openHPI – Confidential Communication in the Internet

Trust Models

Prof. Dr. Christoph Meinel

Hasso Plattner Institute
University of Potsdam, Germany

Trust Models

Solution of the trust problem for asymmetric cryptoprotocols needs to consider suitable **trust models:**

  - **Direct trust**
  - **Web of trust**
  - **Hierarchical trust**

- Most popular in Internet is the hierarchical trust model as the basis of so-called **Public Key Infrastructures** – **PKI**
- "Web of Trust" and "Hierarchical Trust" use **certificates** – documents signed by a trustworthy third party – which testify the relationship between a person/entity and its public key
  - If one **trusts the third party** who issued the **certificate**, one can rely on the public key assignment to its owner as attested in the certificate

Trust Models
Direct Trust

Alice directly confirms the authenticity of her public key to her communication partners, e.g. key transfer via a **secure second channel**

Advantages

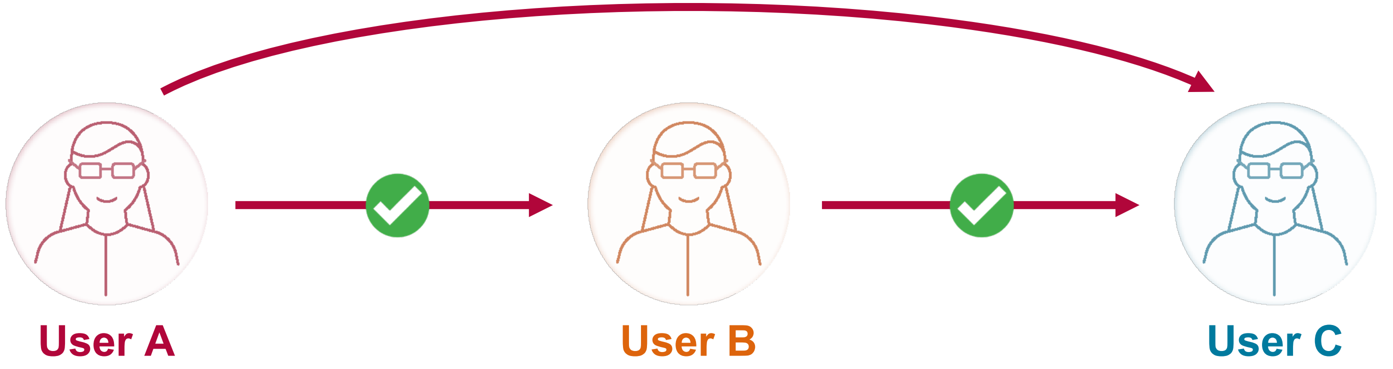
- No infrastructure necessary

Disadvantages

- Key handover to each communication partner necessary
- No binding
- No authority to enforce a security policy for solving all the problems mentioned

Trust Models
Web of Trust (1/2)

- User has his certificate signed by many other users and signs many **certificates of other users**
- The more users have signed a certificate, the more trustworthy it is
- If **user A** trusts **user B** and the certificate from **user C** was signed by **User B**, **A** can also trust certificate from **C**



Trust Models
Web of Trust (2/2)

Advantages

- Little infrastructure required, only a server is needed to store the multiple signed digital certificates

Disadvantages

- Key locking is very tedious
- Binding nature better than in the case of direct trust, but under legal considerations not sufficient
- Security policies difficult to enforce

Trust Models
Hierarchical Trust (1/3)

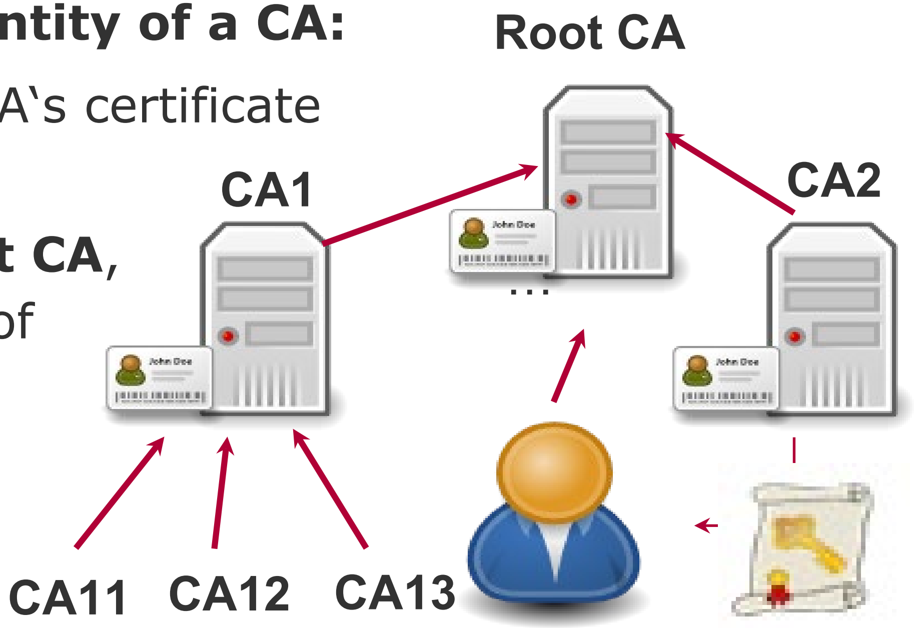
There is a hierarchical system of trusted third party **certification authorities** that issues **certificates**

“**Root CA**” is the initial instance trusted by all subordinate instances (CAs)

- Root CA signs the certificates of the subordinate CAs

To validate and verify identity of a CA:

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



Trust Models
Hierarchical Trust (2/3)

Advantages

- With a **single key** – the public key of the CA –,
  Alice can verify the digital certificates of all participant registered at the PKI
- Key revocation easily realizable
- Binding nature can be established
- Security policies can be enforced and monitored by CA

Trust Models
Hierarchical Trust (3/3)

Price to be paid

- Operation of a CA requires the provision of an extensive infrastructure – **Public Key Infrastructure** – **PKI**
- Potentially operated by independent and trustworthy carrier
- Participants must register with a CA of the PKI and receive their certificates from there
- CA must make certificates accessible, distribute revocation lists, etc.