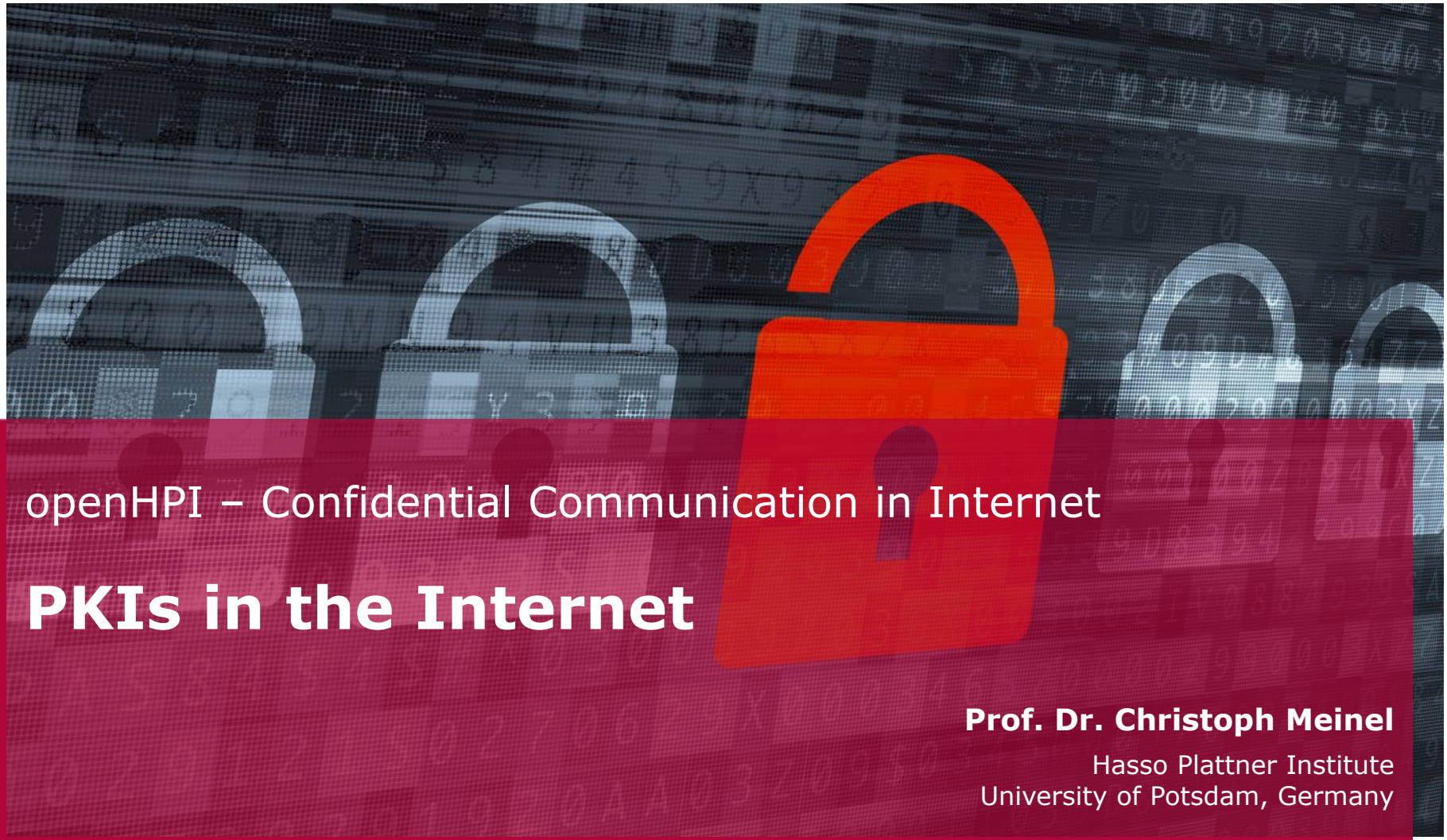


openHPI – Confidential Communication in Internet

PKIs in the Internet

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

Publik Key Infrastructure - Reminder

A **PKI - Public Key Infrastructure** …

- **Solves the trust problem** of **asymmetric cryptosystems**: It provides the means to tamper-proofly liaise the public keys to their users
- Allows the secure application of asymmetric cryptoprotocols for encryption and digital signature
- Based on the **hierarchical trust** model

Hierarchical PKI in the Internet
HTTPS (1/3)

HTTPS – HyperText Transport Protocol Secure:

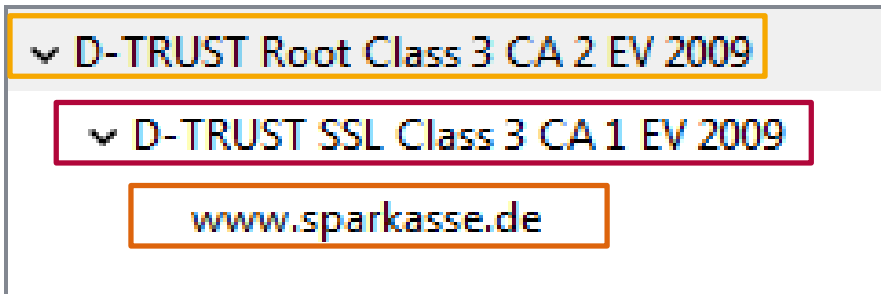
- Secured protocol for communication with web servers
- In case of a HTTPS connection in the Internet:
  - identity of the requested web page is checked, as well as
  - all communications are encrypted
- HTTPS based connections make use of a **hierarchical PKI**
  - **"Root CA" certificates** are stored in the browser or the operating system
- Connections to critical Internet services should always be made via HTTPS, without the browser displays a certificate warning:
  - the **certificate guarantees** that you are communicating with the right owner of that Internet service (address)

Hierarchical PKI in the Internet
HTTPS (2/3)

Example:

Establishing an HTTPS-based connection to the savings bank

- Browser verifies signature of the certificate on *www.sparkasse.de* with the help of a superordinate certificate [D-TRUST]
- Signature of the D-TRUST certificate is verified by the browser using the stored and trustworthy root CA certificate
- Browser establishs a chain of trust up to the certificate of the savings bank and shows a small lock



Hierarchical PKI in the Internet **HTTPS** (3/3)

When connecting to a critical Internet services, the browser should show a lock:

Anyone can view the certificates hierarchy in the browser:

Example for Firefox

- Click on the green lock
- Click on the arrow next to "Secure connection"
- Further information show certificate details

Hierarchical PKIs in Practice
My ELSTER

"**My ELSTER**" – official online portal of German tax authorities for filing e.g. income tax returns

Logging into the "My ELSTER" portal is possible **via a PKI:**

- **Certificate File:**
  - contains signed certificate and private key to prove your identity, and is stored on the user's computer
- **Electronic identity card + ID card App2 software**:
  - chip card which, after checking the authorization certificate of "My ELSTER", issues your stored identity data signed by the BSI
- **Security stick** or **chip card** + **ElsterAuthenticator software**:
  - Contains private key and signed certificate to prove your identity