Varnostni certifikati, šifriranje, elektronski podpis

Priprava varnostnih certifikatov s programom openssl

1. naredimo naslednjo strukturo direktorijev:

```
ssldemo
   demoCA
      private
      newcerts
```

2. Direktorij ssldemo zaščitimo pred ostalimi; chmod 700 ssldemo. Od tu naprej delamo v direktoriju ssldemo

   V direktoriju demoCA naredimo datoteko z imenom `serial`. V njej je serijska številka naslednjega osebnega certifikata, ki ga bomo naredili. Ta številka se avtomatsko povečuje tako, da vsak certifikat dobi svojo serijsko številko. Za začetek v datoteko `serial` vpišemo npr. 1000.

3. V direktoriju demoCA naredimo prazno (dolžina 0 bajtov) datoteko `index.txt`. V njej bodo podatki o izdanih osebnih certifikatih in njihovih serijskih številkah.

CERTIFIKATNA AGENCIJA:
Najprej je potrebno narediti certifikatno agencijo; torej certifikat (javni ključ) in zasebni ključ certifikatne agencije. Zasebni ključ je potrebno skrbno paziti; če ga kdo ukrade, bo lahko izdajal certifikate v našem imenu!!! Certifikat damo našim uporabnikom; ti ga namestijo med zaupanja vredne certifikatne agencije (trusted root certificate authorities).

1. v direktoriju `ssldemo` naredimo:

```
openssl req -new -x509 -extensions v3_ca -keyout
demoCA/private/cakey.pem -out demoCA/cacert.pem -days 365
```

   vpisati moramo:
   geslo za uporabo zasebnega ključa: vso123;to geslo moramo poznati, ko bomo podpisovali osebne certifikate
   kodo države: SI
   ime države: Slovenija
   mesto: Velenje
   ime podjetja: SCV
   ime enote podjetja: VSS
   poljubno ime: Vaje VSO
   elektronski naslov: (pustimo prazno)

dobimo:

`demoCA/private/cakey.pem`: zasebni ključ certifikatne agencije
`demoCA/cacert.pem`:
javni ključ certifikatne agencije; v resnici je to že certifikat, torej
javni ključ skupaj z vnesenimi podatki o certifikatni agenciji. Certifikat smo podpisali sami (selfsigned certificate)...

javni ključ bomo dali našim uporabnikom, ker je v resnici certifikat, mu končnico spremenimo v .cer. Certifikat (in oba ključa) je veljaven 365 dni.

2. `cp demoCA/cacert.pem demoCA/cacert.cer` (obdržimo tudi datoteko s končnico .pem)

OSEBNI CERTIFIKATI:
Naredimo zasebni ključ uporabnika in zahtevo za podpis javnega ključa. Javne ključe uporabnikov mora podpisati certifikatna agencija (to bomo naredili z zasebnim ključem `cakey.pem`); v splošnem je certifikatna agencija podjetje, ki s svojim elektronskim podpisom jamči, da javni ključ res pripada osebi, navedeni v certifikatu.

v direktoriju `ssldemo` naredimo:

```
openssl req -new -out novak-req.pem -keyout
demoCA/private/novak-key.pem -days 365
```

vnesti moramo podatke o Novaku:
geslo za uporabo zasebnega ključa: novak123
kodo države: **SI**
ime države: **Slovenija**
mesto: **Velenje**
ime podjetja: **SCV**
ime enote podjetja: VSS
ime uporabnika: Janez Novak
elektronski naslov: (**obvezno**, če bo uporabnik s tem certifikatom podpisoval e-pošto: **poukXX@vaje.vso.tld**)

Poudarjeni podatki se morajo ujemati s podatki certifikatne agencije!!!

Dobimo zahtevo za podpis javnega ključa: `novak-req.pem`
in zasebni ključ: `demoCA/private/novak-key.pem`

Veljavnost je zopet 365 dni. Sedaj je potrebno podpisati zahtevo z zasebnim ključem certifikatne agencije:

```
openssl ca -out novak-cert.pem -days 365 -infiles novak-req.pem
```

Poznati moramo geslo za uporabo zasebnega ključa certifikatne agencije: vso123

Dobimo s strani certifikatne agencije podpisan osebni certifikat: `novak-cer.pem`

uporabniku damo njegov zasebni ključ in certifikat v formatu `.p12`, ki ga uporabljajo brskalniki in programi za e-pošto. Naredimo:

```
openssl pkcs12 -export -in novak-cert.pem -inkey
demoCA/private/novak-key.pem -certfile demoCA/cacert.pem -name
"Novakov certifikat" -out novak-cert.p12
```

Poznati moramo geslo za uporabo uporabnikovega zasebnega ključa: novak123. Po potrebi vnesemo še geslo za nameščanje certifikatov...

`novak-cert.p12` moramo na nek varen način dati uporabniku; najbolj varno je seveda osebno. Običajno podjetja to naredijo z uporabo več gesel, npr. eno pošljejo po navadni in drugo po elektronski posti, pri prenosu certifikata pa uporabijo ssl...

Za uvoz samo javnega ključa v Outlook in še nekatere druge odjemalce e-pošte moramo certifikat pretvoriti v format DER:

```
openssl crl2pkcs7 -nocrl -certfile novak-cert.pem -outform DER
-out novak-cert.p7c
```

`novak-cert.p7c` nato uporabnik Novak pošlje ljudem, s katerimi želi izmenjevati šifrirano ali digitalno podpisano e-pošto.

Obnašanje openssl (privzeto je npr. da se morajo oznaka in ime države in organizacije certifikatne agencije ujemati s certifikati uporabnikov...) je določeno s konfiguracijsko datoteko `/etc/ssl/openssl.cnf`. Če želimo, lahko openssl konfiguriramo po svoje.

- v direktoriju demoCA/private imamo zasebne ključe uporabnikov (in tudi certifikatne agencije)
- v intex.txt je seznam certifikatov, ki smo jih podpisali z zasebnim ključem certifikatne agencije
- v direktoriju demoCA/newcerts so certifikati (javni ključi) uporabnikov (po serijskih številkah)

PREIZKUS CERTIFIKATA Z ODJEMALCEM ZA E-POŠTO

EVOLUCIJA (EVOLUTION)

1. Poženemo Evolucijo

   Klik na pismo na pultu.

2. Najprej je potrebno konfigurirati poštni račun.

   Uredi -> Možnosti -> Poštni računi

   vnesemo: ime računa (janez@vaje.vso.tld), polno ime (Janez Novak) in e-naslov (poukXX@vaje.vso.tld)
   kliknemo še na Server Settings a in vpišemo podatke: Ime strežnika (192.168.1.???) in uporabniško ime (poukXX).

3. Konfiguriramo še nastavitve strežnika za odhodno pošto:
   Ime strežnika (192.168.1.???)
   vpišemo Uporabniško ime: poukXX

Zapremo okno z nastavitvami (klik na OK).

4. Preizkusimo delovanje poštnega računa tako, da pošljemo sporočilo sami sebi. (Sestavi, vpišemo podatke, pošlji).

5. Namestimo certifikate. Najprej certifikat (javni ključ) certifikatne agencije:

   Uredi -> Možnosti.
   Kliknemo Potrdila
   Kliknemo Overitelji
   Uvozi
   Izberemo certifikat certifikatne agencije (ssldemo/demoCA/cacert.pem)

   Odkljukati je potrebno vsaj *Zaupaj tej CA za ugotovitev istovetnosti uporabnikov elektronske pošte*. Sedaj Evolucija zaupa certifikatom, ki so podpisani s strani naše certifikatne agencije. Med nameščenimi certifikati vidimo 'znana imena' kot so Verisign, AOL, VISA,... To so komercialne certifikatne agencije; če nam certifikate podpisuje komercialna certifikatna agencija, vsi koraki do tu odpadejo, ker je certifikat certifikatne agencije v tem primeru že nameščen...

6. Namestimo še certifikat in zasebni ključ uporabnika Novaka z elektronskim naslovom poukXX@vaje.vso.tld

   Izberemo zavihek Vaša potrdila
   Uvozi

Izberemo ustrezen certifikat v formatu .p12 (PKCS12)
Vnesemo geslo za shrambo certifikatov (vso.vaje) in geslo za nameščanje certifikatov (če ste ga vnesli, sicer prazno)
Izberemo poštni računi in uredimo račun Janeza Novaka
V zavihku varnost izberemo certifikat za elektronsko podpisovanje in šifriranje s S/MIME

7. Poskusimo poslati šifrirano sporočilo sami sebi:
   Nov, vpišemo naslov...,
   Kliknemo Možnosti, izberemo Šifriraj s S/MIME...
   Pošlji

8. Pošljite si še elektronsko podpisano sporočilo.

Razumevanje snovi - odgovorite na naslednja vprašanja:

a) kaj mora imeti oseba, da **vam** lahko pošilja šifrirano pošto?

b) kaj je certifikatna avtoriteta?

c) naštej tri certifikatne avtoritete, ki imajo na vašem računalniku nameščen svoj certifikat.

d) zakaj se pri šifrirani e-pošti uporablja certifikat certifikatne avtoritete.

e) kdo lahko preveri vaš elektronski podpis v e-sporočilu?

f) kakšna je razlika med certifikatom in javnim ključem?

g) kdo podpiše certifikat certifikatne avtoritete?