Istek potpisnog certifikata Porezne uprave za fiskalizaciju

Srpanj 2016.

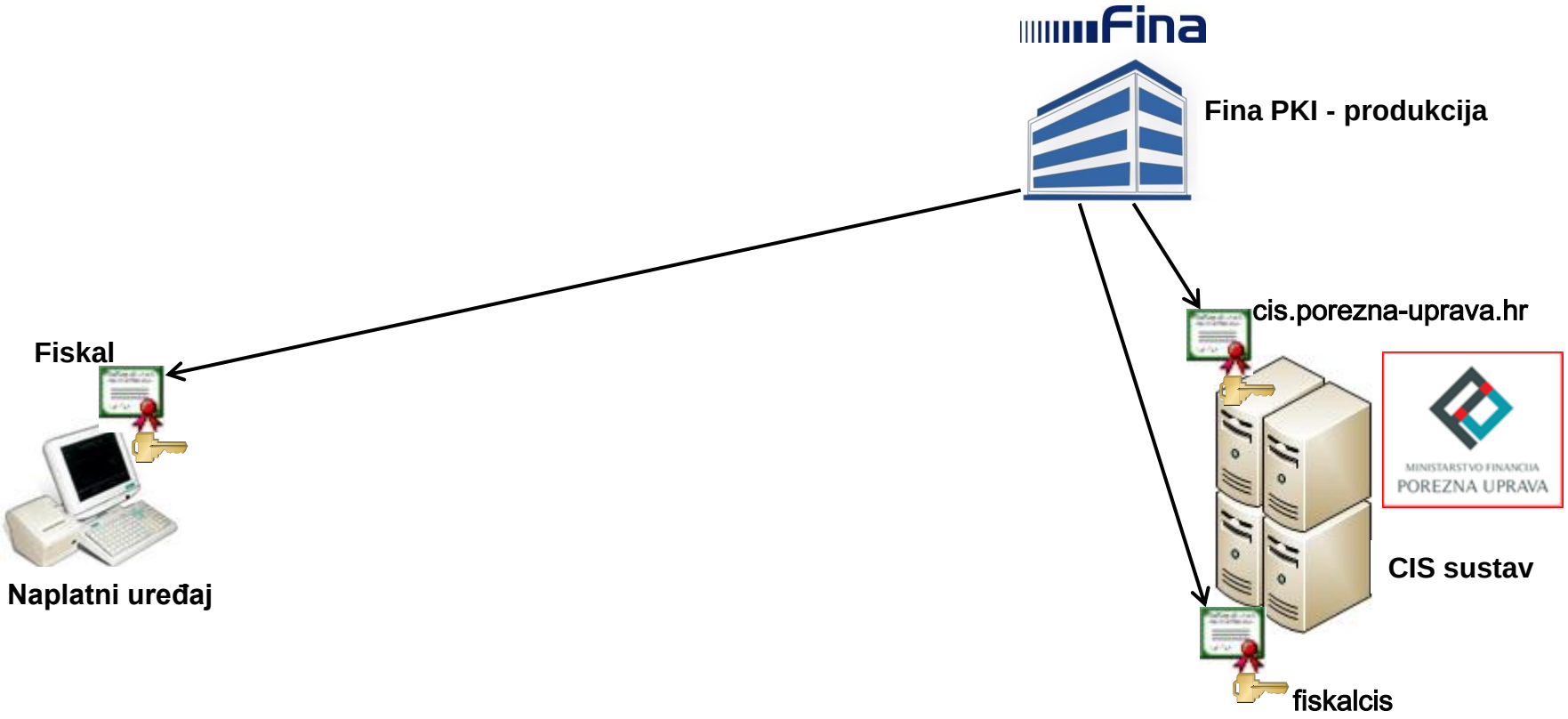
FINA kao izdavatelj certifikata i vremenskih žigova

- Djeluje sukladno Uredbi (EU) br. 910/2014 Europskog parlamenta i Vijeća o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu (eIDAS uredba) i Zakonu o elektroničkom potpisu
- Upisana u Evidenciju davatelja usluga certificiranja u Republici Hrvatskoj
- Upisana u nacionalni pouzdani popis (Trusted lista) koja je dio EU sustava pouzdanih popisa (EU Trusted lists)
- Izdavatelj kvalificiranih i nekvalificiranih certifikata od 2003. godine
- Izdavatelj naprednih vremenskih žigova
- Pod nadzorom Ministarstva gospodarstva
- Obaveza usklađivati se s aktualnim EU i međunarodnim normama iz područja izdavanja certifikata (ITU-T X.509 v3, RFC 5280, HRN ETSI EN 319 411-3, ETSI TS 119 312)

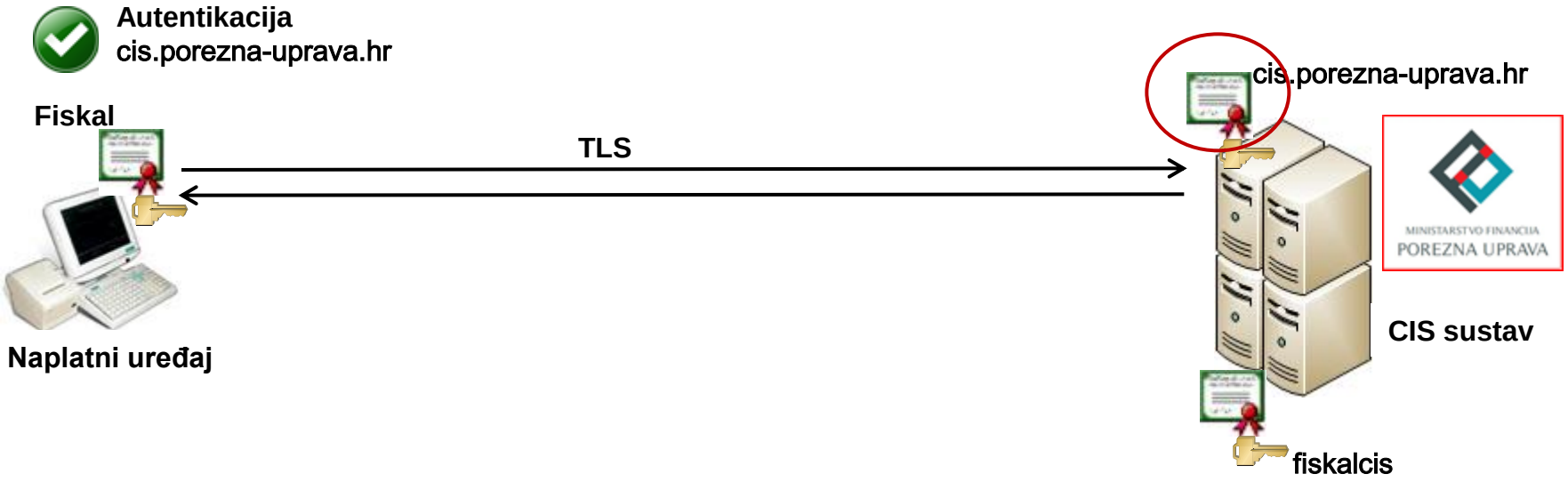
Promjene u certifikatima

- Od 7.12.2015. Fina izdaje certifikate na novim CA-ovima
- Promjene uvjetovane regulativom o elektroničkom potpisu:
  - Pravilnik o izradi elektroničkog potpisa - Ministarstvo gospodarstva
  - Obvezujuće EU norme (ETSI)
- Prijelaz s SHA-1 na SHA-256 algoritam sažetka
- Prijelaz na veće duljine CA ključeva:
  - CA-ovi: s 2048 bita RSA na 4096 bita, RSA
  - Korisnički certifikati: duljina javnih ključeva ostaje ista: 2048 bita, RSA
- Root CA ne smije izdavati korisničke certifikate, uvođenje subordiniranog CA
- Razlozi promjena: radi porasta snage računala i pronalaženja načina djelomičnog proboja SHA-1 algoritma – bilo je potrebno do 31.12.2015. prijeći na jače suvremenije algoritme.
- Prijelaz su morali obaviti svi CA-ovi koji izdaju certifikate za elektronički potpis i SSL/TLS certifikate

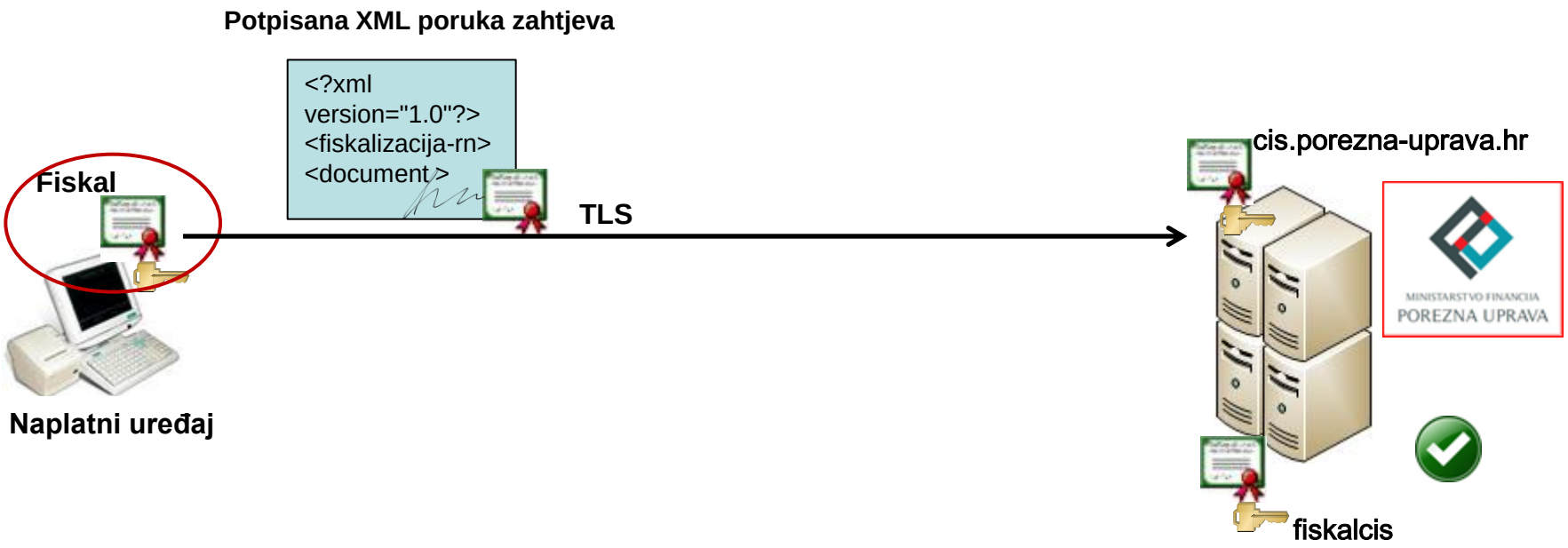
Certifikati u fiskalizaciji



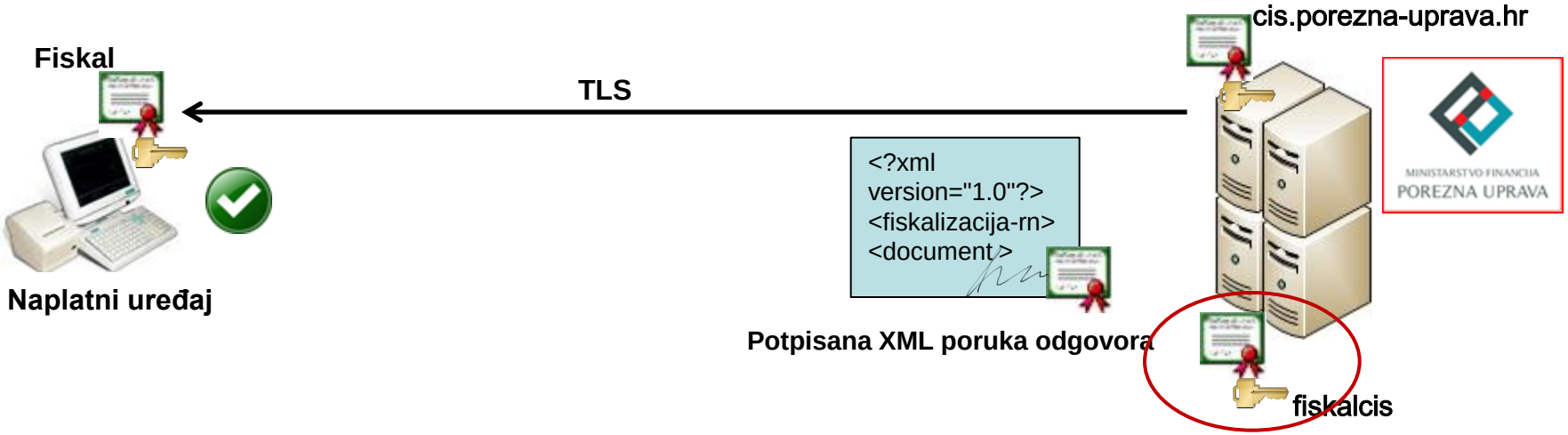
Autentikacija TLS poslužitelja



Potpisivanje poruke zahtjeva



Potpisivanje poruke odgovora



Postojeći fiskal certifikat	Budući fiskal certifikat	Obnovljeni certifikt cis.porezna-uprava.hr
FINA RDC OU=RDC, O=FINA, C=HR fiskalcis CN=fiskalcis, L=ZAGREB, OU=POREZNA UPRAVA, O=MINISTARSTVO FINANCIJA HR18683136487, C=HR	Fina Root CA CN=Fina Root CA, O=Financijska agencija, C=HR Fina RDC 2015 CN=Fina RDC 2015, O=Financijska agencija, C=HR fiskalcis CN=fiskalcis, L=ZAGREB, OU=POREZNA UPRAVA, O=MINISTARSTVO FINANCIJA HR18683136487, C=HR	Fina Root CA CN=Fina Root CA, O=Financijska agencija, C=HR Fina RDC 2015 CN=Fina RDC 2015, O=Financijska agencija, C=HR cis.porezna-uprava.hr CN=cis.porezna-uprava.hr, L=ZAGREB, O=MINISTARSTVO FINANCIJA HR18683136487, C=HR
Vrijedi od: 11. studenog 2014. 10:23:54 Vrijedi do: 11. studenog 2016. 10:53:54	Vrijedi od: ??. listopada 2016. hh:mm:ss Vrijedi do: ??. listopada 2018. hh:mm:ss	Vrijedi od: 9. lipnja 2016. 13:30:29 Vrijedi do: 9. lipnja 2018. 14:00:29
Javni ključ CA cert: 2048 bita, RSA Javni ključ fiskalcis cert: 2048 bita, RSA	Javni ključ CA cert: 4096 bita, RSA Javni ključ fiskalcis cert: 2048 bita, RSA	Javni ključ CA cert: 4096 bita, RSA Javni ključ cis.porezna-uprava.hr cert: 2048 bita, RSA
Algoritam kojim su potpisani certifikati: CA certifikat: sha1WithRSA fiskalcis cert: sha1WithRSA	Algoritam kojim su potpisani certifikati: CA certifikati: sha256WithRSA fiskalcis cert: sha256WithRSA	Algoritam kojim su potpisani certifikati: CA certifikati: sha256WithRSA cis.porezna-uprava.hr: sha256WithRSA
Info o statusu opozvanosti certifikata: CRL	Info o statusu opozvanosti certifikata: CRL i OCSP servis	Info o statusu opozvanosti certifikata: CRL i OCSP servis

Mogući problemi i rješenja

Naplatni uređaj ne podržava sha256WithRSA kriptografski algoritam te se javlja poruka o nepoznatom algoritmu.

Rješenje:

Postojeći “fiskslcis” certifikat potpisan je od strane FINA RDC CA korištenjem sha1WithRSA algoritma, a obnovljeni “fiskalcis” biti će potpisan novijim sha256WithRSA algoritmom. Također, Fina RDC 2015 i Fina Root CA potpisani su istim sha256WithRSA algoritmom. Softver naplatnog uređaja potrebno je ažurirati kako bi prepoznao sha256WithRSA algoritam i ispravno provjerio potpise u certifikatima.

Mogući problemi i rješenja

Fiskalni uređaj ne ostvaruje povjerenje u obnovljeni „fiskalcis” certifikat. Javlja se poruka o nepovjerenju u CA (Certification Authority).

Rješenje:

Postojeći „fiskalcis” certifikat izdao je FINA RDC CA koji je ujedno i root CA. Obnovljeni „fiskalcis” certifikat izdat će Fina RDC 2015 CA, a certifikat za Fina RDC 2015 CA već je izdao je Fina Root CA. Potrebno je ostvariti povjerenje u Fina Root CA, npr. importiranjem Fina Root CA u trusted store ili na sličan način, ovisno o softveru. Po potrebi, treba importirati i Fina RDC 2015 CA certifikat.

Mogući problemi i rješenja

U nekim je naplatnim uređajima postojeći certifikat „fiskalcis” fiksno pohranjen. Kad Porezna uprava započne potpisivanja obnovljenim „fiskalcis” certifikatom verifikacija e-potpisa odgovora će javljati grešku.

Rješenje:

Ako naplatni uređaj ima fiksno pohranjen „fiskalcis” certifikat, neposredno prije prelaska Porezne uprave na potpisivanje obnovljenim „fiskalcis” certifikatom potrebno je postojeći „fiskalcis” certifikat zamijeniti s obnovljenim „fiskalcis” certifikatom kojeg je Porezna uprava objavila na svojim web stranicama. Također potrebno je ostvariti povjerenje u Fina Root CA.

Alternativno, programsko rješenje se može modificirati tako da aktualni „fiskalcis” certifikat uvijek uzima iz e-potpisa odgovora Porezne uprave kojeg provjerava jer „fiskalcis” certifikat uvijek sadržan u e-potpisu odgovora.

Dodatne informacije

- http://www.fina.hr/fiskalizacija
  - Informatičke tvrtke
  - Obveznici fiskalizacije
- http://www.fina.hr/finadigicert
  - Fina PKI sustav
  - Regulativa i dokumenti
    - Pravilnik o postupcima certificiranja za nekvalificirane certifikate, ver. 5.0 od 7.12.2015.
  - CA certifikati
    - Preuzimanje Fina Root CA

      (SHA1: 62:02:bf:16:9a:f2:7f:a6:7e:d0:ce:c6:6b:78:2b:83:22:61:26:e9)
    - Fina RDC 2015

      (SHA1: d8:86:43:90:c7:6c:9b:71:f0:40:4f:f3:76:fc:38:fd:73:78:7d:08)
  - E-mail: certifikati-fiskalizacija@fina.hr