FINA

OPĆA PRAVILA DAVANJA USLUGA CERTIFICIRANJA

Fina Root CA

Verzija 1.0

Datum objave: 7.12.2015.

Datum stupanja na snagu: 7.12.2015.

OID Dokumenta: 1.3.124.1104.5.0.2.1.1.0

Informacije o dokumentu

Ime dokumenta:	Fina - Opća pravila davanja usluga certificiranja Fina Root CA
OID dokumenta:	1.3.124.1104.5.0.2.1.1.0
Tip dokumenta:	Opća pravila davanja usluga certificiranja (*Certificate Policy*, CP)
Oznaka distribucije	Javno
Vlasnik dokumenta	Financijska agencija, Fina
Kontakt	pma@fina.hr

Povijest izmjena

Verzija	Datum	Razlog izmjene
1.0	7.12.2015.	Inicijalna verzija

SADRŽAJ

AUTORSKA PRAVA

REFERENTNE DOKUMENTIRANE INFORMACIJE

Temeljni zakon

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

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

[3] Zakon o izmjeni zakona o elektroničkom potpisu (NN 30/2014)

Podzakonski akti

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

[5] Pravilnik o izradi elektroničkog potpisa, uporabi sredstava za izradu elektroničkog potpisa, općim i posebnim uvjetima poslovanja za davatelje usluga izdavanja vremenskog žiga i certifikata (NN 107/2010)

[6] Pravilnik o izmjenama i dopunama Pravilnika o izradi elektroničkog potpisa, uporabi sredstava za izradu elektroničkog potpisa, općim i posebnim uvjetima poslovanja za davatelje usluga izdavanja vremenskog žiga i certifikata (NN 89/2013)

[7] Popis normizacijskih dokumenata u području primjene Zakona o elektroničkom potpisu i Pravilnika o izradi elektroničkog potpisa, uporabi sredstva za izradu elektroničkog potpisa, općim i posebnim uvjetima poslovanja za davatelje usluga izdavanja vremenskog žiga i certifikata u poslovanju davatelja usluga certificiranja u Republici Hrvatskoj (NN 89/2013)

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

Ostali zakoni

[9] Zakon o zaštiti osobnih podataka (NN 106/2012)

Direktive Europskog parlamenta

[10] Direktiva 1999/93/EZ Europskog parlamenta i Vijeća od 13. prosinca 1999. o okviru Zajednice za elektroničke potpise

Normizacijski dokumenti

[11] HRN ETSI/EN 319 411-2 V1.1.1:2013 Elektronički potpisi i infrastrukture (ESI) – Opća pravila i sigurnosni zahtjevi za vjerodostojne davatelje usluga certificiranja – 2. dio: Zahtjevi za opća pravila za certifikacijska tijela koja izdaju kvalificirane certifikate (EN 319 411-2 V1.1.1:2013)

[12] HRN ETSI/EN 319 411-3 V1.1.1:2013 Elektronički potpisi i infrastrukture (ESI) – Zahtjevi za opća pravila i sigurnost za vjerodostojne davatelje usluga koji

izdaju certifikate – 3. dio: Opća pravila za certifikacijska tijela koja izdaju certifikate s javnim ključem (EN 319 411-3 V1.1.1:2013)

[13] HRN ETSI/EN 319 412-5 V1.1.1:2013 Elektronički potpisi i infrastrukture (ESI) – Profili vjerodostojnih davatelja usluga koji izdaju certifikate – 5. dio: Proširenje za profil kvalificiranoga certifikata (EN 319 412-5 V1.1.1:2013)

[14] ETSI TS 119 312 V1.1.1:2014 - Electronic Signatures and Infrastructures (ESI); Cryptographic Suites

[15] ETSI TS 119 403 V2.2.1:2015 - Electronic Signatures and Infrastructures (ESI);Trust Service Provider Conformity Assessment

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

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

[18] ISO/IEC 27001:2013 - Information technology — Security techniques — Information security management systems — Requirements

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

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

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

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

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

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

[25] NIST FIPS PUB 186-2: Digital Signature Standard (DSS)

[26] ITU-T Recommendation X.509:2000 / ISO/IEC 9594-8:2012: Information technology – Open Systems Interconnection – The Directory: Public-key attribute certificate frameworks

[27] ITU-T Recommendation X.501:2012 – Information technology – Open Systems Interconnection – The Directory: Models

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

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

Finini dokumenti

[30] Fina - Pravilnik o postupcima certificiranja Fina Root CA, ver 1.0

[31] Fina - Opća pravila davanja usluga certificiranja, ver 5.0

[32] Fina - Pravilnik o postupcima certificiranja za kvalificirane certifikate, $CPS_{QC,}$ ver 5.0

[33] Fina - Pravilnik o postupcima certificiranja za nekvalificirane certifikate, $CPS_{NQC,}$ ver 5.0

[34] Fina - Opća pravila davanja usluga izdavanja naprednih vremenskih žigova, ver 1.0

1. UVOD

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

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

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

Finina poslovna mreža ima nacionalnu pokrivenost 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 certificiranja usklađene su sa zakonskom regulativom o elektroničkom potpisu u Republici Hrvatskoj [1] – [8] i europskom Direktivom o elektroničkim potpisima [10] te samim time i s mjerodavnim međunarodnim normama iz djelokruga davanja usluga certificiranja. Fina neprekidno prati potrebe korisnika, razvoj tehnologije i promjene u mjerodavnim normama iz područja davanja usluga certificiranja te sukladno tome unapređuje i usklađuje svoj PKI sustav pritom nastojeći svoje proizvode i usluge što više prilagoditi zahtjevima za međugraničnu interoperabilnost.

1.1. Pregled

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).

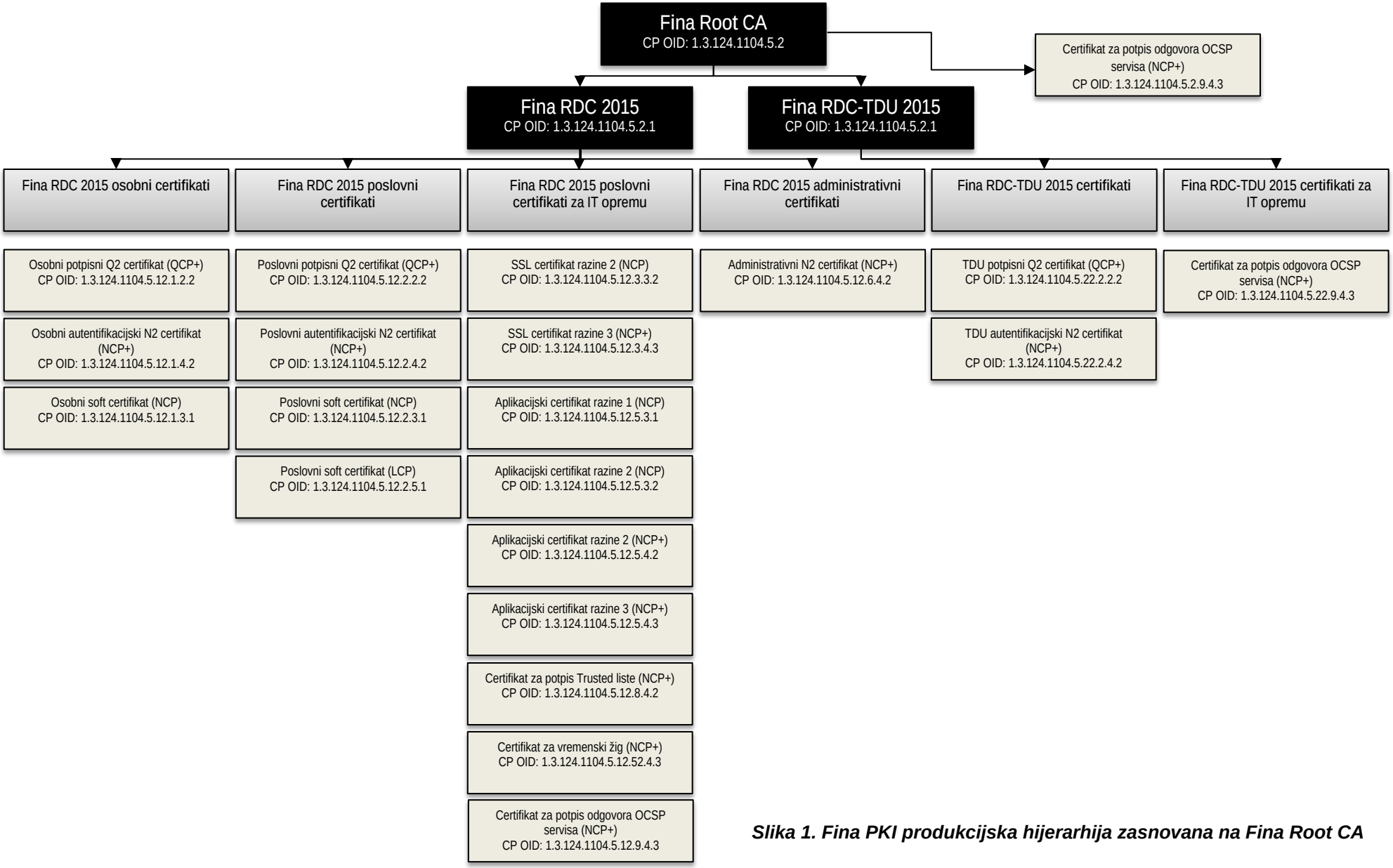
Dvorazinsku arhitekturu produkcijskih certifikacijskih tijela Fine čine:

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

Fina Root CA je samom sebi izdao samopotpisani Fina Root CA certifikat te je certifikate izdao za njemu podređenim subordinirane Fina RDC 2015 i Fina RDC-TDU 2015 CA-ove.

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

Na Slici 1. na sljedećoj stranici prikazana je Fina PKI produkcijska hijerarhija zasnovana na Fina Root CA. Za svaki tip certifikata upisan je pripadajući OID pravila certificiranja (CP OID).



Slika 1. Fina PKI produkcijska hijerarhija zasnovana na Fina Root CA

1.1.2. Opseg i namjena ovih Općih pravila

Opseg ovih Općih pravila davanja usluga certificiranja Fina Root CA (engl. *Certificate Policy* – CP, u daljnjem tekstu: Opća pravila) su Fina PKI usluge certificiranja koje pruža Fina, a koje se odnose na izdavanje i upravljanje životnim ciklusom certifikata u Fina PKI produkcijskoj hijerarhiji zasnovanoj na Fina Root CA.

Ova Opća pravila odnose se na Fina Root CA, a sadrže temeljna pravila i skup načela zajedničkih za davanje usluga certificiranja u Fina PKI hijerarhiji zasnovanoj na Fina Root CA.

Struktura ovih Općih pravila temelji se na normizacijskom dokumentu IETF RFC 3647 [21]

Opća pravila davanja usluga izdavanja certifikata krajnjim korisnicima opisana su u dokumentu Opća pravila davanja usluga certificiranja [31].

Finina usluga izdavanja naprednih vremenskih žigova opisana je u dokumentu Opća pravila davanja usluga izdavanja naprednih vremenskih žigova [34].

Za potrebe testiranja, demonstracije i usklađivanja informatičkih rješenja Fina izdaje Demo digitalne certifikate na zasebnoj Fina PKI hijerarhiji zasnovanoj na Fina Demo Root CA.

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

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 (NCP+)	CP OID: 1.3.124.1104.5.2.9.4.3

Tablica 1.1. Certifikati koje izdaje Fina Root CA

1.1.3.2. Certifikati koje izdaju Fina RDC 2015 i Fina RDC-TDU 2015 CA-ovi

Subordinirani Fina RDC 2015 i Fina RDC-TDU 2015 CA-ovi korisnicima izdaju kvalificirane, normalizirane i *lightweight* certifikate.

Kvalificirani certifikati su kvalificirani certifikati u smislu Zakona o elektroničkom potpisu [1], [2] i [3] te su namijenjeni isključivo za podršku naprednom elektroničkom potpisu koji se izrađuje sredstvima za izradu naprednog elektroničkog potpisa. Kvalificirani certifikati

usklađeni su s općim pravilima za „QCP public + SSCD“ norme HRN ETSI/EN 319 411-2 [11] te zadovoljavaju zahtjeve norme HRN ETSI/EN 319 412-5 [13].

Normalizirani certifikati su certifikati u smislu Zakona o elektroničkom potpisu [1], [2] i [3] te se koriste za podršku elektroničkom potpisu. Normalizirani certifikati usklađeni su s normom HRN ETSI/EN 319 411-3 [12]. Pored podrške elektroničkom potpisu, normalizirani certifikati mogu se koristiti i za druge primjene kao što su autentifikacija i enkripcija.

***Lightweight* certifikati** su certifikati u smislu Zakona o elektroničkom potpisu [1], [2] i [3] te se koriste za podršku elektroničkom potpisu. *Lightweight* certifikati usklađeni su s normom HRN ETSI/EN 319 411-3 [12]. Pored podrške elektroničkom potpisu, *lightweight* certifikati mogu se koristiti i za druge potrebe kao što su autentifikacija i enkripcija.

Normalizirani i *lightweight* certifikati se ne smatraju kvalificiranim certifikatima u smislu Zakona o elektroničkom potpisu [1], [2] i [3] pa se zajednički nazivaju **nekvalificirani certifikati**.

Certifikati za korisnike, njihova područja primjene i druge odredbe vezane uz izdavanje i upravljanje životnim ciklusom korisničkih certifikata detaljno su opisane u Općim pravilima davanja usluga certificiranja [31].

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: Fina – Opća pravila davanja usluga certificiranja Fina Root CA
- Verzija: 1.0
- Datum objave: 7.12.2015.
- Datum stupanja na snagu: 7.12.2015
- OID: 1.3.124.1104.5.0.2.1.1.0
- Internet adresa na kojoj je dokument objavljen je http://rdc.fina.hr/Root/FinaRootCA-CP1-0-hr.pdf

1.3. Sudionici u PKI

Sudionici unutar Fina PKI su:

- tijelo za upravljanje pravilima certificiranja (*Policy Management Authority*, PMA);
- certifikacijska tijela (*Certification Authorities*, CA-ovi);
- registracijska mreža (RA mreža) koja se sastoji od registracijskih ureda (*Registration Authority*, RA) i lokalnih registracijskih ureda (*Local Registration Authority*, LRA);
- korisnici;

- pouzdajuće strane;
- ostali sudionici:
    - proizvođači IT opreme za PKI,
    - proizvođači sigurnih uređaja (smart kartice, USB tokeni i sl.),
    - ovlaštena nadzorna tijela.

1.3.1. Tijelo za upravljanje pravilima certificiranja

Tijelo za upravljanje pravilima certificiranja u Fini je Fina PMA. Fina PMA je tijelo ovlašteno i odgovorno za izradu, uvođenje i administriranje pravila davanja usluga certificiranja, pripadnu dokumentaciju i postupke te za kontrolu provođenja istih.

1.3.2. Certifikacijska tijela u Fina PKI

Certifikacijska tijela u Fina PKI iz opsega ovih Općih pravila 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 koji su vezani uz upite o certifikatima koje je izdao Fina Root CA. Fina Root CA ne izdaje certifikate korisnicima. Fina Roota CA certifikat dostupan je na sljedećoj internetskoj adresi: http://rdc.fina.hr/Root/FinaRootCA.cer.

Fina RDC 2015 CA izdaje kvalificirane, normalizirane i *lightweight* certifikate za javnost. Korisnici kojima Fina RDC 2015 CA izdaje certifikate su fizičke osobe (građani), pripadajuće osobe unutar poslovnih subjekata i poslovni subjekti. Fina RDC 2015 CA certifikat dostupan je na sljedećoj internetskoj adresi: http://rdc.fina.hr/RDC2015/FinaRDCCA2015.cer.

Fina RDC-TDU 2015 CA izdaje kvalificirane, normalizirane certifikate državnim dužnosnicima i zaposlenicima u tijelima državne uprave. Fina RDC-TDU 2015 CA certifikat dostupan je na sljedećoj internetskoj adresi: http://rdc.fina.hr/RDC-TDU2015/FinaRDC-TDUCA2015.cer.

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

1.3.3. Registracijska tijela

Poslovi registracije korisnika za Fina CA-ove obavljaju se u registracijskim uredima Fine. Za potrebe registracije korisnika Fina može s drugim poslovnim subjektima ugovoriti obavljanje usluge registracije (u daljnjem tekstu: vanjski ugovoreni RA).

Fina PKI ima organiziranu mrežu registracijskih ureda (u daljnjem tekstu: RA mreža) koju čine Fina RA mreža i mreža pojedinog vanjskog ugovorenog RA.

Fina RA mrežu čini mreža lokalnih registracijskih ureda (u daljnjem tekstu: Fina LRA) u poslovnoj mreži Fine te Središnji Fina RA koji koordinira poslovima registracije u Fina RA mreže.

1.3.4. Korisnici

Korisnici Fina PKI iz opsega ovih Općih pravila su osobe koje s Finom ugovaraju korištenje usluga certificiranja.

Korisnici Fina PKI mogu biti:

- fizičke osobe – građani;
- poslovni subjekti, uključujući i tijela državne uprave.

Za korištenje usluge certificiranja korisnici trebaju obaviti postupak registracije i predaje zahtjeva te prihvatiti obaveze i odgovornosti korisnika koje su navedene u točki 9.6.3. Općih pravila. U sklopu procedure registracije korisnici s Finom kao davateljem usluga certificiranja sklapaju ugovor o obavljanju usluga certificiranja.

Na temelju sklopljenog ugovora, zaprimljenog zahtjeva i provedenog postupka registracije određeni subordinirani Fina CA izdaje traženi certifikat.

1.3.5. Pouzdajuće strane

Pouzdajuće strane su fizičke osobe ili poslovni subjekti koji su primatelji certifikata i djeluju temeljem razumnog pouzdanja u certifikat. Certifikat omogućuje pouzdajućoj strani provjeru cjelovitosti i izvornosti elektronički potpisanog zapisa, odnosno provjeru identiteta subjekta.

Obaveze i odgovornosti pouzdajuće strane navedene su u točki 9.6.4. Općih pravila.

1.3.6. Ostali sudionici

Ostali sudionici Fina PKI su poslovni subjekti koje ne pružaju i ne koriste usluge certificiranja, ali sudjeluju u dijelovima procesa vezanim uz davanje usluga certificiranja. U ovu grupu sudionika Fina PKI spadaju proizvođači i distributeri hardvera i softvera korištenih u Fina PKI, proizvođači i distributeri *smart* kartica, USB tokena, HSM-ova i sličnih kriptografskih uređaja, neovisni ocjenitelji i dr.

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 isključivo se koriste za izdavanje korisničkih certifikata, izdavanje pripadajućih CRL, za izdavanje certifikata za Fina QTSA 2015 servis, za izdavanje certifikata za Fina OCSP servis kojim ovaj OCSP servis potpisuje odgovore za status certifikata za Fina QTSA 2015 servis i za statuse korisničkih certifikata, a u skladu s

vrijednostima u ekstenzijama *Basic Constraints* i *PathLengthConstraint* u CA certifikatima Fina CA-ova.

Opis primjerene uporabe korisničkih certifikata opisan je u Općim pravilima davanja usluga certificiranja [31].

1.4.2. Zabrane uporabe certifikata

Sve uporabe certifikata različite od uporaba navedenih u točki 1.4.1. ovih Općih pravila su zabranjene.

Preporuka je pouzdajućim stranama da provjeravaju i koriste CP OID certifikata kako bi donijele valjanu odluku o prihvaćanju ili odbacivanju uporabe određenog certifikata na način opisan u točki 9.6.4. Općih pravila. Popis CP OID-ova za certifikate iz opsega ovih Općih pravila naveden na Slici 1. ovih Općih pravila.

1.5. Administracija dokumenta Opća pravila

1.5.1. Organizacija odgovorna za održavanje dokumenta Opća pravila

Za izradu i održavanje dokumenta Općih pravila odgovorno je tijelo za upravljanje pravilima certificiranja Fina PMA (vidi točku 1.3. Općih pravila).

1.5.2. Kontakt podaci

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

Poštanska adresa:

Fina
Sektor financijskih i elektroničkih usluga
Ured za upravljanje politikom e-poslovanja
Koturaška cesta 43
10000 Zagreb
Hrvatska

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

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

Uskladivost ovih Općih pravila s Pravilnikom o postupcima certificiranja Fina Root CA (u daljem tekstu: CPS_{ROOT}) [30] kao i uskladivost s Općim pravilima davanja usluga certificiranja [31] te odgovarajućih CPS_{QC} [32], odnosno CPS_{NQC} [33] dokumenata pravilima utvrđuje Fina PMA.

1.5.4. Procedure odobravanja CPS-a

Prije primjene CPS_{ROOT} [30], CPS_{QC} [32], odnosno CPS_{NQC} [33] ovi dokumenti moraju biti odobreni od strane Fina PMA. Početak i prestanak važenja CPS_{ROOT} [30], CPS_{QC} [32], odnosno CPS_{NQC} [32] dokumenata određuje Fina PMA u skladu sa svojim internim postupcima.

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 u kojem je kao subjekt certificiranja naveden (isti ili neki drugi) CA. CA certifikat sadrži naziv i javni ključ CA.
CA privatni potpisni ključ	Privatni ključ CA koji s javnim CA ključem čini par CA ključeva. CA privatni potpisni ključ koristi se za potpisivanje certifikata koje izdaje taj CA. Pripadni CA javni ključ upisan je u CA certifikat tog CA.
CA *root* certifikat	CA certifikat kojeg je samom sebi izdao i potpisao isti CA, tj. subjekt certificiranja i izdavatelj u CA root certifikatu su jednaki.
Certifikacijsko tijelo (CA)	Treća strana od povjerenja koja potvrđuje identitet subjekta certificiranja, izrađuje i potpisuje te za subjekt certificiranja izdaje traženi certifikat. CA je davatelj usluga certificiranja koji izdaje i upravlja životnom ciklusom izdanih certifikata u skladu s objavljenim CP-om, a može biti fizička osoba, pravna osoba ili njen sastavni dio.
Certifikat	Potvrda u elektroničkom obliku koja: • imenuje i identificira subjekt certificiranja naveden u certifikatu; • sadrži subjektov javni ključ; • ima upisan vremenski period valjanosti certifikata; • ima značenje u skladu s važećim propisima i normama; • identificira CA koji izdaje certifikate; • elektronički je potpisan od strane CA.
Davatelj usluga certificiranja (CSP)	Pravna ili fizička osoba koja izdaje certifikate ili daje druge usluge povezane s elektroničkim potpisima. Druge usluge povezane s elektroničkim potpisom mogu biti usluga izdavanja vremenskog žiga, usluga izrade elektroničkog potpisa, usluga verifikacije elektroničkog potpisa, usluga dugotrajnog čuvanja elektronički potpisanih zapisa i sl.
Dnevnik sustava	Skup zapisa o događajima u informacijskom sustavu (engl. *log, audit log*).
Elektronički potpis	Skup podataka u elektroničkom obliku koji su pridruženi ili su logički povezani s drugim podacima u elektroničkom obliku i koji služe za identifikaciju potpisnika i utvrđivanje vjerodostojnosti potpisanoga elektroničkog dokumenta.
Fina LRA	LRA (lokalni registracijski ured) u Fina poslovnoj mreži.

DEFINICIJA	ZNAČENJE
Fina PKI	Infrastruktura javnog ključa (PKI) uspostavljena u Fini koja je namijenjena za davanje usluga certificiranja fizičkim osobama – građanima, poslovnim subjektima i tijelima državne uprave, a koja djeluje kao treća strana od povjerenja (engl. *Trusted Third Party*).
Fina RA mreža	Mreža registracijskih ureda u inil, a sastoji se od Središnjeg Fina RA 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.
Ime (naziv) subjekta	Polje certifikata koje sadrži jedinstveni identifikator imena odnosno naziva subjekta (polje *subject*).
Infrastruktura javnog ključa (PKI)	Arhitektura, organizacija, hardver, softver, osoblje, pravila, operativni postupci i procedure koje zajednički podržavaju implementaciju i rad kriptografskog sustava javnog ključa za upravljanje životnim ciklusom digitalnih certifikata.
Javni imenik	Informatički sustav u nadležnosti CA koji služi za *online* objavu dokumenata i informacija vezanih uz certifikate, uključujući i informacije o valjanosti ili opozvanosti certifikata.
Javni ključ	Javno dostupan kriptografski ključ koji odgovara uparenom privatnom ključu. Javni ključ može služiti za provjeru elektroničkog potpisa (ako je javno objavljen kao dekripcijski ključ) ili za enkripciju podataka (ako je javno objavljen kao enkripcijski ključ).
Korisnik	Fizička osoba-građanin ili poslovni subjekt kojima davatelj usluga certificiranja daje usluge, odnosno s kojim sklapa ugovor o korištenju usluga certificiranja.
Kriptografski modul	Softver ili uređaj određene razine sigurnosti koji: • generira par ključeva i/ili • štiti kriptografske informacije i/ili • obavlja kriptografske funkcije.
Kvalificirani certifikat	Elektronička potvrda kojom davatelj usluga izdavanja kvalificiranih certifikata potvrđuje napredni elektronički potpis. Kvalificirani certifikat izdaje davatelj usluga izdavanja kvalificiranog certifikata koji ispunjava uvjete propisane Zakonom o elektroničkom potpisu.
LCP certifikat	LCP certifikat, vidi pojam „*Lightweight* certifikat“
***Lightweight* certifikat**	Certifikat koji pruža manje zahtjevnu razinu kvalitete usluge u odnosu na certifikate izdane sukladno Općim pravilima izdavanja kvalificiranih certifikata opisanim u HRN ETSI/EN 319 411-2, LCP certifikat.
***Lightweight Directory Acess Protocol* (LDAP)**	Aplikacijski protokol koji radi iznad TCP/IP sloja, a služi za pristup i održavanje distribuiranih usluga povezivanja, pretraživanja i izmjena informacija putem mrežnog internetskog protokola.
Lista opozvanih certifikata (CRL)	Potpisana lista koja ukazuje na skup certifikata koji se od strane izdavatelja certifikata više ne smatraju važećim.

DEFINICIJA	ZNAČENJE
Napredan elektronički potpis	Elektronički potpis koji pouzdano jamči identitet potpisnika i koji: • je povezan isključivo s potpisnikom; • nedvojbeno identificira potpisnika; • nastaje korištenjem sredstava kojima potpisnik može samostalno upravljati i koja su isključivo pod nadzorom potpisnika; • sadržava izravnu povezanost s podacima na koje se odnosi i to na način koji nedvojbeno omogućava uvid u bilo koju izmjenu izvornih podataka.
Napredan vremenski žig	Elektronički potpisana potvrda izdavatelja naprednog vremenskog žiga koja potvrđuje sadržaj podataka na koji se odnosi u navedenom vremenu i koja ispunjava uvjete za napredan elektronički potpis.
Normalizirani certifikat	Certifikat koji pruža istu kvalitetu kao i certifikati izdani sukladno općim pravilima izdavanja kvalificiranih certifikata opisanim u HRN ETSI/EN 319 411-2, ali bez pravne valjanosti u smislu Direktive 1999/93/EC te bez zahtijevanja uporabe sigurnog sredstva za izradu elektroničkog potpisa (sredstva za izradu naprednog elektroničkog potpisa).
Opća pravila davanja usluga certificiranja - *Certificate Policy* (CP)	Imenovani skup pravila koji ukazuje na primjenjivost certifikata za određenu skupinu i/ili klasu primjena sa zajedničkim zahtjevima na sigurnost.
Opoziv certifikata	Radnja koja certifikat nepovratno čini nevažećim od tog trenutka pa na nadalje. Opoziv postaje važećim objavom CRL u kojoj je naznačen i opoziv tog certifikata.
Period valjanosti certifikata	Vremenski period tijekom kojeg vrijedi certifikat. Ovaj vremenski period počinje vremenom označenim u polju „vrijedi od“ i završava vremenom „vrijedi do“.
Poslovni subjekt	1. Pravne osobe, primjerice: • trgovačka društva; • kreditne i financijske institucije; • javne i privatne ustanove; • udruge s pravnom osobnošću; • neprofitne i nevladine organizacije s pravnom osobnošću; • fondovi s pravnom osobnošću; • jedinice lokalne i područne (regionalne) samouprave (općine, gradovi i županije) i dr. 2. Tijela javne vlasti, primjerice: • tijela državne vlasti; • tijela državne uprave; • državne agencije i dr. 3. Fizičke osobe s registriranom djelatnošću, primjerice: • obrtnici; • odvjetnici; • javni bilježnici; • javni ovršitelji i dr.
Potpisnik	Osoba koja posjeduje sredstvo za izradu elektroničkog potpisa kojim se potpisuje, a koja djeluje u svoje ime ili u ime fizičke ili pravne osobe koju predstavlja.
Pouzdajuća strana	Primatelj certifikata koji djeluje temeljem razumnog pouzdanja u certifikat. Certifikat omogućuje pouzdajućoj strani provjeru cjelovitost i izvornosti elektronički potpisanog zapisa odnosno provjeru identiteta subjekta.

DEFINICIJA	ZNAČENJE
Povjerljive uloge	Uloge koje se dodjeljuju djelatnicima i o kojima ovisi sigurnost rada davatelja usluga certificiranja. Povjerljive uloge (engl. Trusted Roles) i pripadne odgovornosti moraju biti jasno određene i opisane u opisu posla djelatnika.
Pravilnik o postupcima certificiranja (CPS)	Dokument koji sadrži operativne postupke davatelja usluga certificiranja. Operativni postupci definirani Pravilnikom o postupcima certificiranja moraju biti sukladni odredbama definiranim u dokumentu Opća pravila davanja usluga certificiranja (CP).
Pripadajuća osoba	Fizička osoba zaposlena u poslovnom subjektu ili na drugi način povezana s poslovnim subjektom, a koja je od strane istog poslovnog subjekta autorizirana za dobivanje certifikata. Takav certifikat identificira osobu i poslovni subjekt te naznačuje da je ta osoba povezana s poslovnim subjektom.
Privatni ključ	Kriptografski ključ kojeg korisnik čuva u tajnosti, a koji odgovara uparenom javnom ključu. Koristi se za izradu elektroničkog potpisa ili za dekriptiranje podataka enkriptiranih odgovarajućim javnim ključem.
Profil certifikata	Detaljan popis i opis gradivnih elemenata certifikata i njihovih vrijednosti.
RA mreža	Cjelokupna mreža registracijskih ureda, a sastoji se od središnjeg Fina RA, Fina LRA ureda te od vanjskih ugovorenih RA s kojima Fina ima sklopljen ugovor o obavljanju poslova registracije.
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.
Razumno pouzdanje	Razumnim pouzdanjem smatra se odluka pouzdajuće strane da se pouzda u certifikat ako je u vrijeme ostvarenja pouzdanja: • koristila certifikat u svrhe propisane CP-om pod okolnostima u kojima je pouzdanje razumno i u dobroj namjeri te pod okolnostima koje su poznate ili bi trebale biti poznate pouzdajućoj strani prije ostvarenja pouzdanja; • provjerila da certifikat nije istekao u vrijeme ostvarenja pouzdanja te da certifikat nije opozvan ili suspendiran, a što pouzdajuća strana treba utvrditi provodeći provjeru statusa certifikata temeljem zadnje izdane CRL kako je propisano u CP-u; • provjerila da su svi podaci o identitetu subjekta certifikata ispravno prikazani aplikacijom u koju se može pouzdati; • ako je u pitanju elektronički potpis, provjerila da je elektronički potpis izrađen privatnim ključem koji odgovara javnom ključu u certifikatu za vrijeme perioda valjanosti certifikata. Pouzdajuća strana snosi sve rizike pouzdanja u certifikat ako zna ili ima razloga smatrati da postoje činjenice koje mogu uzrokovati osobnu ili poslovnu štetu prouzročenu korištenjem certifikata.
Reaktivacija certifikata	Postupak ponovnog aktiviranja suspendiranog certifikata nakon prestanka postojanja razloga za suspenziju.
Registracijski ured (RA)	Pravna ili fizička osoba ovlaštena od davatelja usluga certificiranja zadužena za identifikaciju i potvrdu identiteta podnositelja zahtjeva za izdavanje, opoziv, suspenziju ili reaktivaciju certifikata, za obradu zahtjeva te za isporuku certifikata i uređaja korisnicima.

DEFINICIJA	ZNAČENJE
Sigurno sredstvo za izradu elektroničkog potpisa (SSCD)	Vidi pojam: „Sredstvo za izradu naprednog elektroničkog potpisa“.
Središnji RA	Središnji registracijski ured. Može registrirati korisnike, ali primarno je zadužen za koordiniranje cjelokupne RA mreže.
Sredstvo elektroničke identifikacije	Materijalna i/ili nematerijalna jedinica koja sadrži osobne identifikacijske podatke i koja se koristi za autentikaciju na *online* uslugu.
Sredstvo za izradu elektroničkog potpisa	Odgovarajuća računalna oprema ili računalni program kojeg potpisnik koristi pri izradi elektroničkog potpisa.
Sredstvo za izradu naprednog elektroničkog potpisa (SSCD)	Sredstvo za izradu elektroničkog potpisa koje osigurava: • da se podaci za izradu naprednoga elektroničkog potpisa mogu pojaviti samo jednom te da je ostvarena njihova sigurnost; • da se podaci za izradu naprednoga elektroničkog potpisa ne mogu ponoviti te da je potpis zaštićen od krivotvorenja pri korištenju postojeće raspoložive tehnologije; • da podatke za izradu naprednoga elektroničkog potpisa subjekt može pouzdano zaštititi protiv korištenja od strane drugih. Sredstvo za izradu naprednoga elektroničkog potpisa ne smije pri izradi naprednoga elektroničkog potpisa promijeniti podatke koji se potpisuju ili onemogućiti subjektu uvid u te podatke prije procesa izrade naprednoga elektroničkog potpisa.
Subjekt ili subjekt certificiranja	Subjekt (certificiranja) je entitet za kojeg se izdaje certifikat, tj. može biti fizička osoba – građanin, fizička osoba povezana s poslovnim subjektom (vidi pojam: „Pripadajuća osoba“), poslužitelj, aplikacija i sl. Podaci o subjektu sastavni su dio certifikata.
Suspenzija certifikata	Postupak kojim certifikat privremeno postaje nevažećim.
Tijelo (tijela) državne uprave (TDU)	Tijelo državne uprave je tijelo državne vlasti nadležno za obavljanje poslova državne uprave u upravnom području za koje je nadležno. Tijela državne uprave su ministarstva, državni uredi Vlade Republike Hrvatske, 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 koje je ovlašteno i odgovorno za izradu, uvođenje i administriranje pravila davanja usluga certificiranja, pripadnu dokumentaciju i procedure te za kontrolu provođenja istih.
Ugovor o obavljanju usluga certificiranja	Ugovor između fizičke osobe odnosno poslovnog subjekta zastupanog po ovlaštenoj osobi za zastupanje i davatelja usluge certificiranja koji detaljno opisuje prava i obveze svake strane u odnosu na certifikat koji se izdaje subjektu.
Vremenski žig	Elektronički potpisana potvrda izdavatelja koja potvrđuje sadržaj podataka na koji se odnosi u navedenom vremenu.

1.6.2. Kratice

KRATICA	PUNI NAZIV	ZNAČENJE
CA	*Certification Authority*	Certifikacijsko tijelo
CP	*Certification Policy*	Opća pravila davanja usluga certificiranja
CPS	*Certification Practice Statement*	Pravilnik o postupcima certificiranja
CPS_{ROOT}	*Certification Practice Statement for Fina Root CA*	Pravilnik o postupcima certificiranja za Fina Root CA
CPS_{NQC}	*Certification Practice Statement for Non-Qualified Certificates*	Pravilnik o postupcima certificiranja za nekvalificirane certifikate
CPS_{QC}	*Certification Practice Statement for Qualified Certificates*	Pravilnik o postupcima certificiranja za kvalificirane certifikate
CRL	*Certificate Revocation List*	Lista opozvanih certifikata
CSP	*Certification Service Provider*	Davatelj usluga certificiranja
CSP_{QC}	*Certification Service Provider Issuing Qualified Certificates*	Davatelj usluga izdavanja kvalificiranih certifikata
DN	*Distinguished Name*	Razlikovno ime
ISO	*International Standards Organization*	Međunarodna organizacija za normizaciju
LCP	*Lightweight Certificate Policy*	Opća pravila certificiranja za *lightweight* (lagane) certifikate
LDAP	*Lightweight Directory Access Protocol*	Protokol za pristup informacijskim direktorijima
LRA	*Local Registration Authority*	Lokalni registracijski ured
NCP	*Normalized Certificate Policy*	Opća pravila certificiranja za normalizirane certifikate
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
SSCD	*Secure Signature Creation Device*	Sredstvo za izradu naprednog elektroničkog potpisa (sigurno sredstvo za izradu elektroničkog potpisa)
SSL	*Secure Sockets Layer*	Kriptografski protokol za sigurnu razmjenu podataka putem Interneta
TDU	Tijelo (ili tijela) državne uprave	Tijelo (ili tijela) državne uprave
QTSA	*Advanced Time-Stamping Authority*	Davatelj usluga izdavanja naprednog vremenskog žiga
URL	*Uniform Resource Locator*	Internetska adresa određenog resursa

2. OBJAVE I ODGOVORNOSTI ZA REPOZITORIJ

2.1. Identifikacija tijela koje vodi repozitorij

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

Repozitorij se sastoji od dijela dostupnog na internetskim stranicama i dijela dostupnog preko javnog LDAP imenika, sukladno opisu iz točke 2.2. ovih Općih pravila.

2.2. Objava informacija o certificiranju

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

Na internetskim stranicama Fina PKI repozitorija objavljuju se:

- Opća pravila davanja usluga certificiranja,
- Uvjeti pružanja usluga certificiranja,
- cjenik usluga certificiranja,
- obrasci za korisnike,
- Fina Root CA certifikat i certifikati subordiniranih Fina CA-ova,
- CRL Fina Root CA i CRL subordiniranih CA-ova,
- obavijesti korisnicima vezane uz davanje usluga certificiranja,
- ostale informacije vezane uz rad Fina Root CA i njemu subordiniranih CA-ova.

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

Dio Fina PKI repozitorija koji je objavljen na internetskim stranicama dostupan je s adrese http://www.fina.hr/finadigicert.

U dijelu Fina PKI repozitorija dostupnog preko javnog LDAP imenika objavljuju se certifikati i CRL koje izdaju subordinirani Fina CA-ovi te je korištenjem LDAP-a omogućen dohvat pojedinog izdanog certifikata. Adrese LDAP imenika je ldap://rdc-ldap2.fina.hr.

Putem Fina OCSP servisa dostupne su informacije o statusu izdanih certifikata. Internetska adresa Fina OCSP servisa je http://ocsp.fina.hr.

Na Fina PKI repozitoriju nisu javno objavljeni dokumenti i informacije koje predstavljaju povjerljivi dio internih postupaka certificiranja.

2.3. Vrijeme ili učestalost objavljivanja

Opća pravila davanja usluga certificiranja, drugi Fina PKI dokumenti i ostale relevantne informacije objavljuju se po potrebi nakon odobrenja odgovornog tijela unutar davatelja usluga certificiranja.

Certifikati se u javnom imeniku objavljuju odmah po izdavanju.

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 4.9.10. ovih Općih pravila.

2.4. Kontrole pristupa repozitoriju

Informacije objavljene na repozitoriju su javno dostupne.

Izmjene sadržaja na internetskim stranicama Fina PKI repozitorija obavljaju ovlaštene osobe Fine nakon odobrenja odgovornog tijela unutar davatelja usluga certificiranja.

Izmjene sadržaja LDAP imenika mogu obavljati samo ovlaštene osobe s povjerljivim ulogama u Fina PKI.

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

3. IDENTIFIKACIJA I POTVRĐIVANJE IDENTITETA

Fina Root CA i njemu subordinirani Fina CA-ovi u polje „Subject“ certifikata upisuju podatke o imenu, odnosno nazivu subjekta za kojeg se certifikat izdaje. Razlikovno ime (engl. *Distinguished Name*, DN) u polju „Subject“ u certifikatima usklađeno je s preporukom IETF RFC 5280 [23] i normom X.501 [27].

Razlikovno ime u polju „Subject“ certifikata jedinstveno je unutar Fina PKI produkcijske hijerarhije zasnovane 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. Certifikati za korisnike zadovoljavaju odredbe europske Direktive o elektroničkim potpisima [10].

Postupak identifikacije i autentifikacije za potrebe Fina Root CA te za njemu subordinirane Fina CA-ove opisan je u internim Fininim dokumentima.

Identifikacija i autentifikacija korisnika kojima subordinirani Fina CA-ovi izdaju certifikate u skladu je s odredbama navedenim u poglavlju 7.3 normi HRN ETSI/EN 319 411-2 [11] i HRN ETSI/EN 319 411-3 [12], a opisana je u Općim pravilima davanja usluga certificiranja [31].

4. OPERATIVNI ZAHTJEVI NA ŽIVOTNI CIKLUS CERTIFIKATA

4.1. Podnošenje zahtjeva za izdavanje certifikata

Postupak odobravanja izdavanja Fina Root CA certifikata i certifikata za njemu subordinirane Fina CA-ove opisan je u internim Fininim dokumentima.

Postupak odobravanja izdavanja certifikata za Fina OCSP servis opisan je u internim Fininim dokumentima.

Podnošenje zahtjeva za izdavanje korisničkih certifikata opisano su u Općim pravilima davanja usluga certificiranja [31].

4.2. Obrada zahtjeva za izdavanje certifikata

Postupak odobravanja izdavanja Fina Root CA certifikata i certifikata za njemu subordinirane Fina CA-ove opisan je u internim Fininim dokumentima.

Postupak obrade zahtjeva za izdavanje certifikata za Fina OCSP servis opisan je u internim Fininim dokumentima.

Registracija i identifikacija korisnika te obrada zahtjeva za izdavanje korisničkih certifikata opisana je u Općim pravilima davanja usluga certificiranja [31].

4.3. Izdavanje certifikata

4.3.1. Radnje CA tijekom izdavanja certifikata

Temeljem potvrđenog zahtjeva za izdavanje certifikata Fina Root CA, odnosno njegovi subordinirani Fina CA-ovi obavljaju provjeru cjelovitosti i autentičnosti zahtjeva. Nakon uspješne provjere cjelovitosti i autentičnosti zahtjeva odgovarajući Finin CA smješten u Fina PKI štićenom prostoru izdaje certifikat.

4.3.2. Obavještavanje korisnika od strane CA o izdavanju certifikata

Obavještavanje korisnika o izdavanju traženog certifikata opisano je u Općim pravilima davanja usluga certificiranja [31].

4.4. Prihvaćanje certifikata

4.4.1. Provedba prihvaćanja certifikata

Prihvaćanje certifikata od strane korisnika detaljno je opisano u Općim pravilima davanja usluga certificiranja [31].

4.4.2. Objava izdanog certifikata od strane CA

Fina Root CA certifikat i certifikati njemu subordiniranih Fina CA-ova objavljuju se na internetskim stranicama Fina PKI repozitorija iz točke 2.2. ovih Općih pravila.

Certifikat kojeg Fina Root CA izdaje za Fina OCSP servis objavljuje se na internetskim stranicama Fina PKI repozitorija iz točke 2.2. ovih Općih pravila.

Korisnički certifikati objavljuju se, uz odobrenje korisnika, na javnom LDAP imeniku iz točke 2.2. ovih Općih pravila.

4.4.3. Obavještavanje drugih strana od strane CA o izdavanju certifikata

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

Obavještavanje drugih strana o izdavanju korisničkih certifikata detaljnije je opisano u Općim pravilima davanja usluga certificiranja [31].

4.5. Par ključeva i korištenje certifikata

Privatni ključ Fina Root CA i privatni ključevi njegovih subordiniranih Fina CA-ova jedini su privatni ključevi u Fina PKI iz opsega ovih Općih pravila kojima je dopušteno potpisivanje certifikata i CRL te stoga oni u ekstenziji *Key Usage* pripadajućih certifikata imaju postavljenu vrijednost *keyCertSign* i *CRLSign*.

Potpisivanje odgovora Fina OCSP servisa za status opozvanosti certifikata koje je izdao Fina Root CA dozvoljeno je samo privatnim ključem čiji je pripadajući certifikat izdao Fina Root CA, a koji u ekstenziji certifikata *Extended Key Usage* sadrži vrijednost *OCSPSigning*. Privatni ključ ovog certifikata ne smije se upotrijebiti u druge svrhe.

Korištenje privatnog ključa i pripadajućeg certifikata od strane korisnika i korištenje javnog ključa i cerifikata od strane pouzdajuće strane opisano je u Općim pravilima davanja usluga certificiranja [31].

4.6. Obnova certifikata

Obnova certifikata je postupak izrade novog certifikata korisniku. Novi certifikat sadrži nove informacije za validiranje, ali zadržava podatke o ključu i subjektu certificiranja.

Fina PKI ne podržava obnovu certifikata na ovaj način.

4.7. Obnova certifikata uz generiranje novog para ključeva

Obnova certifikata uz generiranje novog para ključeva za Fina OCSP servis opisana je u internim Fininim dokumentima.

Obnova korisničkih certifikata uz generiranje novog para ključeva opisana je u Općim pravilima davanja usluga certificiranja [31].

4.8. Izmjena unutar certifikata

Izmjena unutar certifikata je postupak u kojem korisnici podnose zahtjev za certifikat s izmijenjenim podacima povezanih sa subjektom certificiranja, a može se zatražiti samo za certifikat koji nije istekao te nije opozvan ili suspendiran.

Izmjena unutar Fina Root CA certifikata i certifikata njemu subordiniranih Fina CA-ova se ne provode.

Provođenje izmjene unutar korisničkih certifikata opisano je u Općim pravilima davanja usluga certificiranja [31].

4.9. Opoziv i suspenzija certifikata

4.9.1. Razlozi za opoziv

Certifikati se opozivaju iz sljedećih razloga:

- ako dođe do kompromitiranja privatnog ključa,
- ako neka od informacija sadržanih u certifikatu postane netočna,
- u slučaju trajne nedosupnosti ili gubitka privatniog ključa,
- u slučaju da korišteni kriptografski algoritmi i parametri prestanu pružati zahtijevanu sigurnost i zaštitu,
- ako subordinirani Fina CA ili Fina Root CA prestaje s radom, a Fina nije u mogućnosti osigurati nastavak obavljanja usluga certificiranja kod drugog davatelja usluga,
- ako certifikat nije izdan sukladno zahtjevu ili odredbama iz ovih Općih pravila.

Razlozi za opoziv korisničkih certifikata detaljnije su opisani u Općim pravilima davanja usluga certificiranja [31].

4.9.2. Tko može tražiti opoziv

Detaljan opis nalazi se u Općim pravilima davanja usluga certificiranja [31].

4.9.3. Procedura za zahtjev za opozivom

Detaljan opis nalazi se u Općim pravilima davanja usluga certificiranja [31].

4.9.4. Poček zahtjeva za opozivom

Detaljan opis nalazi se u Općim pravilima davanja usluga certificiranja [31].

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

Subordinirani Fina CA koji je izdao korisnički certifikat opozvat će izdani certifikat u najkraćem razumnom roku, a najkasnije u roku od 24 sata od primitka valjanog zahtjeva za opoziv.

Detaljan opis nalazi se u Općim pravilima davanja usluga certificiranja [31].

4.9.6. Zahtjevi za provjeru opoziva za pouzdajuće strane

Pouzdanje u opozvan ili suspendiran certifikat može imati osobnu ili poslovnu štetu za pouzdajuću stranu. Zbog toga, pouzdajuća strana pri korištenju certifikata kojeg je izdao subordinirani Fina CA ili Fina Root CA mora provesti njegovu validaciju, a što uključuje i provjeru statusa certifikata u cilju utvrđivanja njegove opozvanosti ili suspenzije.

4.9.7. Učestalost izdavanja CRL

Fina Root CA izdaje CRL svako 365 dana te u roku od 24 sata od opoziva certifikata kojeg je izdao Fina Root CA.

Subordinirani Fina CA izdaje CRL u roku od 6 sati te odmah po opozivu, suspenziji ili reaktivaciji certifikata.

4.9.8. Maksimalno kašnjenje za CRL

Subordinirani Fina CA-ovi nakon opoziva, suspenzije i reaktivacije certifikata odmah izrađuju i potpisuju CRL. Maksimalno kašnjenje CRL od trenutka njene izrade i potpisivanja do trenutka njene objave u redovitim uvjetima iznosi do dvije minute.

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

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

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

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

4.9.10. Zahtjevi na *online* provjeru opozvanih certifikata

Ne postoji obaveza korištenja Fina OCSP servisa.

4.9.11. Drugi dostupni načini objave opozvanih certifikata

Osim načina objave informacija o statusu opozvanosti certifikata opisanih u poglavlju 4.9. ovih Općih pravila Fina trenutno ne podržava druge načine objave opozvanosti certifikata.

4.9.12. Posebni zahtjevi vezani uz kompromitiranost ključa

Nema zahtjeva.

4.9.13. Razlozi za suspenziju certifikata

Suspenzija Fina Root CA certifikata i certifikata njemu subordiniranih Fina CA-ova nije dozvoljena.

Suspenzija certifikata za Fina OCSP servis nije dozvoljena.

Razlozi za suspenziju korisničkih certifikata opisani su u Općim pravilima davanja usluga certificiranja [31].

4.9.14. Tko može tražiti suspenziju certifikata

Detaljan opis nalazi se u Općim pravilima davanja usluga certificiranja [31].

4.9.15. Procedura za zahtjev za suspenziju certifikata

Detaljan opis nalazi se u Općim pravilima davanja usluga certificiranja [31].

4.9.16. Ograničenje na trajanje suspenzije

Detaljan opis nalazi se u Općim pravilima davanja usluga certificiranja [31].

4.10. Usluge statusa certifikata

4.10.1. Operativna svojstva

Usluge provjere statusa certifikata osiguravaju informaciju o statusu opozvanosti certifikata čiji vremenski period valjanosti nije istekao. Provjera statusa certifikata obavlja se korištenjem CRL ili OCSP servisa.

Integritet i autentičnost informacije o statusu certifikata u CRL osigurani su elektroničkim potpisom Fininog CA koji je izdao CRL. Adrese na kojima je objavljena CRL sadržane su u ekstenziji CRLDistributionPoints u svakom izdanom certifikatu.

Integritet i autentičnost informacije o statusu certifikata u Fina OCSP servisu osigurani su elektroničkim potpisom koji je izrađen certifikatom za Fina OCSP servis, a kojeg je izdao onaj Finin CA koji je ujedno izdao i certifikat čiji se status provjerava. Adresa Fina OCSP servisa sadržana je u ekstenziji *Authority Information Access* u svakom izdanom certifikatu.

4.10.2. Dostupnost usluga

Dostupnost CRL je 24 sata na dan, 7 dana u tjednu. U slučaju ispada sustava, nastanka okolnosti koje su izvan kontrole Fine ili uslijed utjecaja više sile, usluga će biti dostupna maksimalno moguće vrijeme u skladu s najboljim poslovnim praksama.

Točke pristupa usluzi za provjeru valjanosti certifikata dane su u točki 4.10.1. ovih Općih pravila.

4.10.3. Opcionalna svojstva

Nema odredbi.

4.11. Kraj korištenja

Odredbe vezane uz kraj korištenja korisničkih certifikata koje izdaju subordinirani Fina CA-ovi navedene su u Općim pravilima davanja usluga certificiranja [31].

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 Općim pravilima davanja usluga certificiranja [31].

5. PROVJERA SUSTAVA, UPRAVLJANJA I RADNIH POSTUPAKA

Mjere fizičke zaštite, postupci koje Fina primjenjuje u zaštiti Fina PKI sustava, kao i postupci provjere sustava, upravljanja i radnih postupaka u Fina PKI interne su prirode te se njihovi detalji ne objavljuju javno. Detaljnije mjere i postupci opisani su u internim dokumentima Fine koji su na raspolaganju ovlaštenim tijelima iz poglavlja 8. ovih Općih pravila.

5.1. Kontrole fizičke sigurnosti

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

5.1.1. Lokacija objekta i njegova 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.

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

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 Fina Root CA sustavu, sustavi njemu subordiniranih Fina CA-ova te fizički pristup repozitoriju i arhivi dopušten je ovlaštenim zaposlenicima Fine u skladu s njihovim povjerljivim ulogama i ovlastima.

O svakom fizičkom pristupu Fina PKI štićenom prostoru vodi se evidencija.

5.1.3. Sustavi za napajanje i klimatizaciju

Fina PKI štićeni prostor u kojem se nalazi Fina Root CA sustav i sustavi njemu subordiniranih Fina CA-ova te pripadajući uređaji opskrbljeni su neprekidnim napajanjem električnom energijom i klimatizacijom koja je dimenzionirana na način da osigura odgovarajuće radne uvjete i u slučaju prekida vanjskog napajanja.

5.1.4. Opasnost od poplave

Oprema Fina Root CA sustava i sustavi njemu subordiniranih Fina CA-ova smještena je na lokacijama koje su osigurano od poplave.

5.1.5. Protupožarna zaštita

Oprema Fina Root CA sustava i sustavi njemu subordiniranih Fina CA-ova zaštićena je sustavom protupožarne zaštite sukladno propisanoj i važećoj zakonskoj regulativi te Fininim internim dokumentima.

5.1.6. Pohrana medija

Sigurnosne kopije Fina Root CA sustava, sigurnosne kopije podataka i arhive, kopije sadržaja repozitorija te sigurnosne kopije programske opreme pohranjuju se na siguran način kako bi se zaštitile od oštećenja, otuđenja ili neovlaštenog pristupa.

5.1.7. Zbrinjavanje otpada

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

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

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

5.1.8. Sigurnosne kopije na drugoj lokaciji

Sigurnosne kopije Fina Root CA sustava, arhivske ili sigurnosne kopije podataka, kopije sadržaja repozitorija te sigurnosne kopije programske opreme pohranjuju se na udaljenoj pričuvnoj lokaciji iz točke 5.1.1. ovih Općih pravila, izdvojeno od primarnog produkcijskog sustava certificiranja. Ove su sigurnosne kopije u odnosu na njihove originale zaštićene jednakom ili višom razinom mjera fizičke zaštite.

5.2. Kontrola procedura

5.2.1. Povjerljive uloge

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

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

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

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

5.2.2. Broj osoba potrebnih za obavljanje zadataka

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

Rad u Fina PKI štićenom prostoru provodi se isključivo uz istovremenu prisutnost najmanje dvije ovlaštene osobe s ulogama u Fina PKI koje imaju pravo pristupa određenom dijelu sustava.

5.2.3. Identifikacija i potvrđivanje identiteta za svaku ulogu

Identifikacija ovlaštenih osoba i određivanje prava pristupa za obavljanje određenih poslova provodi se u skladu s organizacijom Fina PKI, kroz sigurnosne procedure i postupke provjere te se ostvaruje pomoću sigurnosnih mehanizama u sustavu.

5.2.4. Uloge koje zahtijevaju odvajanje dužnosti

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

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

5.3. Provjere osoblja

5.3.1. Kvalifikacije, radno iskustvo i zahtjevi za provjerom osoblja

Fina osigurava da sve ovlaštene osobe koje obavljaju poslove vezane uz Fina Root CA imaju odgovarajuća stručna znanja u radu s kriptografskim tehnologijama te stručna znanja iz zaštite računalnih sustava i informacijskih baza.

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

5.3.2. Procedure provjere primjerenosti osoblja

Prije početka rada na poslovima u Fina PKI, Fina provodi odgovarajuće provjere kandidata da bi procijenila njihovu sposobnost i pouzdanost u skladu s potrebama poslova u Fina PKI.

5.3.3. Zahtjevi za školovanjem

Ovlaštenim osobama s povjerljivim ulogama u Fina PKI osigurava se školovanje i usavršavanje sukladno ulogama koje su im dodijeljene.

5.3.4. Učestalost i uvjeti za obnovu znanja

Usavršavanje specijalističkih znanja i vještina ovlaštenih osoba s povjerljivim ulogama u Fina PKI obavlja se pri dodjeli uloge i prema potrebi.

5.3.5. Učestalost i slijed izmjene zaposlenika

Promjena poslova zaposlenika obavlja se kada se za to javi potreba, ovisno o zahtjevima organizacijskih jedinica Fine ili na temelju zahtjeva zaposlenika.

5.3.6. Kazne za neovlaštene radnje

U slučaju izvođenja neovlaštene radnje ili zlonamjerne radnje koju je izvela ovlaštena osoba u Fina PKI primjenjuju se odredbe važeće zakonske regulative i internih pravilnika Fibe.

5.3.7. Zahtjevi na vanjske suradnike

Vanjskim suradnicima ne dodjeljuju se uloge na sustavima u Fina PKI.

Vanjskim suradnicima pristup u Fina PKI štićeni prostor dopušten je jedino uz dualnu pratnju ovlaštenih osoba s ulogama u Fina PKI.

Zahtjevi na vanjske suradnike određuju se ugovorom sklopljenim između Fine i vanjskog suradnika.

Fizički pristup vanjskim suradnicima Fina Root CA sustavu, sustavu njemu subordiniranih Fina CA-ova te fizički pristup repozitoriju i arhivi propisan je Fininim internim procedurama odobravanja i kontrole pristupa opremi za izdavanje digitalnih certifikata i vremenskih žigova.

5.3.8. Dokumentacija koja je dostupna osoblju

Ovlaštenim osobama u Fina PKI dostupna je dokumentacija potrebna za obavljanje njihovih radnih zadataka sukladno dodijeljenim ulogama i pripadnim ovlaštenjima.

5.4. Postupci s dnevnicima sustava

5.4.1. Tipovi događaja koji se zapisuju

Tipovi događaja koji se bilježe u Fina PKI vezani su uz:

- upravljanje životnim ciklusom ključeva Fina Root CA i njemu subordiniranih CA-ova,
- upravljanje životnim ciklusom ključeva koje generiranih na Fina PKI sustavima,
- životni ciklus kriptografskih uređaja u Fina PKI,
- upravljanje životnim ciklusom certifikata koje izdaju Fina Root CA i njemu subordiniranih CA-ovi,
- informacije o statusima opozvanosti certifikata,

- sigurnosne događaje vezane uz pristup Fina Root CA sustavu, sustavu njemu subordiniranih Fina CA-ova te fizički pristup repozitoriju i arhivi,
- sustave tehničke zaštite Fina PKI štićenog prostora,
- ostale bitne elemente vezane uz sigurnost Fina PKI sustava.

5.4.2. Učestalost obrade dnevnika sustava

Zapisi dnevnika sustava u Fina PKI kontinuirano se prikupljaju.

Zapisi dnevnika sustava za Fina Root CA pregledavaju se nakon svakog izvođenja operacija na Fina Root CA te u slučaju izvanrednih situacija.

Pregled zapisa dnevnika sustava za subordinirane Fina CA-ove opisan je u Općim pravilima davanja usluge certificiranja [31].

Radnje poduzete na osnovu prikupljanja dnevnika sustava se dokumentiraju.

5.4.3. Vremenski period pohrane dnevnika sustava

Dnevnici sustava sa zapisima iz točke 5.4.1. čuvaju se najmanje 10 godina.

5.4.4. Zaštita dnevnika sustava

Dnevnici sustava zaštićuju se mehanizmima i postupcima koji osiguravaju povjerljivost i cjelovitost dnevnika. Novi zapisi dnevnika sustava ne zapisuju se preko postojećih zapisa.

Pregled dnevnika sustava u Fina PKI dopušten je samo ovlaštenim osobama s povjerljivom ulogom Službenik za nadzor.

5.4.5. Postupci izrade sigurnosnih kopija dnevnika sustava

Novonastali dnevnici Fina PKI sustava u elektroničkom obliku se kopiraju te se njihove kopije pohranjuju na udaljenoj pričuvnoj lokaciji Fine iz točke 5.1.1. ovih Općih pravila. Kopije dnevnika sustava se, u odnosu na dnevnike na primarnoj produkcijskoj lokaciji, zaštićuju jednakom ili višom razinom zaštite.

5.4.6. Sustav prikupljanja dnevnika sustava (unutarnji ili vanjski)

Ovisno o vrsti podataka, dnevnici sustava na internom sustavu prikupljaju se automatski ili ih prikuplja ovlaštena osoba s povjerljivom ulogom.

Detaljnije odredbe koje se odnose na sustav prikupljanja dnevnika sustava nalaze se u internim dokumentima Fine.

5.4.7. Obavještavanje subjekta uzročnika događaja

U ovisnosti o težini zapisanog događaja u dnevniku sustava i kada je to primjenjivo, Fina zadržava pravo obavještavanja uzročnika događaja o zapisu događaja i o posljedicama događaja.

5.4.8. Procjena ranjivosti

Procjena ranjivosti temeljena na analizi dnevnika sustava sastavni je dio kontinuirane analize rizika.

5.5. Arhiviranje zapisa

5.5.1. Tipovi arhiviranih zapisa

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

- podaci o registraciji korisnika,
- svi certifikati koje izdaje Fina Root CA i njemu subordinirani Fina CA-ovi,
- evidencija o statusu opozvanosti certifikata,
- zapisi dnevnika sustava iz točke 5.4.1. ovih Općih pravila,
- drugi podaci i Finina dokumentacija, sukladno važećim propisima.

5.5.2. Vremenski period arhiviranja

Svi arhivirani podaci i dokumentacija čuvaju se najmanje 10 godina.

5.5.3. Zaštita arhive

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

Pregled arhiviranih podataka i dokumentacije u Fina PKI obavlja Službenik za nadzor sustava.

Pristup arhiviranim podacima i dokumentaciji o registraciji korisnika u papirnatom obliku dopušten je Službenik za nadzor sustava i osobama ovlaštenim osobama koji obavljaju poslove arhiviranja.

Arhivirani zapisi su na zahtjev raspoloživi samo ovlaštenim tijelima, posebice u svrhu pružanja dokaza o izdanom certifikatu i vremenskom žigu za potrebe sudskih postupaka.

5.5.4. Postupci izrade sigurnosnih kopija arhive

Sigurnosna kopija elektroničkog dijela arhive Fina PKI izrađuje se u Fina PKI štićenom prostoru na primarnoj produkcijskoj lokaciji te se na siguran način čuva u Fina PKI štićenom prostoru na udaljenoj pričuvnoj lokaciji iz točke 5.1.1. ovih Općih pravila.

5.5.5. Zahtjevi na zaštitu zapisa vremenskim žigom

Nema odredbi.

5.5.6. Sustav prikupljanja arhiva (unutarnji ili vanjski)

Zapisi za arhiviranje prikupljaju se na način koji ovisi o vrsti zapisa i mjestu na kojem su prikupljeni.

Zapisi za arhiviranje vezani uz rad Fina Root CA prikupljaju se i arhiviraju interno.

Zapisi za arhiviranje vezani uz rad subordiniranih Fina CA-ova koji su nastali u Fini prikupljaju se i arhiviraju interno, a prikupljanje i arhiviranje zapisa koji su nastali u vanjskim ugovorenim RA-ovima regulirano je ugovorom.

5.5.7. Postupci pristupa i verifikacije podataka iz arhiva

Pristup zapisima iz arhive imaju samo osobe ovlaštene za pristup tim podacima, a sukladno internim Fininim dokumentima. Verifikacija podataka iz arhive obavlja se provjerom njihove cjelovitosti.

5.6. Promjena CA ključa

Fina provodi redovitu promjenu ključeva subordiniranih Fina CA-ova na način da nove ključeve za Fina CA-ove generira razumno vrijeme prije isteka valjanosti njihovih certifikata, a tijekom perioda valjanosti Fina Root CA certifikata. Fina Root CA kao Finin krovni CA s dugim vremenom važenja certifikata potpisuje certifikate svojih subordiniranih Fina CA-ova. Certifikati subordiniranih Fina CA-ova dostupni su za preuzimanje s internetskih stranica repozitorija iz točke 2.2 ovih Općih pravila.

5.7. Oporavak od kompromitiranja ili katastrofe

5.7.1. Postupci u slučaju incidenta ili kompromitiranja

Fina ima Plan kontinuiteta poslovanja Fina PKI čija je svrha uspostava sustava nadležnosti i odgovornosti te određivanje postupaka koji se izvršavaju u slučaju katastrofe. Cilj plana je osiguravanje kontinuiteta poslovanja u slučaju incidenta koji ozbiljnije ugrožava poslovni proces. Plan kontinuiteta poslovanja Fina PKI sadrži i plan oporavka od katastrofe.

5.7.2. Oštećenja u računalnim resursima, programima i/ili podacima

Postupcima koji su određeni u okviru Plana kontinuiteta poslovanja Fina PKI obuhvaćen je i povrat podataka te izmjenu opreme u slučaju oštećenja Fina PKI računalnih i mrežnih resursa, softvera ili podataka.

5.7.3. Postupci u slučaju kompromitiranja privatnog ključa

U slučaju kompromitiranja privatnog potpisnog ključa Fina Root CA ili njemu subordiniranih Fina CA-ova pripadajući certifikat bit će opozvan.

Fina će odmah opozvati sve certifikate izdane uporabom kompromitiranog privatnog ključa.

O opozivu certifikata Fina će obavijestiti sudionike Fina PKI te objaviti informaciju o njihovom opozivu.

Nakon ustanovljavanja i otklanjanja uzroka koji su prouzročili kompromitiranje ključa, Finin CA čiji je certifikat opozvan će generirati novi par CA ključeva, ponovno će izdati certifikate postojećim korisnicima te će sve naredne informacije o opozvanosti certifikata potpisivati uporabom novog ključa. Novi CA certifikat biti će dostupan sudionicima Fina PKI na način na koji je bio dostupan i opozvani CA certifikat.

Detaljnije odredbe koje se odnose na postupke u slučaju kompromitiranja ili sumnje u kompromitiranost privatnog ključa CA nalaze se u internim dokumentima Fine.

5.7.4. Mogućnost nastavka poslovanja nakon katastrofe

Vidi točku 5.7.1.

5.8. Prestanak rada CA ili RA

U slučaju prestanka davanja usluga certificiranja ili jednog dijela tih usluga, Fina će osigurati da prekid korištenja usluga i utjecaj na korisnike i pouzdajuće strane bude što je moguće manji.

U slučaju prestanka rada vanjskog ugovorenog RA njegove poslove može preuzeti Fina RA mreža. Detaljnije odredbe vezane uz prekid rada vanjskog ugovorenog RA određuju se međusobnim ugovornim obvezama.

O mogućem planiranom prestanku davanja usluga certificiranja Fina će obavijestiti svakog korisnika usluge, ministarstvo nadležno za gospodarstvo i pouzdajuće strane najmanje tri mjeseca ranije.

U slučaju prestanka davanja usluga certificiranja iz bilo kojeg razloga Fina će kod drugog davatelja usluga certificiranja osigurati nastavak davanja usluga certificiranja te će drugom davatelju usluga certificiranja dostaviti svu dokumentaciju prikupljenu u postupku registracije korisnika kao i svu dokumentaciju o izdanim certifikatima.

U slučaju da Fina iz bilo kojeg razloga nije u mogućnosti osigurati nastavak obavljanja usluga certificiranja kod drugog davatelja usluga tada će Fina opozvati sve izdane certifikate.

U slučaju prestanka obavljanja usluga certificiranja Fina će nastaviti održavati podatke korisnika koji su prikupljeni u postupku registracije te podatke nastale za vrijeme davanja usluga certificiranja koji su potrebni za pružanje dokaza u sudskim, upravnim i drugim postupcima, ili će Fina s drugim poslovnim subjektom ugovoriti održavanje istih.

6. UPRAVLJANJE TEHNIČKOM SIGURNOŠĆU

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 te za Fina OCSP servisa i Fina QTSA 2015 servis izdavanja naprednih vremenskih žigova.

Upravljanje tehničkom sigurnošću vezanoj uz izdavanje korisničkih certifikata opisano ju u dokumentu Opća pravila davanja usluga certificiranja [31].

6.1. Generiranje i instalacija para ključeva

6.1.1. Generiranje para ključeva

Postupak generiranja para ključeva za Fina Root provodi se formalnom ceremonijom generiranja para ključeva za Fina Root CA.

Postupak generiranja parova ključeva za subordinirane Fina CA-ove provodi se formalnom ceremonijom generiranja parova ključeva za subordinirane Fina CA-ove.

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. ovih Općih pravila.

Fina Root CA i njemu subordinirani Fina CA-ovi nalaze se tijekom i nakon ceremonije generiranja parova ključeva u Fina PKI štićenom prostoru iz točke 5.1.1. ovih Općih pravila, a pristup ovim CA-ovima dopušten je ovlaštenim osobama Fina PKI s povjerljivim ulogama, uz 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 te parova ključeva za njemu subordinirane Fina CA-ove se snima ili provođenju postupka svjedoči kvalificirani auditor.

Za cijeli postupak ceremonije generiranja parova ključeva Fina Root CA i njemu subordinirane Fina CA-ova izrađuju se video zapisi ceremonija koji se nakon ceremonije čuvaju u Fina PKI štićenom prostoru.

Generiranje para ključeva za potpis odgovora Fina OCSP servisa certifikatom kojeg izdaje Fina Root CA provodi se u HSM modulu koji zadovoljava zahtjeve točke 6.2.1. ovih Općih pravila, a koji je smješten u Fina PKI štićenom prostoru iz točke 5.1.1. ovih Općih pravila.

Par ključeva za Fina QTSA 2015 generira se u HSM modulu koji zadovoljava zahtjeve iz točke 6.2.1. ovih Općih pravila, a koji je smješten u Fina PKI štićenom prostoru iz točke 5.1.1. ovih Općih pravila.

U postupku generiranja para ključeva za Fina QTSA servis sudjeluju sljedeće ovlaštene osobe s povjerljivim ulogama u Fina QTSA:

- Službenik za sigurnost, 1 osoba;
- Administrator sustava, 2 osobe;
- Službenik za nadzor sustava, 1 osoba.

Generiranje parova ključeva za potpis odgovora Fina OCSP servisa certifikatima koje izdaju subordinirani Fina CA-ovi opisano je u Općim pravilima davanja usluga certificiranja [30].

Fina Root CA ne generira parove korisničkih ključeva i ne izdaje korisničke certifikate. Generiranje parova ključeva za korisničke certifikate koje izdaju subordinirani Fina CA-ovi opisano je u Općim pravilima davanja usluga certificiranja [31].

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 Općim pravilima davanja usluga certificiranja [31].

6.1.3. Dostava javnog ključa CA-u

Fina Root CA ne izdaje korisničke certifikate.

Dostava javnih korisničkih ključeva povezanih s korisničkim certifikatima koje izdaju subordinirani Fina CA-ovi opisana je u Općim pravilima davanja usluga certificiranja [31].

6.1.4. Dostava CA javnog ključa pouzdajućim stranama

Pouzdajuće strane mogu preuzeti Fina Root CA certifikat i certifikate njemu subordiniranih Fina CA-ova s internetskih stranica Fina PKI repozitorija iz točke 2.2. ovih Općih pravila.

Izvornost Fina Root CA certifikata osigurava se dostavom njegova sažetka pouzdanim kanalom, na zahtjev.

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 (Fina RDC 2015 i Fina RDC-TDU 2015) upotrebljavaju sha256WithRSA algoritam s ključem duljine 4096 bita,
- Fina OCSP servis upotrebljava RSA ključeve duljine 2048 bita,
- Fina QTSA 2015 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 [14].

Ključevi koje upotrebljavaju Fina OCSP servis i Fina QTSA 2015 servis izdavanja naprednih vremenskih žigova generiraju se sukladno normizacijskom dokumentu ETSI TS 119 312 [14].

Ključevi koje upotrebljavaju korisnici generiraju se na način opisan u Općim pravilima davanja usluga certificiranja [31].

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

Fina Root CA i njemu subordinirani Fina CA-ovi koriste privatne potpisne ključeve samo za potpisivanje izdanih certifikata i odgovarajuće CRL.

Privatni ključ za Fina QTSA 2015 koristi se samo za elektronički potpis naprednih vremenskih žigova.

Privatni ključevi Fina OCSP servisa koriste se samo za potpise odgovora Fina OCSP servisa.

Namjene ključeva (po X.509 v3 polju uporabe ključa) za korisničke certifikate opisane su u točki 6.1.7. Općih pravila davanja usluga certificiranja [31].

6.2. Zaštita privatnog ključa i tehnike upravljanja kriptografskim modulom

6.2.1. Norme i upravljačke funkcije kriptografskog modula

Privatni ključ za Fina Root CA generira se i štiti HSM-om koji zadovoljava zahtjeve prema FIPS 140-2 [24] razina 3. Fina Root CA s pripadajućim HSM-om je cijelo vrijeme izdvojen od računalne mreže (*offline*).

Privatni ključevi za subordinirane Fina CA-ove generiraju se i štite HSM-om koji zadovoljava zahtjeve prema FIPS 140-2 [24] razina 3.

Privatni ključevi za Fina OCSP servis te za Fina QTSA 2015 generiraju se i štite HSM-om koji zadovoljava zahtjeve prema FIPS 140-2 [24] razina 3.

Norme i upravljačke funkcije kriptografskih modula u kojem se generiraju privatni ključevi korisnika opisani su u točki 6.2.1. Općih pravila davanja usluga certificiranja [31].

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

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

HSM kojim se štiti privatni ključ Fina Root CA te HSM kojim se štite privatni ključevi subordiniranih CA-ova smješteni su u prostoru najviše razine sigurnosti unutar Fina PKI štićenog prostora. Fizički pristup ovim HSM-ovima provodi se uz dualnu kontrolu ovlaštenih osoba s povjerljivim ulogama u Fina PKI.

Upravljanje privatnim 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 kojim se štiti privatni ključ Fina OCSP servisa i privatni ključ Fina QTSA 2015 smješten je u prostoru najviše razine sigurnosti unutar Fina PKI štićenog prostora. Upravljanje privatnim ključem Fina OCSP servisa i privatnim ključem Fina QTSA 2015 provodi se fizičkim pristupom HSM-u uz dualnu kontrolu te autorizacijom dvije ovlaštene osobe s povjerljivim ulogama u Fina PKI.

6.2.3. Sigurno skladištenje privatnog ključa (*key escrow*)

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

Za skladištenje privatnih ključeva Fina OCSP servisa i Fina QTSA 2015 vrijede ista pravila kao za Fina Root CA i njemu subordiniranih Fina CA-ova.

6.2.4. Sigurnosno kopiranje privatnog ključa

Sigurnosno kopiranje privatnog ključa Fina Root CA i njemu subordiniranih Fina CA-ova provodi se u prostoru najviše razine sigurnosti unutar Fina PKI štićenog prostora pod dualnom kontrolom od strane ovlaštenih osoba s povjerljivim ulogama u Fina PKI. Privatni ključ Fina Root CA i njemu subordiniranih Fina CA-ova kopira se iz kriptografskog modula isključivo u enkriptiranom obliku. Sigurnosne kopije privatnog ključa Fina Root CA i njemu subordiniranih Fina CA-ova čuvaju se u enkriptiranom obliku u kontroliranom broju kopija privatnog ključa u sigurnim prostorima najviše razine sigurnosti unutar Fina PKI štićenih prostora na odvojenim lokacijama.

Sigurnosne kopije privatnih ključeva Fina OCSP servisa te privatnog ključa Fina QTSA 2015 čuvaju se u enkriptiranom obliku na magnetskim trakama u kontroliranom broju kopija privatnog ključa u sigurnom prostoru najviše razine sigurnosti 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 te sigurnosne kopije privatnih ključeva Fina OCSP servisa i privatnog ključa Fina QTSA 2015 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 te privatnih ključeva Fina OCSP servisa i privatnog ključa Fina QTSA 2015, osim navedenih.

6.2.5. Arhiviranje privatnog ključa

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

Privatni ključevi Fina OCSP servisa te privatni ključ Fina QTSA 2015 ne arhiviraju se.

6.2.6. Prijenos privatnog ključa u ili iz kriptografskog modula

Ako privatni ključ Fina Root CA ili njemu subordiniranih Fina CA-ova treba prenijeti iz ili u HSM, za vrijeme dok je izvan HSM-a privatni ključ je zaštićen na način koji osigurava jednaku razinu sigurnosti kao i kad se nalazi u HSM-u. Postupak prijenosa privatnog ključa provode samo ovlaštene osobe s povjerljivim ulogama u Fina PKI, uz dualnu kontrolu.

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

Prijenos privatnog ključa Fina OCSP servisa te privatnog ključa Fina QTSA 2015 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 kriptografskim modulima i mogu se koristiti jedino ako su propisno aktivirani.

Privatni ključevi TSA zaštićeni su kriptografskim modulima i mogu se koristiti jedino ako su propisno aktivirani.

Privatni ključevi za potpis odgovora Fina OCSP servisa zaštićeni su kriptografskim modulima i mogu se koristiti jedino ako su propisno aktivirani.

6.2.8. Metoda aktivacije privatnog ključa

Aktivaciju privatnih ključeva Fina Root CA ili njemu subordiniranih Fina CA-ova provode dvije ovlaštene osobe s povjerljivim ulogama u Fina PKI. Svaka od ovih ovlaštenih osoba za aktivaciju HSM-a upotrebljava hardversko sredstvo za aktivaciju i pripadajući tajni PIN.

Aktivacija privatnog ključa za potpis odgovora Fina OCSP servisa te aktivacija privatnog ključa Fina QTSA 2015 provodi se na isti način kao i aktivacija privatnih ključeva Fina Root CA ili njemu subordiniranih Fina CA-ova.

Aktivacija privatnih ključeva korisnika opisana je u Općim pravilima davanja usluga certificiranja [31].

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.

Privatni ključevi subordiniranih Fina CA-ova deaktiviraju se:
- zaustavljanjem CA serverskog procesa,
- odjavom s HSM-a,
- isključenjem HSM-a,
- isključenjem servera povezanim s HSM-om.

Privatni ključevi za potpis odgovora Fina OCSP servisa i privatni ključ Fina QTSA deaktiviraju se na isti način kao i privatni ključevi subordiniranih Fina CA-ova.

6.2.10. Metoda uništavanja privatnog ključa

Postupak uništavanja privatnog ključa Fina Root CA i privatnih ključeva njemu subordiniranih Fina CA-ova provodi se nakon isteka perioda njihove valjanosti, a izvodi se od strane ovlaštenih osoba s povjerljivim ulogama u Fina PKI pod minimalno dualnom kontrolom.

Uništavanje privatnog ključa Fina Root CA ili privatnih ključeva njemu subordiniranih Fina CA-ova provodi se na siguran način, sukladno internim Fininim dokumentima. Postupak uništavanja privatnih ključeva Fina Root CA ili njemu subordiniranih Fina CA-ova osigurava da se nakon uništavanja privatni ključevi ni na koji način ne mogu oporaviti ili ponovno koristiti.

Uništenje privatnog ključa za Fina OCSP servis i Fina QTSA provodi se na isti način kao i uništenje privatnih ključeva subordiniranih Fina CA-ova.

6.2.11. Ocjena kriptografskog modula

Ocjena HSM-ova za Fina Root CA i njemu subordinirane Fina CA-ove provodi se sukladno zahtjevima opisanim u točki 6.2.1. Ovih općih pravila.

Ocjena HSM-ova modula za Fina OCSP servis i Fina QTSA provodi se na isti način kao i ocjena kriptografskih modula subordiniranih Fina CA-ova.

6.3. Ostali vidovi upravljanja parom ključeva

6.3.1. Arhiviranje javnog ključa

Javni ključ Fina Root CA kao i javni ključevi njemu subordiniranih Fina CA-ova su sastavni dio pripadajućih CA certifikata koji se arhiviraju sukladno točkama 5.5.3. i 5.5.4. ovih Općih pravila.

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

Ovi ključevi u arhivi čuvaju se na rok iz točke 5.5.2. ovih Općih pravila.

6.3.2. Periodi valjanosti certifikata i korištenja para ključeva

Predviđeni vremenski period valjanosti certifikata po vrstama određen je u Tablici 6.1.

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

Tablica 6.1. Rokovi uporabe certifikata

Vremenski period valjanosti privatnog ključa jednak je vremenskom periodu valjanosti pripadajućeg certifikata. Certifikati i pripadajući ključevi ne smiju se upotrebljavati nakon isteka roka valjanosti certifikata, nakon opoziva certifikata ili za vrijeme dok je certifikat suspendiran.

Vremenski periodi valjanosti korisničkih certifikata definirani su u Općim pravilima davanja usluga certificiranja [31].

6.4. Aktivacijski podaci

6.4.1. Generiranje i instalacija aktivacijskih podataka

Aktivacijski podaci povezani s privatnim ključem za Fina Root CA generiraju se i instaliraju prilikom provođenja formalne ceremonije generiranja para ključeva za Fina Root CA.

Aktivacijski podaci povezani s privatnim ključevima za subordinirane Fina CA-ove generiraju se i instaliraju prilikom provođenja formalne ceremonije generiranja para ključeva za subordinirane Fina CA-ove.

Aktivacijski podaci povezani s privatnim ključem za Fina OCSP servis i aktivacijski podaci povezani s privatnim ključem za Fina QTSA 2015 generiraju se i instaliraju u prilikom postupka generiranja pripadajućeg privatnog ključa.

Generiranje i instalacija aktivacijskih podataka povezanih s privatnim ključevima korisničkih certifikata opisana je u Općim pravilima davanja usluga certificiranja [31].

6.4.2. Zaštita aktivacijskih podataka

Aktivacijski podaci povezani s privatnim ključem za Fina Root CA te aktivacijski podaci povezani s privatnim ključevima za subordinirane Fina CA-ove podijeljeni su na hardverska sredstva za aktivaciju, sukladno točki 6.2.2. ovih Općih pravila, a koja se zaštićena pripadajućim PIN-ovima na siguran način čuvaju u Fina PKI štićenom prostoru.

Zaštita aktivacijskih podataka povezanih s privatnim ključem za Fina OCSP servis i aktivacijski podaci povezani s privatnim ključem za Fina QTSA 2015 provodi se na jednak način kao i zaštita aktivacijskih podataka povezanih s privatnim ključevima subordiniranih Fina CA-ova.

Zaštita aktivacijskih podataka povezanih s privatnim ključevima korisničkih certifikata opisana je u Općim pravilima davanja usluga certificiranja [31].

6.4.3. Ostale odredbe o aktivacijskim podacima

Dodatni zahtjevi za aktivacijske podatke povezane s privatnim potpisnim ključevima definirani su internim Fininim dokumentima.

6.5. Upravljanje računalnom sigurnošću

Fina osigurava da su svi zahtjevi na računalnu sigurnost Fina PKI sustava usklađeni s normom HRN ETSI/EN 319 411-3 [12] i normom HRN ETSI/EN 319 411-2 [11] u slučajevima kada ona postavlja zahtjeve za višom razinom računalne sigurnosti, te sa zahtjevima iz dokumenta CA/Browser Forum Baseline Requirements [28].

Računalni resursi štite se sigurnosnim mjerama sukladno normama ISO/IEC 27001 [18] i ISO/IEC 27002 [19].

6.6. Tehničko upravljanje životnim ciklusom

Ako Fina obavlja razvoj softvera za Fina PKI posebno se vodi računa o:

- sigurnosti razvojne okoline,
- smjernicama o sigurnosti u životnog ciklusa razvoja softvera,
- metodologiji za siguran razvoj softvera i sigurnoj izradi koda,
- posebnim i specifičnim smjernicama za korišteni programski jezik,
- sigurnošću u upravljanju verzijama,

- sposobnošću za izbjegavanje, pronalaženje i popravljanje ranjivosti na sustavima.

Kada se nabavlja razvoj informacijskog sustava i softvera od vanjskog izvođača, Fina ugovorom s dobavljačem osigurava sigurnosne principe razvoja 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. ovih Općih pravila.

6.7. Provjera mrežne sigurnosti

Sigurnost računalne mreže Fina PKI sustava zasnovana je na konceptu odjeljivanja mreže na mrežne zone različitih razina. Mrežne zone odjeljuju se vatrozidima koji propuštaju samo nužan mrežni promet.

Detaljniji opis provjere mrežne sigurnosti opisan je u internim Fininim dokumentima.

6.8. Uporaba vremenskog žiga

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

Podatak o vremenu dobiven s internog servisa točnog vremena ugrađuje se u zapise dnevnika sustava opisanim u točki 5.4. ovih Općih pravila.

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 Općim pravilima davanja usluga certificiranja [31].

7.1. Profil certifikata

Profili certifikata koje izdaje Fina Root CA za subordinirane Fina CA-ove usklađeni su s CA/Browser Forum Baseline Requirements [28].

Profili certifikata koje izdaje Fina Root CA za potpisivanje CRL usklađeni su s preporukom IETF RFC 5280 [23].

Profili certifikata koje izdaje Fina Root CA za potpisivanje OCSP odgovora usklađeni su s preporukom IETF RFC 5280 [23], i IETF RFC 6960 [29].

Osnovna polja Fina Root CA certifikata navedena su u Tablici 7.1.

Polje	Atribut	Vrijednost
Version	Version	X.509 V3
serialNumber	CertificateSerialNumber	Serijski broj certifikata s entropijom od 32 bita (duljina serijskog broja:12 ili 13 bajtova)
signatureAlgorithm	AlgorithmIdentifier	sha256WithRSAEncryption OID: 1.2.840.113549.1.1.11
signatureValue		Potpis izdavatelja certifikata
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
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption OID: 1.2.840.113549.1.1.1
	subjectPublicKey	Javni ključ CA: 4096 bita

Tablica 7.1. Osnovna polja Fina Root CA certifikata

Osnovna polja certifikata subordiniranih Fina CA-ova navedena su u Tablici 7.2.

Polje	Atribut	Vrijednost
Version	Version	X.509 V3
serialNumber	CertificateSerialNumber	Serijski broj certifikata s entropijom od 32 bita (duljina serijskog broja:12 ili 13 bajtova)
signatureAlgorithm	AlgorithmIdentifier	sha256WithRSAEncryption OID: 1.2.840.113549.1.1.11
signatureValue		Potpis izdavatelja certifikata
Issuer	commonName	Fina Root CA
	organizationName	Financijska agencija
	countryName	HR
Validity	notBefore	Vrijeme izdavanja certifikata
	notAfter	Vrijeme izdavanja certifikata + 10 godina
Subject	commonName	Fina RDC 2015 Fina RDC-TDU 2015
	organizationName	Financijska agencija
	countryName	HR
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption OID: 1.2.840.113549.1.1.1
	subjectPublicKey	Javni ključ CA: 4096 bita

Tablica 7.2. Osnovna polja certifikata subordiniranih Fina CA-ova

Osnovna polja certifikata za Fina OCSP servis kojeg izdaje Fina Root CA navedena su u Tablici 7.3.

Polje	Atribut	Vrijednost
Version	Version	X.509 V3
serialNumber	CertificateSerialNumber	Serijski broj certifikata s entropijom od 32 bita (duljina serijskog broja:12 ili 13 bajtova)
signatureAlgorithm	AlgorithmIdentifier	sha256WithRSAEncryption OID: 1.2.840.113549.1.1.11
signatureValue		Potpis izdavatelja certifikata
Issuer	commonName	Fina Root CA
	organizationName	Financijska agencija
	countryName	HR
Validity	notBefore	Vrijeme izdavanja certifikata
	notAfter	Vrijeme izdavanja certifikata + 12 mjeseci
Subject	commonName	Fina Root OCSP
	organizationName	Financijska agencija
	countryName	HR
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption OID: 1.2.840.113549.1.1.1
	subjectPublicKey	Javni ključ CA: 2048 bita

Tablica 7.3. Osnovna polja certifikata za Fina OCSP servis kojeg izdaje Fina Root CA

7.1.1. Broj(evi) verzije

Koristi se X.509 verzija 3 certifikata.

7.1.2. Ekstenzije certifikata

Ekstenzije Fina Root CA certifikata navedene su u Tablici 7.4.

Ekstenzije	Kritično	Vrijednost
KeyUsage	DA	KeyCertSign, cRLSign
BasicConstraints	DA	cA=true
AuthorityKeyIdentifier	NE	160-bit SHA-1 hash vrijednost (određeno prema RFC 5280, točka 4.2.1.2 metoda (1))
SubjectKeyIdentifier	NE	160-bit SHA-1 hash vrijednost (određeno prema RFC 5280, točka 4.2.1.2 metoda (1))

Tablica 7.4. Ekstenzije Fina Root CA certifikata

Ekstenzije certifikata subordiniranih Fina CA-ova navedene su u Tablici 7.5.

Ekstenzije	Kritično	Vrijednost	
KeyUsage	DA	KeyCertSign, cRLSign	
BasicConstraints	DA	cA=true pathLen=0	
AuthorityKeyIdentifier	NE	160-bit SHA-1 hash vrijednost (određeno prema RFC 5280, točka 4.2.1.2 metoda (1))	
SubjectKeyIdentifier	NE	160-bit SHA-1 hash vrijednost (određeno prema RFC 5280, točka 4.2.1.2 metoda (1))	
certificatePolicies	NE	policyIdentifier	OID: 1.3.124.1104.5.2.1
		cPSuri	http://rdc.fina.hr/Root/FinaRootCA-CP1-0-hr.pdf http://rdc.fina.hr/Root/FinaRootCA-CP1-0-en.pdf
		policyQualifiers	CPS
Authority Information Access	NE	id-ad-ocsp	[1]Authority Info Access Access Method=Online Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.fina.hr
		id-ad-caIssuers	[2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://rdc.fina.hr/Root/FinaRootCA.cer
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://rdc.fina.hr/Root/FinaRootCA.crl

Tablica 7.5. Ekstenzije certifikata subordiniranih Fina CA-ova

Ekstenzije certifikata Fina OCSP servisa kojim se potpisuju odgovori za certifikate koje izdaje Fina Root CA prikazane su u Tablici 7.6.

Ekstenzija	Kritično	Atribut	Vrijednost
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
		nonRepudiation	Uključen nonRepudiation bit
extKeyUsage	NE	OCSPSigning	OID: 1.3.6.1.5.5.7.3.9
ocsp-nocheck	NE		OID: 1.3.6.1.5.5.7.48.1.5, vrijednost NULL
certificatePolicies	NE	policyIdentifier	Visoka razina sigurnosti: OID: 1.3.124.1104.5.2.9.4.3
		cPSuri	http://rdc.fina.hr/Root/FinaRootCA-CP1-0-hr.pdf http://rdc.fina.hr/Root/FinaRootCA-CP1-0-en.pdf
		policyQualifierID	CPS
CRLDistributionPoints	NE	DistributionPoint	[1]URI: http://rdc.fina.hr/Root/FinaRootCA.crl
AuthorityKeyIdentifier	NE	keyIdentifier	160-bit SHA-1 hash vrijednost (određeno prema RFC 5280, točka 4.2.1.2 metoda (1))
SubjectKeyIdentifier	NE	keyIdentifier	160-bit SHA-1 hash vrijednost (određeno prema RFC 5280, točka 4.2.1.2 metoda (1))
BasicConstraints	NE		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-ocsp	http://ocsp.fina.hr
		id-ad-caIssuers	http://rdc.fina.hr/Root/FinaRootCA.cer

Tablica 7.6. Ekstenzije certifikata Fina OCSP servisa

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 7.7.

Algoritam	OID
sha256WithRSAEncryption	1.2.840.113549.1.1.11
rsaEncryption	1.2.840.113549.1.1.1

Tablica 7.7. Algoritmi s pripadajućim OID identifikatorima

7.1.4. Oblici naziva

Fina Root CA, njemu subordinirani Fina CA-ovi, certifikati Fina 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 tablicama 7.1., 7.2. i 7.3 prikazani su oblici naziva izdavatelja certifikata i subjekta certificiranja Fina Root CA certifikata, certifikata njegovih subordiniranih Fina CA-ova i certifikata za Fina OCSP servis kojim se potpisuju odgovori za certifikate koje izdaje Fina Root CA.

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.

Identifikator objekta (OID) općih pravila certificiranja u certifikatu za potpis odgovora OCSP servisa je: 1.3.124.1104.5.2.9.4.3.

7.1.7. Uporaba ekstenzije *Policy Constraints*

Ne koristi se.

7.1.8. Sintaksa i semantika kvalifikatora općih pravila

U tablici 7.8. prikazana je sintaksa i semantika ekstenzije *certificatePolicies* i njenih vrijednosti.

Polje	Kritično	Atribut	Vrijednost
certificatePolicies	NE	policyIdentifier	OID dokumenta općih pravila za pripadajući certifikat.
		cPSuri	URI s kojeg se može dohvatiti dokument općih pravila za pripadajući certifikat
		policyQualifiers	CPS

Tablica 7.8. Sintaksa i semantika kvalifikatora općih pravila

7.1.9. Procesne semantike za kritičnu ekstenziju *Certificate Policies*

Ne koristi se.

7.2. Profil CRL

Profil CRL koje izdaje Fina Root CA i subordinirani Fina CA-ovi sukladan je preporuci IETF RFC 5280 [23].

7.2.1. Broj(evi) verzije

Koristi se X.509 verzija 2.

7.2.2. CRL i ekstenzije unosa u CRL

Korištene ekstenzije CRL liste i elemenata CRL liste definirane su u tablici 7.10:

Polje / Atribut	Komentar/Sadržaj Polja
crlEntryExtensions	
reasonCode	Upisuje se kod razloga opoziva*
crlExtensions	
cRLNumber	Redni broj CRL, format: 24 bitni broj
AuthorityKeyIdentifier	60-bitna SHA-1 hash vrijednost javnog ključa izdavatelja

Tablica 7.10. Ekstenzije CRL liste i elemenata CRL liste

* Razlozi opoziva (*reasonCode*) mogu biti:

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

7.3. OCSP profil

Profil odgovora Fina OCSP servisa sukladan je s preporukom IETF RFC 6960 [29].

7.3.1. Broj(evi) verzije

Koristi se *Version*: 1 (0x0).

7.3.2. OCSP ekstenzije

U odgovor Fina OCSP servisa uključene su slijedeće ekstenzije:

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

8. PROVJERA USKLAĐENOSTI

Inspekcijski nadzor nad radom Fina PKI reguliran je Zakonom o elektroničkom potpisu [1], [2] i [3], a provodi ga ministarstvo nadležno za gospodarstvo.

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

Unutarnju kontrolu provođenja propisanih postupaka vezanih uz rad Fina PKI i provedbu unutarnjeg procesa odobravanja rada Fina CA sukladno pravilima definiranim u ovim Općim pravilima provodi Fina PMA.

Provjera usklađenosti provodi se sukladno Zakonu o elektroničkom potpisu [1], [2] i [3], podzakonskim propisima [4], [5], [6], [7] donijetih temeljem Zakona, zahtjevima obvezujućih normizacijskih dokumenata te zahtjevima iz dokumenta CA/Browser Forum Baseline Requirements [28].

Detaljnije mjere i postupci provjere usklađenosti za svaki Finin CA opisani su Općim pravilima davanja usluga certificiranja [31], Pravilniku o postupcima certificiranja za kvalificirane certifikate [32] i Pravilniku o postupcima certificiranja za nekvalificirane certifikate [33].

8.1. Učestalost ili okolnosti provjere usklađenosti

Provjera usklađenosti rada Fina PKI provodi se redovito, najmanje jedanput godišnje.

Provjeru usklađenosti potrebno je provesti i prije početka rada novog Fina CA te nakon značajnijih promjena u radu Fina PKI, odnosno nakon katastrofe ili sumnje u kompromitiranje sustava.

8.2. Identitet/kvalifikacije ocjenitelja

Interni ocjenitelji moraju:

- raspolagati znanjima i razumijevanjem odredbi normi HRN ETSI/EN 319 411-2 [11] i HRN ETSI/EN 319 411-3 [12] te odredbi iz normizacijskog dokumenta CWA 14167-1 [16];
- raspolagati znanjima i vještinama iz područja PKI te područja informacijske sigurnosti;
- poznavati zakonsku regulativu iz područja davanja usluga certificiranja.

Vanjski ocjenitelji moraju zadovoljavati zahtjeve iz CA/Browser Forum Baseline Requirements dokumenta [28] i ETSI EN119 403 [15] dokumenta.

8.3. Odnos ocjenitelja s tijelom koje se ocjenjuje

Interni ocjenitelji usklađenosti moraju biti organizacijski odvojeni od Fina CA-a kako bi obavljali neovisnu provjeru.

8.4. Predmeti provjera

Interni ocjenitelji provjeravaju postupa li Fina PKI sukladno zahtjevima iz važeće zakonske regulative, prema ovim Općim pravilima, Općim pravilima davanja usluga certificiranja, Pravilniku o postupcima certificiranja za kvalificirane certifikate i Pravilniku o postupcima certificiranja za nekvalificirane certifikate te ostaloj mjerodavnoj internoj Fininoj dokumentaciji.

8.5. Mjere u slučaju neusklađenosti

U slučaju utvrđivanja neusklađenosti u radu Fina PKI, interni ocjenitelj izrađuje izvješće i dostavlja ga Fina PMA na osnovu kojeg Fina PMA izrađuje plan akcija, mjera i postupaka koji će se, u ovisnosti o težini neusklađenosti, u danom roku poduzeti kako bi se otklonile utvrđene neusklađenosti.

Mjere i postupci koji će se poduzeti u slučaju utvrđivanja neusklađenosti opisani su u Općim pravilima davanja usluga certificiranja i internim dokumentima Fine.

8.6. Priopćavanje rezultata

Fina PMA kao nadležno tijelo, dužno je izvještaj o provjeri usklađenosti i plan akcija, mjera i postupaka koje će se poduzeti ukoliko su otkrivene neusklađenosti dostaviti svim odgovornim osobama unutar Fina PKI sustava koje su odgovorne za rad pojedinih dijelova sustava u kojima je izvedena provjera usklađenosti.

U cilju dokazivanja usklađenosti, korisnicima i pouzdajućim stranama je na zahtjev dostupan izvještaj o provjeri usklađenosti koju je obavio interni ili vanjski neovisni ocjenitelj.

Rezultate vanjske provjere usklađenosti Fina može javno objaviti. Rezultati se u tom slučaju objavljuju na web stranicama repozitorija iz točke 2.2.

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

9.2. Financijska odgovornost

Fina kao davatelj usluga certificiranja raspolaže financijskim sredstvima koja osiguravaju nesmetano davanje usluga certificiranja sukladno ovim Općim pravilima, neovisno o broju korisnika usluga i za cijelo vrijeme obavljanja usluga certificiranja.

9.2.1. Pokrivenost osiguranjem

Fina kao davatelj usluga certificiranja ima osiguran rizik od odgovornosti za štete koje nastanu obavljanjem usluga izdavanja kvalificiranih i nekvalificiranih certifikata.

Fina dodatno osigurava imovinu policom osiguranja koja pokriva osiguranje od rizika požara, vremenskih nepogoda, poplava, eksplozija i slično te osiguranja od loma stroja (industrijski lom) kojima se pokrivaju moguće nastale štete od ispada ili oštećenja instalacija i/ili strojne opreme, kao i osiguranje od loma stakla.

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 davanjem usluga certificiranja, a koje sudionici označe povjerljivim, ili određenom vrstom ili stupnjem tajnosti, ili koji su po prirodi povjerljivi jer bi njihovo neovlašteno otkrivanje moglo prouzročiti štetu sudioniku.

Povjerljivi su i svi podaci koji se odnose na način i na sredstva kojim Fina CA upravlja certifikatima.

9.3.2. Podaci koji se ne smatraju povjerljivim poslovnim podacima

Poslovni podaci u bilo kojem obliku koje na bilo koji način između sebe razmjene sudionici u svezi s uspostavom i davanjem usluga certificiranja, a koje sudionici ne označe povjerljivim, ili određenom vrstom ili stupnjem tajnosti, ili koji po svojoj prirodi nisu povjerljivi, jer se njihovim neovlaštenim otkrivanjem ne bi mogla prouzročiti šteta sudioniku, su podaci koji se ne smatraju povjerljivim poslovnim podacima.

Poslovni podaci koji se ugrađuju u sadržaj certifikata, koji se prikazuju u javnim evidencijama i/ili registrima, koji se za potrebe davanja usluge certificiranja moraju propisano voditi, ne smatraju se povjerljivim poslovnim podacima.

9.3.3. Odgovornost za zaštitu povjerljivih poslovnih podataka

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

9.4. Zaštita osobnih podataka

Fina primjenjuje odredbe Zakona o zaštiti osobnih podataka [9] i drugih propisa kojima je uređena zaštita osobnih podataka te tajnost podataka u Republici Hrvatskoj.

9.4.1. Plan zaštite osobnih podataka

Fina planira i provodi propisane tehničke, kadrovske i organizacijske mjere za zaštitu osobnih podataka od slučajne ili namjerne zlouporabe, uništenja, gubitka, neovlaštenih promjena ili dostupa.

9.4.2. Povjerljivi osobni podaci

U postupku registracije korisnika i nakon toga Fina je ovlaštena prikupljati osobne podatke koji su potrebni za valjano utvrđivanje identiteta korisnika te druge podatke potrebne za valjano davanje usluga certificiranja. Osobni podaci koje prikupi Fina i koji nisu sadržaj certifikata, koji se ne prikazuju u javnim evidencijama i/ili registrima koji se za potrebe davanja usluge certificiranja moraju propisano voditi, su povjerljivi osobni podaci koje Fina propisano 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, koji se prikazuju u javnim evidencijama i/ili registrima, koji se za potrebe davanja usluge certificiranja moraju propisano voditi, su osobni podaci koji zbog dostupnosti svima zainteresiranima nisu povjerljivi.

9.4.4. Odgovornost za zaštitu osobnih podataka

Fina je odgovorna za zaštitu osobnih podatka, sukladno odredbama Zakona o zaštiti osobnih podataka [9] i drugih propisa, posebno onih kojima je uređena zaštita osobnih podataka u Republici Hrvatskoj.

9.4.5. Ovlaštenje za korištenje osobnih podataka

Fina je ovlaštena, osim za potrebe ispunjenja zakonskih obveza, odnosno ugovornih obveza po ugovoru o certificiranju, koristiti osobne podatke samo temeljem pisane privole korisnika koja se može dati u zahtjevu za izdavanje certifikata ili kasnije.

9.4.6. Dostupnost podataka mjerodavnim tijelima

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

9.4.7. Ostale okolnosti objave podataka

Nema odredbi.

9.5. Prava intelektualnog vlasništva

Ova Opća pravila kao i druga Finina dokumentacija objavljena na internetskim stranicama repozitorija iz točke 2.2. je Finino vlasništvo i bez Fininog izričitog ovlaštenja nije dozvoljeno njeno neovlašteno korištenje.

Sudionici PKI dužni su poštivati prava intelektualnog vlasništva.

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

9.6. Obveze i odgovornosti

9.6.1. Obveze i odgovornosti CA

Fina, kao davatelj usluga certificiranja, pri davanju usluga izdavanja i upravljanja životnim ciklusom certifikata primjenjuje Zakon o elektroničkom potpisu [1], [2] i [3], podzakonske propise [4], [5], [6], [7] i [8] donijete temeljem Zakona o elektroničkom potpisu [1], [2] i [3], obvezujuće međunarodne norme i preporuke, ova Opća pravila, Opća pravilima davanja usluga certificiranja [31] te druge interne akte koji se temelje na ovim Općim pravilima.

Fina na web stranicama repozitorija iz točke 2.2. ovih Općih pravila objavljuje sve obavijesti i informacije o promjenama u radu koje na bilo koji način mogu utjecati na sudionike Fina PKI.

Fina se obvezuje da će CA usluge obavljati s pažnjom dobrog stručnjaka.

Detaljnije odredbe koje se odnose na obveze i odgovornosti Fine kao davatelja usluga certificiranja navedene su u Općim pravilima davanja usluga certificiranja [31].

9.6.2. Obveze i odgovornosti RA

Obveze i odgovornosti RA mreže su:

- provođenje postupka registracije i identifikacije fizičkih osoba i poslovnih subjekata na način propisan Općim pravilima davanja usluga certificiranja [31];
- prosljeđivanje cjelovitih, točnih i provjerenih korisničkih podataka na daljnju obradu u Fina CA;
- čuvanje, arhiviranje i zaštita podataka i dokumentacije na period od najmanje 10 godina od dana isteka zadnjeg obnovljenog certifikata za istog korisnika;
- osiguravanje od gubitka ili povrede povjerljivosti, cjelovitosti i dostupnosti arhiviranih podataka korisnika, na način propisan ovim Općim pravilima davanja usluga certificiranja [31].

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

9.6.3. Obveze i odgovornosti korisnika

Korisnik je dužan:

- u procesu registracije predstaviti se na način propisan Općim pravilima davanja usluga certificiranja [31];
- pažljivo koristiti i čuvati sredstvo za izradu elektroničkog potpisa, sredstvo elektroničke identifikacije, privatne ključeve i aktivacijske podatke te ih koristiti u skladu s odredbama Općih pravila davanja usluga certificiranja [31];
- poduzeti odgovarajuće mjere zaštite sredstva za izradu elektroničkog potpisa, sredstva elektroničke identifikacije, privatnog ključa i aktivacijskih podataka od neovlaštenog pristupa i uporabe;
- 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 Općim pravilima davanja usluga certificiranja [31];
- djelovati u skladu sa svim ostalim odredbama iz Općih pravila davanja usluga certificiranja [31], 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 propise, ova Opća pravila te Opća pravila davanja usluga certificiranja [31] 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 Općim pravilima davanja usluga certificiranja [31].

9.6.5. Obveze i odgovornosti ostalih sudionika

Nema odredbi.

9.7. Odricanje od odgovornosti

Osim onog što je za Finu izričito navedeno u točki 9.6. ovih Općih pravila te Općih pravila davanja usluga certificiranja [31] Fina kao davatelj usluga certificiranja ne odgovora ni za koje drugo jamstvo ili odgovornost, posebno ne u slučaju ako bi do odgovornosti Fine prema danim jamstvima došlo zbog povrede jamstava i odgovornosti drugih sudionika navedenih u Općim pravila davanja usluga certificiranja [31].

Sveukupna Finina odgovornost kao davatelja usluga certificiranja odnosi se i na poslove registracije korisnika koje obavlja vanjski ugovoreni RA s kojim Fina ima sklopljen ugovor o obavljanju usluga registracije korisnika.

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

- štete pretrpljene u vremenu od opoziva certifikata do dostupnosti informacije o statusu certifikata;
- štete zbog neautorizirane uporabe korisničkih ključeva i certifikata;
- štete nastale uporabom certifikata u primjenama koje nisu dopuštene ovim Općim pravilima;
- štete prouzročene lažnom ili nemarnom uporabom certifikata ili CRL;
- štete nastale kao rezultat neispravnosti i pogrešaka u softveru i hardveru subjekta i pouzdajuće strane.

RA mreža nije odgovorna za štete, uključujući indirektne i specijalne štete, štete za slučaj nezgode, štete za slučaj nepogode s posljedicama ili za bilo koji gubitak dobiti, gubitak podataka ili druge indirektne štete koje su proizašle iz veze s uslugama certificiranja nastale kao rezultat prijevarnog davanja podataka i predstavljanja korisnika tijekom procesa identifikacije i potvrde identiteta ako je provjeru podataka provodila u skladu sa zahtjevima iz ovih Općih pravila.

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.

9.9. Naknada štete

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

Korisnik odnosno pravna 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 Općim pravilima davanja usluga certificiranja [31] .

Fina je odgovorna osobi koja se pouzdaje u certifikat samo ako je ta odgovornost jasno uspostavljena ugovorom, Općim pravilima davanja usluga certificiranja [31] ili hrvatskom zakonskom regulativom.

9.10. Trajanje i prestanak važenja

9.10.1. Trajanje

Ovaj dokument Općih pravila važi do stupanja na snagu novog dokumenta Općih pravila ili do objave prestanka njegovog važenja. Nova verzija dokumenta ili objava prestanka važenja biti će objavljena na web stranicama repozitorija iz točke 2.2. ovih Općih pravila s naznačenim danom stupanja na snagu.

9.10.2. Prestanak važenja

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

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

9.10.3. Posljedice prestanka važenja i nastavak djelovanja

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

Novi dokument Općih pravila ne utječe na važenje certifikata koji su izdani primjenom prethodnih dokumenata Općih pravila. Certifikati izdani primjenom prethodnih Općih pravila

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

9.11. Pojedinačne obavijesti i komunikacija sa sudionicima

Pojedinačne obavijesti i druga službena komunikacija treba se provoditi dopisima koji se dostavljaju u papirnatom obliku ili elektronički na adresu objavljenu na internetskim stranicama repozitorija iz točke 2.2.

9.12. Izmjene i dopune

9.12.1. Procedure izmjena i dopuna

Ova Opća pravila revidiraju se po potrebi. Za sve izmjene i dopune odgovoran je Fina PMA.

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

Sve izmjene ovih Općih pravila koje mogu bitno utjecati na sudionike zahtijevaju njihovo obavještavanje.

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

9.12.2. Mehanizmi obavještavanja i vremenski periodi

Ovaj dokument dostupan je na internetskim stranicama repozitorija iz točke 2.2. ovih Općih pravila.

Datum objave i datum stupanja na snagu novoobjavljenog dokumenta Općih pravila naznačeni su na njegovoj naslovnoj strani kao i na internetskim stranicama na kojima je objavljen.

9.12.3. Okolnosti pod kojima se mora mijenjati OID

Manje izmjene sadržaja u dokumentu Općih pravila koje ne utječu bitno na sudionike ne uvjetuju izmjene OID-a dokumenta.

Veće izmjene u dokumentu Općih pravila koje mogu utjecati na sudionike zahtijevaju i izmjenu OID-a Općih pravila.

9.13. Postupak rješavanja sporova

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

Korisnik odnosno pravna ili fizička osoba u čije ime korisnik djeluje i koju predstavlja može Fini uputiti prigovor ako smatra da u njegovu slučaju postoji odstupanje sadržaja usluge u odnosu na ugovoreno. Fina će povodom prigovora odgovoriti podnositelju prigovora. Prigovor i odgovor na prigovor upućuju se pisano u papirnatom ili elektroničkom obliku na način opisan u točki 9.11.

U slučaju spora ili neslaganja između Fine (kao davatelja usluge certificiranja uređene ovim Općim pravilima) i korisnika, odnosno pravne ili fizičke osobe u čije ime korisnik djeluje i koju predstavlja, povodom prigovora o navodnom odstupanju sadržaja usluge u odnosu na ugovoreno, isti će se nastojati razriješiti sporazumno. Ako sporazumno razrješenje spora nije moguće isti će se razriješiti pred mjerodavnim sudom u Zagrebu uz primjenu hrvatskog prava.

U slučaju spora ili neslaganja između Fine, kao davatelja usluge certificiranja uređene ovim Općim pravilima, i vanjskog ugovorenog RA, postupak rješavanja spora reguliran je međusobnim ugovorom.

9.14. Važeći propisi

Za tumačenje odredaba ovih Općih pravila mjerodavne su odredbe Zakona o elektroničkom potpisu [1], [2] i [3], podzakonskih akata donesenih temeljem tog zakona [4], [5], [6] i [7] te propisa, normizacijskih dokumenata i preporuka na koje iste upućuju.

9.15. Usklađenost s važećim propisima

Ova Opća pravila, Opća pravila davanja usluga certificiranja [31] kao i davanje usluga certificiranja koje su obuhvaćene tim Općim pravilima usklađena su s propisima iz točke 9.14.

9.16. Razne odredbe

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