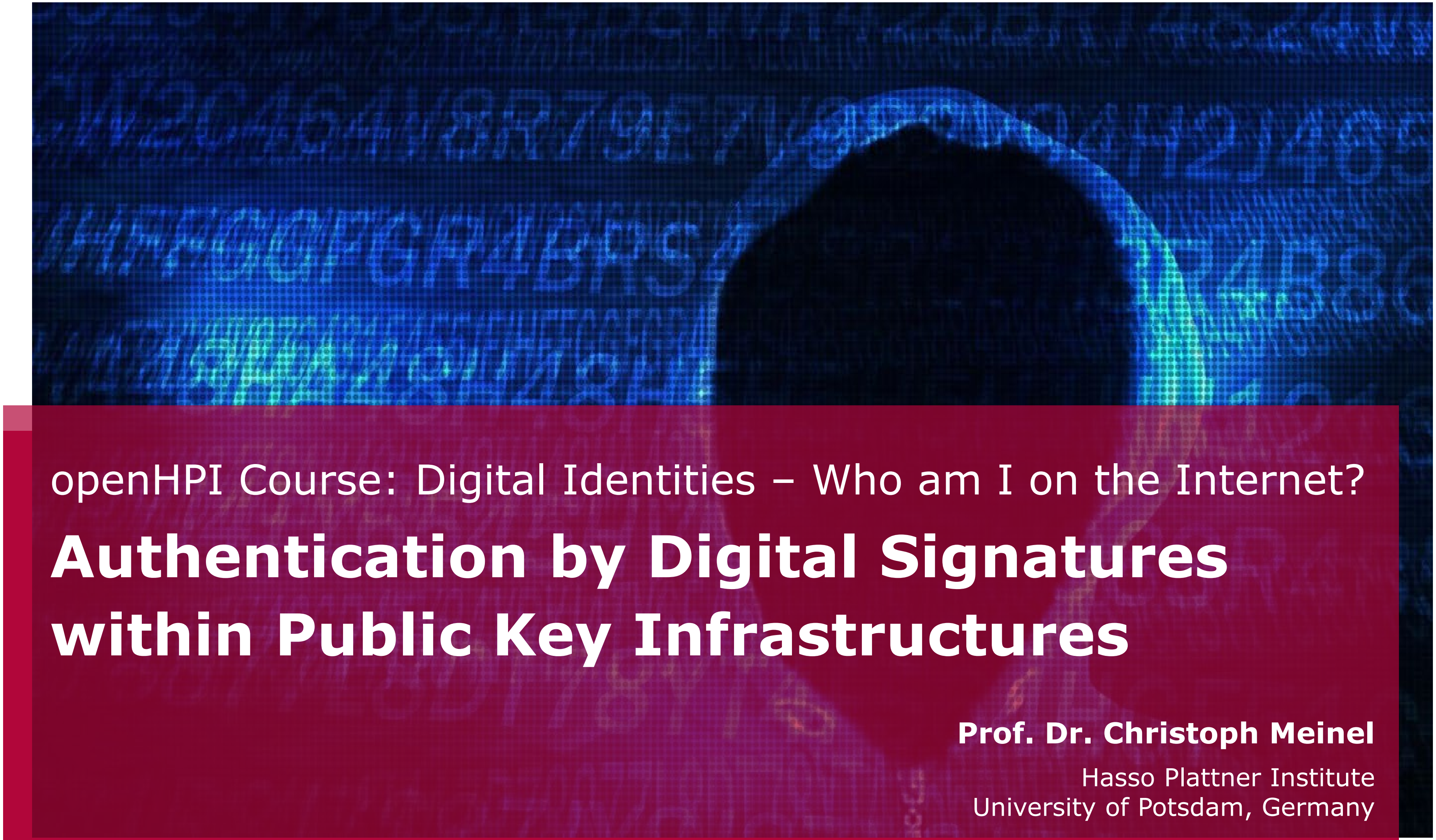


openHPI Course: Digital Identities – Who am I on the Internet?

Authentication by Digital Signatures within Public Key Infrastructures

Prof. Dr. Christoph Meinel

Hasso Plattner Institute
University of Potsdam, Germany

Introduction of Digital Signatures

With methods from asymmetric cryptography on can guarantee sender and message integrity

→ **Digital signatures**

Digital signatures model handwritten signatures:

Example:

- Signature when purchasing with the bank card
  - buyer signs a receipt
  - cashier compares signature with the signature on card
- Signature with digital signatures
  - online service sends user a random data object
  - user signs this object and sends it back to the service
  - service verifies the signature

Public Key Infrastructure – PKI

- Digital signatures are created with **asymmetric cryptographic methods** which are characterized by encrypting / decrypting with different keys. To this end each user needs 2 keys …
- The secure use of asymmetric cryptographic methods is only possible within **public key infrastructures – PKIs**
- The most important **components of a PKI** are:
  - Certification Authority (CA)
  - Registration Authority (RA)
  - Validation Authority (VA)

Digital Signatures

Each participant (identity) of a **PKI** has two encryption keys:

- **Private Key**
  - □ to create a signature
  - □ must be kept secret by the participant
- **Public Key**
  - □ to verify a signature
  - □ is distributed to each participant of the PKI

Illustration:

- Signet ring and wax
  - □ Seal ring corresponds to secret key
  - □ Public key corresponds to template for checking seal

PKIs – Public Key Infrastructures and Signatures

Basic idea:

- At the **PKI registry**, a user can request a "**certificate**" confirming his public key
- **Certification Authority** (CA) creates a **certificate** which proves that a public key actually belongs to a user. Certificate is authenticated by the CA’s **digital signature**
- **Digital signature** is a (hash of a) message encrypted by the senders private key. It can be (only) decrypted with the associated public key of the sender
- Receiver of a digitally signed message can check its authenticity by decrypting (verifying) the signature with the public key of the sender out of the certificate

Application Scenarios of PKIs in Practice

Communication with web pages using the HTTPS protocol (HTTPS - Secure Web Protocol):

- If a browser connects to a website (server) via HTTPS, the authenticity of the page is checked
- For this purpose, the website sends its certificate to the browser
- Browser has a list of certification authorities that it (the browser manufacturer) considers trustworthy
- Browser checks whether the certificate has been certified (digitally signed) by one of these certification authorities
  - if yes, the **green icon** is shown in front of the URL
  - if no, the **red icon** warns that the browser does not consider the website trustworthy

Authentication by Digital Signatures (1/4)

Digital Signatures can also be used for authentication

To this end we need **certificates**

- How does online service know that a user's published public key actually belongs to that user (identity)?
- Proof is provided by a **certificate** that proves that the public key belongs to this user
- **To authenticate a user**, the online service needs the public key of the user out his/her certificate
- Service trusts the certificate since it is issued and digitally signed by a **certification authority** that it considers trustworthy
- By the way, authentication with digital signatures is an authentication by ownership (private key)

Authentication by Digital Signatures (2/4)

Prerequisite: Public key infrastructure

Procedure:

1. A key pair consisting of a private and a public key is generated for the user
2. The public key is registered with the **Registration Authority**. This checks the authenticity and validity of the public key by verifying possession of the private key
3. If the validity is confirmed, the **Certification Authority** becomes active
4. Certificate Authority creates certificate that binds the public key to the identity of the user. User receives the certificate
5. …

Authentication by Digital Signatures (3/4)

Prerequisite: Public key infrastructure

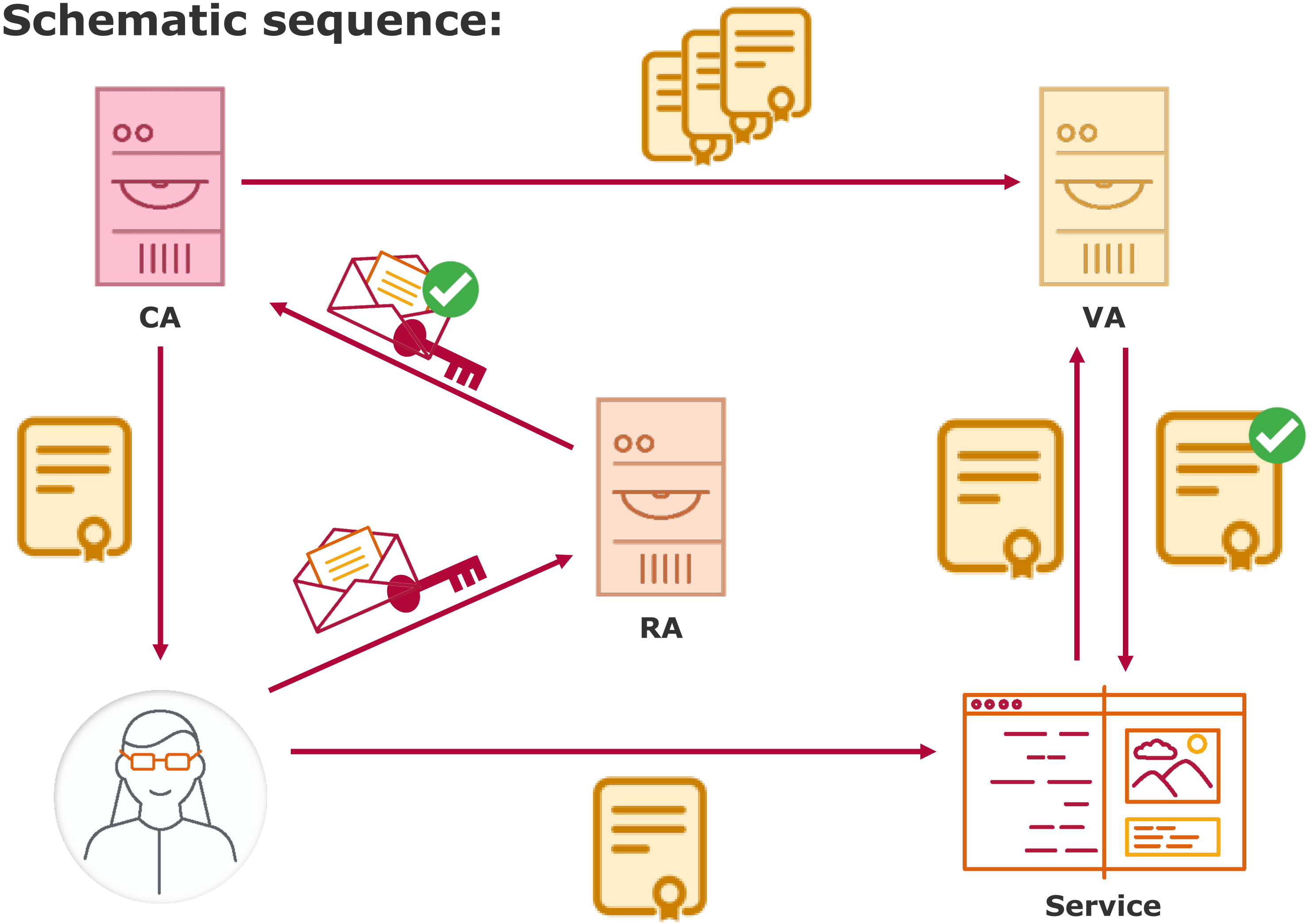
Procedure:

…

5. To register with a service, a user creates a digital signature (data is encrypted with a private key) and sends it to the service together with the certificate
6. The service validates the certificate with the help of the **Validation Authority**
7. Result of the validation is transmitted to the service
8. Now the service can **verify the signature with the public key from the certificate** and give the user access …

Authentication by Digital Signatures (4/4)

Schematic sequence:



Authentication by Digital Signatures
Advantages and Disadvantages

Advantages:

- (Mostly) no knowledge necessary: Private key is property
  - Private key can be password protected
- No previous contact between user and online service is necessary. Sending a (valid) signature and certificate is sufficient. No password or other secrets will be exchanged
- Certificate must have been "only" certified by a trustworthy authority

Disadvantages:

- Complex PKI is required and trust in this is necessary
- Experience in correct use of the method is required
- If a hacker gains access to a user's private key, he/she can impersonate the user

Authentication by Digital Signatures
Summary

- The basic prerequisite for authentication with digital signatures is the existence of a **public key infrastructure**
- Public key infrastructures work with **certificates** and **digital signatures**
- User has two keys, a private and a public one
- Digital signature is created with the private key of the user. Therefore protection of the private key must be guaranteed
- Digital signature is verified with the public key of the user
- A certificate attests the user's public key