Primenjena kriptografija

...podsetnik

- Na čemu se zasniva tajnost simetričnih / asimetričnih algoritama?
- Šta je predstavljalo najveći problem u komunikaciji između Alice i Boba?
- Kako da budemo sigurni da prilikom slanja poruke koristimo *baš* javni ključ one osobe kojoj je poruka namenjena?

Man-in-the-middle napad

Prvi korak pri uspostavljanju sigurne komunikacije -> razmena ključeva

Problem: Man-in-the-middle napad

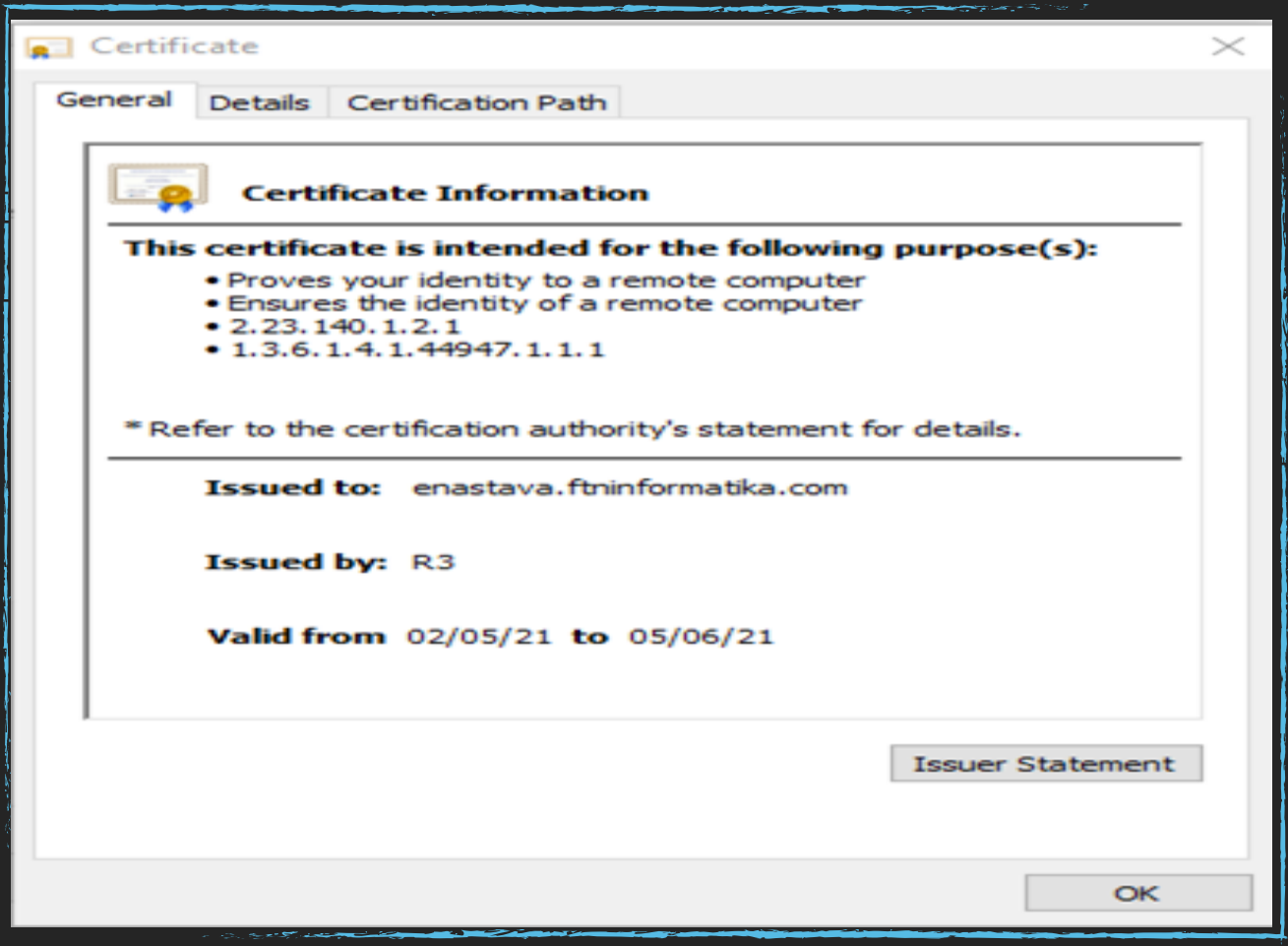
Rešenje: Infrastruktura javnih ključeva

- Infrastruktura javnih ključeva (engl. *Public key infrastructure*; *PKI*) predstavlja sistem koji vezuje javne ključeve za identitete subjekata kojim pripadaju
- PKI koristi kriptografske primitive kako bi kreirali, upravljali, distribuirali, koristili, skladištili i opozivali digitalne sertifikate

Šta je to digitalni sertifikat?

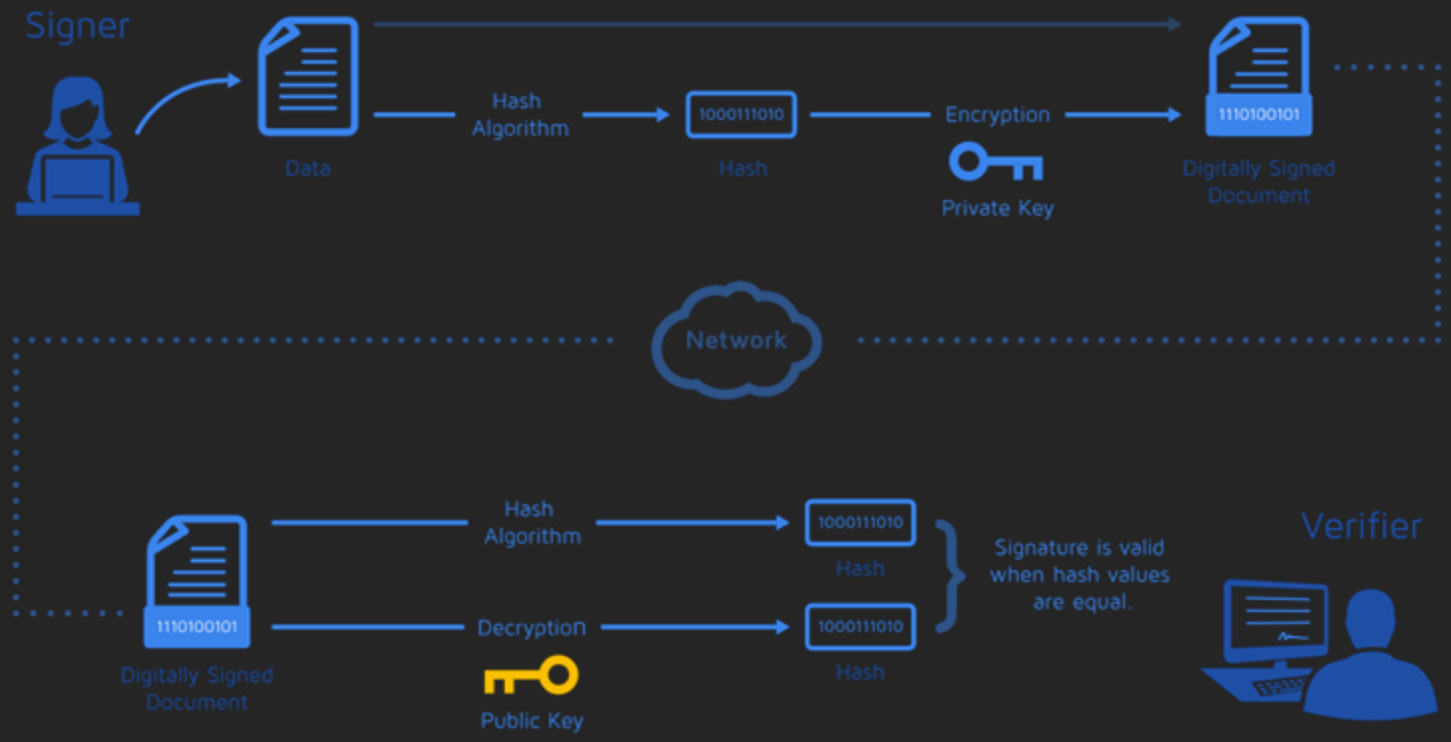
- Elektronski dokument koji sadrži sledeće podatke:
  - Ko je izdao sertifikat (issuer)
  - Kome je sertifikat izdat (subject)
  - Kada je sertifikat izdat
  - Do kada je sertifikat validan
  - Javni ključ povezan sa sertifikatom i identitetom kom je sertifikat izdat
  - Digitalni potpis formiran od strane izdavaoca sertifikata
  - Dodatne informacije (ekstenzije)

Primer digitalnog sertifikata



Digitalni potpis

- obezbeđuje potvrdu identiteta i integrtitet informacije koja je potpisana



Provera validnosti sertifikata

- sertifikati poznatih sertifikacionih tela interneta dolaze ugrađeni u operativni sistem, ili sam veb-čitač
- Ako se ode na domen sa sertifikatom u čijem lancu se nalazi poznato sertifikaciono telo, smatra se da se može verovati sertifikatu
- Kada je sertifikat neispravan?
- Nevalidan vs. povučen sertifikat?
- Tehnike za proveru povučenosti: CRL, OCSP

OCSP zahtev

1. Alisa i Bob imaju sertifikat izdat od strane Ivana, koji predstavlja sertifikaciono telo;
2. Alisa želi da komunicira sa Bobom, i šalje mu svoj sertifikat;
3. Bob šalje OCSP zahtev koji uključuje serijski broj Alisinog sertifikata, kako bi bio siguran da sertifikat nije povučen;

OCSP zahtev

4. Ivan proverava svoju bazu podataka i gleda koji je status sertifikata sa datim serijskim brojem. Pronalazi da je sertifikat validan i da nije povučen;
5. Bob dobija odgovor, potpisan od strane Ivana, koji tvrdi da je Alisin sertifikat ispravan;
6. Bob, koji ima uskladišten Ivanov sertifikat, proverava digitalan potpis i uspostavlja komunikaciju sa Alisom.

...vraćamo se na Alice i Boba

- Problem razmene ključeva je rešen pomoću sertifikata
- Utvrdili smo da su sertifikati validni
- Razmena poruka može da počne

- Kako će običan korisnik da ostvari bezbednu komunikaciju preko interneta, ako ne poseduje sertifikat?
- Priču svodimo na komunikaciju web browser - server

Generisanje sertifikata

- Keytool alat – dolazi zajedno sa instalacijom JDK-a

- Komanda za generisanje sertifikata

```
keytool -genkeypair -keyalg RSA -alias root
-keystore root.jks -storepass password -validity 360 -
keysize 2048
```

- Izvoz sertifikata u .cer format

```
keytool -export -keystore root.jks -alias root -file
root.cer
```

- Provera sadržaja izgenerisanog *keystore* fajla:

```
keytool -list -keystore keystore.jks -storepass password
```

OpenSSL

- OpenSSL nudi grupu alata otvorenog koda za kriptografiju i bezbednu komunikaciju
- Koristi se izvršavanjem komandi kroz terminal
- Generisanje privatnog ključa

  openssl genrsa -out root.key 4096
- Generisanje samopotpisanog sertifikata

  openssl req -x509 -new -key root.key -sha256 -days 1024 -out rootCA.pem
- Provera sertifikata

  openssl x509 -in rootCA.pem -text -noout

ILI

openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -sha256 -days 365

Zadaci

1. Izgenerisati CA korenski sertifikat
2. Izgenerisati sertifikat za korisnika, potpisan od strane prethodno izgenerisanog CA korenskog sertifikata

1. Obratiti pažnju na:
   - trajanje sertifikata
   - namenu sertifikata
   - algoritam za generisanje ključeva i digitalno potpisivanje