Curs 9
PKI & TLS

Gestiunea serviciilor de rețea (GSR)
8 decembrie 2016

Departamentul de Calculatoare, Comunitatea RLUG

Cuprins

PKI - Introducere

- PKI (Public Key Infrastructure) este utilizat pentru validarea certificatelor digitale.
- Principalele cazuri de utilizare sunt validarea identității și integrității mesjelor trimise între două entități.
- PKI permite maparea sigură între cheia publică a unei entități și identitatea acele entități.
- PKI se bazează pe un lanț de încredere pentru validarea cheilor.

- `Root CA`
  - Cea mai "înaltă" autoritate în ierarhia PKI
  - Nu emite certificate digitale pentru clienți
  - Se ține "offline"
- `Subordinate CA` sau `Issuing CA`
  - Are cheia publică semnată de către `Root CA`
  - Poate emite certificate digitale pentru clienți
  - Poate semna certificate digitale pentru alte CA-uri subordonate
  - Numit câteodată și `Intermediate CA`

PKI - Definiții (2)

- `CSR` sau "Certificate Signing Request"
  - Reprezintă informațiile trimise de client către un `CA` pentru emiterea unui certificat
  - Conține cheia publică a certificatului ce urmează a fi emis
  - În afară de câmpul `CN`, `CA`-ul poate modifica orice alt câmp din `CSR`, în funcție de politica acestuia
- `RA` sau "Registration Authority"
  - Rolul unui RA este de a verifica corectitudinea și validitatea datelor din CSR

PKI - Definiții (3)

- `CRL` sau "Certificate Revocation List"
  - Conține lista cu toate certificatele revocate de către un `CA`
  - Se publică la intervale prestabilite de timp (1-2 săptămâni)
  - Lista este folosita de clienți pentru a verifica dacă un certificat este revocat sau nu
  - Pentru că un `CRL` poate ajunge la dimensiuni foarte mari, un `CA` poate emite și `Delta CRL` la intervale de timp mai scurte
- `OCSP` sau "Online Certificate Status Protocol"
  - Permite verificarea în timp real a stării unui certificat digital
  - În funcție de implementarea CA-ului se poata uita direct în baza de date cu certificate sau poate răspunde din CRL

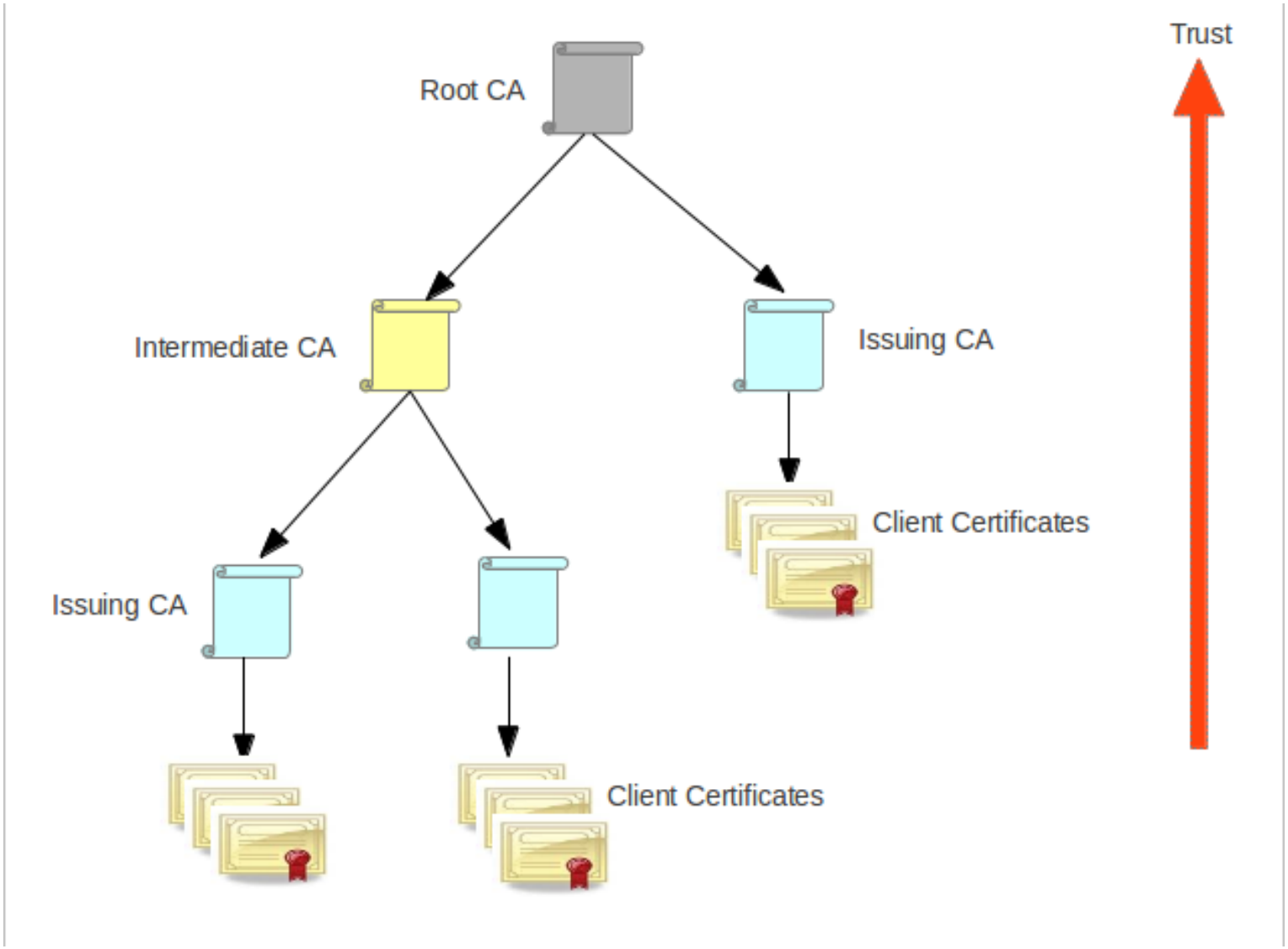
PKI - Definiții (4)

- `X.509`
  - Standardul pe care se bazează ierarhia de certificate digitale (foarte asemănător cu LDAP)
    - Exemplu certificat CA emitent
      `/C=US/O=Google Inc/CN=Google Internet Authority G2`
    - Exemplu certificat client
      `subject=/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com`

PKI - Definiții(5)

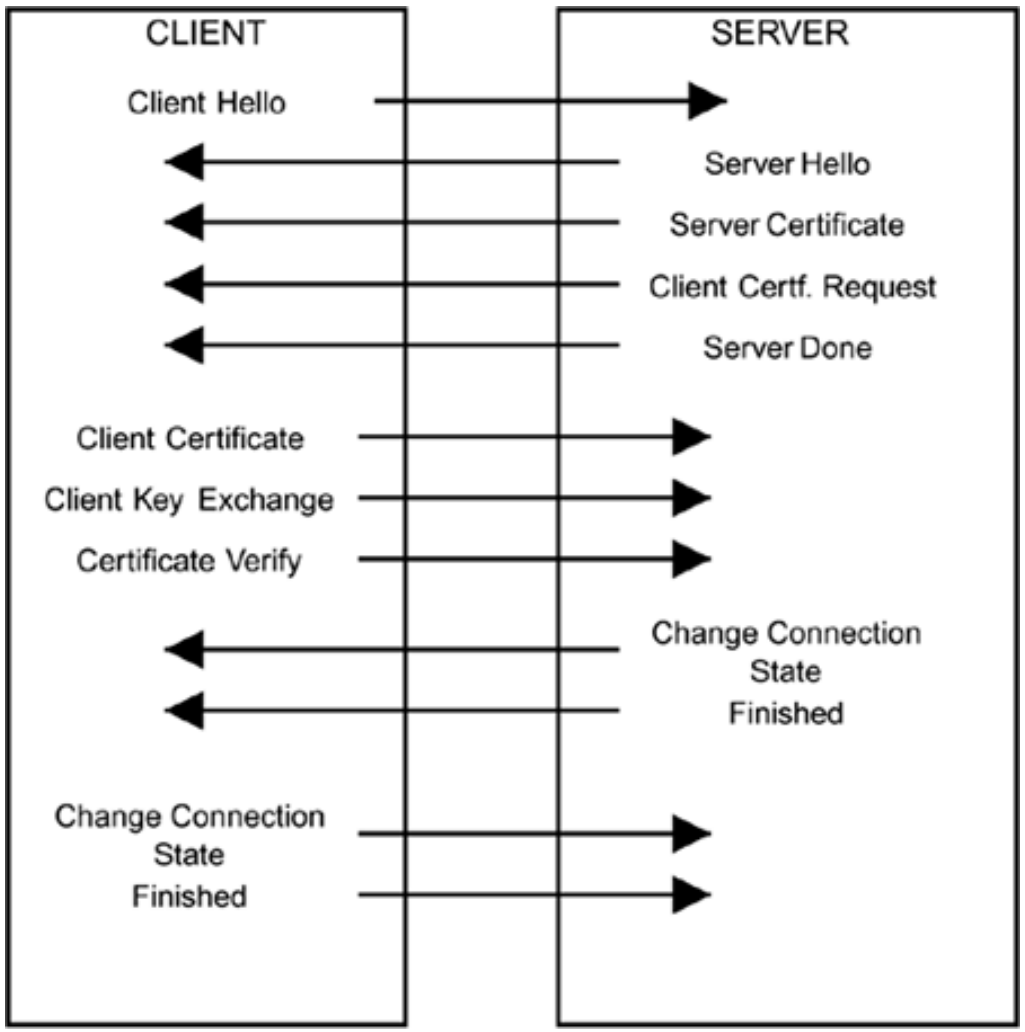
- Extensii ale certificatelor
  - `Key Usage`
    - `Digital Signature`
    - `Key Encypherment`
  - `Extended Key Usage`
    - `Server Authentication`
    - `Client Authentication`
  - `Subject Alternative Name`
    - `DNS`
    - `IP`
  - `CRL Distribution Points`
    - `URI`

Chain of Trust



Cuprins

- TLS se bazează pe certificate digitale pentru a securiza și autentifica traficul între două entități
  - `Client - Server`
  - `Server - Server`


CLIENT
SERVER
Client Hello
Server Hello
Server Certificate
Client Certf. Request
Server Done
Client Certificate
Client Key Exchange
Certificate Verify
Change Connection State
Finished
Change Connection State
Finished

Key Exchange

- Algoritmi pentru "Key Exchange"
  - RSA
  - DHE
  - ECDHE
- PFS sau "Perfect Forward Secrecy"
  - Traficul înregistrat dintr-o sesiune TLS nu poate fi decriptat dacă ulterior este compromisă cheia privată a certificatului digital folosit de server