http://www.cyber.ee/turve/info/smail/

Sertifitseerimine

Sertifitseerimine on tegevus, mille käigus kolmas, usaldatav osapool (**sertifitseerimiskeskus**), tõendab oma digitaalsignatuuriga avaliku võtme kuulumist teatud kasutajale.

Andmestruktuuri, mis seob kasutaja nime, avaliku võtme ning muud sertifitseerimise juures olulised atribuudid ning mis on kinnitatud sertifitseerimiskeskuse digitaalsignatuuriga, nimetatakse **sertifikaadiks**.

Sertifikaadis toodud andmete õigsust on võimalik kontrollida sertifitseerimiskeskuse avaliku võtme abil, mida levitatakse süsteemiväliste vahenditega.

Sertifikaadi vorming

X.509 sertifikaadivorming:

- sertifikaadi keha
  - versiooni number
  - sertifikaadi number antud sertifitseerimiskeskuses
  - sertifitseerimiskeskuse nimi
  - omaniku eraldusnimi
  - omaniku avalik võti
  - kehtivusaeg
- sertifitseerimiskeskuse signatuur

Omaniku avalik võti koosneb kahest osast - algoritmi identifikaatorist ja tegelikust võtmest. See teeb X.509 poolt kirjeldatava vormingu paindlikuks, võimaldades väljastada sertifikaate eri algoritmide avalike võtmete kohta.

Kehtivusaegade range jälgimine ei kaitse signatuuri loomise kuupäevaga teostatavate manipulatsioonide eest, kuid aitab vältida aegunud sertifikaatide kasutamist.

Signatuur on sertifitseerimiskeskuse salajase võtmega krüpteeritud sõnumilühend, mis moodustatakse DER-kujul kodeeritud sertifikaadi kehast.

DER-kuju: sertifikaadis sisalduvaid andmeid kujutatakse kindlal, arvuti arhitektuurist sõltumatul viisil, mis tagab täpselt sama sõnumilühendi kõigi arvutitüüpide korral.

Sertifikaadi autentsuse kontrolli käigus:

- kodeeritakse sertifikaadi keha DER-kujule
- leitakse DER-kuju sõnumilühend (*digest)*
- võrreldakse seda signatuuris sisaldunud sõnumilühendiga, mis saadakse signatuuri dekrüpteerimisel sertifitseerimiskeskuse avaliku võtme abil.

Eraldusnimed

Eraldusnimede puhul tagatakse ühesus hierarhilise nimeskeemi kasutamisega. Näiteks neljatasemeline nimi

C=EE, O=IOC, OU=IT, CN=Riho Leevike

annab teada, et isik on Eesti Vabariigis asuva organisatsiooni (C=EE), millenimi on IOC, (O=IOC), IT nimelise allüksuse (OU=IT) töötaja, kelle pärisnimi on Riho Leevike (CN=Riho Leevike).

Eraldusnimede moodustamisel võib kasutada järgmisi atribuute:

C - Maa kood standardi ISO 3166 järgi. Eesti on näiteks EE
S - Osariigi, maakonna või provintsi nimi
L - Asukoha nimi (näiteks linna või asula nimi)
ST - Tänava nimi ja majanumber

O - Organisatsiooni nimi
OU - Allüksuse nimi
T - Tiitel (ametinimi)

CN - Üldkasutusnimi (nimi, mille all subjekti üldiselt tuntakse)
SN - Perekonnanimi
PA - Postiaadress

Autentimine sertifikaadi kasutamisega

SSA sidekanali loomine

[5] Kliendi salajane võti
[6] Kliendi sertifikaat
[7] Sertifitseerimiskeskuse avalik võti
[8] Serveri salajane võti
[9] Serveri sertifikaat
[10] Seanssi loomise shiffer

1. Klient shifreerib [10] abil oma sertifikaadi ja nime ning saadab serverile

2. Server kontrollib kliendi sertifikaadi autentsust:

    - deshifreerib [10] abil kliendi sertifikaadi ja nime
    - moodustab sertifikaadi DER-kuju ja [7] abil signatuuri, mida võrdleb sertifikaadis oleva signatuuriga
    - võtab sertifikaadist kliendi avaliku võtme
    - saadab kliendile oma sertifikaadi ja oma nime, mis on krüpteeritud [10] abil

3. Klient kontrollib serveri sertifikaadi autentsust