PKI - Public Key Infrastructure

Is een verzameling van
- toepassingen
- beleidslijnen
- praktijken
- standaarden
- wetten

die vertrekken vanuit publieke-sleuteltechnologie

Doel:
- beheer van certificaten
- sterke authenticatie

Authenticatie: zwak ← → sterk

Zwakke authenticatie
- identiteitscontrole d.m.v.
  - gebruikersnaam
  - wachtwoord

Sterke authenticatie
- identiteitscontrole d.m.v.
  - iets wat men bezit (*token*)
    - digipass, smartcard, usb-stick, biometrisch gegeven, ...
  - iets wat men weet
    - wachtwoord, pincode
- token met zorg uitgedeeld
- verantwoordelijkheid van bezitter van token

PKI - definitie-elementen

Toepassingen:

browsers, mailclients, webservers, mailservers, …

Standaarden:

LDAP, S/MIME, X.509, IPSec, SSL, PKCS#11, …

zorgen voor interoperabiliteit

Beleidslijnen, praktijken

wat is de waarde van een certificaat?

richtlijnen voor gebruik van bv. smartcard

Wetten

verzekeren de rechtsgeldigheid

PKI functies

Hoofdfuncties

- Certificatie: verbinden van de identiteit aan een publieke sleutel (via certificaat)
- Verificatie en validatie: informeren over de geldigheid van certificaten
  - via de *zwarte* lijst: CRL (revocatielijst)
  - via verificatieserves (OCSP)

Andere

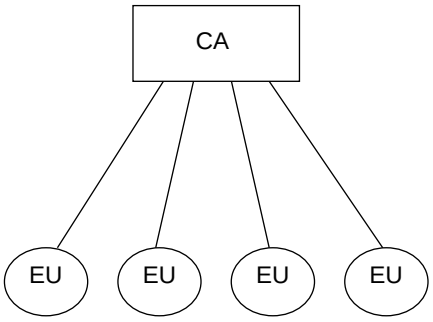
- Publicatie: beschikbaar stellen van certificaten en CRL's via LDAPservers
- Registratie: van gebruikers

PKI Root CA: vertrouwensbron

- probleem van de kip en het ei: wat eerst?
- **Elke** PKI vertrekt van 1 vertrouwde instantie, d.i. de **Root-CA** (certificatieautoriteit)
  - beschikt over een zelf-getekend certificaat
  - certificeert sub-CA's en RA's (registratieautoriteit)
- **Bescherming** van de private sleutel van CA:
  - controle van fysieke toegang
  - opslag van sleutel in cryptografisch bord
  - sleutel niet zichtbaar in geheugen (*tamper detection*)
  - 4-ogen principe

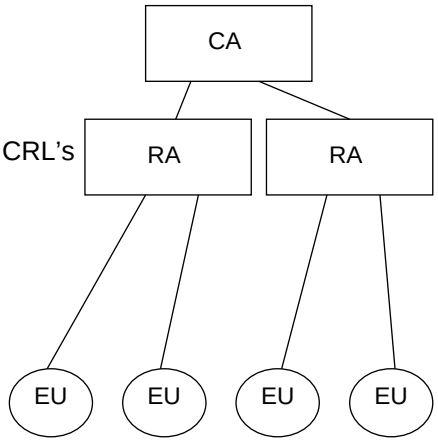
PKI eerste generatie

- CA verricht alle activiteiten
  - registratie van de gebruiker
  - maken van certificaten
  - herroepen van certificaten
- volledige centralisatie
- 1 beleid
- basisfunctionaliteit
- geen flexibiliteit



PKI tweede generatie

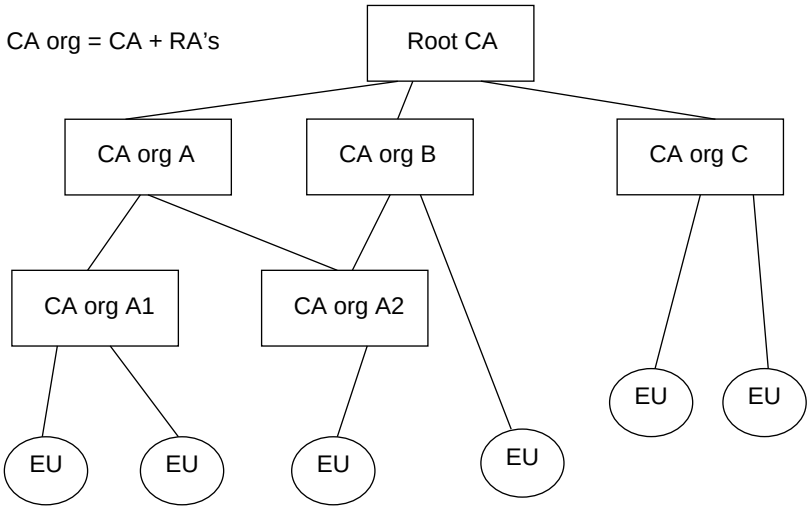
- **CA** verantwoordelijk voor
  - tekenen certificaten
  - revocatie en tekenen CRL's
  - publicatie van certificaten en CRL's
- **RA** (registratie autoriteit) is verantwoordelijk voor
  - identificatie
  - registratie
  - revocatieverzoeken
- 1 beleid voor CA en RA's



Kerberos - X509 - PKI 57

PKI huidige generatie

CA org = CA + RA's



Kerberos - X509 - PKI 58

Een certificaat verkrijgen (vb)

1. gebruiker vraagt ID aan RA
2. RA initieert aanvraag bij CA
3. CA beantwoordt aanvraag naar RA
4. RA stuurt sleutelinformatie naar gebruiker
5. gebruiker genereert RSA-sleutelpaar (smartcard)
6. gebruiker vraagt certificaat bij CA
7. CA genereert certificaat en plaatst in directory
8. CA stuurt certificaat naar gebruiker, certificaat wordt opgeslagen in smartcard

Smartcard

- soort bankkaart met chip (cfr proton, EID-kaart)
- bevat volgende info
  - private sleutel van gebruiker (niet te lezen !)
  - publieke sleutel van CA
  - algoritme voor sleutelgeneratie
  - PIN-code (ter beveiliging van smartcard)
  - algoritme voor handtekening
  - certificaat (1 of meerdere)
- gebruikt voor *sterke* authenticatie

Andere tokens

- USB-tokens
  - cfr smartcard-technologie
- Synchrone tokens
  - bevatten klok; genereren op gepaste tijden wachtwoord dat dan door gebruiker wordt ingegeven
- Asynchrone tokens (digipass)
  - beveiligd met PIN
  - genereert eenmalig wachtwoord op basis van opgegeven seed
- Biometrie:
  - smartpen (beeldherkenning en druksensor, handschrift)
  - vingerafdruk (camera, opto-elektrische sensor, capacitief)
  - ogenscanners
  - gezichtherkenning via camera
  - stemherkenning

PKI en beveiligingsservices

	geen cryptografie
Authenticatie	- login met gebruikersnaam en wachtwoord - **fysische** bank**kaart**, digipass - biometrie
Confidentialiteit & Integriteit	- **beleid and procedures** - **aanvaardbare waarden** van bepaalde velden - message authentication codes
Non-repudiation	- **logs** van het audit-systeem - one-time ticket

PKI en beveiligingsservices (2)

	Cryptografie zonder PKI (zonder certificaten)
Authenticatie	-"challenge response“ gebruik makend van **gekende publieke sleutel** - digital ticket (Kerberos)
Confidentialiteit & Integriteit	- **encryptie** van data met symmetrische sleutel - **encryptie** geheime sleutel met publieke sleutel & contoleer digitale handtekening met **gekende publieke sleutel**
Non-repudiation	contoleer digitale handtekening met **gekende publieke sleutel**

PKI en beveiligingsservices (3)

	Weinig PKI (server certificaten)
Authenticatie	**gebruik publieke sleutel** van certificaat van identiteit om "challenge response" authenticatie mogelijk te maken
Confidentialiteit & Integriteit	**gebruik publieke sleutel** van anoniem certificaat om geëncrypteerde communicatie mogelijk te maken & **gebruik publieke sleutel** om digitale handtekening op document te verifiëren
Non-repudiation	**gebruik publieke sleutel** om digitale handtekening op document te verifiëren

PKI en beveiligingsservices (4)

	Veel PKI (client certificaten)
Authenticatie	valideer identiteit m.b.v. **certificaat**
Confidentialiteit & Integriteit	valideer encryptie m.b.v. **certificaat** valideer anonieme handtekening m.b.v. **certificaat**
Non-repudiation	valideer handtekening m.b.v. **certificaat** voor elke digitale handtekening vereist in de transactie, incl. • digital time stamp • legalisatie • document ontvangstbewijs