openHPI – Confidential Communication in the Internet

Digital Certificates

Prof. Dr. Christoph Meinel
Hasso Plattner Institute
University of Potsdam, Germany

Certificates

Certificate is a document signed by a trustworthy third party **("Trust Center")**

- It attests the connection between a person/entity and its public key
- If one trusts the trust center that signed a certificate, one can trust the certificate

Certificates need to contain the following information:

- Owner of the certificate (person, company, web server, ...)
- Public key of the owner, and
- Digital signature of the trust center that issued the certificate

Trust Center guarantees the accuracy of these information

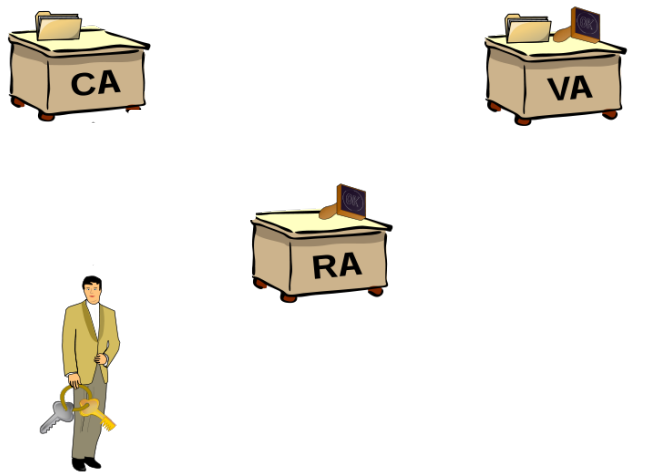
Application for a Certificate

1. User proves his identity to the **RA (Registration Authority)** and submits his public key
2. RA transfers login data - identity data, public key – to the **Certification Authority (CA)**
3. CA creates a certificate and signs it
4. CA sends the Certificate to the user and deposits the certificate information at the **Validation Authority (VA)**

http://de.wikipedia.org/wiki/Datei:Public-Key-Infrastructure.svg

Use of the Certificate

1. User sends certificate to the **communication partner**
2. The partner validates certificate with the help of the **VA**
3. The VA checks the certificate against the stored information and **confirms its validity**



http://de.wikipedia.org/wiki/Datei:Public-Key-Infrastructure.svg

Hierarchical PKIs

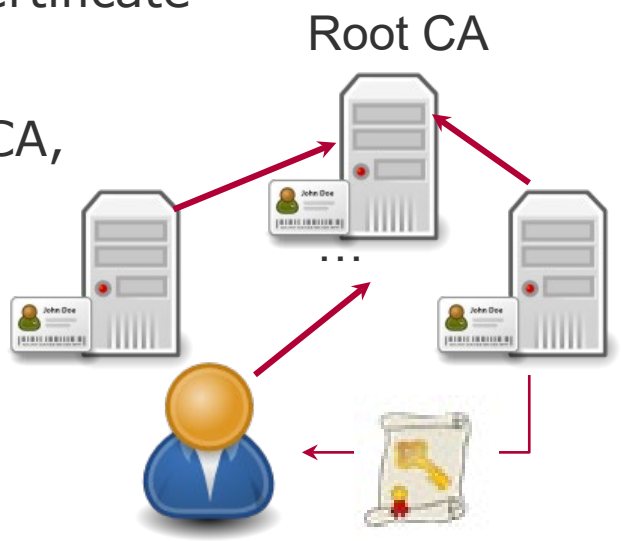
Typically a PKI is organized in a hierarchical way:

Here a PKI has an initial CA instance "**Root CA„**

- Trusted by all subordinate instances (CAs)
- Root CA signs certificates of subordinate CAs

To validate and verify the identity of a CA:

- User validates that the CA‘s certificate is signed by the root CA
- Because users trust the Root CA, they trust its signature, thus trust its certificates



Cross-Certification

Different PKIs can be linked together via **cross-certification**

- The Root CAs of both PKIs issue certificates to each other and sign them
- This means that the instances on one side trust those on the other side