje smiju dobiti samo ovlaštene osobe u Fini s povjerljivim ulogama u Fina PKI,
- upravljačke kartice kriptografskog modula koje smiju dobiti samo ovlaštene osobe u Fini s povjerljivim ulogama u Fina PKI, sukladno ulogama iz točke 5.2.1. ovog dokumenta.

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

Fina Root CA sustav bilježi, sprema i čuva događaje povezane s aktivnostima prijavljene osobe.

5.2.4. Uloge koje zahtijevaju odvajanje dužnosti

Za poslove povezane uz Fina Root CA provodi se sljedeće odvajanje dužnosti:

- Službeniku za sigurnost, Službeniku za registraciju i Službeniku za opoziv certifikata ne smije ne smije biti dodijeljena uloga Službenik za nadzor sustava,
- Administratoru sustava ne smije biti dodijeljena uloga Službenika za sigurnost ili poslove Službenika za nadzor sustava.

5.3. Osoblje

5.3.1. Kvalifikacije, radno iskustvo i zahtjevi za provjerom osoblja

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

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

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

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

5.3.2. Procedure provjere prikladnosti osoblja

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

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

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

5.3.3. Zahtjevi za školovanjem

Osoblje u Fina PKI prije početka obavljanja poslova u Fina PKI, prolaze edukaciju sukladno poslovima koje će obavljati.

Fina PKI osoblju s povjerljivim ulogama u radu na Fina Root CA i Fina CA sustavima osigurava se edukacija i usavršavanje sukladno njihovim povjerljivim ulogama.

Edukacija i usavršavanje osoblja s povjerljivim ulogama u radu na Fina Root CA i Fina CA sustavima obuhvaća:

- Fina CA i Fina RA sigurnosni principi i mehanizmi,
- svjesnost o sigurnosti,
- CA softver koji je u uporabi u Fina CA sustavu,
- zadaci povezani s povjerljivim ulogama koje će obavljati na Fina CA sustavima,
- postupci oporavka od nezgode i nastavka poslovanja.

5.3.4. Periodičko obavljanje znanja i osvješćivanje

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

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

5.3.5. Učestalost i slijed izmjene zaposlenika

Ne primjenjuje se.

5.3.6. Kazne za neovlaštene radnje

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

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

5.3.7. Zahtjevi na vanjske suradnike

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

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

5.3.8. Dokumentacija koja je dostupna osoblju

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

5.4. Postupci upravljanja revizijskim zapisima

5.4.1. Tipovi događaja koji se zapisuju

Svi važni događaji u Fina Root CA sustavu zapisuju se kao revizijski zapisi u elektroničkom ili papirnatom obliku. Revizijski zapisi sadrže:

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

Fina Root CA zapisuje u elektroničkom ili papirnatom obliku revizijske zapise događaja vezanih uz:

- upravljanje životnim ciklusom ključeva Fina Root CA i ključevima povezanim s Fina Root OCSP certifikatom za Fina OCSP servis,
- upravljanje životnim ciklusom HSM modula kojim je zaštićeni privatni ključ Fina Root CA,
- izdavanje Fina Root CA certifikata i certifikata njemu subordiniranih Fina CA-ova,
- izdavanje Fina Root OCSP certifikata za Fina OCSP servis,
- opoziv certifikata koje izdaje Fina Root CA,
- pokretanje i zaustavljanje funkcije generiranja revizijskih zapisa,
- pokušaje pristupa Fina Root CA sustavu i pripadajućem HSM-u,
- sigurnosne događaje, uključujući događaje uspješnog i neuspješnog pokušaja pristupa PKI sustavu, aktivnosti na PKI i sigurnosnim sustavima podizanja i spuštanja sustava, ispada sustava i kvara hardvera, izmjene sigurnosnih postavki sustava te ulaske i izlaske i Fininih PKI štićenih prostora.

Tipovi događaja koji se zapisuju, a koji su povezani sa subordiniranim Fina CA-ovima detaljnije su opisani u pripadajućim CPS dokumentima.

5.4.2. Učestalost obrade revizijskih zapisa

Postupak pregleda revizijskih zapisa Fina Root CA sustava obuhvaća:

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

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

Preglede revizijskih zapisa Fina Root CA sustava i pripadajućeg HSM modula obavlja Službenik za nadzor sustava. Ovi pregledi revizijskih zapisa sustava obavljaju se nakon izvođenja operacija na Fina Root CA sustavu te u okviru njegove redovite provjere, a najmanje jednom godišnje. O obavljenom pregledu revizijskih zapisa vodi se evidencija u papirnatom ili elektroničkom obliku, a vodi je osoba s povjerljivom ulogom Službenik za nadzor sustava.

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

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

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

Pregled revizijskih zapisa sustava za subordinirane Fina CA-ove opisan je u pripadajućim CPS dokumentima.

5.4.3. Vremenski period pohrane revizijskih zapisa

Revizijski zapisi Fina Root CA sustava iz točke 5.4.1. čuvaju se 15 godina od isteka Fina Root CA certifikata.

5.4.4. Zaštita revizijskih zapisa

Revizijski zapisi Fina Root CA sustava zaštićuju se mehanizmima i postupcima koji osiguravaju povjerljivost i cjelovitost zapisa te ne dozvoljavaju njihovu izmjenu, kao ni jednostavno brisanje ili uništenje zapisa.

Zaštita cjelovitosti kritičnih revizijskih zapisa Fina Root CA osigurana je pri generiranju zapisa.

Povjerljivost revizijskih zapisa Fina Root CA sustava osigurava se i kontrolom pristupa sustavu i pravom za čitanje zapisa. Pristup revizijskim zapisima ograničen je na ovlašteno

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

Neposredno prije isključivanja Fina Root CA sustava revizijski zapisi se kopiraju na odgovarajući medij za arhiviranje podataka. Zaštita medija s podacima se provodi sukladno točki 5.5.3. ovog dokumenta.

Revizijski zapisi koji se vode u papirnatom obliku štite se od neovlaštenog pregleda, brisanja, izmjene ili uništenja korištenjem uobičajenim metoda za zaštitu papirnate dokumentacije.

Zaštita revizijskih zapisa za subordinirane Fina CA-ove opisane je u pripadajućim CPS dokumentima.

5.4.5. Postupci izrade sigurnosnih kopija revizijskih zapisa

Novonastali revizijski zapisi Fina Root CA sustava u elektroničkom obliku kopiraju se te se njihove kopije pohranjuju i čuvaju u sigurnosnom spremniku smještenom unutar primarnog Fina PKI štićenog prostora. Dodatno, kopije datoteka revizijskih zapisa za Fina Root CA se na medijima za pohranu podataka pohranjuju u Fina PKI štićeni prostor na sekundarnoj lokaciji, sukladno točki 5.1.8. ovog dokumenta. Kopije revizijskih zapisa Fina Root CA sustava pohranjene u Fina PKI štićenom prostoru na sekundarnoj lokaciji se, u odnosu na takve zapise na primarnoj produkcijskoj lokaciji, zaštićuju jednakom ili višom razinom zaštite.

Postupci izrade sigurnosnih kopija revizijskih zapisa za subordinirane Fina CA-ove opisani su u pripadajućim CPS dokumentima.

5.4.6. Sustav prikupljanja revizijskih zapisa (unutarnji ili vanjski)

Revizijski zapisi Fina Root CA sustava nalaze se na Fina Root CA poslužitelju te se prikupljaju 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 Fina PKI provodi se jednom godišnje. Procjena ranjivosti sustava za prepoznate javne i privatne adrese Fina PKI provodi se kvartalno. Penetracijski test za subordinirane Fina CA-ove i pripadajuće sustave provodi se jednom godišnje. Procjene rizika i ranjivosti te penetracijski test provode se i nakon značajnih promjena.

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

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

5.5. Arhiviranje zapisa

5.5.1. Tipovi arhiviranih zapisa

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

- opća pravila pružanja usluga certificiranja,
- pravilnici o postupcima certificiranja,
- sve zapise nastale provedbom ceremonije generiranja ključeva za Fina Root CA,
- sve certifikate koje izdaje Fina Root CA,
- evidencije o statusu opozvanosti certifikata koje izdaje Fina Root CA,
- revizijske zapise sustava iz točke 5.4.1. ovog dokumenta,
- relevantne zapisnike vezane uz rad i održavanje Fina Root CA,
- druge podatke i relevantnu Fininu dokumentaciju, sukladno važećim propisima.

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

Tipovi arhiviranih zapisa koji se odnose na subordinirane Fina CA-ove opisani su u pripadajućim CPS dokumentima.

5.5.2. Vremenski period arhiviranja

Svi arhivirani podaci i dokumentacija vezana uz Fina Root CA čuva se 15 godina od isteka Fina Root CA certifikata.

5.5.3. Zaštita arhive

Arhivirani podaci i dokumentacija zaštićuju se mehanizmima i postupcima razine sigurnosti koja osigurava povjerljivost i cjelovitost arhive. Arhiva se štiti od neovlaštenog pregleda, modificiranja, oštećenja i brisanja.

Arhivirani zapisi u elektroničkom obliku iz točke 5.5.1. ovog dokumenta čuvaju se na odgovarajućim medijima za arhiviranje podataka u Fina PKI štićenom prostoru. Arhivirani zapisi štite se mehanizmima i postupcima koji osiguravaju povjerljivost i cjelovitost zapisa. Povjerljivost arhiviranih zapisa u elektroničkom obliku osigurava se pohranom medija u

sigurnosnom spremniku, a cjelovitost zapisa uporabom medija koje ne dozvoljavaju izmjenu i brisanje zapisa.

Arhivirani podaci i dokumentacija dostupni su samo ovlaštenim osobama.

Minimalno jednom godišnje Fina PKI osoblje provjerava integritet arhive, te ako je arhiva oštećena, ona se obnavlja pomoću sigurnosne kopije.

Zaštita arhive koja se odnosi na subordinirane Fina CA-ove opisana je u pripadajućim CPS dokumentima.

5.5.4. Postupci izrade sigurnosnih kopija arhive

Sigurnosne kopije arhiviranih zapisa u elektroničkom obliku iz točke 5.5.1. ovog dokumenta čuvaju se u sekundarnom Fina PKI štićenom prostoru na pričuvnoj lokaciji koji ima jednaku ili višu razinu zaštite u odnosu na Fina PKI štićeni prostor na primarnoj lokaciji.

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

5.5.5. Zahtjevi na zaštitu zapisa vremenskim žigom

Nema odredbi.

5.5.6. Sustav prikupljanja arhivskih zapisa (unutarnji ili vanjski)

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

Dokumentacija Fina Root CA sustava u papirnatom obliku prikuplja se manualno i arhivira se interno.

Zapisi u elektroničkom obliku iz točke 5.5.1. ovog dokumenta prikupljaju se ručno te se arhiviraju interno u Fina PKI štićenom prostoru na primarnoj lokaciji te u sekundarnom Fina PKI štićenom prostoru na pričuvnoj lokaciji.

5.5.7. Postupci dobivanja i provjere arhiviranih zapisa

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

Cjelovitost arhiviranih zapisa Fina Root CA osigurana je korištenjem medija za arhiviranje podataka koji onemogućuje izmjene ili brisanje nakon zapisivanja.

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

5.6. Promjena CA ključa

Radi potrebe osiguranja kontinuiteta pružanja usluge izdavanja certifikata Fina će dovoljno vremena prije isteka CA certifikata, generirati novi par ključeva za Fina CA. Također, Fina 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.

Novi certifikat Fina CA s novo generiranim javnim ključem potpisuje se privatnim ključem Fina Root CA. Novi certifikat Fina CA dostupan je sudionicima Fina PKI putem javnog imenika i internetskih stranica repozitorija.

Novi certifikat Fina CA dostavit će se Korisnicima i Pouzdajućim stranama na način na koji se dostavlja postojeći Fina CA certifikat, sukladno točki 6.1.4. ovog dokumenta.

5.7. Oporavak od kompromitiranja ili nepogode

5.7.1. Postupci u slučaju incidenta ili kompromitiranja

Fina ima Plan kontinuiteta poslovanja Fina PKI kojim su regulirani postupci u slučajevima:

- prirodnih katastrofa,
- napada, pljački ili blokade zgrade,
- uništenja IT infrastrukture na primarnoj produkcijskoj lokaciji,
- nedostupnost IT infrastrukture na primarnoj produkcijskoj lokaciji uslijed kvara hardvera ili softvera većih razmjera,
- nedostupnosti radnika,
- prekida usluga dobavljača,
- za događaje gubitka ili kompromitiranja ili sumnje u kompromitiranost privatnog ključa Fina Root CA,
- internim planovima obuhvaćeni su i postupci koje treba poduzeti u cilju oporavka i uspostave prvotnih sigurnosnih prilika RA sustava, arhive i repozitorija.

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

Obavještavanje u slučaju kompromitiranja ili sumnje u kompromitiranost privatnog ključa Fina Root CA opisano je u točki 5.7.3. ovog dokumenta.

Plan kontinuiteta poslovanja revidira se jednom godišnje.

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

Fina Root CA sustav certificiranja zasnovan je na pouzdanim hardverskim i softverskim komponentama. Funkcionalnost, ispravnost rada i otklanjanje oštećenja komponenti sustava osigurano je kroz ugovore o podršci i održavanju s dobavljačima opreme.

Plan kontinuiteta poslovanja za Fina PKI regulira postupke oporavka sustava u slučaju kvara ili oštećenja opreme te povrat podataka. Pri oporavku Fina Root CA sustava koriste se sigurnosne kopije elektroničkih zapisa.

5.7.3. Postupci u slučaju kompromitiranja privatnog ključa

U slučaju kompromitiranja privatnog potpisnog ključa Fina Root CA ili njemu subordiniranih Fina CA-ova Fina će odmah po saznanju prekinuti s uporabom kompromitiranog privatnog ključa Fina CA te će ispitati okolnosti kompromitiranja ključa. Ako se potvrdi kompromitiranje ključa Fina donosi odluku o opozivu CA certifikata povezanog s kompromitiranim ključem te svih certifikata koje je izdao taj CA. Fina će obavijestiti sudionike da se u takvom slučaju podacima o opozvanosti ne mora nužno vjerovati.

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

- Fina RA mrežu i vanjske ugovorene RA,
- Korisnike,
- Pouzdajuće strane.

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

Fina će za Fina CA čiji je privatni ključ kompromitiran organizirati ceremoniju generiranja novog para CA ključeva i izdavanje CA certifikata.

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 i vanjske ugovorene RA,
- 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 te će o njima i rokovima obavijestiti Korisnike i Pouzdajuće strane te će provest odgovarajuće aktivnosti u cilju nastavka pružanja usluge Korisnicima.

5.7.4. Mogućnost nastavka poslovanja nakon katastrofe

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 sekundarnom sustavu certificiranja do oporavka svojeg primarnog produkcijskog sustava.

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

5.8. Prestanak rada CA ili RA

U slučaju prestanka rada vanjskog ugovorenog RA raskida se ugovor između Fine i vanjskog RA te se ukidaju sva ovlaštenja vanjskog RA, uključujući ovlaštenja Službenika za registraciju, Službenika za opoziv certifikata u vanjskom RA te sva ovlaštenja vanjskog RA za dostavu zahtjeva za izdavanje, opoziv suspenziju i reaktivaciju certifikata u Fina PKI sustav. Poslove ugovorenog RA koji prestaje s radom može preuzeti Fina RA mreža. Detaljnije odredbe vezane uz prekid rada vanjskog ugovorenog RA određuju se ugovorom.

O planiranom prestanku pružanja usluga certificiranja 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 certificiranja,
- za svaki vanjski RA raskinuti ugovor između Fine i vanjskog RA te time ukinuti sva ovlaštenja vanjskog RA sukladno opisu navedenom prethodno u ovoj točki,
- uložiti sav napor da kod drugog kvalificiranog pružatelja usluga povjerenja osigura nastavak pružanja usluga certificiranja te će tom pružatelju usluga dostaviti svu dokumentaciju prikupljenu u postupku registracije Korisnika kao i svu dokumentaciju o izdanim certifikatima,
- opozvati Korisničke certifikate i uništiti privatne ključeve Korisnika u slučajevima kad Fina čuva i upravlja Korisničkim ključevima,
- opozvati certifikate Fina CA-ova koji prestaju s radom te uništiti pripadajuće privatne ključeva tih CA-ova.

U slučaju prestanka pružanja usluga certificiranja Fina će arhivirati, zaštititi i čuvati zapise prema odredbama iz točke 5.5. ovog dokumenta i odredbama drugih važećih CPS dokumenata 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 Root CA, njemu subordinirane CA-ove i za Fina OCSP servis.

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

6.1. Generiranje i instalacija para ključeva

6.1.1. Generiranje para ključeva

Postupak generiranja para ključeva za Fina Root CA provodi se formalnom ceremonijom generiranja para ključeva za Fina Root CA, a postupak generiranja parova ključeva za subordinirane Fina CA-ove provodi se formalnom ceremonijom generiranja parova ključeva za subordinirane Fina CA-ove. U ovim ceremonijama generiranja parova ključeva sudjeluju ovlaštene osobe Fina PKI s povjerljivim ulogama.

Ceremoniji generiranja para ključeva za Fina Root CA prisustvuje Kvalificirani ocjenitelj. Također, Kvalificirani ocjenitelj može prisustvovati ceremoniji generiranja parova ključeva za FINA CA. Kvalificirani ocjenitelj svjedoči da je ceremonija generiranja parova ključeva navedenih CA-ova provedena u skladu s Fininom dokumentacijom, u skladu sa zahtjevima dokumenata CA/Browser Forum BRG [16] i CA/Browser Forum EVCG [17] te u skladu s mjerama tehničke sigurnosti prema normama ETSI EN 319 411-1 [8] i ETSI EN 319 411-2 [9].

Kriptografski algoritmi koji se koriste za generiranje ključeva kao i duljina ključeva za Fina Root CA i njemu subordinirane Fina CA-ove odabrani su sukladno normizacijskom dokumentu ETSI TS 119 312 [11] tako da budu prikladni za cijelo vrijeme važenja CA certifikata.

Par ključeva za Fina Root CA te parovi ključeva za njemu subordinirane Fina CA-ove generiraju se, uz minimalno dualnu kontrolu ovlaštenih osoba s povjerljivim ulogama u Fina PKI, u HSM modulima koji zadovoljavaju zahtjeve iz točke 6.2.1. ovog dokumenta.

Fina Root CA i njemu subordinirani Fina CA-ovi nalaze se tijekom i nakon ceremonije generiranja parova ključeva u Fina PKI štićenom, a pristup ovim CA-ovima dopušten je ovlaštenim osobama Fina PKI s povjerljivim ulogama, uz minimalno dualnu kontrolu.

Ceremonija generiranja para ključeva za Fina Root CA ili za njemu subordinirane Fina CA-ove se provodi prema protokolu za generiranje ključeva u kojem su dokumentirani koraci koji se izvode za vrijeme pojedine ceremonije.

Provođenje postupka ceremonije generiranja para ključeva za Fina Root CA se snima i provođenju postupka svjedoči Kvalificirani ocjenitelj.

Provođenje postupka ceremonije generiranja para ključeva za subordinirane Fina CA-ove se snima ili provođenju postupka svjedoči Kvalificirani ocjenitelj.

Fina posjeduje izvješće Kvalificiranog ocjenitelja koje svjedoči da je postupak generiranja parova ključeva za Fina Root CA te parova ključeva za njemu subordinirane Fina CA-ove proveden sukladno zahtjevima protokola.

Par ključeva za Fina Root CA generira se u HSM-u za Fina Root CA. Fina Root CA je zajedno s pripadajućim HSM-om cijelo vrijeme izdvojen od računalne mreže (*offline*).

Generiranje para ključeva za potpis odgovora OCSP servisa provodi se na u HSM modulu koji zadovoljava zahtjeve iz točke 6.2.1. ovog dokumenta, a koji je smješten u Fina PKI štićenom prostoru i kojemu se pristupa uz dualnu kontrolu ovlaštenih osoba Fina PKI.

O provedenom postupku ceremonije generiranju para ključeva za Fina Root CA te parova ključeva za njemu subordinirane Fina CA-ove vode se zapisnici koje potpisuju ovlaštene osobe Fina PKI koje su sudjelovale u postupku ceremonije te Kvalificirani ocjenitelj, sukladno popisu u prilogu dokumenta ceremonije.

6.1.2. Dostava privatnog ključa korisniku

Fina Root CA ne izdaje Korisničke certifikate.

Dostava privatnih Korisničkih ključeva povezanih s Korisničkim certifikatima koje izdaju subordinirani Fina CA-ovi opisana je u pripadajućim CPS dokumentima.

6.1.3. Dostava javnog ključa CA-u

Dostava javnih ključeva subordiniranih Fina CA-ova u Fina Root CA regulirana je i opisana u ceremoniji generiranja parova ključeva za Fina CA-ove.

Dostava javnih Korisničkih ključeva povezanih s Korisničkim certifikatima koje izdaju subordinirani Fina CA-ovi opisana je u pripadajućim CPS dokumentima.

6.1.4. Dostava javnog ključa CA pouzdajućim stranama

Javni ključevi Fina Root CA Fina i njemu subordiniranih Fina CA-ova su u pripadajućim certifikatima objavljni na internetskim stranicama Fina PKI repozitorija iz točke 2.2.1. ovog dokumenta te su tako dostupni svim Pouzdajućim stranama. Izvornost certifikata osigurava se njihovim preuzimanjem uporabom HTTPS protoklola. Internetske adrese za izravno preuzimanje Fina Root CA certifikata i certifikate njemu subordiniranih Fina CA-ova su:

- Fina Root CA: https://rdc.fina.hr/Root/FinaRootCA.cer
- Fina RDC 2015 CA: https://rdc.fina.hr/RDC2015/FinaRDCCA2015.cer
- Fina RDC-TDU 2015 CA: http://rdc.fina.hr/RDC-TDU2015/FinaRDC-TDUCA2015.cer

Izvornost certifikata dostavljenim drugim kanalima može se utvrditi i usporedbom njihovih SHA sažetaka (*fingerprint)* sa sažecima objavljenim na na internetskim stranicama Fina PKI repozitorija iz točke 2.2.1. ovog dokumenta, uz korištenje HTTPS protokola.

6.1.5. Duljine ključeva

Duljine ključeva u Fina PKI su sljedeće:

- Fina Root CA upotrebljava sha256WithRSA algoritam s ključem duljine 4096 bita,
- Fina CA-ovi upotrebljavaju sha256WithRSA algoritam s ključem duljine 4096 bita,
- Fina OCSP servis upotrebljava RSA ključeve duljine 2048 bita,
- Fina QTSA servis upotrebljava RSA ključ duljine 2048 bita,
- Korisnici upotrebljavaju RSA ključeve duljine 2048 bita.

6.1.6. Generiranje i provjera kvalitete parametara javnog ključa

Ključevi koje upotrebljava Fina Root CA i ključevi koje upotrebljavaju njemu subordinirani Fina CA-ovi generiraju se sukladno normizacijskom dokumentu ETSI TS 119 312 [11].

Ključevi koje upotrebljava Fina OCSP servis generiraju se sukladno normizacijskom dokumentu ETSI TS 119 312 [11].

Generiranje i provjera kvalitete javnih ključeva koje upotrebljavaju Korisnici provodi se na način opisan u pripadajućim CPS dokumentima.

6.1.7. Namjene ključeva

Fina Root CA i njemu subordinirani Fina CA-ovi koriste privatne potpisne ključeve samo za potpisivanje izdanih certifikata i odgovarajuće CRL. U ekstenziji *Key Usage* te imaju postavljene bitove za *keyCertSign, cRLSign*.

Privatni ključevi Fina OCSP servisa namijenjeni su samo za potpisivanje odgovora Fina OCSP servisa. U ekstenziji *Key Usage* ima postavljene bitove za *digitalSignature* i *nonRepudiation*, a u ekstenziji *extKeyUsage* postavljenu vrijednost *OCSPSigning*.

Namjene ključeva za Korisničke certifikate opisane su u pripadajućim CPS dokumentima.

6.2. Zaštita privatnog ključa i tehnike upravljanja kriptografskim modulom

6.2.1. Norme i tehničke mjere zaštite kriptografskog modula

Privatni ključ za Fina Root CA generira se i štiti HSM modulom koji zadovoljava zahtjeve norme FIPS 140-2 [12] razina 3. Fina Root CA s pripadajućim HSM-om cijelo je vrijeme izdvojen od računalne mreže (*offline*).

Privatni ključevi za subordinirane Fina CA-ove generiraju se i štite HSM-om koji zadovoljava zahtjeve norme FIPS 140-2 [12] razina 3.

Privatni ključevi za Fina OCSP servis generiraju se i štite HSM-om koji zadovoljava zahtjeve norme FIPS 140-2 [12] razina 3.

Norme i upravljačke funkcije kriptografskog modula u kojem se generiraju privatni ključevi Korisnika opisani su u pripadajućim CPS dokumentima.

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

HSM kojim se štiti privatni ključ Fina Root CA te HSM-ovi kojim se štite privatni ključevi subordiniranih CA-ova smješteni su u CA prostoru Fina PKI štićenog prostora. Fizički pristup ovim HSM-ovima provodi se uz dualnu kontrolu ovlaštenih osoba s povjerljivim ulogama u Fina PKI. Upravljanje privatnim ključem Fina Root CA i privatnim ključevima njemu subordiniranih Fina CA-ova provodi se fizičkim pristupom HSM-u, uz autorizaciju dvije ovlaštene osobe s povjerljivim ulogama u Fina PKI.

HSM-ovi kojim se štite privatni ključevi Fina OCSP servisa smješteni su u CA prostoru Fina PKI štićenog prostora. Fizički pristup ovim HSM-ovima provodi se uz dualnu kontrolu ovlaštenih osoba s povjerljivim ulogama u Fina PKI. Upravljanje privatnim ključevima Fina OCSP servisa provodi se fizičkim pristupom HSM-u, uz autorizaciju dvije ovlaštene osobe s povjerljivim ulogama u Fina PKI.

Dualna kontrola potrebna za autorizaciju upravljanja privatnim ključevima na HSM-ovima temelji se na principu n od m za pojedini Fina PKI štićeni prostor.

6.2.3. Sigurno skladištenje privatnog ključa

Sigurno skladištenje privatnih ključeva za Fina Root CA i njemu subordiniranih Fina CA-ova Fine ne primjenjuje se.

Sigurno skladištenje privatnih ključeva za Fina OCSP servisa ne primjenjuje se.

Sigurno skladištenje Korisničkih privatnih ključeva provodi se samo za određene tipove Korisničkih nekvalificiranih certifikata, sukladno opisu u $CPS_{NQC\text{-}Non\text{-}eIDAS}$ [27] dokumentu.

6.2.4. Sigurnosno kopiranje privatnog ključa

Sigurnosno kopiranje privatnog ključa Fina Root CA provodi se u CA prostoru Fina PKI štićenog prostora pod dualnom kontrolom od strane ovlaštenih osoba s povjerljivim ulogama u Fina PKI. Privatni ključ Fina Root CA kopira se iz HSM-a isključivo u enkriptiranom obliku na magnetske trake koje ne omogućavaju izmjenu i brisanje zapisa, a čuvaju se u sigurnosnim spremnicima unutar Fina PKI štićenih prostora na primarnoj i sekundarnoj lokaciji. Ne postoje druge sigurnosne kopije privatnog ključa Fina Root CA.

Sigurnosno kopiranje privatnih ključeva subordiniranih Fina CA-ova provodi se u CA prostoru Fina PKI štićenog prostora, pod dualnom kontrolom od strane ovlaštenih osoba s povjerljivim ulogama u Fina PKI. Privatni Fina CA ključ se izvan HSM modula nalazi isključivo u enkriptiranom obliku te se u tom obliku kopira i čuva u CA prostoru unutar Fina PKI štićenih prostora na odvojenim lokacijama.

Fizički pristup sigurnosnim kopijama privatnih ključeva Fina Root CA i njemu subordiniranih Fina CA-ova imaju isključivo ovlaštene osobe s povjerljivim ulogama u Fina PKI pod dualnom kontrolom.

Sigurnosne kopije privatnih ključeva Fina Root CA i njemu subordiniranih Fina CA-ova zaštićene su mjerama koje pružaju jednaku ili višu razinu sigurnosti u odnosu na privatni ključ u uporabi.

Ne postoje druge kopije privatnih ključeva Fina Root CA i njemu subordiniranih Fina CA-ova, osim navedenih.

Za sigurnosne kopije privatnih ključeva Fina OCSP servisa vrijede ista pravila kao za subordinirane Fina CA-ove.

6.2.5. Arhiviranje privatnog ključa

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

Privatni ključevi Fina OCSP servisa se ne arhiviraju.

Ovi privatni ključevi uništavaju se sukladno točki 6.2.10. ovog dokumenta.

6.2.6. Prijenos privatnog ključa

Za vrijeme dok je izvan HSM modula privatni ključ Fina Root CA je zaštićen enkriptiranjem. Enkriptiranje privatnog ključa Fina Root CA provodi se strogim pridržavanjem zahtjeva navedenih u certifikacijskoj dokumentaciji HSM modula te se time osigurava jednaka razina sigurnosti privatnog ključa kao i kad se ključ nalazi u HSM modulu. Prijenos privatnog ključa Fina Root CA iz HSM modula autoriziraju ovlaštene osobe s povjerljivim ulogama u Fina PKI, uz dualnu kontrolu unutar CA prostora Fina PKI štićenog prostora.

Jednak postupak uz jednake uvjete provodi se i za prijenos privatnih ključeva Fina CA-ova iz HSM modula.

Za prijenos privatnog ključa Fina Root CA ili njemu subordiniranih Fina CA-ova u HSM modul mora se osigurati da se privatni ključ prenosi samo u kriptografski modul jednake ili više razine sigurnosti u odnosu na kriptografski modul iz kojega je privatni ključ prenosi.

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

6.2.7. Spremanje privatnog ključa u kriptografskom modulu

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

Privatni ključevi Fina OCSP servisa zaštićeni su HSM modulima i mogu se koristiti jedino ako su propisno aktivirani.

6.2.8. Metoda aktivacije privatnog ključa

Aktivaciju privatnog ključa Fina Root CA i aktivaciju privatnih ključeva subordiniranih Fina CA-ova provode dvije ovlaštene osobe s povjerljivim ulogama u Fina PKI. Svaka od ovih ovlaštenih osoba za aktivaciju HSM-a upotrebljava pripadajuću smart karticu za HSM i pripadajući PIN.

Aktivacija privatnih ključeva Fina Root CA i aktivacija privatnih ključeva Fina CA-ova temelji se na principu n od m.

Aktivacija privatnih ključeva Fina OCSP servis obavlja se na jednak način kao i aktivacija privatnih ključeva Fina CA-ova.

6.2.9. Metoda deaktivacije privatnog ključa

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

Privatni ključ Fina Root CA deaktivira se:

- zaustavljanjem CA serverskog procesa,
- isključenjem napajanja Fina Root CA servera, a time i napajanja HSM-a.

Deaktivacija privatnih ključeva subordiniranih Fina CA-ova, provodi se kada postoji neposredan zahtjev za privremenim obustavljanjem aktivnosti sustava, u slučajevima isteka perioda važenja privatnog ključa te u slučaju opoziva pripadajućeg certifikata.

Privatni ključevi subordiniranih Fina CA-ova deaktiviraju se:

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

Privatni ključevi Fina OCSP servisa deaktiviraju se u istim slučajevima i na isti način kao i privatni ključevi subordiniranih Fina CA-ova, uz zaustavljanje OCSP servisa.

6.2.10. Metoda uništavanja privatnog ključa

Postupak uništavanja privatnih ključeva Fina Root CA i postupak uništavanje privatnih ključeva Fina CA-ova provodi se nakon isteka perioda njihovog važenja, zbog kompromitiranja ili sumnje u kompromitiranost privatnog ključa, ili zbog prestanka njegova korištenja, a provode ga ovlaštene osobe s povjerljivim ulogama u Fina PKI. Postupkom uništavanja privatnog Fina Root CA ključa ili privatnog ključa Fina CA trajno su onesposobljene sve sigurnosne kopije tog privatnog ključa te ih više nije moguće upotrijebiti.

Uništavanje privatnog ključa Fina Root CA i uništavanje privatnih ključeva Fina CA-ova provodi se uz prisutnost osoba s povjerljivim ulogama u Fina PKI.

Uništavanje privatnih ključeva za odgovora Fina OCSP servisa provodi se na jednak način kao i uništavanje privatnih ključeva Fina CA-ova.

6.2.11. Ocjena kriptografskog modula

Ocjena HSM modula za Fina Root CA i HSM modula za Fina CA-ove provodi se sukladno zahtjevima opisanim u točki 6.2.1. ovog dokumenta.

Ocjena HSM modula za Fina OCSP servis provodi se na isti način kao i ocjena HSM modula za Fina CA-ove.

6.3. Ostali vidovi upravljanja parom ključeva

6.3.1. Arhiviranje javnog ključa

Javni ključevi Fina Root CA kao i javni ključevi njemu subordiniranih Fina CA-ova arhiviraju se na način da se arhiviraju certifikati koji su izdani za te javne ključeve. Arhiviranje certifikata se provodi sukladno točkama 5.5.3. i 5.5.4. ovog dokumenta.

Certifikat za Fina Root CA čuva se u arhivi na rok iz točke 5.5.2. ovog dokumenta.

Rok arhiviranja certifikata za subordinirane Fina CA-ove te rok arhiviranja certifikata za Fina OCSP servis je najmanje 10 godina od prestanka valjanosti certifikata.

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

6.3.2. Vremenski period važenja certifikata i korištenja para ključeva

Rok važenja certifikata definiran u Tablici 6.1.

Certifikat	Rok
Fina Root CA	20 godina
Fina RDC 2015 i Fina RDC-TDU 2015 CA-ovi	10 godina
Certifikati za potpis odgovora Fina OCSP servisa	12 mjeseci

Tablica 6.1. Rokovi uporabe certifikata

Fina CA certifikati se izdaju s vremenom važenja koje ne prelazi perioda važenja Fina Root CA certifikata.

Vremenski period važenja privatnog CA ključa jednak je vremenskom periodu važenja pripadajućeg certifikata. Pripadajući privatni ključevi CA certifikata ne smiju se upotrebljavati nakon isteka roka važenja certifikata ili nakon opoziva certifikata.

6.4. Aktivacijski podaci

6.4.1. Generiranje i instalacija aktivacijskih podataka

Aktivacijski podaci za privatni ključ Fina Root CA generiraju se i instaliraju prilikom provođenja formalne ceremonije generiranja para ključeva za Fina Root CA. Aktivacijski podaci instaliraju se na pripadajuće upravljačke kartice kriptografskog modula koje se koriste za aktivaciju privatnog ključa Fina Root CA na principu n od m , sukladno točki 6.2.2. ovog dokumenta.

Aktivacijski podaci za privatni ključ pojedinog subordiniranog Fina CA generiraju se i instaliraju prilikom provođenja formalne ceremonije generiranja para ključeva za Fina CA. Aktivacijski podaci instaliraju se na pripadajuće upravljačke kartice kriptografskog modula koje se koriste za aktivaciju privatnog ključa subordiniranog Fina CA na principu n od m, sukladno točki 6.2.2. ovog dokumenta.

Aktivacijski podaci za privatne ključeve Fina OCSP servisa generiraju se i instaliraju prilikom postupka generiranja pripadajućeg para ključeva. Aktivacijski podaci postavljaju se na pripadajuće upravljačke kartice kriptografskog modula koje se koriste za aktivaciju privatnog ključa Fina OCSP servisa na principu n od m , sukladno točki 6.2.2. ovog dokumenta.

Podaci za upravljačke kartice kriptografskog modula generiraju se u Fina PKI štićenom prostoru pod nadzorom ovlaštenih osoba s povjerljivim ulogama u Fina PKI.

6.4.2. Zaštita aktivacijskih podataka

Aktivacijski podaci za privatni ključ Fina Root CA i aktivacijski podaci za privatne ključeve subordiniranih Fina CA-ova iz točke 6.4.1. ovog dokumenta koji su smješteni na pripadajuće upravljačke kartice kriptografskog modula zaštićeni su pripadajućim zaporkama koje u Fina PKI štićenom prostoru generiraju nositelji tih kartica. Upravljačke kartice kriptografskog modula dodjeljuju se ovlaštenim osobama s povjerljivim ulogama u Fina PKI. Upravljačke kartice kriptografskog modula i pripadajuće zaporke čuvaju se odvojeno u sigurnosnim spremnicima pojedinog Fina PKI štićenog prostora.

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

6.4.3. Ostale odredbe o aktivacijskim podacima

Nema odredbi.

6.5. Upravljanje računalnom sigurnošću

6.5.1. Posebni tehnički zahtjevi na računalnu sigurnost

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

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

Fina provodi odvajanje dužnosti i odgovornosti za povjerljive uloge osoblja u Fina PKI, sukladno točki 5.2.4. ovog dokumenta.

Identifikacija i potvrđivanje identiteta za svaku povjerljivu ulogu u Fina PKI provodi se korištenjem odgovarajućih sredstava za autentikaciju sukladno točki 5.2.3. ovog dokumenta.

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

Provodi se test CA softvera u cilju provjere njegove autentičnosti i cjelovitosti.

Dodatne odredbe povezane uz Fina CA sustave za izdavanje Korisničkih certifikata mogu biti navedene u pripadajućim CPS dokumentima.

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]. Sukladnost se potvrđuje certifikatom izdanim od strane neovisnog certifikacijskog tijela.

6.6. Tehničke kontrole životnog ciklusa

Softver kojeg koristi Fina Root CA 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.

Softver kojeg koristi Fina Root CA obavlja periodičku provjeru integriteta baze podataka kojom se provjerava konzistentnosti podataka u bazi. Fina Root CA provodi provjeru integriteta svojih revizijskih zapisa sustava.

Pri pokretanju HSM modula provodi se automatska provjera njegovog integriteta.

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

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

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

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

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

Dodatne odredbe povezane uz Fina CA sustave za izdavanje Korisničkih certifikata mogu biti navedene su u pripadajućim CPS dokumentima.

6.7. Provjera mrežne sigurnosti

Fina Root CA je zajedno s pripadajućim HSM-om cijelo vrijeme izdvojen od računalne mreže (*offline*).

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.

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

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

Fina Root CA sustav i sustavi Fina CA-ova posebno su sigurnosno podešeni i očvršćeni.

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

Dodatne odredbe povezane uz Fina CA sustave za izdavanje Korisničkih certifikata mogu biti navedene su u pripadajućim CPS dokumentima.

6.8. Uporaba vremenskog žiga

Vremenski žig se ne upotrebljava u opsegu usluga povjerenja iz ovog dokumenta.

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

Revizijski zapisi Fina Root CA 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

U ovom poglavlju opisana su pravila i smjernice za profile certifikata koje Fina PKI primjenjuje pri izdavanju certifikata, CRL i OCSP odgovora od strane Fina Root CA.

Opis profila certifikata, CRL i odgovora OCSP servisa koje izdaju subordinirani Fina CA-ovi opisan je u pripadajućim CPS dokumentima.

7.1. Profil certifikata

Profil Fina Root CA certifikata i profil certifikata koje Fina Root CA izdaje za subordinirane Fina CA-ove usklađeni su s CA/Browser Forum BRG [16] i CA/Browser Forum EVCG [17] dokumentima.

Profil certifikata koje Fina Root CA izdaje za potpisivanje OCSP odgovora usklađen je s preporukama IETF RFC 5280 [14], i IETF RFC 6960 [15].

7.1.1. Broj(evi) verzije

Certifikati su sukladni verziji 3 prema X.509 specifikaciji.

7.1.2. Ekstenzije certifikata

Dokument s opisom profila Fina Root CA certifikata, certifikata subordiniranih Fina CA-ova te profilom certifikata kojim Fina OCSP servis potpisuje odgovore za certifikate koje izdaje Fina Root CA dostupan je na internetskim stranicama Fina repozitorija iz točke 2.2.1. ovog dokumenta te izravno putem internetske adrese: https://rdc.fina.hr/dokumentacija/Profili_certifikata_eIDAS.pdf.

7.1.3. Identifikator objekta (OID) algoritama

Algoritmi s pripadajućim OID identifikatorima za Fina Root CA certifikat, za certifikate njemu subordiniranih Fina CA-ova, za certifikat Fina OCSP servisa te za sve certifikate koji se izdaju u Fina PKI produkcijskoj hijerarhiji zasnovanoj na Fina Root 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

Fina Root CA, njemu subordinirani Fina CA-ovi, certifikat Fina Root OCSP servisa te svi certifikati koji se izdaju u Fina PKI produkcijskoj hijerarhiji zasnovanoj na Fina Root CA u

polju *Issuer* i *Subject* sadrže puno razlikovno ime (*Distinguished name*) izdavatelja certifikata, odnosno Subjekta certificiranja. U Tablici 7.2 prikazani su oblici naziva Subjekta certificiranja u polju *Subject* certifikata za Fina Root CA, certifikata za njemu subordinirane Fina CA-ove i certifikat za Fina OCSP servisa kojim se potpisuju odgovori za certifikate koje izdaje Fina Root CA.

Polje	Atribut	Vrijednost
Subject za Funa Root CA certifikat	commonName	Fina Root CA
	organizationName	Financijska agencija
	countryName	HR
Subject za certifikate subordiniranih Fina CA-ova	commonName	Fina RDC 2015, ili Fina RDC-TDU 2015
	organizationName	Financijska agencija
	countryName	HR
Subject za certifikat Fina OCSP servisa	commonName	Fina Root OCSP
	organizationName	Financijska agencija
	countryName	HR

Tablica 7.2. Oblici naziva Subjekta certificiranja

7.1.5. Ograničenja u nazivima

Ne koristi se.

7.1.6. Identifikator objekta (OID) općih pravila certificiranja

Identifikator objekta (OID) općih pravila certificiranja ne koristi se u Fina Root certifikatu.

Identifikator objekta (OID) općih pravila certificiranja u certifikatima Fina CA-ova je: 1.3.124.1104.5.2.1.

7.1.7. Uporaba ekstenzije *Policy Constraints*

Ne koristi se.

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 općih pravila 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 Root CA i subordinirani Fina CA-ovi sukladan je preporuci IETF RFC 5280 [14].

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 u CRL listi koju izdaje Fina Root CA definirane su u Tablici 7.3.

Ekstenzije	Kritično	Vrijednost
crlExtensions		
cRLNumber	NE	Jednolično rastući serijski broj CRL duljine do 20 okteta.
AuthorityKeyIdentifier	NE	SHA-1 hash vrijednost duljine 160 bita
crlEntryExtensions		
reasonCode	NE	Kod razloga opoziva certifikata

Tablica 7.3. Ekstenzije CRL liste i elemenata CRL liste

7.3. OCSP profil

Profil odgovora Fina OCSP servisa sukladan je s preporukom IETF RFC 6960 [15].

7.3.1. Broj(evi) verzije

Profil odgovora Fina OCSP servisa sukladan je verziji 1 prema IETF RFC 6960 [15].

7.3.2. OCSP ekstenzije

Ekstenzije odgovora Fina OCSP servisa prikazane su u Tablici 7.4.

Ekstenzije	Kritično	Vrijednost
Nonce	NE	Vrijednost Nonce iz zahtijeva za status certifikata.
Extended Revoked Definition	NE	Kod razloga opoziva certifikata (*Reason code*)

Tablica 7.4. Ekstenzije odgovora Fina OCSP servisa

8. PROVJERA SUKLADNOSTI

Nadzor nad radom Fine kao kvalificiranog 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.

Fina ima implementiran sustav upravljanja kvalitetom prema normi ISO 9001 [6] te se nalazi u certifikacijskom ciklusu čime dokazuje da ispunjava zahtjeve te norme, da ima dokumentiran sustav, definirane ovlasti, odgovornosti te opisane procese.

Također, Fina ima uspostavljen, kontinuirano nadziran, certificiran i prema poslovnim potrebama unaprjeđivan vlastiti sustav informacijske sigurnosti u skladu sa normom ISO/IEC 27001 [5].

8.1. Učestalost ili okolnosti provjere usklađenosti

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

Vanjske i interne provjere sukladnosti provode se ovisno o vrsti usluge povjerenja, a sukladno opisu u pripadajućim CPS dokumentima.

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 [10].

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

- odredbi norme ETSI EN 319 411-2 [9],
- PKI područja te područja informacijske sigurnosti,
- zakonske regulative iz područja pružanja usluga povjerenja.

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

8.3. Odnos ocjenitelja s 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.

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

8.5. Mjere u slučaju nesukladnosti

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

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

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

Preporuke vanjskih ocjeniterlja Fina će, uz konzultaciju sa vanjskim ocjeniteljem, Fina će otkloniti do slijedeće ocjene sukladnosti.

Vanjski ocjenitelj može predložiti i savjetovati izmjenu kojom se poboljšava pružanje usluga povjerenja. U tom slučaju Fina zadržava pravo prihvaćanja prijedloga.

8.6. Priopćavanje rezultata

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

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

Rezultate vanjske provjere sukladnosti Fina priopćava ovisno o vrsti usluge povjerenja, a sukladno opisu u pripadajućim CPS dokumentima.

9. OSTALE POSLOVNE I PRAVNE ODREDBE

9.1. Naknade za usluge

Ako posebnim ugovorom nije drugačije određeno, usluge certificiranja se naplaćuju sukladno cjeniku Fine objavljenom na Fina repozitoriju na internetskim stranicama repozitorija iz točke 2.2.1. ovog dokumenta.

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 dokumentom.

9.2.1. Pokrivenost osiguranjem

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

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

Fina može od vanjskog ugovorenog RA-a zahtijevati da se osigura od šteta koje mogu nastati obavljanjem usluga ugovorenih s vanjskim RA.

9.2.2. Druga sredstva

Nema odredbi.

9.2.3. Osiguranje ili garancije krajnjim korisnicima

Vidi točku 9.2.1.

9.3. Povjerljivost poslovnih podataka

9.3.1. Opseg povjerljivih poslovnih podataka

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

Povjerljivi su svi podaci koji se odnose na način i na sredstva kojima Fina Root CA i njemu subordinirani Fina CA-ovi upravljaju certifikatima.

Povjerljivi su svi privatni Korisnički ključevi povezani s Korisničkim certifikatima koje generiraju Fina CA-ovi.

9.3.2. Podaci koji se ne smatraju povjerljivim poslovnim podacima

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

9.3.3. Odgovornost za zaštitu povjerljivih poslovnih podataka

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

9.4. Zaštita osobnih podataka

Fina 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 [3] i Zakonu o provedbi Opće uredbe o zaštiti podataka [4]

Podnošenjem zahtjeva za izdavanje certifikata i sklapanjem ugovora o pružanju usluga certificiranja Korisnici daju Fini suglasnost za korištenje i obradu njihovih osobnih podatka prikupljenih u postupku registracije sukladno važećoj zakonskoj regulativi te suglasnost za čuvanje tih podataka u trajanju od najmanje 10 godina od prestanka valjanosti certifikata na kojeg se zapisi 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 provodi tehničke, kadrovske i organizacijske mjere zaštite osobnih podataka sukladno Zakonu o provedbi Opće uredbe o zaštiti podataka [4] u svrhu zaštite privatnosti osoba i zaštite podataka od moguće zlouporabe te očuvanja točnosti, potpunosti i ažurnosti osobnih podataka.

Fina stručnim znanjem, pouzdanošću, resursima, poštivanjem propisanih tehničkih, organizacijskih i sigurnosnih mjera jamči obradu osobnih podataka sukladno Uredbi (EU) 2016/679 [3] i Zakonu o provedbi Opće uredbe o zaštiti podataka [4].

9.4.2. Povjerljivi osobni podaci

U postupku registracije Korisnika i nakon toga Fina je ovlaštena prikupljati osobne podatke koji su potrebni za valjano utvrđivanje identiteta Korisnika te druge podatke potrebne za valjano pružanje usluga certificiranja. Osobni podaci koje prikupi Fina i koji nisu sadržaj certifikata su povjerljivi osobni podaci koje Fina propisno štiti.

9.4.3. Osobni podaci koji nisu povjerljivi

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

9.4.4. Odgovornost za zaštitu osobnih podataka

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

Ugovorima s vanjskim ugovorenim RA Fina regulira odgovornost za zaštitu osobnih podataka u ugovorenim RA.

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 Korisnika.

9.4.6. Dostupnost podataka mjerodavnim tijelima

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

9.4.7. Ostale okolnosti objave podataka

Nema odredbi.

9.5. Prava intelektualnog vlasništva

Ovaj CP/CPS_{ROOT} dokument kao i druga Finina dokumentacija objavljena na internetskim stranicama repozitorija iz točke 2.2.1. ovog dokumenta je intelektualno vlasništvo Fine.

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

Fina kao pružatelj usluga certificiranja vlasnik je certifikata koje izdaje.

9.6. Obveze i odgovornosti

9.6.1. Obveze i odgovornosti CA

Fina je odgovorna je za usklađenost Pravilnika o postupcima certificiranja s odgovarajućim Općim pravilima pružanja usluga certificiranja, njegovu usklađenost sa zakonskom regulativom te za provođenje odredbi Pravilnika o postupcima certificiranja, uvjetima pružanja usluga certificiranja i sukladno obvezama iz ugovora o obavljanju usluga certificiranja sklopljenim s Korisnikom.

Fina na internetskim stranicama repozitorija iz točke 2.2.1. ovog dokumenta objavljuje uvjete pružanja usluga certificiranja, ovaj dokument i sve obavijesti i informacije o promjenama u radu koje na bilo koji način mogu utjecati na sudionike Fina PKI.

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

Fina je odgovorna za:

- ispravnu provjeru identiteta i podataka fizičke osobe i/ili Poslovnog subjekta u cilju izdavanja certifikata,
- izdavanje certifikata na siguran način radi očuvanja njegove autentičnosti i točnosti,
- usklađenost sa svojim obvezama.

Sukladno obvezama i odgovornostima Fina:

- pri pružanju usluge certificiranja primjenjuje odredbe važećih propisa iz točke 9.14. ovog dokumenta,
- izdaje certifikat na siguran način radi očuvanja njegove autentičnosti i točnosti, temeljeći ga na pouzdano utvrđenom identitetu fizičke osobe i/ili Poslovnog subjekta sukladno pripadajućim CPS dokumentima,
- izdaje certifikat s profilom sukladnim s pripadajućim CPS dokumentom, a prema tipu certifikata navedenom u zahtjevu za izdavanje certifikata,
- parovi Korisničkih ključeva koje generiraju Fina CA-ovi generiraju se na siguran način i uz osiguranje tajnosti privatnog ključa, sukladno pripadajućem CPS dokumentu,
- provodi potrebne provjere sukladno pripadajućem CPS dokumentu kada se javni ključ Fini dostavlja na certificiranje,
- provodi sve potrebne radnje određene pripadajućim CPS dokumentom kada Fina CA izdaje Korisnički certifikat na sigurnom kriptografskom, odnosno QSCD uređaju,
- izdani certifikat čini dostupnim sukladno točki 4.4.2. ovog dokumenta,
- temeljem autenticiranog i autoriziranog zahtjeva, po provedenom propisanom postupku, opoziva, suspendira ili reaktivira certifikat te ga objavljuje u listi opozvanih certifikata,
- pruža informaciju o statusu opozvanosti ili suspendiranosti certifikata,

- provodi zahtijevane sigurnosne mjere za zaštitu prostora i opreme sustava certificiranja,
- primjenjuje organizacijske i tehničke mjere zaštite ključeva i certifikata sukladno ovom dokumentu i pripadajućem CPS dokumentu,
- sukladno Planu kontinuiteta poslovanja osigurava nesmetan rad i maksimalnu raspoloživost usluga certificiranja,
- prati raspoloživost kapaciteta, planira održavanje i daljnji razvoj sustava certificiranja sukladno budućim potrebama, zahtjevima normi i razvoju tehnologije,
- podatke koji se sukladno točkama 9.3. i 9.4. ovog dokumenta smatraju povjerljivima štiti i te podatke koristiti isključivo za potrebe usluga certificiranja iz opsega ovog dokumenta,
- osigurava da se interne i vanjske provjere sukladnosti Fine kao pružatelja usluga povjerenja provode sukladno točki 8.1. ovog dokumenta.

U slučaju prekida poslovanja Fina će postupiti sukladno točki 5.8. ovog dokumenta.

Ograničenja odgovornosti Fine kao davatelja usluga certificiranja opisana su u točki 9.8. ovog dokumenta.

9.6.2. Obveze i odgovornosti RA

Obveze i odgovornosti RA mreže su:

- provođenje postupka registracije, identifikacije i provjere podataka fizičkih osoba i Poslovnih subjekata na način propisan pripadajućim CPS dokumentima,
- odobravanje zahtjeva za izdavanje certifikata te zahtjeva za opoziv, suspenziju i reaktivaciju certifikata na način propisan pripadajućim CPS dokumentima,
- prosljeđivanje cjelovitih, točnih i provjerenih podataka registriranih fizičkih osoba i Poslovnih subjekata u Fina CA-ove,
- čuvanje, arhiviranje i zaštita prikupljenih 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 registriranih fizičkih osoba i Poslovnih subjekata, na način propisan pripadajućim CPS dokumentima.

9.6.3. Obveze i odgovornosti korisnika

Korisnik je dužan:

- u procesu registracije predstaviti se na način propisan pripadajućim CPS dokumentom,
- pažljivo koristiti i čuvati sredstva za izradu elektroničkog potpisa, sredstva elektroničke identifikacije, privatne ključeve i aktivacijske podatke te ih koristiti u skladu s odredbama pripadajućeg CPS dokumenta,
- poduzeti odgovarajuće mjere zaštite sredstva za izradu elektroničkog potpisa, sredstva elektroničke identifikacije, privatnog ključa i aktivacijskih podataka od

neovlaštenog pristupa i uporabe, u skladu s odredbama pripadajućeg CPS dokumenta,
- u najkraćem mogućem roku zatražiti opoziv, odnosno suspenziju svog certifikata u slučaju kompromitiranja privatnog ključa, gubitka sredstva za izradu elektroničkog potpisa, sredstva elektroničke identifikacije, privatnog ključa i aktivacijskih podataka,
- dostaviti u registracijski ured RA mreže sve potrebne podatke i informacije o promjenama koje utječu ili mogu utjecati na točnost elektroničkog potpisa, odnosno elektroničke identifikacije u rokovima propisanim pripadajućim CPS dokumentom,
- djelovati u skladu sa svim ostalim odredbama ovog dokumenta i pripadajućeg CPS dokumenta, koje se odnose na obveze Korisnika.

9.6.4. Obveze i odgovornosti pouzdajuće strane

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

Pouzdajuća strana koja se, ne poštujući pripadajući CPS dokument pouzdala u nevažeći certifikat (opozvani, istekli ili suspendirani certifikat) sama snosi sve rizike pouzdanja u takav certifikat.

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

Detaljnije odredbe navedene su u pripadajućim CPS dokumentima.

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 poslovnog subjekta 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 izdane certifikate i za transakcije obavljene na temelju pouzdavanja u tako izdane certifikate iznosi najviše 3.500.000,00 kuna.

Finine financijske odgovornosti u ovisnosti o tipovima certifikata koje izdaju Fina CA-ovi posebno su iskazane u pripadajućim CPS dokumentima.

9.9. Naknada štete

Svaki sudionik odgovara oštećenom za štetu koju je počinio zbog nepoštivanja odredbi iz ovog dokumenata i važećih relevantnih propisa.

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

Pouzdajuća strana odgovora oštećenom odnosno svakom drugom sudioniku ako se pouzda u izdani certifikat bez provjere njegove valjanosti ili ga koristi protivno svrhama određenim u pripadajućim CPS dokumentima.

9.10. Trajanje i prestanak važenja

9.10.1. Trajanje

Ovaj dokument važi do stupanja na snagu novog CP/CPS_{ROOT} dokumenta ili do objave prestanka njegovog važenja.

Novm CP/CPS_{ROOT} dokumentu biti će dodijeljena nova verzija i/ili podverzija te će u njemu biti naznačene obavljene izmjene. Taj će dokument biti objavljena na internetskim stranicama Fina PKI repozitorija iz točke 2.2.1. ovog dokumenta s naznačenim danom stupanja na snagu.

O potrebi izmjena i/ili dopunama CP/CPS_{ROOT} dokumenta, o broju njegove verzije i/ili podverzije odlučuje Fina PMA.

9.10.2. Prestanak važenja

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

9.10.3. Posljedice prestanka važenja i nastavak djelovanja

Stupanjem na snagu novog CP/CPS_{ROOT} dokumenta, za sve certifikate izdane prema ovom dokumentu ostaju važiti one odredbe iz ovog dokumenta koje se ne mogu smisleno zamijeniti odredbama novog CP/CPS_{ROOT} dokumenta.

Za pojedine odredbe važećeg CP/CPS_{ROOT} dokumenta Fina može izraditi izmjene i dopune, kao što je to navedeno u točki 9.12. ovog dokumenta.

9.11. Pojedinačne obavijesti i komunikacija sa sudionicima

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

- besplatni telefon: 0800 0080

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

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

9.12. Izmjene i dopune

9.12.1. Procedure izmjena i dopuna

Ovaj dokument revidira se po potrebi.

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

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

Izradu novog ili izmjenu i dopunu postojećeg CP/CPS_{ROOT} dokumenta odobrava i provodi Fina PMA, a sukladno poslovnim zahtjevima Fine i zahtjevima zakonske regulative i propisa iz točke 9.14 ovog dokumenta.

9.12.2. Mehanizmi obavještavanja i vremenski periodi

Sve izmjene i dopune CP/CPS_{ROOT} dokumenta prikladne za javnu objavu objavljuju se u elektroničkom obliku na internetskim stranicama repozitorija iz točke 2.2.1. ovog dokumenta.

Nove verzije CP/CPS_{ROOT} dokumenta za javnu objavu s izmijenjenim OID-om CP/CPS_{ROOT} dokumenta objavljuju se u elektroničkom obliku na internetskim stranicama repozitorija iz točke 2.2.1. ovog dokumenta.

Datum stupanja na snagu novoobjavljenog CP/CPS_{ROOT} dokumenta naznačen je na njegovoj naslovnoj strani kao i na internetskim stranicama na kojima je objavljen.

9.12.3. Okolnosti pod kojima se mora mijenjati OID

Veće izmjene u CP/CPS_{ROOT} dokumentu koje mogu utjecati na sudionike zahtijevaju i izmjenu OID-a CP/CPS_{ROOT} dokumenta. Novi OID za novu verziju CP/CPS_{ROOT} 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 dokumentom, isti će se nastojati razriješiti sporazumno. Ako sporazumno razrješenje spora nije moguće, isti će se razriješiti pred mjerodavnim sudom u Zagrebu uz primjenu hrvatskog prava.

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

9.14. Važeći propisi

Usluge povjerenja iz opsega ovog dokumenta Fina pruža sukladno odredbama Uredbe (EU) br. 910/2014 [1], Zakona o provedbi Uredbe (EU) br. 910/2014 [2] te normizacijskih dokumenata ETSI EN 319 401 [7], ETSI EN 319 411-1 [8], ETSI EN 319 411-2 [9], CA/Browser Forum BRG [16] i CA/Browser Forum EVCG [17].

Odredbe o važećim propisima u ovisnosti o tipovima certifikata koje izdaju Fina CA-ovi posebno su iskazane u pripadajućim CPS dokumentima.

9.15. Usklađenost s primjenjivim propisima

Ovaj dokument i pružanje usluga certificiranja koje su obuhvaćene ovim dokumentom usklađeni su s propisima iz točke 9.14. ovog dokumenta.

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

9.16. Razne odredbe

Nema odredbi.

9.17. Ostale odredbe

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

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

Odredbe za certifikate koje izdaju Fina CA-ovi posebno su iskazane u pripadajućim CPS dokumentima.