OPIS PROMJENA U STRUKTURI FININIH DIGITALNIH CERTIFIKATA

Verzija 1.1

Informacije o dokumentu

Ime dokumenta:	Opis promjena u strukturi Fininih digitalnih certifikata
Oznaka distribucije	Javno
Vlasnik dokumenta	FINA
Kontakt	info.pki@fina.hr

Povijest izmjena

Verzija	Datum	Razlog izmjene
1.0	1.09.2014.	
1.1	17.02.2015.	Promjene u nazivima produkcijskih CA-ova i nazivima dodatnih servisa buduće produkcijske okoline.

SADRŽAJ

1. Uvod 4
   1.1. Razlozi uvođenja promjena 4
2. Postojeći produkcijski i Demo certifikati 6
   2.1. Izdavanje produkcijskih certifikata i vremenskih žigova 6
      2.1.1. Certifikacijsko tijelo FINA RDC CA 6
      2.1.2. Certifikacijsko tijelo FINA RDC-TDU CA 7
      2.1.3. Provjera statusa postojećih produkcijskih certifikata 8
      2.1.4. FINA Servis vremenske ovjere 9
      2.1.5. Postojeća produkcijska okolina 10
   2.2. Izdavanje Demo certifikata 10
      2.2.1. Certifikacijsko tijelo FINA Demo CA 10
      2.2.2. Provjera statusa postojećih Demo certifikata 11
      2.2.3. Izdavanje Demo vremenskih žigova 11
3. Promjene u sustavima za izdavanje produkcijskih certifikata i vremenskih žigova 12
   3.1. Buduća dvorazinska arhitektura produkcijskih certifikacijskih tijela 12
   3.2. Prijelaz na sigurnije kriptografske algoritme i dulje ključeve 14
      3.2.1. Karakteristike Fina Root CA certifikata 14
      3.2.2. Karakteristike certifikata za Fina RDC 2015 i Fina RDC-TDU 2015 CA-ove 15
      3.2.3. Karakteristike certifikata koje će izdavati Fina RDC 2015 i Fina RDC-TDU 2015 CA-ovi 16
   3.3. Uspostava nove usluge za provjeru statusa certifikata 17
   3.4. Prijelaz na servis kvalificiranog vremenskog žiga 18
   3.5. Prikaz buduće produkcijske okoline 19
   3.6. Početak primjene i potreba prilagodbe korisničkih informatičkih rješenja 20
4. Izdavanje novih Demo certifikata i vremenskih žigova 22
   4.1. Dvorazinska arhitektura certifikacijskih tijela u novoj Demo okolini 22
      4.1.1. Karakteristike Fina Demo Root CA certifikata 23
      4.1.2. Karakteristike certifikata za Fina Demo CA 2014 24
      4.1.3. Karakteristike korisničkih certifikata koje izdaje Fina Demo CA 2014 25
      4.1.4. Fina Demo OCSP 2014 servis 26
      4.1.5. Servis vremenskog žiga Fina Demo TSA 2014 27
   4.2. Prikaz nove Demo okoline 29
5. Dodatne informacije 30
   5.1. Važeća zakonska regulativa 30
   5.2. Popis normizacijskih dokumenata i preporuka 30
   5.3. Konstrukcija i provjera lanca certifikata 31
   5.4. Obrada i prikaz naziva u certifikatima 32

1. Uvod

Fina priprema promjene na sustavima za izdavanje digitalnih certifikata i vremenskih žigova. Promjene se odnose na uvođenje korijenskog (*root*) CA certifikata, promjene u strukturi CA certifikata te promjene u strukturi korisničkih certifikata i vremenskih žigova. Ove promjene utjecat će na postojeća korisnička informatička rješenja koja koriste Finine certifikate i vremenske žigove te će stoga **na svim korisničkim rješenjima koja koriste Finine certifikate biti potrebno prethodno provjeriti njihovu spremnost za korištenje izmijenjenih certifikata te po potrebi obaviti prilagodbu korisničkih rješenja**.

Sva korisnička informatička rješenja moraju do početka primjene navedenih promjena u produkciji biti prilagođena za rad s izmijenjenim certifikatima koji će se izdavati na način opisan u ovom dokumentu, ali istovremeno moraju i dalje podržavati rad s postojećim certifikatima do isteka perioda njihove valjanosti. Istek perioda valjanosti postojećih korisničkih certifikata na smart karticama i USB tokenima (certifikati srednje razine sigurnosti) je dvije godine od njihova izdavanja, a istek perioda valjanosti većine soft certifikata (certifikati standardne razine sigurnosti) je pet godina od njihova izdavanja. Dvije godine od početka primjene navedenih promjena isteći će zadnji izdani certifikati srednje razine sigurnosti, a pet godina od početka primjene navedenih promjena prestat će važiti i zadnji certifikati standardne razine sigurnosti izdani na postojećem produkcijskom sustavu.

Također, do početka primjene navedenih promjena sva rješenja koja koriste postojeći servis vremenskog žiga moraju biti prilagođena za rad s novim servisom vremenskog žiga opisanim u ovom dokumentu.

Certifikati i vremenski žigovi koji će se izdavati sukladno promjenama opisanim u ovom dokumentu bit će usklađeni s važećim međunarodnim normama iz područja izdavanja digitalnih certifikata, EU normama iz područja elektroničkog potpisa i najboljom praksom.

Kako bi korisnicima Fininih certifikata dali potpunu informaciju o planiranim promjena, u ovom dokumentu opisani su detalji tih promjena.

Aktualnu verziju ovog dokumenta moguće je preuzeti s adrese:
http://rdc.fina.hr/dokumentacija/opis_promjena_2014.pdf.

1.1. Razlozi uvođenja promjena

Kriptografski algoritmi vremenom gube na snazi i postupno pružaju sve manju sigurnost. To se događa kao posljedica povećanja procesorske snage novijih računala i kao posljedica napretka kriptografske analize. Da bi se zadržala ili povećala sigurnost i povjerenje u izdane certifikate i vremenske žigove te osigurala njihova daljnja nesmetana primjena potrebno je pravodobno obaviti promjene u duljinama kriptografskih ključeva, odnosno prijeći na korištenje adekvatnih sigurnijih kriptografskih algoritama. Na uvođenje promjena u certifikatima i vremenskim žigovima Finu kao davatelja usluga certificiranja obvezuje zakonska regulativa iz područja elektroničkog potpisa kao i pripadni obvezujući međunarodni normizacijski dokumenti.

Cilj ovih promjena je povećanje sigurnosti i povjerenja u izdane certifikate i vremenske žigove koje izdaje Fina te posljedično povećanje sigurnosti i povjerenja u napredni elektronički potpis, autentifikaciju i druge primjene certifikata i vremenskih žigova.

2. Postojeći produkcijski i Demo certifikati

Fina korisnicima izdaje **produkcijske certifikate i vremenske žigove** na svojim produkcijskim sustavima. Ovi certifikati i vremenski žigovi izdaju se i koriste sukladno Zakonu o elektroničkom potpisu.

Za potrebe testiranja, demonstracije i usklađivanja informatičkih rješenja korisnika koja koriste Finine certifikate i vremenske žigove Fina na svojem Demo sustavu izdaje **Demo certifikate**.

U ovom poglavlju opisani su **postojeći produkcijski certifikati** i **postojeći Demo certifikati** te **postojeći produkcijski vremenski žigovi** koje izdaje Fina. Navedeni opisi u ovom poglavlju odgovaraju postojećem stanju prije uvođenja promjena.

Opis **budućih produkcijskih certifikata** i **budućih vremenskih žigova** koje će izdavati Fina te opis **buduće dvorazinske arhitekture produkcijskih CA-ova** nalazi se u poglavlju 3.

Opis **novih Demo certifikata** i **novih vremenskih žigova** koje izdaje Fina te opis **nove dvorazinske arhitekture CA-ova u novoj Demo okolini** nalazi se u poglavlju 4.

2.1. Izdavanje produkcijskih certifikata i vremenskih žigova

U **postojećoj** Fininoj produkcijskoj okolini produkcijske certifikate izdaju dva certifikacijska tijela (engl. *Certification Authority* - CA): **FINA RDC CA** i **FINA RDC-TDU CA**, a produkcijske vremenske žigove izdaje **FINA Servis vremenske ovjere**.

Pružanje usluga izdavanja produkcijskih certifikata i vremenskih žigova Fina obavlja sukladno Zakonu o elektroničkom potpisu. Ovim Zakonom ujedno je regulirano korištenje i pouzdanje u tako izdane certifikate i vremenske žigove.

2.1.1. Certifikacijsko tijelo FINA RDC CA

FINA RDC CA izdaje kvalificirane, normalizirane i *lightweight* certifikate za:

- fizičke osobe – građane (osobni certifikati);
- fizičke osobe povezane s poslovnim subjektom (poslovni certifikati); i
- IT opremu povezanu s poslovnim subjektom (poslovni certifikati za IT opremu).

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

Osnovni podaci o FINA RDC CA *root* certifikatu prikazani su u Tablici 1. U ovoj i narednim tablicama posebno su istaknute informacije o kriptografskim algoritmima koji se koriste u opisanom certifikatu: potpisni algoritmi koji su korišteni pri potpisivanju certifikata (*signatureAlgorithm*), algoritam povezan s javnim ključem u certifikatu kao i duljina javnog ključa (*SubjectPublicKeyInfo*).

Osnovno polje	Vrijednost za FINA RDC CA *root* certifikat
Version	X.509 V3, vrijednost="2"
serialNumber	3f 1b ce 21
signatureAlgorithm	**sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)**
Issuer	ou=RDC, o=FINA, c=HR
Validity	NotBefore: 21. srpanj 2003 11:57:43 NotAfter: 21. srpanj 2023 12:27:43
Subject	ou=RDC, o=FINA, c=HR
SubjectPublicKeyInfo	**rsaEncryption (OID: 1.2.840.113549.1.1.1), javni ključ duljine 2048 bitova** Pripadajućim privatnim ključem FINA RDC CA potpisuje svaki izdani certifikat i CRL.

Tablica 1. Osnovni podaci o FINA RDC CA root certifikatu

FINA RDC CA *root* certifikat može se preuzeti s adrese http://rdc.fina.hr/CA/RDCca.cer, a vrijednost njegova SHA-1 sažetka (*Thumbprint* ili *Fingerprint*) je:

4c:4b:ed:f2:a8:d7:64:c1:fe:dc:81:af:d6:37:0f:50:30:7a:0a:12.

Osnovni podaci o korisničkim certifikatima koje izdaje FINA RDC CA prikazani su u Tablici 2.

Osnovno polje	Vrijednost za certifikate koje izdaje FINA RDC CA
Version	X.509 V3, vrijednost="2"
serialNumber	32-bitni neponovljivi cijeli broj
signatureAlgorithm	**sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)**
Issuer	ou=RDC, o=FINA, c=HR
Validity	NotBefore: Vrijeme izdavanja certifikata NotAfter: Ovisno o tipu certifikata: 1, 2, ili 5 godina.
Subject	Ovisno o tipu certifikata
subjectPublic KeyInfo	**rsaEncryption (OID: 1.2.840.113549.1.1.1), javni ključ duljine 1024 ili 2048 bita, ovisno o tipu certifikata**

Tablica 2. Osnovni podaci o korisničkim certifikatima koje izdaje FINA RDC CA

Detaljan opis za svaki tip certifikata koje izdaje FINA RDC CA nalazi se u točki 7.1.1.1. dokumenta Opća pravila davanja usluga certificiranja.

2.1.2. Certifikacijsko tijelo FINA RDC-TDU CA

FINA RDC-TDU CA izdaje kvalificirane i normalizirane certifikate državnim dužnosnicima i zaposlenicima u tijelima državne uprave.

FINA RDC-TDU CA ima vlastiti samopotpisani (*root*) certifikat koji je namijenjen za provjeru certifikata koje izdaje FINA RDC-TDU CA.

Osnovni podaci o FINA RDC-TDU CA *root* certifikatu prikazani su u Tablici 3.

Osnovno polje	Vrijednost za FINA RDC-TDU CA *root* certifikat
Version	X.509 V3, vrijednost="2"
serialNumber	41 db f1 61
signatureAlgorithm	**sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)**
Issuer	ou=RDC-TDU, o=FINA, c=HR
Validity	NotBefore: 5. siječanj 2005 14:23:47 NotAfter: 5. siječanj 2025 14:53:47
Subject	ou=RDC-TDU, o=FINA, c=HR
SubjectPublicKeyInfo	**rsaEncryption (OID: 1.2.840.113549.1.1.1), javni ključ duljine 2048 bitova** Pripadajućim privatnim ključem FINA RDC-TDU CA potpisuje svaki izdani certifikat i CRL.

Tablica 3. Osnovni podaci o FINA RDC-TDU CA root certifikatu

FINA RDC-TDU CA *root* certifikat može se preuzeti s adrese http://rdc-tdu.fina.hr/CA/RDC-TDUCA.cer, a vrijednost njegova SHA-1 sažetka (*Thumbprint* ili *Fingerprint*) je:

6e:46:67:b5:5e:5e:e3:4e:ad:8c:c2:1c:fa:a1:0b:b8:bf:c9:a5:30.

Osnovni podaci o korisničkim certifikatima koje izdaje FINA RDC-TDU CA prikazani su u Tablici 4.

Osnovo polje	Vrijednost za certifikate koje izdaje FINA RDC-TDU CA
Version	X.509 V3, vrijednost="2"
serialNumber	32-bitni neponovljivi cijeli broj
signatureAlgorithm	**sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)**
Issuer	ou=RDC-TDU, o=FINA, c=HR
Validity	NotBefore: Vrijeme izdavanja certifikata NotAfter: Vrijeme izdavanja certifikata + 2 godine.
Subject	cn=ime i prezime potpisnika, serialNumber=serijski broj, l=mjesto sjedišta TDU, ou=org. jedinica TDU 2. razine, oU=org. jedinica TDU 1. razine, o=naziv i identifikator TDU, c=HR
subjectPublic KeyInfo	**rsaEncryption (OID: 1.2.840.113549.1.1.1), javni ključ duljine 1024 bita**

Tablica 4. Osnovni podaci o korisničkim certifikatima koje izdaje FINA RDC-TDU CA

Detaljan opis za svaki tip certifikata koje izdaje FINA RDC-TDU CA nalazi se u točki 7.1.1.2. dokumenta Opća pravila davanja usluga certificiranja.

2.1.3. Provjera statusa postojećih produkcijskih certifikata

Certifikat prije vremena svojeg isteka može biti opozvan, suspendiran ili reaktiviran. Jednom opozvani certifikat nepovratno se smatra nevažećim. Suspenzija je privremeni opoziv certifikata, a suspendirani certifikat može se ponovno smatrati važećim nakon postupka njegove reaktivacije. U certifikat se pouzdajuća strana smije pouzdati ukoliko certifikat nije istekao i ukoliko nije opozvan ili suspendiran. Pouzdajuća strana koja se namjerava pouzdati u certifikat prethodno mora obavezno obaviti provjeru statusa certifikata kako bi utvrdila njegovu eventualnu opozvanost ili suspenziju.

Provjera statusa certifikata obavlja se provjerom liste opozvanih certifikata (*Certificate Revocation List*, CRL) koju objavljuje CA. FINA RDC CA i FINA RDC-TDU CA objavljuju pripadajuće liste opozvanih certifikata. Svaki od ova dva CA objavljuje svoju CRL putem HTTP i putem LDAP protokola. HTTP i LDP URI za pristup CRL na kojoj se može provjeriti status certifikata naveden je u ekstenziji *CRL Distribution Points* u svakom izdanom produkcijskom certifikatu. Više informacija o objavi CRL za postojeće FINA RDC CA i FINA RDC-TDU CA može se pronaći u točki 4.10.1 dokumenta Opća pravila davanja usluga certificiranja.

2.1.4. FINA Servis vremenske ovjere

FINA Servis vremenske ovjere dio je postojeće produkcijske okoline i može se koristiti za bilo koju primjenu koja zahtjeva pouzdano utvrđivanje postojanja određenog elektroničkog zapisa prije nekog vremenskog trenutka. Vremenski žig kojeg izdaje FINA Servis vremenske ovjere koristi se i za očuvanje dugotrajnosti elektroničkih potpisa.

Korisnici usluge izdavanja vremenskog žiga mogu biti:

- fizičke osobe – građani;
- poslovni subjekti i TDU;
- fizičke osobe unutar poslovnih subjekata ili unutar TDU.

Osnovni podaci o certifikatu kojim FINA Servis vremenske ovjere potpisuje vremenske žigove dani su u Tablici 5.

Polje	Vrijednost za certifikat FININOG Servisa vremenske ovjere
Version	X.509 V3, vrijednost="2"
serialNumber	32-bitni neponovljivi cijeli broj: 3f 1c 8a 93
signatureAlgorithm	**sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)**
Issuer	ou=RDC-TDU, o=FINA, c=HR
Validity	NotBefore: 08. lipnja 2006. 11:33:09 NotAfter: 08. lipnja 2016. 12:03:09
Subject	cn=SERVIS VREMENSKE OVJERE TSA1, o=FINA 00332852, c=HR
SubjectPublicKeyInfo	**rsaEncryption (OID: 1.2.840.113549.1.1.1), javni ključ duljine 2048 bitova** Pripadajućim privatnim ključem FINA Servis vremenske ovjere potpisuje svaki izdani vremenski žig.

Tablica 5. Osnovni podaci o certifikatu FINA Servisa vremenske ovjere

Osnovni podaci o profilu vremenskih žigova koje izdaje FINA Servis vremenske ovjere dani su u Tablici 6. Posebno su istaknute informacije o korištenom kriptografskom algoritmu za izračun sažetka podataka za koje se traži izdavanje vremenskog žiga (*messageImprint*) te o potpisnim algoritmima koji se koriste za potpisivanje vremenskog žiga (*signatureAlgorithm*).

Polje	Vrijednost za vremenski žig FINA Servisa vremenske ovjere
Version	V1, vrijednost="1"
Policy OID	1.3.124.1104.2.1.1.1.2
messageImprint	**hashAlgorithm: sha-1 (OID: 1.3.14.3.2.26)**
serialNumber	Cijeli broj
genTime	UTC vrijeme, razlučivost od 1 sekunde
Nonce	Cijeli broj
signatureAlgorithm	**sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)**

Tablica 6. Osnovni podaci o vremenskog žigu kojeg izdaje FINA Servis vremenske ovjere

2.1.5. Postojeća produkcijska okolina

Detaljnije informacije o Fininoj postojećoj produkcijskoj okolini za izdavanje certifikata i vremenskih žigova mogu se pronaći u dokumentima Opća pravila davanja usluga certificiranja, Pravilnik o postupcima certificiranja za kvalificirane certifikate, Pravilnik o postupcima certificiranja za nekvalificirane certifikate, Opća pravila davanja usluga izdavanja vremenskog žiga, te na web stranicama www.fina.hr/finadigicert.

2.2. Izdavanje Demo certifikata

Fina Demo digitalni certifikati su digitalni certifikati koji se izdaju za potrebe testiranja, demonstracije i usklađivanja informatičkih rješenja kako bi ta rješenja ispravno koristila Finine postojeće produkcijske digitalne certifikate. Demo certifikati su u tehnološkom i funkcionalnom smislu potpuno jednaki postojećim Fininim produkcijskim certifikatima.

Demo certifikate na **postojećoj Fina Demo okolini** uspostavljenoj 2003. godine izdaje **FINA Demo CA**. Demo certifikati potpisani su privatnim potpisnim ključem FINA Demo CA.

Budući da postojeća i nova informatička rješenja trebaju i dalje podržavati rad s certifikatima koje izdaju postojeći produkcijski CA-ovi (FINA RDC CA i FINA RDC-TDU CA), osobe i poslovni subjekti koji će testirati i razvijati informatička rješenja mogu zatražiti izdavanje Demo certifikata na postojećoj Fina Demo okolini koji odgovara određenom tipu postojećeg Fininog produkcijskog certifikata.

Postojeća i nova rješenja trebaju također podržavati rad s izmijenjenim certifikatima koje će izdavati budući produkcijski Fina RDC 2015 i Fina RDC-TDU 2015 CA-ovi. Promjene koje se uvode u izdavanje produkcijskih certifikata i vremenskih žigova opisane u poglavlju 3., a rok za početak primjene tih promjena i za prilagodbu korisničkih informatičkih rješenja naveden je u točki 3.6.

2.2.1. Certifikacijsko tijelo FINA Demo CA

FINA Demo CA izdaje sve tipove certifikata koji su u tehnološkom i funkcionalnom smislu potpuno jednaki tipovima certifikata koje izdaju produkcijska certifikacijska tijela FINA RDC CA i FINA RDC-TDU CA. Iako su tehnološki i funkcionalno jednaki produkcijskim

certifikatima, certifikati koje izdaje **FINA Demo CA** smiju se koristiti **isključivo u svrhe testiranja i provjere ispravnosti informatičkih rješenja**. Uporaba Demo certifikata smije rezultirati pouzdanjem u elektronički potpis, autentifikaciju, enkripciju ili u bilo koji drugi vid korištenja Demo certifikata za primjene isključivo u testnoj ili prezentacijskoj okolini.

FINA Demo CA ima vlastiti samopotpisani (*root*) certifikat koji je namijenjen za provjeru certifikata koje izdaje FINA Demo CA.

Osnovni podaci o FINA Demo CA *root* certifikatu dani su u Tablici 7.

Polje	Vrijednost za FINA Demo CA *root* certifikat
Version	X.509 V3, vrijednost="2"
serialNumber	3e c9 fd 21
signatureAlgorithm	**sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)**
Issuer	ou=DEMO, o=FINA, c=HR
Validity	NotBefore: 20. svibnja 2003. 11:32:11 NotAfter: 20. svibnja 2023. 12:02:11
Subject	ou=DEMO, o=FINA, c=HR
SubjectPublicKeyInfo	**rsaEncryption (OID: 1.2.840.113549.1.1.1), javni ključ duljine 2048 bitova**
Thumbprint	Thumbprint algorithm: SHA-1 64 51 28 b9 d9 42 60 64 1b d5 a5 f6 af 4f a6 8e 35 e2 f1 ae

Tablica 7. Osnovni podaci o FINA Demo CA root certifikatu

FINA Demo CA *root* certifikat može se preuzeti s adrese http://demo-pki.fina.hr/crl/democacert.cer, a vrijednost njegova SHA-1 sažetka (*Thumbprint* ili *Fingerprint*) je:

64:51:28:b9:d9:42:60:64:1b:d5:a5:f6:af:4f:a6:8e:35:e2:f1:ae.

2.2.2. Provjera statusa postojećih Demo certifikata

Provjera statusa postojećih Demo certifikata obavlja se provjerom CRL, tj. na jednak način kao i provjera statusa postojećih produkcijskih certifikata. FINA Demo CA objavljuje CRL putem HTTP i putem LDAP protokola. HTTP i LDP URI za pristup CRL na kojoj se može provjeriti status certifikata naveden je u ekstenziji *CRL Distribution Points* u svakom izdanom Demo certifikatu.

2.2.3. Izdavanje Demo vremenskih žigova

Unutar Fina Demo okoline (postojeća Demo okolina) ne izdaju se vremenski žigovi.

Novi servis vremenskog žiga uspostavljen je u **Fina Demo 2014 okolini (nova Demo okolina)**.

Fina Demo 2014 okolina opisana je u poglavlju 4., a novi servis vremenskog žiga **Fina Demo TSA 2014** opisan je u točki 4.1.5 ovog dokumenta.

3. Promjene u sustavima za izdavanje produkcijskih certifikata i vremenskih žigova

Promjene koje se uvode u izdavanju produkcijskih certifikata i vremenskih žigova odnose se na:

- uspostavu dvorazinske arhitekture certifikacijskih tijela (CA-ova);
- prijelaz na korištenje sigurnijih kriptografskih algoritama i duljih kriptografskih ključeva;
- uspostavu nove usluge za provjeru statusa certifikata,
- prijelaz na servis kvalificiranog vremenskog žiga.

U nastavku ovog poglavlja detaljnije su opisane promjene u sustavima za izdavanje produkcijskih certifikata i vremenskih žigova.

3.1. Buduća dvorazinska arhitektura produkcijskih certifikacijskih tijela

U sklopu ovih promjena Fina uvodi dvorazinsku arhitekturu produkcijskih certifikacijskih tijela (CA-ova). Sustav za izdavanje certifikata sastojat će se od novog korijenskog certifikacijskog tijela (engl. *Root Certification Authority, Root CA*) koji izdaje certifikate za subordninirana certifikacijska tijela (eng. *Subordinate Certification Authority, Subordinate CA*). Subordinirana certifikacijska tijela izdaju certifikate krajnjim korisnicima.

U budućoj dvorazinskoj arhitekturi produkcijskih certifikacijskih tijela Fina će imati:

- jedno korijensko certifikacijsko tijelo: **Fina Root CA**
- dva subordinirana certifikacijska tijela:
    - **Fina RDC 2015**
    - **Fina RDC-TDU 2015**

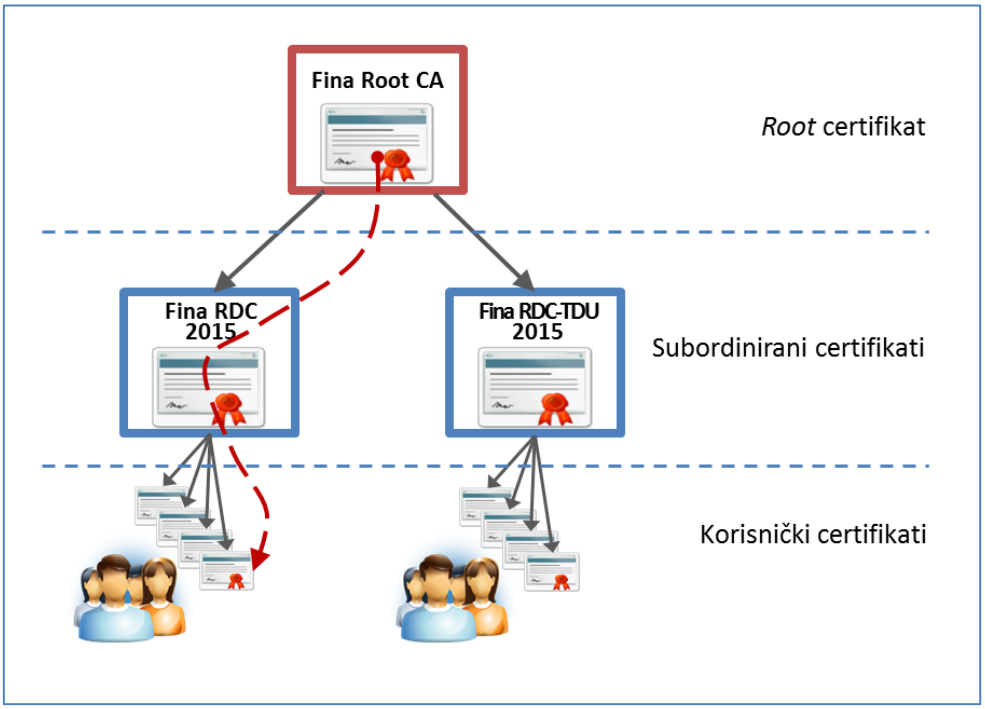
Fina RDC 2015 CA preuzet će ulogu sadašnjeg FINA RDC CA te će izdavati kvalificirane, normalizirane i *lightweight* certifikate za:

- fizičke osobe – građane (osobni certifikati);
- fizičke osobe povezane s poslovnim subjektom (poslovni certifikati); i
- IT opremu povezanu s poslovnim subjektom (poslovni certifikati za IT opremu).

Fina RDC-TDU 2015 CA preuzet će ulogu sadašnjeg FINA RDC-TDU CA te će izdavati kvalificirane i normalizirane certifikate državnim dužnosnicima i zaposlenicima u tijelima državne uprave.

Fina Root CA će izdati certifikate za subordinirane **Fina RDC 2015** i **Fina RDC-TDU 2015** CA-ove**.**

Slika 1. prikazuje buduću dvorazinsku arhitekturu Fininih produkcijskih CA-ova.



Slika 1. Buduća dvorazinska arhitektura Fininih produkcijskih CA-ova

Korisnički certifikati prikazani na Slici 1. izdani su, tj. potpisani su od Fina RDC 2015, odnosno Fina RDC-TDU 2015 CA, a certifikat Fina RDC 2015 i certifikat Fina RDC-TDU 2015 potpisani su od Fina Root CA kao *root* CA buduće dvorazinske arhitekture Fininih produkcijskih CA-ova.

Prateći certifikacijsku stazu, počevši od Fina Root CA certifikata, preko jednog od subordiniranih (Fina RDC 2015 ili Fina RDC-TDU 2015) CA certifikata do korisničkog certifikata formira se lanac certifikata. Na Slici 1. to je prikazano crvenom isprekidanom linijom koja označava lanac certifikata Fina Root CA - Fina RDC 2015 – Korisnički certifikat.

Fina Root CA certifikat je samopotpisani korijenski CA certifikat kojeg je samom sebi izdao i potpisao Fina Root CA. Fina RDC 2015 certifikat je za Fina RDC 2015 CA izdao i potpisao Fina Root CA. Korisnički certifikat je certifikat kojeg je na temelju zahtjeva korisnika izdao i potpisao Fina RDC 2015 CA.

Ovakva arhitektura CA-ova utječe na implementaciju provjere certifikata koju je obavezna provesti svaka strana koja želi ostvariti pouzdanje u certifikat (pouzdajuća strana). Da bi se određeni korisnički certifikat smatrao valjanim jedan od koraka provjere certifikata je konstrukcija i provjera kompletnog lanca certifikata počevši od korisničkog certifikata, certifikata subordiniranog CA do *root* CA certifikata. Stoga je potrebno provjeriti može li određeno korisničko informatičko rješenje koje koristi certifikate ispravno obaviti konstrukciju i provjeru kompletnog lanca certifikata. Konstrukcija i provjera lanca certifikata objašnjena je u točki 5.3.

Za provjeru potpisa u certifikatu nužan je javni ključ CA koji je izdao certifikat. Ako prilikom konstrukcije lanca certifikata određeni CA certifikat nije raspoloživ, moguće ga je dohvatiti koristeći vrijednost *Certification Authority Issuer* unutar ekstenzije certifikata *Authority Information Access*. Ova vrijednost sadrži informaciju o načinu dohvata CA certifikata.

3.2. Prijelaz na sigurnije kriptografske algoritme i dulje ključeve

Sukladno odredbama zakonske regulative iz područja elektroničkog potpisa, za izdavanje certifikata i vremenskih žigova potrebno je obaviti promjene u duljinama kriptografskih ključeva, odnosno prijeći na korištenje adekvatnih, sigurnijih kriptografskih algoritama. Na taj način ostvaruje se povećanje sigurnosti i povjerenja u izdane certifikate i vremenske žigove te se osigurava njihova daljnja nesmetana primjena.

Prijelaz na korištenje sigurnijih kriptografskih algoritama i duljih kriptografskih ključeva realizirat će se:

- Promjenom algoritma za izračunavanje sažetka (*hash* algoritam) - umjesto dosadašnjeg korištenja SHA-1 algoritma za potpisivanje certifikata, CRL i vremenskih žigova koristit će se **SHA-256** algoritam.
- Povećavanjem duljine RSA parova ključeva:
    - umjesto dosadašnjeg RSA javnog ključa duljine 2048 bitova, svi CA certifikati sadržavat će RSA javni ključ duljine **4096 bitova**.
    - Umjesto dosadašnjeg RSA javnog ključa duljine 1024 bita, svi korisnički certifikati sadržavat će RSA javni ključ duljine **2048 bitova**.

U nastavku se nalazi detaljniji opis promjena kriptografskih algoritama i duljina kriptografskih ključeva.

3.2.1. Karakteristike Fina Root CA certifikata

Fina Root CA bit će *root* CA za sve Finine produkcijske certifikate te će izdati i potpisati Fina Root CA certifikat koji će biti „sidro povjerenja“ (*trust anchor*) buduće Finine dvorazinske arhitekture, kao što je to prikazano na Slici 1. Fina Root CA certifikat sadržavat će RSA javni ključ Fina Root CA duljine 4096 bitova, a svaki certifikat i CRL koju izda ovaj CA bit će potpisan pripadnim Fina Root CA privatnim ključem. Za potpisivanje certifikata i CRL Fina Root CA koristit će kriptografske algoritme SHA-256 i RSA. Fina Root CA izdat će i potpisati certifikate za subordinirane CA-ove Fina RDC 2015 i Fina RDC-TDU 2015.

Podaci o budućem Fina Root CA certifikatu dani su u Tablici 8.

Polje	Vrijednost za Fina Root CA certifikat	
Osnovna polja		
Version	X.509 V3, vrijednost="2"	
serialNumber	Serijski broj duljine 12 ili 13 bajtova	
signatureAlgorithm	**sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)**	
Issuer	cn=Fina Root CA, o=Financijska agencija, c=HR	
Validity	NotBefore: Vrijeme izdavanja certifikata NotAfter: 31.12.2029.	
Subject	cn=Fina Root CA, o=Financijska agencija, c=HR	
subjectPublicKeyInfo	**rsaEncryption (OID: 1.2.840.113549.1.1.1), javni ključ duljine 4096 bitova**	
Polje	**Kritično**	**Vrijednost**
Ekstenzije		
KeyUsage	DA	KeyCertSign, cRLSign
BasicConstraints	DA	cA=true
AuthorityKeyIdentifier	NE	160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (određeno prema RFC 5280, točka 4.2.1.2 metoda (1))
SubjectKeyIdentifier	NE	160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (određeno prema RFC 5280, točka 4.2.1.2 metoda (1))

Tablica 8. Podaci o budućem Fina Root CA certifikatu

3.2.2. Karakteristike certifikata za Fina RDC 2015 i Fina RDC-TDU 2015 CA-ove

Certifikati za Fina RDC 2015 i Fina RDC-TDU 2015 bit će subordinirani certifikati Fina Root CA certifikata kao što je to prikazano na Slici 1. U odnosu na postojeće certifikate za FINA RDC CA i FINA RDC-TDU CA koji su opisani u točkama 2.1.1. i 2.1.2., certifikati za Fina RDC 2015 i Fina RDC-TDU 2015 sadržavat će RSA javni ključ duljine 4096 bitova te će od strane Fina Root CA biti potpisani RSA privatnim ključem duljine 4096 bitova korištenjem kriptografskih algoritama SHA-256 i RSA.

Podaci o budućim certifikatima za Fina RDC 2015 i Fina RDC-TDU 2015 CA-ove dani su u Tablici 9.

Polje	Vrijednosti za Fina RDC 2015 i Fina RDC-TDU 2015 certifikate
Osnovna polja	
Version	X.509 V3, vrijednost="2"
serialNumber	Serijski broj duljine 12 ili 13 bajtova
signatureAlgorithm	**sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)**
Issuer	cn=Fina Root CA, o=Financijska agencija, c=HR
Validity	NotBefore: Vrijeme izdavanja certifikata NotAfter: Vrijeme izdavanja certifikata + 10 godina
Subject	Za Fina RDC 2015: cn=Fina RDC 2015, o=Financijska agencija, c=HR Za Fina RDC-TDU 2015: cn=Fina RDC-TDU 2015, o=Financijska agencija, c=HR
subjectPublic KeyInfo	**rsaEncryption (OID: 1.2.840.113549.1.1.1), javni ključ duljine 4096 bitova**

Polje	Kritično	Vrijednost
Ekstenzije		
KeyUsage	DA	KeyCertSign, cRLSign
BasicConstraints	DA	cA=true pathLen=0
AuthorityKeyIdentifier	NE	160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (određeno prema RFC 5280, točka 4.2.1.2 metoda (1))
SubjectKeyIdentifier	NE	160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (određeno prema RFC 5280, točka 4.2.1.2 metoda (1))
certificatePolicies	NE	policyIdentifier: CertPolicyId (OID) za Fina subordinirani certifikat, policyQualifiers: policyQualifierId i URI za CP/CPS
Authority Information Access	NE	[1]Authority Info Access accessMethod=Online Certificate Status Protocol (OID: 1.3.6.1.5.5.7.48.1), accessLocation: URL OCSP respondera [2]Authority Info Access accessMethod=Certification Authority Issuer (OID: 1.3.6.1.5.5.7.48.2) accessLocation: HTTP URL FINA Root CA certifikata
CRLDistributionPoints	NE	• Adresa segmentirane CRL dostupne preko LDAP protokola • Adresa CRL dostupne preko LDAP protokola • HTTP URL na kojem je dostupna CRL lista

Tablica 9. Podaci o certifikatima za Fina RDC 2015 i Fina RDC-TDU 2015 CA-ove

3.2.3. Karakteristike certifikata koje će izdavati Fina RDC 2015 i Fina RDC-TDU 2015 CA-ovi

U odnosu na postojeće korisničke certifikate koje izdaju FINA RDC CA, odnosno FINA RDC-TDU CA, a čija su osnovna polja prikazana u Tablici 2. i Tablici 4., korisnički certifikati koje će izdavati Fina RDC 2015, odnosno Fina RDC-TDU 2015 imat će osnovna polja sukladno Tablici 10.

Osnovo polje	Vrijednost za certifikate koje će izdavati Fina RDC 2015 i Fina RDC-TDU 2015 CA-ovi
Version	X.509 V3, vrijednost="2"
serialNumber	Pozitivni cijeli broj duljine 16-17 bajtova
signatureAlgorithm	**sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)**
Issuer	Za Fina RDC 2015: cn=Fina RDC 2015, o=Financijska agencija, c=HR Za Fina RDC-TDU 2015: cn=Fina RDC-TDU 2015, o=Financijska agencija, c=HR
Validity	NotBefore: Vrijeme izdavanja certifikata NotAfter: Ovisno o tipu certifikata: 1, 2 ili 5 godina od izdavanja certifikata
Subject	Ovisno o tipu certifikata, jednako kao za certifikate koje izdaju postojeći FINA RDC CA i FINA RDC-TDU CA
subjectPublic KeyInfo	**rsaEncryption (OID: 1.2.840.113549.1.1.1), javni ključ duljine 2048 bitova**

Tablica 10. Osnovni podaci o korisničkim certifikatima koje će izdavati Fina RDC 2015 i Fina RDC-TDU 2015 CA-ovi

3.3. Uspostava nove usluge za provjeru statusa certifikata

Kod povećanja broja izdanih certifikata raste i broj opozvanih, odnosno suspendiranih certifikata te se povećava duljina CRL koja time postaje sve zahtjevnija za prijenos. Također, zbog obveze pouzdajuće strane da obavlja provjeru statusa svakog certifikata prije ostvarenja povjerenja u certifikat, dulja CRL povećava vrijeme njene obrade i vrijeme provjere statusa certifikata. Iz tog razloga za provjeru statusa certifikata sve se više preporuča korištenje posebnog *online* protokola: *Online Certificate Status Protocol* (OCSP), a u dogledno vrijeme se može očekivati i njegova obvezna uporaba.

OCSP servis zasniva se na klijent-server modelu u kojem OCSP klijent pouzdajuće strane šalje OCSP serveru (OCSP *Responder*) upit o statusu certifikata, a OCSP servis klijentu vraća odgovor o statusu certifikata.

Fina će u sklopu buduće dvorazinske arhitekture uspostaviti OCSP servis pod nazivom **Fina OCSP 2015** koji će davati informacije o statusima certifikata izdanih od strane Fina Root CA, Fina RDC 2015 i Fina RDC-TDU 2015, sukladno prikazu na Slici 2. u točki 3.5. Informacija o pristupnoj adresi Fina OCSP 2015 servisa nalazit će se u *Authority Information Access* ekstenziji svakog Fininog produkcijskog certifikata. Rad Fina OCSP 2015 servisa bit će sukladan s preporukom IETF RFC 6960.

Fina OCSP 2015 servis će potpisati odgovor onim OCSP certifikatom kojeg je izdao Finin produkcijski CA koji je izdao i korisnički certifikat čiji se status provjerava. Ako se traži provjera statusa korisničkog certifikata kojeg je izdao Fina RDC 2015 tada će Fina OCSP 2015 servis odgovor potpisati certifikatom kojeg je OCSP servisu izdao Fina RDC 2015. Analogno vrijedi i za korisnički certifikat kojeg je izdao Fina RDC-TDU 2015. Odgovor za status Fina RDC 2015 certifikata i status Fina RDC-TDU 2015 certifikata bit će potpisan certifikatom kojeg je OCSP servisu izdao Fina Root CA.

Fina OCSP 2015 servis će potpisivati odgovore RSA privatnim ključem duljine 2048 bitova uz korištenje kriptografskih algoritama SHA-256 i RSA.

Korištenjem Fina OCSP 2015 servisa smanjit će se količina mrežnog prometa te ubrzati provjera statusa certifikata.

Pored korištenja Fina OCSP 2015 servisa, provjere statusa certifikata moći će se i nadalje obavljati dohvatom CRL. Preporuka je da se za provjeru statusa certifikata koristi OCSP servis, a provjera statusa dohvatom CRL može se koristiti kao alternativna metoda provjere u slučaju nedostupnosti OCSP servisa.

U Tablici 11. prikazani su osnovni podaci o certifikatima kojima će Fina OCSP 2015 servis potpisivati odgovore.

Polje	Vrijednost za certifikate Fina OCSP 2015 servisa
Version	X.509 V3, vrijednost="2"
serialNumber	Pozitivni cijeli broj duljine 16-17 bajtova
signatureAlgorithm	**sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)**

Polje	Vrijednost za certifikate Fina OCSP 2015 servisa
Issuer	Certifikat za OCSP servis će izdati: • cn=Fina Root CA, o=Financijska agencija, c=HR; • cn=Fina RDC 2015, o=Financijska agencija, c=HR; i • cn=Fina RDC-TDU 2015, o=Financijska agencija, c=HR.
Validity	NotBefore: Vrijeme izdavanja certifikata NotAfter: Biti će naknadno definirano
Subject	Ovisno o izdavatelju certifikata za OCSP servis, Subject DN će biti: • cn=Fina Root OCSP, o=Financijska agencija, c=HR; • cn=Fina RDC OCSP 2015, o=Financijska agencija, c=HR; ili • cn=Fina RDC-TDU OCSP 2015, o=Financijska agencija, c=HR.
SubjectPublicKeyInfo	**rsaEncryption** (**OID: 1.2.840.113549.1.1.1), javni ključ duljine 2048 bitova** OCSP servis će odgovore potpisivati pripadajućim privatnim ključem.

Tablica 11. Osnovni podaci o certifikatima Fina OCSP 2015 servisa

3.4. Prijelaz na servis kvalificiranog vremenskog žiga

U sklopu predmetnih promjena Fina će uspostaviti novi servis vremenskog žiga koji će izdavati napredne vremenske žigove sukladno zakonskoj regulativi iz područja elektroničkog potpisa. Kako se napredni vremenski žigovi mogu koristiti zajedno s kvalificiranim certifikatima te se izdaju na sustavu koji je po razini sigurnosti izjednačen sa sustavom za izdavanje kvalificiranih certifikata, praksa je da se takve napredne vremenske žigove naziva kvalificiranim vremenskim žigovima. Kvalificirane vremenske žigove izdavat će servis kvalificiranog vremenskog žiga **Fina QTSA 2015** te će on zamijeniti postojeći produkcijski servis vremenskog žiga FINA Servis vremenske ovjere. Način pristupa Fina QTSA 2015 servisu bit će jednak kao i pristup postojećem FINA Servisu vremenske ovjere, tj. mogućnost korištenja Fina QTSA 2015 servisa imat će samo autorizirani korisnici koji će se na servis prijavljivati certifikatom (SSL/TLS uz klijentsku autentifikaciju certifikatom – *two-way* SSL).

Certifikat za Fina QTSA 2015 izdat će Fina RDC 2015, a kvalificirani vremenski žigovi bit će potpisani RSA privatnim ključem Fina QTSA 2015 servisa, duljine 2048 bitova uz korištenje kriptografskih algoritama SHA-256 i RSA.

Osnovni podaci o certifikatu servisa Fina QTSA 2015 kojim će taj servis potpisivati kvalificirane vremenske žigove dani su u Tablici 12.

Polje	Vrijednost za certifikat Fina QTSA 2015 servisa
Version	X.509 V3, vrijednost="2"
serialNumber	Pozitivni cijeli broj duljine 16-17 bajtova
signatureAlgorithm	**sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)**
Issuer	cn=Fina RDC 2015, o=Financijska agencija, c=HR
Validity	NotBefore: Vrijeme izdavanja certifikata NotAfter: Biti će naknadno definirano
Subject	cn=*Naziv TSU*, o=Financijska agencija, c=HR
SubjectPublicKeyInfo	**rsaEncryption** (**OID: 1.2.840.113549.1.1.1), javni ključ duljine 2048 bitova** Pripadajućim privatnim ključem Fina QTSA 2015 servis potpisuje svaki izdani kvalificirani vremenski žig.

Tablica 12. Osnovni podaci o certifikatu Fina QTSA 2015 servisa

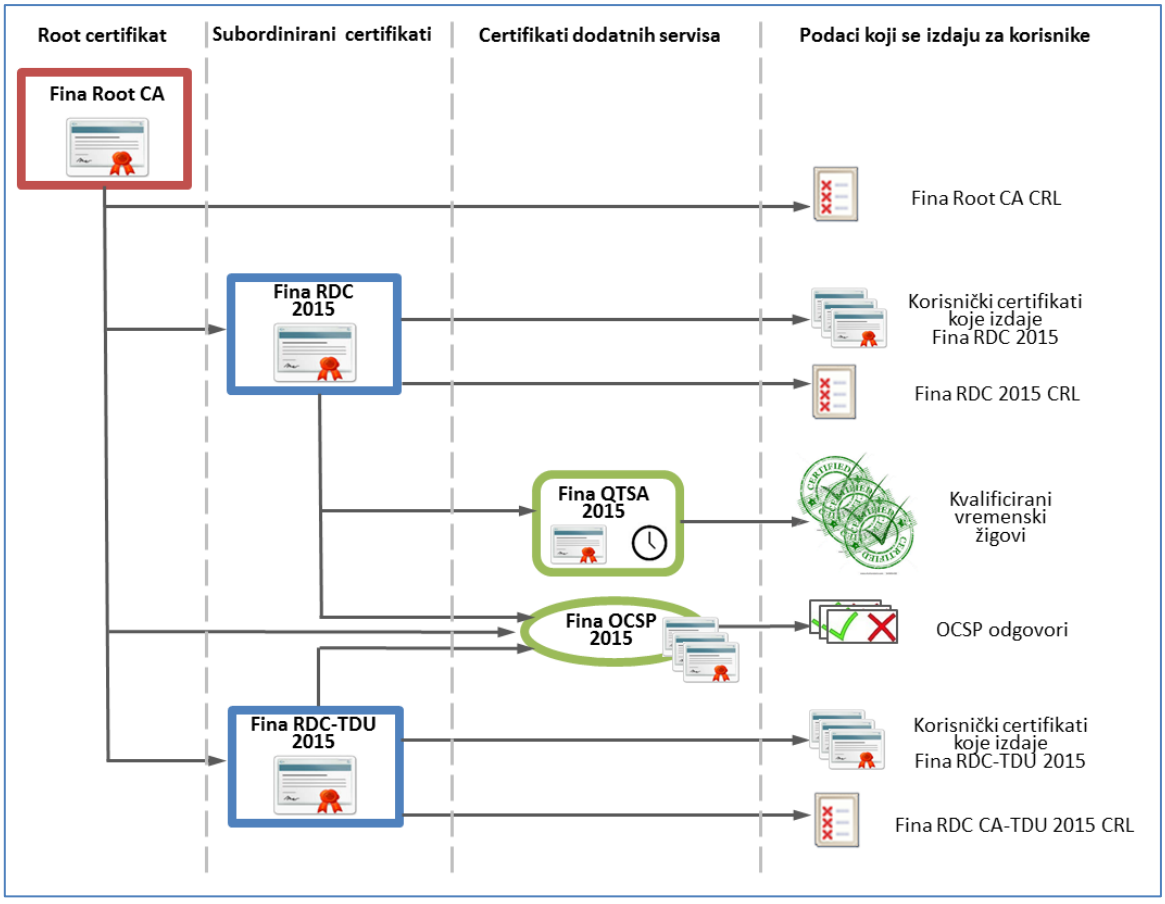
Osnovni podaci o profilu vremenskih žigova koje će izdavati Fina QTSA 2015 servis dani su u Tablici 13. Posebno su istaknute informacije o korištenom kriptografskom algoritmu za izračun sažetka podataka za koje se traži izdavanje vremenskog žiga (*messageImprint*) te o potpisnim algoritmima koji se koriste za potpisivanje vremenskog žiga (*signatureAlgorithm*).

Polje	Vrijednost za vremenski žig FINA QTSA 2015 servisa
Version	V1, vrijednost="1"
Policy OID	*Finin Policy OID za servis kvalificiranog vremenskog žiga*
messageImprint	**Podržani hash algoritmi:** • **hashAlgorithm: sha-1 (OID: 1.3.14.3.2.26) i** • **hashAlgorithm: sha-256 (OID: 2.16.840.1.101.3.4.2.1)**
serialNumber	Cijeli broj
genTime	UTC vrijeme, razlučivost od 1 sekunde
Nonce	Cijeli broj
signatureAlgorithm	**sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)**

Tablica 13. Osnovni podaci o vremenskog žigu kojeg će izdavati Fina QTSA 2015 servis

3.5. Prikaz buduće produkcijske okoline

Slika 2. prikazuje certifikate i servise buduće dvorazinske Finine produkcijske okoline za izdavanje certifikata i vremenskih žigova koja je opisana u točkama 3.1 do 3.4.



Slika 2. Buduća produkcijska okolina za izdavanje certifikata i vremenskih žigova

Kako bi olakšali provjeru i prilagodbu postojećih korisničkih informatičkih rješenja za rad s budućim produkcijskim certifikatima i vremenskim žigovima, Fina je uspostavila novu Fina Demo 2014 okolinu koja je opisana u poglavlju 4.

3.6. Početak primjene i potreba prilagodbe korisničkih informatičkih rješenja

Promjene opisane u ovom poglavlju utjecat će na postojeća i nova korisnička informatička rješenja koja koriste Finine certifikate i vremenske žigove te će stoga na svim korisničkim rješenjima biti potrebno prethodno provjeriti njihovu spremnost za korištenje izmijenjenih budućih produkcijskih certifikata te po potrebi obaviti prilagodbu pojedinih rješenja.

Opseg prilagodbe ovisi o konkretnom rješenju, načinu na koji je rješenje realizirano i mogućnostima ugrađenim u rješenje. Zbog velikog broja korisnika i raznovrsnosti postojećih rješenja s jedne strane, te obzirom na nužnost i važnost promjena s druge strane, pri odabiru roka početka primjene nastojalo se osigurati dovoljno vremena za testiranje i prilagodbu informatičkih rješenja, a istovremeno osigurati pravodobni početak primjene predmetnih promjena u kojem sigurnost certifikata neće biti narušena.

Početak primjene predmetnih promjena u produkciji biti će u **4. kvartalu 2015. godine**. Fina RDC 2015 i Fina RDC-TDU 2015 će tada početi izdavati prve produkcijske korisničke certifikate, a status tih certifikata moći će se provjeriti i uporabom Fina OCSP 2015 servisa. Svako izdavanje i obnova certifikata obavljat će se na Fina RDC 2015, odnosno na Fina RDC-TDU 2015 CA. Neposredno prije početka izdavanja prvih produkcijskih korisničkih certifikata od strane Fina RDC 2015 i Fina RDC-TDU 2015, postojeći FINA RDC CA i FINA RDC-TDU CA prestat će s izdavanjem i obnovom korisničkih certifikata, ali će i dalje nastaviti izdavati pripadajuće CRL u propisanim vremenskim intervalima.

Također, početak primjene predmetnih promjena uključuje i početak rada Fina QTSA 2015 servisa koji će tada započeti izdavati kvalificirane vremenske žigove svim dotadašnjim korisnicima FINA Servisa vremenske ovjere. Neposredno prije početka primjene promjena u produkciji FINA Servis vremenske ovjere će prestati sa svojim radom.

Do početka primjene predmetnih promjena u produkciji sva rješenja koja koriste postojeći FINA Servis vremenske ovjere trebaju biti prilagođena za korištenje servisa kvalificiranog vremenskog žiga Fina QTSA 2015.

Postojeći korisnički certifikati čiji rok važenja ističe nakon početka primjene navedenih promjena u produkciji i dalje će biti važeći te će se moći neometano koristiti do kraja svojeg roka važenja, a status certifikata moći će se, kao i do tada, provjeriti pomoću FINA RDC CRL, odnosno FINA RDC-TDU CRL. Ovi certifikati će se moći kao i do sada obnoviti pred kraj njihova važenja, a obnovljeni certifikat izdat će Fina RDC 2015, odnosno Fina RDC-TDU 2015.

Do početka primjene predmetnih promjena u produkciji, sva prilagođena korisnička informatička rješenja i eventualna nova rješenja trebaju biti prilagođena za rad:

- s certifikatima izdanim od strane Fina RDC 2015 i Fina RDC-TDU 2015, uključujući obavljanje ispravne provjere certifikata prema opisanoj dvorazinskoj arhitekturi CA-ova; te
- s certifikatima izdanim od strane postojećih FINA RDC CA i FINA RDC-TDU CA.

Sva prilagođena korisnička rješenja trebaju osigurati navedenu istovremenu podršku jer će u razdoblju od dvije ili pet godina (ovisno o tipovima certifikata koje konkretno rješenje koristi) postojati korisnici kojima su certifikate izdali postojeći FINA RDC CA i FINA RDC-TDU CA, ali će se istovremeno javljati sve veći broj korisnika kojima su certifikate izdali budući Fina RDC 2015 i Fina RDC-TDU 2015. Naime, certifikati izdani u 4. kvartalu 2015. od strane postojećih CA-ova (ovisno o tipovima certifikata) važit će do 4. kvartala 2017., odnosno do 4. kvartala 2020. te će do tada postojat krajnji korisnici koji još imaju važeće certifikate izdane od strane postojećih FINA RDC CA i FINA RDC-TDU CA, a istovremeno će se postupno pojaviti i rasti broj korisnika s certifikatima koje su izdali Fina RDC 2015 i Fina RDC-TDU 2015 CA-ovi.

Kako bi svim vlasnicima informatičkih rješenja koja koriste Finine digitalne certifikate što više olakšali testiranje i prilagodbu postojećih rješenja uspostavljena je Fina Demo 2014 okolina koja izdaje Demo certifikate i vremenske žigove za potrebe testiranja i prilagodbe rješenja. Izdavanje certifikata i vremenskih žigova u Fina Demo 2014 okolini opisano je u sljedećem poglavlju.

4. Izdavanje novih Demo certifikata i vremenskih žigova

Fina Demo CA 2014 okolina je novouspostavljena Demo okolina Finine dvorazinske arhitekture CA-ova u kojoj se izdaju Demo digitalni certifikati i Demo vremenski žigovi, a koji se koriste za provjeru i prilagodbu postojećih korisničkih informatičkih rješenja za rad s budućim produkcijskim certifikatima i vremenskim žigovima. Certifikati i vremenski žigovi izdani u Fina Demo 2014 okolini smiju se koristiti **isključivo u svrhe testiranja i provjere ispravnosti informatičkih rješenja**. Uporaba Demo certifikata i Demo vremenskih žigova smije rezultirati pouzdanjem u elektronički potpis, autentifikaciju, enkripciju ili u bilo koji drugi vid korištenja Demo certifikata, odnosno Demo vremenskih žigova za primjene isključivo u testnoj ili prezentacijskoj okolini.

Demo certifikati se u Fina Demo 2014 okolini izdaju prema novim (izmijenjenim) profilima koji su u tehnološkom i funkcionalnom smislu potpuno jednaki profilima budućih Fininih produkcijskih certifikata. U ovoj okolini certifikate za krajnje korisnike izdaje **Fina Demo 2014 CA**.

Provjera statusa certifikata koje izdaje **Fina Demo 2014 CA** može se obaviti korištenjem CRL ili korištenjem **Fina Demo OCSP 2014** servisa. Način rada Fina Demo OCSP 2014 servisa jednak je radu budućeg produkcijskog Fina OCSP 2014 servisa.

Demo vremenski žigovi koji se izdaju u Fina Demo 2014 okolini su u tehnološkom i funkcionalnom smislu potpuno jednaki izmijenjenom profilu budućih Fininih kvalificiranih vremenskih žigova. U Fina Demo 2014 okolini vremenske žigove izdaje **Fina Demo TSA 2014** servis vremenskog žiga.

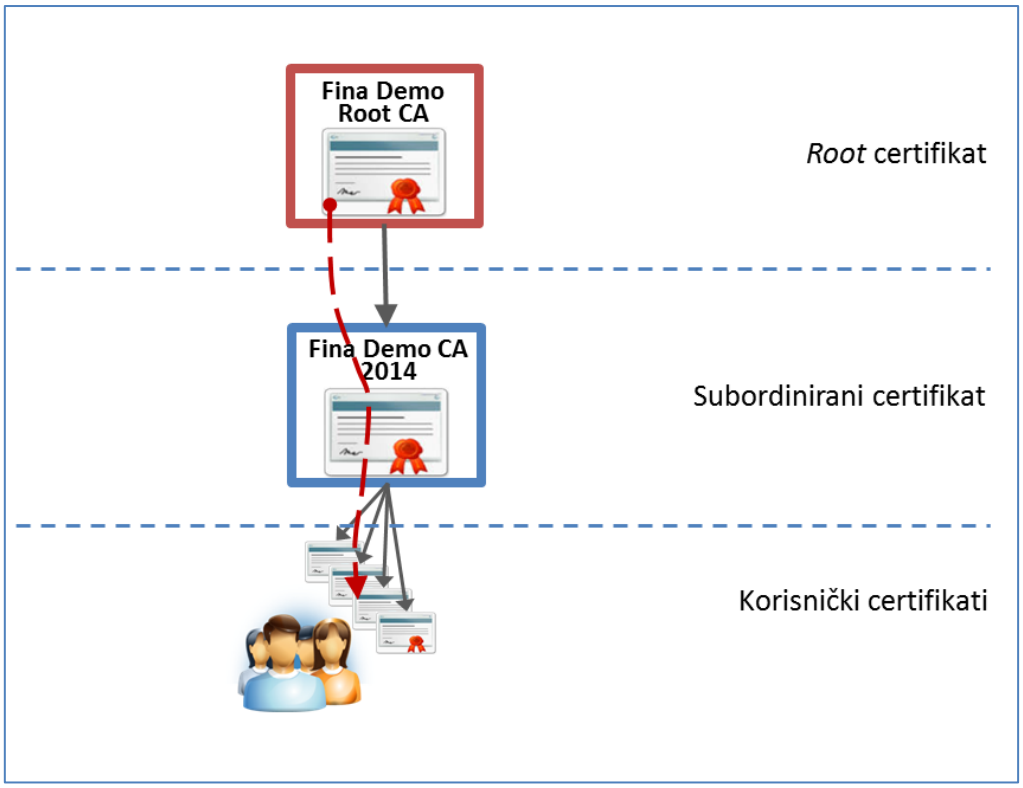
Root CA za Fina Demo 2014 okolinu je **Fina Demo Root CA** koji je samom sebi izdao i potpisao Fina Demo Root CA certifikat.

4.1. Dvorazinska arhitektura certifikacijskih tijela u novoj Demo okolini

Arhitektura CA-ova Fina Demo 2014 okoline prikazana je na Slici 3., a sastoji se od Fina Demo Root CA i subordiniranog Fina Demo CA 2014.

Korisničke Demo certifikate izdao je i potpisao Fina Demo CA 2014, a certifikat Fina Demo CA 2014 potpisao je Fina Demo Root CA.

Na Slici 3. crvenom isprekidanom linijom prikazana je certifikacijska staza koja počinje od Fina Demo Root CA certifikata, ide preko Fina Demo CA 2014 do korisničkog certifikata te se tako formira lanac certifikata.



Slika 3. Arhitektura CA-ova u Fina Demo 2014 okolini

4.1.1. Karakteristike Fina Demo Root CA certifikata

Fina Demo Root CA je *root* CA za Fina Demo 2014 okolinu te ima izdan Fina Demo Root CA certifikat u kojem je sadržan RSA javni ključ tog CA. Duljina javnog ključa je 4096 bitova, a svaki certifikat i CRL koju izda Fina Demo Root CA potpisan je pripadnim Fina Demo Root CA privatnim ključem. Za potpisivanje certifikata i CRL Fina Demo Root CA koristi kriptografske algoritme SHA-256 i RSA.

Podaci o Fina Demo Root CA certifikatu dani su u Tablici 14.

Polje	Vrijednost za Fina Demo Root CA certifikat	
Osnovna polja		
Version	X.509 V3, vrijednost="2"	
serialNumber	Serijski broj duljine 12 ili 13 bajtova	
signatureAlgorithm	**sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)**	
Issuer	cn=Fina Demo Root CA, o=Financijska agencija, c=HR	
Validity	NotBefore: 18. ožujka 2014. 11:45:00 NotAfter: 18. ožujka 2034. 12:15:00	
Subject	cn=Fina Demo Root CA, o=Financijska agencija, c=HR	
subjectPublicKeyInfo	**rsaEncryption (OID: 1.2.840.113549.1.1.1), javni ključ duljine 4096 bitova**	
Polje	**Kritično**	**Vrijednost**
Ekstenzije		
KeyUsage	DA	KeyCertSign, cRLSign

Polje	Kritično	Vrijednost
Ekstenzije		
BasicConstraints	DA	cA=true
AuthorityKeyIdentifier	NE	160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (određeno prema RFC 5280, točka 4.2.1.2 metoda (1))
SubjectKeyIdentifier	NE	160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (određeno prema RFC 5280, točka 4.2.1.2 metoda (1))

Tablica 14. Podaci o Fina Demo Root CA certifikatu

Fina Demo Root CA certifikat može se preuzeti s adrese: http://demo-pki.fina.hr/certifikati/demo2014_root_ca.cer, a vrijednost njegova SHA-1 sažetka (*Thumbprint* ili *Fingerprint*) je:

cf:06:2e:51:85:79:c3:ad:c6:ce:20:a9:4a:88:52:89:88:3b:aa:2a.

4.1.2. Karakteristike certifikata za Fina Demo CA 2014

Certifikat za Fina Demo CA 2014 je subordinirani certifikat Fina Demo Root CA certifikata kao što je to prikazano na Slici 3. te sadrži RSA javni ključ duljine 4096 bitova. Ovaj certifikat potpisao je Fina Demo Root CA svojim RSA privatnim ključem duljine 4096 bitova uz korištenje kriptografskih algoritama SHA-256 i RSA.

Podaci o certifikatu za Fina Demo CA 2014 dani su u Tablici 15.

Polje	Vrijednost za Fina Demo CA 2014 certifikat	
Osnovna polja		
Version	X.509 V3, vrijednost="2"	
serialNumber	Serijski broj duljine 12 ili 13 bajtova	
signatureAlgorithm	**sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)**	
Issuer	cn=Fina Demo Root CA, o=Financijska agencija, c=HR	
Validity	NotBefore: 25. ožujka 2014. 6:45:47 NotAfter: 25. ožujka 2024. 7:15:47	
Subject	cn=Fina Demo CA 2014, o=Financijska agencija, c=HR	
subjectPublic KeyInfo	**rsaEncryption (OID: 1.2.840.113549.1.1.1), javni ključ duljine 4096 bitova**	
Polje	**Kritično**	**Vrijednost**
Ekstenzije		
KeyUsage	DA	KeyCertSign, cRLSign
BasicConstraints	DA	cA=true pathLen=0
AuthorityKeyIdentifier	NE	160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (određeno prema RFC 5280, točka 4.2.1.2 metoda (1))
SubjectKeyIdentifier	NE	160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (određeno prema RFC 5280, točka 4.2.1.2 metoda (1))

Polje	Kritično	Vrijednost
Ekstenzije		
certificatePolicies	NE	policyIdentifier: CertPolicyId (OID): 1.3.124.1104.5.1.1 policyQualifiers: • policyQualifierId za CP/CP • http://demo-pki.fina.hr/cps/cpdemoroot1-0.pdf
Authority Information Access	NE	[1]Authority Info Access accessMethod=Online Certificate Status Protocol (OID: 1.3.6.1.5.5.7.48.1) accessLocation: URL=http://demo2014-ocsp.fina.hr [2]Authority Info Access accessMethod=Certification Authority Issuer (OID: 1.3.6.1.5.5.7.48.2) accessLocation: http://demo-pki.fina.hr/certifikati/demo2014_root_ca.cer
CRLDistributionPoints	NE	• HTTP URL na kojem je dostupna CRL lista • Adresa segmentirane CRL dostupne preko LDAP protokola

Tablica 15. Podaci o certifikatu za Fina Demo CA 2014

Fina Demo CA 2014 certifikat može se preuzeti s adrese: http://demo-pki.fina.hr/certifikati/demo2014_sub_ca.cer, a vrijednost njegova SHA-1 sažetka (*Thumbprint* ili *Fingerprint*) je:

be:50:56:0c:61:64:97:ce:7d:75:8d:0c:f3:b9:89:76:6e:ef:8f:81.

4.1.3. Karakteristike korisničkih certifikata koje izdaje Fina Demo CA 2014

Profili korisničkih certifikata koje izdaje Fina Demo CA 2014 jednaki su budućim profilima koje će izdavati Fina RDC 2015 i Fina RDC-TDU 2015. Osnovna polja korisničkih certifikata koje izdaje Fina Demo CA 2014 prikazana su u Tablici 16.

Osnovo polje	Vrijednost za certifikate koje izdaje Fina Demo CA 2014
Version	X.509 V3, vrijednost="2"
serialNumber	Pozitivni cijeli broj duljine 16-17 bajtova
signatureAlgorithm	**sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)**
Issuer	cn=Fina Demo CA 2014, o=Financijska agencija, c=HR
Validity	NotBefore: Vrijeme izdavanja certifikata NotAfter: Ovisno o tipu certifikata: 1, 2 ili 5 godina od izdavanja certifikata
Subject	Ovisno o tipu certifikata, jednako kao za certifikate koje izdaju postojeći FINA RDC CA i FINA RDC-TDU CA
subjectPublic KeyInfo	**rsaEncryption (OID: 1.2.840.113549.1.1.1), javni ključ duljine 2048 bitova**

Tablica 16. Osnovni podaci o korisničkim certifikatima koje izdaje Fina Demo 2014 CA

Potpuni opis svih profila korisničkih certifikata koje izdaje Fina Demo 2014 CA objavljen je u dokumentu Profili korisničkih Fina Demo 2014 certifikata.

4.1.4. Fina Demo OCSP 2014 servis

U sklopu Fina Demo 2014 okoline uspostavljen je OCSP servis pod nazivom **Fina Demo OCSP 2014** koji daje informacije o statusima certifikata izdanih od strane Fina Demo Root CA i Fina Demo CA 2014, sukladno prikazu na Slici 4. u točki 4.2. Rad ovog servisa sukladan je s preporukom IETF RFC 5019, dok će budući produkcijski Fina OCSP 2015 servis biti u potpunosti kompatibilan s preporukom IETF RFC 6960.

Pristupna adresa ovog servisa je http://demo2014-ocsp.fina.hr. Informacija o pristupnoj adresi servisa nalazi se u *Authority Information Access* ekstenziji svakog certifikata izdanog u Fina Demo 2014 okolini.

Fina Demo OCSP 2014 servis će potpisati odgovor OCSP certifikatom kojeg je izdao Fina Demo CA 2014, odnosno Fina Demo Root CA, ovisno o izdavatelju certifikata čiji se status traži. Ako se traži provjera statusa korisničkog certifikata kojeg je izdao Fina Demo CA 2014, tada će Fina Demo OCSP 2014 servis odgovor potpisati certifikatom kojeg je OCSP servisu izdao Fina Demo CA 2014. Odgovor za status Fina Demo CA 2014 certifikata bit će potpisan certifikatom kojeg je OCSP servisu izdao Fina Demo Root CA.

Fina Demo OCSP 2014 servis odgovore će potpisivati RSA privatnim ključem duljine 2048 bitova uz korištenje kriptografskih algoritama SHA-256 i RSA.

Provjera statusa Demo certifikata moći će se i nadalje obavljati dohvatom CRL.

U Tablici 17. prikazani su podaci o certifikatima kojima će Fina Demo OCSP 2014 servis potpisivati odgovore.

Polje	Vrijednost za certifikat Fina Demo OCSP 2014 servisa	
Osnovna polja		
Version	X.509 V3, vrijednost="2"	
serialNumber	Serijski broj duljine 12 ili 13 bajtova	
signatureAlgorithm	**sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)**	
Issuer	cn=Fina Demo Root CA, o=Financijska agencija, c=HR	
Validity	NotBefore: Vrijeme izdavanja certifikata NotAfter: Vrijeme izdavanja certifikata + 12 mjeseci	
Subject	Za potpis statusa certifikata koje izdaje Fina Demo Root CA cn=Fina Demo Root OCSP, o=Financijska agencija, c=HR Za potpis statusa certifikata koje izdaje Fina Demo CA 2014 cn=Fina Demo OCSP 2014, o=Financijska agencija, c=HR	
subjectPublic KeyInfo	**rsaEncryption (OID: 1.2.840.113549.1.1.1), javni ključ duljine 2048 bitova**	
Polje	**Kritično**	**Vrijednost**
Ekstenzije		
KeyUsage	DA	digitalSignature, nonRepudiation
extKeyUsage	NE	OCSPSigning
ocsp-nocheck	NE	vrijednost NULL
AuthorityKeyIdentifier	NE	160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (određeno prema RFC 5280, točka 4.2.1.2 metoda (1))

Polje	Kritično	Vrijednost
Ekstenzije		
SubjectKeyIdentifier	NE	160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (određeno prema RFC 5280, točka 4.2.1.2 metoda (1))
certificatePolicies	NE	policyIdentifier: CertPolicyId (OID): 1.3.124.1104.5.32.9.3.2 policyQualifiers: • policyQualifierId za CP/CP • http://demo-pki.fina.hr/cps/cpdemoroot1-0.pdf
Authority Information Access	NE	[1]Authority Info Access accessMethod=Online Certificate Status Protocol (OID: 1.3.6.1.5.5.7.48.1) accessLocation: URL=http://demo2014-ocsp.fina.hr [2]Authority Info Access accessMethod=Certification Authority Issuer (OID: 1.3.6.1.5.5.7.48.2) accessLocation: Za potpis statusa certifikata koje izdaje Fina Demo Root CA http://demo-pki.fina.hr/certifikati/demo2014_root_ca.cer Za potpis statusa certifikata koje izdaje Fina Demo CA 2014 http://demo-pki.fina.hr/certifikati/demo2014_sub_ca.cer
CRLDistributionPoints	NE	• HTTP URL na kojem je dostupna CRL lista • Adresa CRL dostupne preko LDAP protokola • Adresa segmentirane CRL dostupne preko LDAP protokola
BasicConstraints	NE	cA=FALSE pathLenConstraint=None

Tablica 17. *Podaci o certifikatima Fina Demo OCSP 2014 servisa*

4.1.5. Servis vremenskog žiga Fina Demo TSA 2014

Unutar Fina Demo 2014 okoline uspostavljen je servis vremenskog žiga **Fina Demo TSA 2014**. Pristup ovom servisu i oblik vremenskog žiga jednak je kvalificiranim vremenskim žigovima koje će izdavati budući servis kvalificiranog vremenskog žiga Fina QTSA 2014.

Pristup Fina Demo TSA 2014 servisu imaju samo autorizirani korisnici. Prijava na ovaj servis obavlja se korisničkim certifikatom (uspostava SSL/TLS uz klijentsku autentifikaciju certifikatom – *two-way* SSL). Korisnički certifikat za prijavu na servis izdaje Fina Demo CA 2014.

Certifikat za Fina Demo TSA 2014 izdao je Fina Demo CA 2014, a izdani vremenski žigovi potpisani su RSA privatnim ključem Fina Demo TSA 2014 servisa duljine 2048 bitova uz korištenje kriptografskih algoritama SHA-256 i RSA.

Podaci o certifikatu servisa Fina Demo TSA 2014 kojim servis potpisuje vremenske žigove dani su u Tablici 18.

Polje	Vrijednost za certifikat Fina Demo TSA 2014 servisa
Osnovna polja	
Version	X.509 V3, vrijednost="2"
serialNumber	Serijski broj duljine 16 ili 17 bajtova
signatureAlgorithm	**sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)**
Issuer	cn=Fina Demo CA 2014, o=Financijska agencija, c=HR

Polje	Vrijednost za certifikat Fina Demo TSA 2014 servisa	
Osnovna polja		
Validity	NotBefore: Vrijeme izdavanja certifikata NotAfter: Biti će naknadno definirano	
Subject	cn=Fina Demo TSA1 2014, o=Financijska agencija, c=HR	
subjectPublic KeyInfo	**rsaEncryption (OID: 1.2.840.113549.1.1.1), javni ključ duljine 2048 bitova**	
Polje	**Kritično**	**Vrijednost**
Ekstenzije		
KeyUsage	DA	digitalSignature, nonRepudiation
extKeyUsage	NE	timeStamping
AuthorityKeyIdentifier	NE	160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (određeno prema RFC 5280, točka 4.2.1.2 metoda (1))
SubjectKeyIdentifier	NE	160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (određeno prema RFC 5280, točka 4.2.1.2 metoda (1))
certificatePolicies	NE	policyIdentifier: CertPolicyId (OID): 1.3.124.1104.5.32.52.4.3 policyQualifiers: • policyQualifierId za CP/CP • http://demo-pki.fina.hr/cp/cpdemo2014v1-0.pdf
Authority Information Access	NE	[1]Authority Info Access accessMethod=Online Certificate Status Protocol (OID: 1.3.6.1.5.5.7.48.1) accessLocation: URL=http://demo2014-ocsp.fina.hr [2]Authority Info Access accessMethod=Certification Authority Issuer (OID: 1.3.6.1.5.5.7.48.2) accessLocation: http://demo-pki.fina.hr/certifikati/demo2014_sub_ca.cer
CRLDistributionPoints	NE	• HTTP URL na kojem je dostupna CRL lista • Adresa CRL dostupne preko LDAP protokola • Adresa segmentirane CRL dostupne preko LDAP protokola
BasicConstraints	NE	cA=FALSE pathLenConstraint=None

Tablica 18. Podaci o certifikatu Fina Demo TSA 2014 servisa

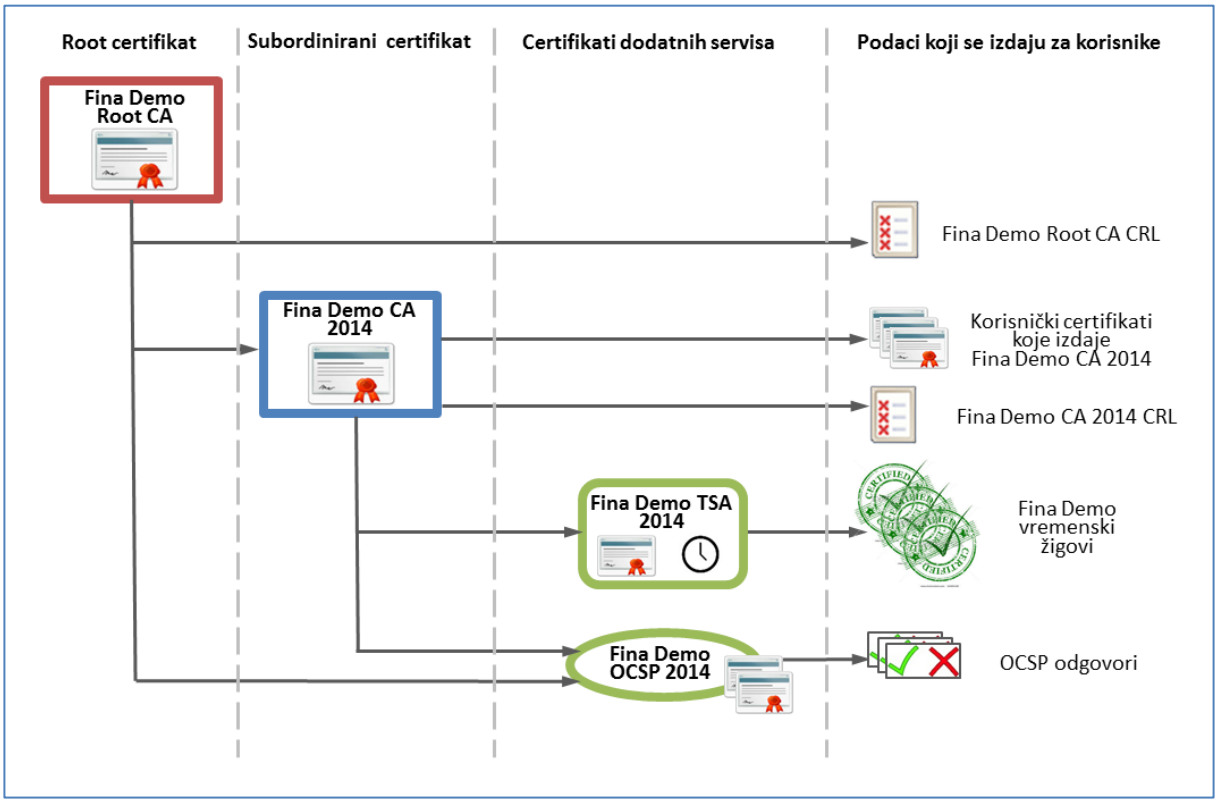
Osnovni podaci o profilu vremenskih žigova koje će izdavati Fina Demo TSA 2014 servis dani su u Tablici 19.

Polje	Vrijednost za vremenski žig kojeg izdaje Fina Demo TSA 2014 servis
Version	V1, vrijednost="1"
Policy OID	1.3.124.1104.2.32.1.1.0
messageImprint	**Podržani hash algoritmi:** • **hashAlgorithm: sha-1 (OID: 1.3.14.3.2.26) i** • **hashAlgorithm: sha-256 (OID: 2.16.840.1.101.3.4.2.1)**
serialNumber	Cijeli broj
genTime	UTC vrijeme, razlučivost od 1 sekunde
Nonce	Cijeli broj
signatureAlgorithm	**sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)**

Tablica 19. Osnovni podaci o vremenskog žigu kojeg izdaje Fina Demo TSA 2014 servis

4.2. Prikaz nove Demo okoline

Slika 4. prikazuje certifikate i servise nove dvorazinske Fina Demo 2014 okoline za izdavanje certifikata i vremenskih žigova koja je opisana u točkama 4.1.1 do 4.1.5.



Slika 4. Fina Demo 2014 okolina

5. Dodatne informacije

5.1. Važeća zakonska regulativa

U nastavku je naveden popis važeće zakonske regulative iz područja elektroničkog potpisa.

Zakonsku regulativu iz područja elektroničkog potpisa u Republike Hrvatske čine:

- Zakon o elektroničkom potpisu (NN 10/02, 80/08 i 30/14);
- Pravilnik o evidenciji davatelja usluga certificiranja u Republici Hrvatskoj (NN 107/10);
- Pravilnik o izradi elektroničkog potpisa, uporabi sredstva za izradu elektroničkog potpisa, općim i posebnim uvjetima poslovanja za davatelje usluga izdavanja vremenskog žiga i certifikata (NN 107/10 i 89/13);
- 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 89/13);
- Uredba o djelokrugu, sadržaju i nositelju poslova certificiranja elektroničkih potpisa za tijela državne uprave (NN 146/04).

Navedena zakonska regulativa usklađena je s Direktivom 1999/93/EZ-a Europskoga parlamenta i Vijeća u okviru Zajednice za elektroničke potpise.

5.2. Popis normizacijskih dokumenata i preporuka

Iz područja promjena opisanih u ovom dokumentu mjerodavni su sljedeći HRN i HRS hrvatski normizacijski dokumenti te IETF RFC preporuke:

Profil certifikata i CRL

- IETF RFC 5280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- IETF RFC 6818 – Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

Profil kvalificiranih certifikata

Pored prethodna dva dokumenta kojima se regulira profil certifikata i CRL, za profil kvalificiranih certifikata važeća su i dodatna dva dokumenta:

- 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)
- IETF RFC 3739 – Internet X.509 Public Key Infrastructure: Qualified Certificates Profile

- IETF RFC 6960 – X.509 Internet Public Key Infrastructure – Online Certificate Status Protocol - OCSP
- IETF RFC 5019 - The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments

Kriptografski algoritmi i parametri

- HRS ETSI/TS 102 176-1 V2.1.1:2012 – Elektronički potpisi i infrastrukture (ESI) – Algoritmi i parametri za sigurne elektroničke potpise – 1. dio: Hash funkcije i asimetrični algoritmi (ETSI/TS 102 176-1 V2.1.1:2011)

Profil vremenskog žiga

- HRS ETSI/TS 101 861 V1.4.1:2012 – Elektronički potpisi i infrastrukture (ESI) – Profil vremenskoga žiga (ETSI/TS 101 861 V1.4.1:2011)
- IETF RFC 3161 (2001) Internet X.509: Public Key Infrastructure: Time Stamp Protocol (TSP)

5.3. Konstrukcija i provjera lanca certifikata

Za konstrukciju i provjeru lanca certifikata, uz certifikat kojeg se provjerava nužni su i svi certifikati koji tvore lanac certifikata do *root* certifikata (*trust anchor*). Da bi se provjerila ispravnost certifikata potrebno je provjeriti ispravnost svih certifikata koji tvore taj lanac. Za ispravnu konstrukciju lanca certifikata nužna je usklađenost implementacije s preporukama IETF RFC 5280 i IETF RFC 6818.

Jedini certifikat kojeg je nužno unaprijed odrediti je *root* certifikat. Do ostalih certifikata za konstrukciju lanca moguće je doći korištenjem podatka o izdavatelju certifikata u ekstenziji *Authority Information Access*, putem niza certifikata dostupnih pri razmjeni poruka ili iz privremenog spremišta certifikata.

Preporuka je da se jedino definira *root* certifikat, na primjer fiksno, kao resurs softverskog rješenja ili na razini operacijskog sustava, odnosno programske biblioteke (ovisno o namjeni softverskog rješenja), a da se certifikati posrednih izdavatelja smatraju varijabilnim.

Prilikom implementacije može se konzultirati IETF RFC 5914.

Također, preporuka je da se prilikom razmjene poruka uključi cijeli lanac certifikata od vršnog do predmetnog certifikata (npr. potpisnog ili poslužiteljskog certifikata).

Na primjer, u SSL/TLS inicijalnoj razmjeni poslužitelj može u *Server Certificate* poruci uključiti cijeli lanac certifikata. Nadalje, XAdES standard za napredni XML elektronički potpis dozvoljava niz certifikata u *CertificateValues* elementu, i sl.

5.4. Obrada i prikaz naziva u certifikatima

Imena ili nazivi u certifikatima (npr. DN-ovi u atributima *Subject* i *Issuer*) koje izdaju Fina CA-ovi kodirani su u UTF-8 kodnoj stranici (UTF8String prema ISO/IEC 10646, IETF RFC 2279), stoga se u prikazu, odnosno manipulaciji ovih podataka (npr. operacije usporedbe ili raščlanjivanja) mora uzeti u obzir mogućnost da imena mogu sadržavati znakove izvan US-ASCII kodne stranice.

Za zapis imena koristi se X.501 *Name* (ISO/IEC 9594-2:2005) struktura koja se sastoji od niza relativnih imena (engl. R*elative Distinguished Name*, RDN), a svako relativno ime sastoji se od jednog ili više parova ime atributa - vrijednost atributa čiji poredak može biti proizvoljan.

Preporuka je da se za obradu imena u certifikatima koristi podrška operacijskog sustava ili programskih biblioteka koje imaju ugrađena sva potrebna pravila kodiranja imena i raščlambe pojedinih njihovih dijelova. Implementacija raščlambe pojedinih dijelova imena implementirana nad imenom iz certifikata kodiranom kao niz znakova može dovesti do pogrešne interpretacije imena.

Preporuka ovog dokumenta je da se ime iz certifikata kodirano kao niz znakova koristi samo u svojstvu prikaza i da se tada koristi standardna reprezentacija imena u nizu znakova definirana IETF RFC 4514.