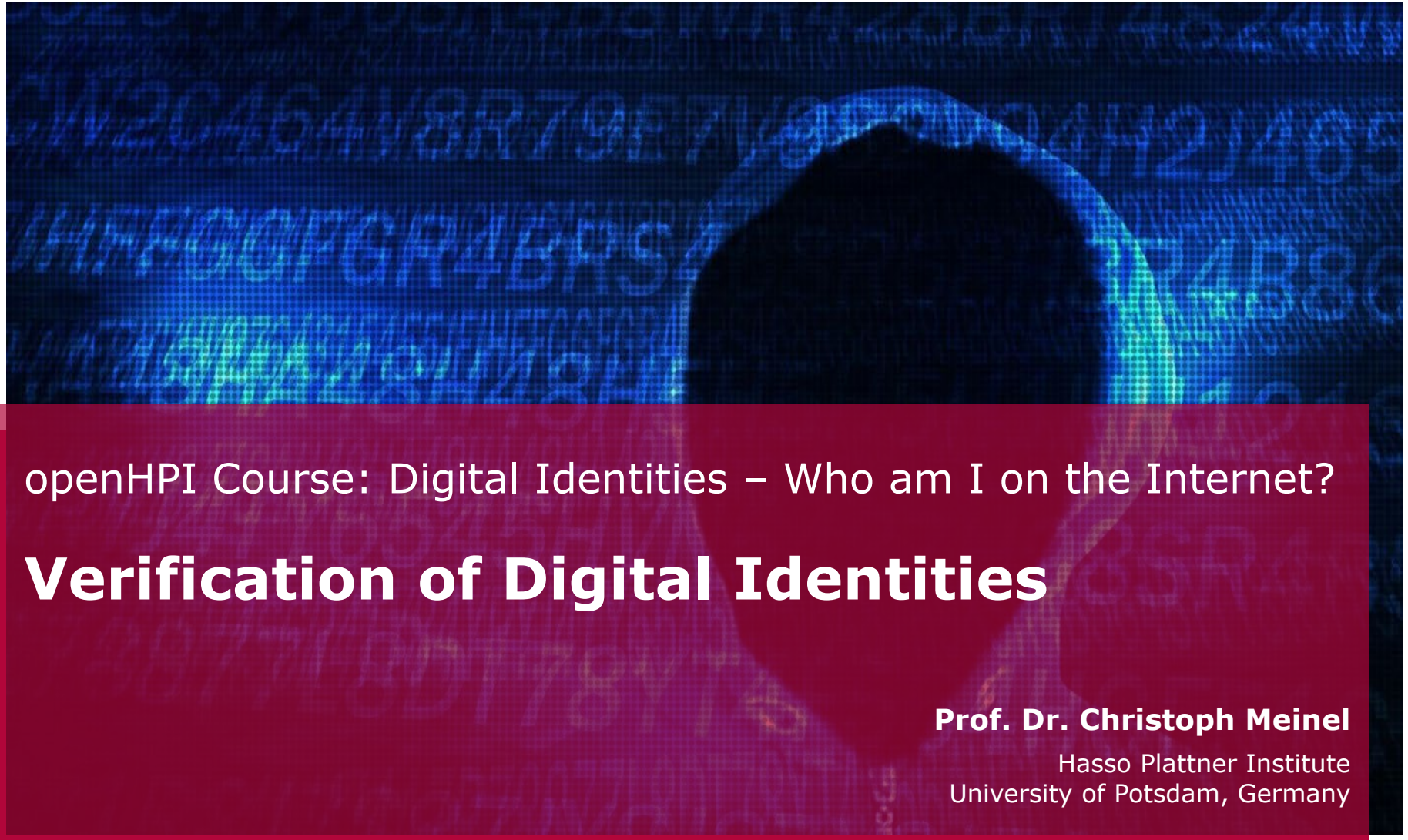


openHPI Course: Digital Identities – Who am I on the Internet?

Verification of Digital Identities

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

Binding Digital to Physical Identities (1/2)

When registering with an online service – **creating a digital identity** – the user himself enters his data

Online services want/need to know whether these information really …

- belongs to a real person
- belongs to the person who made the entry

Binding Digital to Physical Identities (2/2)

Example:

Create an online banking account or apply for a credit card

- User enters his/her name, address, etc. on the bank's website and a digital identity is created there
- The bank now wants to know whether the entered data really belongs to the specified person

For this purpose, it is necessary to **securely connect and confirm a digital identity with a physical identity**.
The user must prove his identity to bind his digital to his physical identity

- Often this is part of the **registration process**

Methods for Binding Digital to Physical Identities

- Digital identities can be linked in different ways to a physical identity that actually exists, e.g.
  - Post-Ident procedure
  - Video Identification - **VideoIdent** -, e.g. via WebID
  - Smart identity card, ...
- Mostly in a cooperation with an external, trustworthy provider, e.g.
  - post office branch
  - trusted online service
  - electronic ID card technology

We take a closer look at two methods:

- WebID
- Smart Identity cards

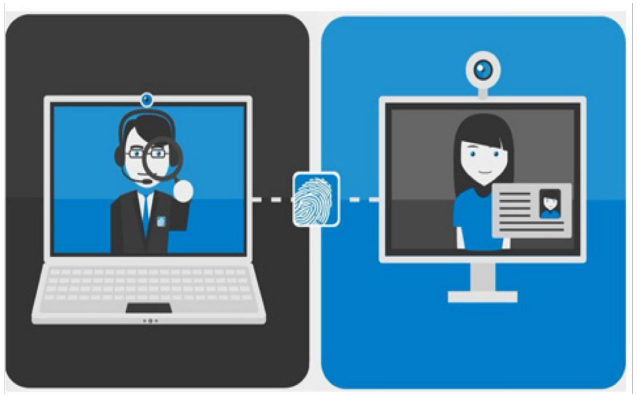
Video Identification with WebID
What do I need?

Best known provider for video identification is **WebID**

- Prerequisites for the use of WebID are:
  - computer with camera, microphone with access to the Internet
  - valid identity document: Identity card or passport
  - browser or a WebID app

Video Identification with WebID
How does it work?

- First, users enter their data into an online service, e.g., a bank
- User will then be redirected to the WebID website
- Here the user starts a **video chat** with an employee of WebID
- User must hold his ID card in the camera and answer some questions
- After the chat has ended, WebID transmits the result to the online service
- Thereafter, the user is entitled to use the online service, e.g. of the bank



Advantages and Disadvantages of Video Identification with WebID

Advantages:

- Identification possible at any time
- Video chat only takes a few minutes
- Can be done from home, no way e.g. to a post office necessary

Disadvantages:

- Trust necessary in the WebID company
- Video chat employee learns personal data (from ID card and which service to use)

Identification by Means of Smart Identity Cards (1/2)

- In some countries, the identity cards provides online functionalities – "**smart identity card**"
- To this end smart identity cards include a digital identity
- Digital identity can be used for accessing online services

Example from Germany

- German **national identity card** (nPA)
  - was introduced in 2010 and can be used for online registration
  - number of supporting online services is still very small

Identification by Means of Smart Identity Cards (2/2)

Example from Estonia

- **e-Estonia** is a movement by the government of Estonia
  - Facilitate interactions with the state via the usage of electronic (online) solutions
  - Various e-services can be accessed via smart ID card, e.g.
    - i-Voting
    - e-Ticket
    - e-Tax Board
    - e-School

Identification by Means of Smart Identity Cards
What is needed?

For the usage of smart identity cards is needed:

- Identity card with activated online function
- Card reader
- Software, e.g. App

What is behind the Online Functionalities? Public Key Infrastructure

Smart identity cards are based on a PKI – Public Key Infrastructure

Example: **German identity card** (nPA)

A number of state authorities serves to this PKI:

- Federal Office for Information Security (BSI) as **Root-CA**
- Federal Administration Office with the Issuing Authority for Authorization Certificates (VfB) as **Registration Authority** for the services
- Authorization Certificate Providers (BerCA) issue the actual technical certificates, e.g.
  - D-Trust GmbH (Federal Printing Office)

What's behind the online ID?
Identity card also contains a certificate

- Beside the user attributes and a private key a (identification) certificate is also stored on the identity card
- Identity card first checks the (authorization) certificate of the online service for a request
  - checks validity of the authorization certificate provider
  - checks validity of the Root-CA
- Authorization certificate also specifies the data required by the service and displayed this to the user
- Only after the user's consent (entry of the PIN) the required data will be transferred signed with the private key
- The online service can then verify the signature by means of the identification certificate

Identification by Means of Smart Identity Cards Advantages and Disadvantages

Advantages

- High protection of the digital identity (data)
  - combination of identity card and PIN required
  - mutual identification:
    - By receiving the authorization certificate, one can check whether the service is allowed to read data from the badge at all
  - end-to-end transmission is encrypted
- Everyone has an identity card at hand

Disadvantages

- Card reader required
- In some countries, only few services support identity card

Verification of Digital Identities
Summary

- In different contexts, verification of the binding of a digital identity with a physical identity is necessary
- There are different ways to do this:
  - video identification (Video-Ident), e.g. with WebID
    - easily possible
  - with smart identity card
    - users need card reader and
    - online service requires valid authorization certificate
  - user must authorize the transmission of identity data with PIN