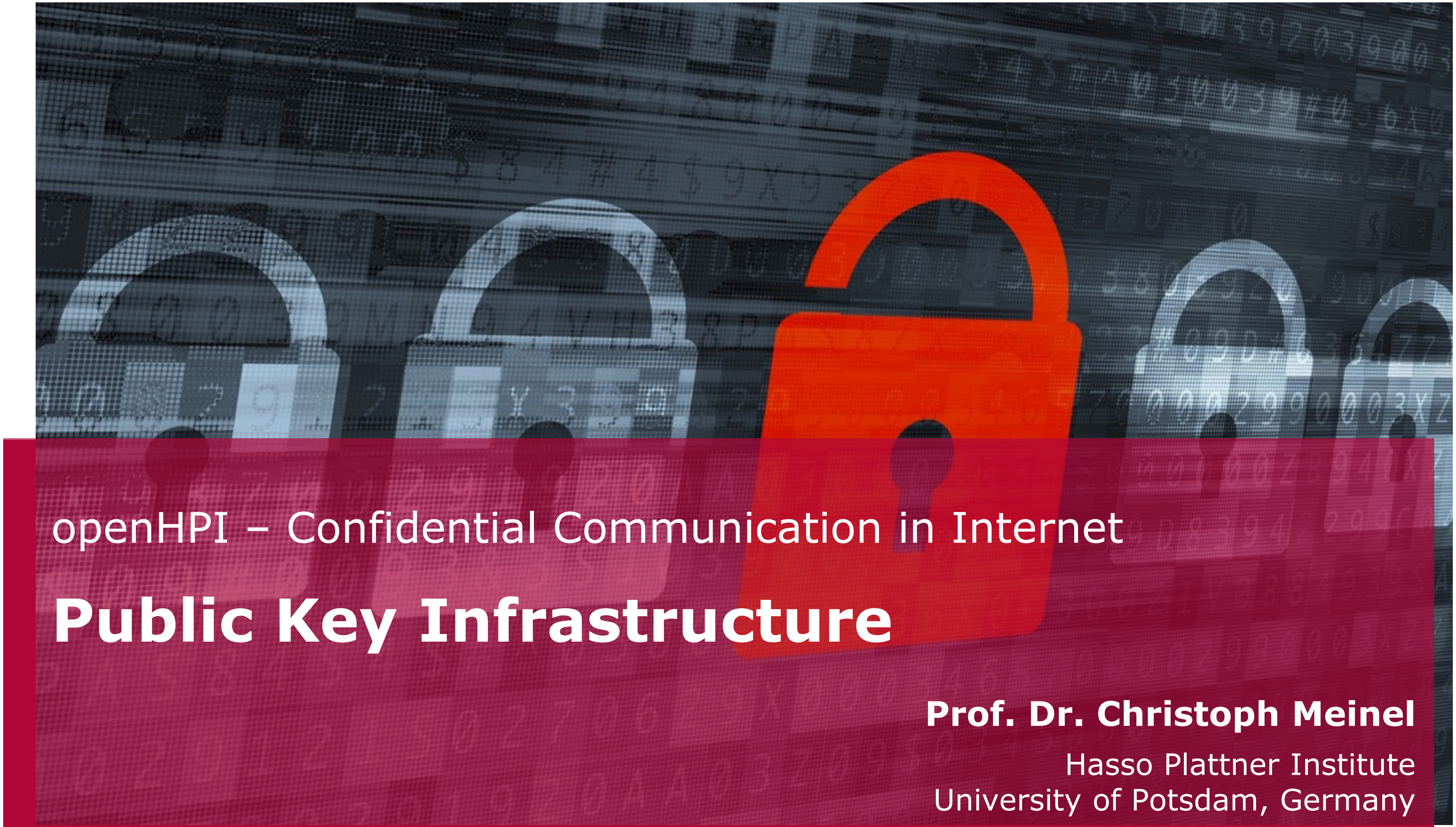


openHPI – Confidential Communication in Internet

Public Key Infrastructure

Prof. Dr. Christoph Meinel

Hasso Plattner Institute
University of Potsdam, Germany

Trust Centers and Certificates

Idea for solving the trust problem:

Independent authority – **Trust Center** – certifies the binding of a public key to a person

- Digitally signed binding of a user (name) and it public key and is called a **certificate** (more precisely a key certificate)
- Certificates are used to ensure that the exchange of information is legally binding. The identity of a user is ensured!
- Participants only have to trust the **Trust Center (TC)**

  ...

More in our openHPI- course on Digital Identities!

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 the 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

PKI – Public Key Infrastructure

To solve the trust problem by means of certificates, a complete infrastructure "**Public-Key Infrastructure - PKI**" is required

The task of a PKI is the **certificate management**

- Specification and enforcement of a security policy
- Creation of certificates
- Managing certificates
- Revoking digital certificates

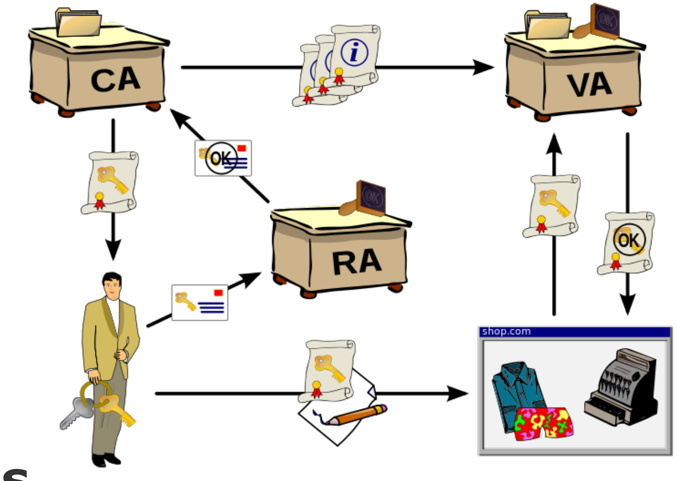
To this end PKI includes software and hardware components as well as staff to manage the **certificate management**

- Interaction of the individual components of a **Trust Center** / **PKI** to solve these tasks is ruled by **Certificate Management Protocols (CMP)**

Trust Center and its Components

At the center of a PKI is the **Trust Center** with the following components

- **Certification** Authority, CA
- **Registration** Authority, RA
- **Validation** Authority, VA



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

In addition to the trust center,
a PKI includes the following **components**,
which can/must be operated **decentralized**:

- **Local Registration Authority**, LRA
- **Revocation Authority**, REV
- **Personal Security Environment**, PSE

Trust Center and its Components
CA – Certification Authority

Certification authority – CA is the most important component of a Trust Center

- CA generates **certificate**
  - □ receives all information necessary for the certificate
  - □ generates the certificate and
  - □ signs the certificate digitally
- CA is a very **security-critical** component – if the CA's private key gets into the hands of cybercriminals, the entire PKI is worthless – the cybercriminals can then issue certificates as they wish

Signature acts require high demands on the security of a CA before it is allowed to issue certificates for legally binding "qualified digital signatures”

Trust Center and its Components
RA – Registration Authority

Registration Authority – RA is the registration office for applying for a digital certificate

- RA can be implemented centralized in a trust center or operated decentralized
- RA collects the necessary data for the creation of a digital certificate and transfers it to the CA
- The type of interaction and verification (personal registration, registration via the Internet) against an RA determines the security level of the PKI
- PKIX standard does not prescribe RA; however, PKI implemented in practice generally does not allow direct communication between users and the CA

Trust Center and its Components
VA - Validation Authority

Validation Authority – VA checks the certificate against the stored information and confirms its validity

- Once the certificate is validated, the client can further verify the corresponding digital signature itself
- Communication with the Trust Center is in real time and is also signed
- Simultaneous verification of several certificates is possible

Decentralized Components of a PKI
Local Registration Authority

Local registration authority takes over tasks from the central registration authority:

- Not all users can **verify themselves in person** at one central registration authority
- Therefore, multiple LRAs take over that task
- Can be located at / operated by fitting places/companies
  - Telecommunication provider
  - Universities
  - Technology Companies
  - …

Decentralized Components of a PKI
Revocation Authority

Revocation authority is responsible for the “deletion” (**revocation**) of a certificate:

- To remove a certificate, it is not enough to delete it, as it is still signed and malicious people could still abuse it
- The trust of the CA to the particular certificate has to be removed
- This is done by **certificate revocation**
- Could be needed in several situations
  - private key to a certificate has been lost / stolen
  - information connected to the certificate has changed (such as a URL/Hostname)
  - certificate has expired
  - …

Decentralized Components of a PKI
PSE – Personal Security Environment

- Successful use of asymmetric cryptosystems and protocols (encryption, digital signature, ...) is based on the **secrecy of private keys**
- If the private key is not kept secret, the identity of the owner can be misused
- Therefore private certificates and keys should be kept in a so-called **personal security environment**
- As private keys should not leave the environment, several tasks have to be performed inside
  - private keys generated
  - decryption of ciphertexts with the private key
  - signing documents (with the private key)

PSE – Personal Security Environment
Example: Software Key

Simple Security Environment – Software Key:

- Usually password protected area on the PC’s hard disk
- Managed with special software
- Security depends on
  - the operating system of the PC and
  - the strength of the password

PSE – Personal Security Environment
Example: Harware Key

Derived from Chipcard.jpg, Monarch, CC BY-SA 3.0, from Wikimedia Commons

Secure Environment - Hardware Key:

- **Smart card** - a separate computer which stores
  - □ User's private key
  - □ Signed certificates
- **Advantages**:
  - □ Card can easily be carried along
  - □ Only few accesses/manipulations are possible via card readers
  - □ Access to keys is not possible/difficult for hackers
- **Disadvantages**:
  - □ Calculations on the chip card are slow
  - □ Solution: only encrypt session keys or document hash values asymmetrically ...