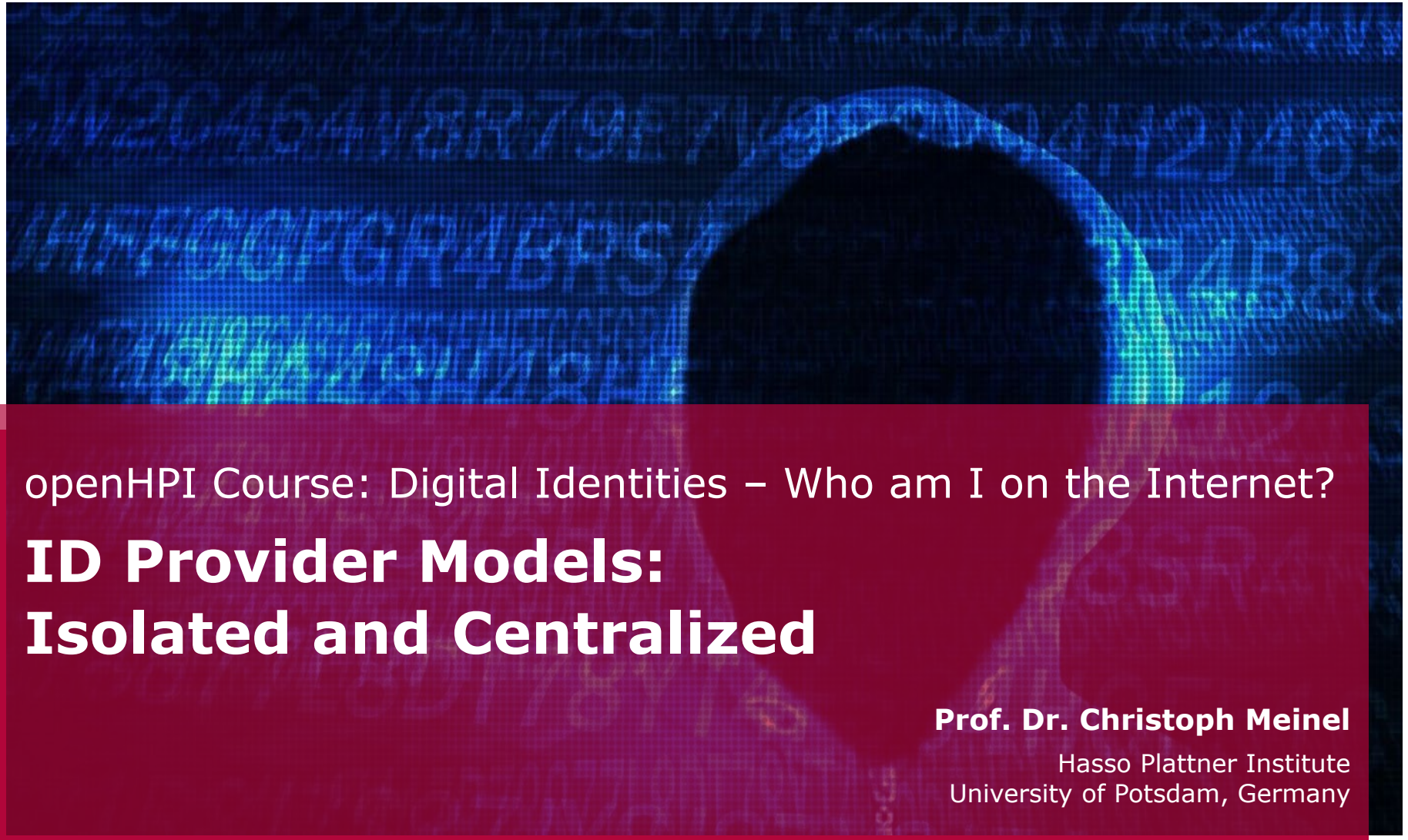


openHPI Course: Digital Identities – Who am I on the Internet?

ID Provider Models: Isolated and Centralized

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

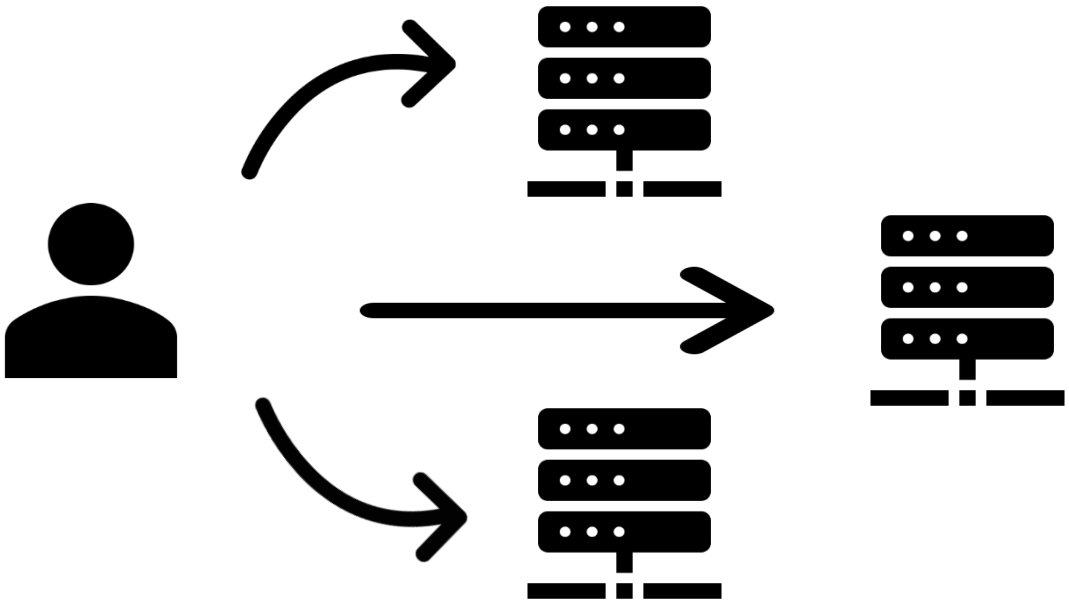
Dealing with Digital Identities

- **Different models of digital identities** have developed over time for dealing with digital identities
- With each new model, the handling of digital identities should become less and easier
- The main difference between all models is **who and where digital identities are stored or managed**
- In the following we consider the **isolated** and the **centralized model** of a digital signature

Isolated ID Provider Model

In the **isolated model**, each service manages and stores digital identities by itself

- So each service is isolated and works independently
- Users have to create "register" a new digital identity for each single service



Isolated ID Provider Model
Advantages and Disadvantages

Advantages:

- Services have full control over the identities of their users
- Digital identities are trustworthy for the service because they are self-created

Disadvantages:

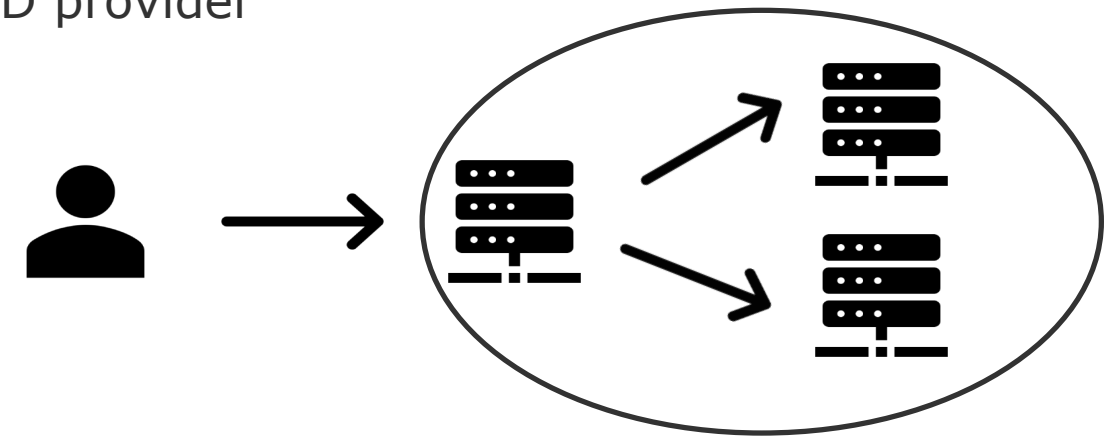
- Users have many identities if many services are used
- High effort due to the use of same attributes, e.g., address, bank details, …, having to be repeated often
- Every service, no matter how small, must take care and protect the database of the user's identities
  - protection against false authentication
  - protection against hacking of the database

Centralized ID Provider Model

There is a (**central**) **service** that only takes care of the registration and management of digital identities

→ **identity provider**, **ID provider**

- ID provider also handles the authentication process
- Other services which have to trust this ID provider can then be used via this one identity
- If services need certain attributes, they get them from the ID provider



Centralized ID Provider Model
Advantages and Disadvantages

Advantages:

- A dedicated service specialized on identity management
- Other services can only care about their own functionality
- Users have can use different services with one digital identity

Disadvantages:

- Single-Point-of-Failure
  - Failure (e.g. identity leak) makes all other services unusable
  - ID provider needs a high protection, because all services depend on it
- Trust is necessary
  - Services must trust the ID provider that its tokens contain valid data

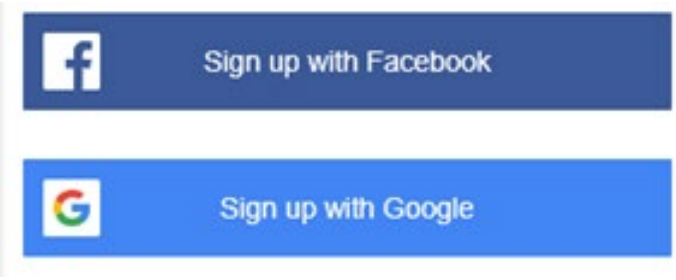
Centralized ID Provider Model
Applications

The central ID provider model is often found in companies

- A service that manages employee's identities
- With this one identity the employees can access emails, calendars, internal file systems and databases, …
- Often used systems: LDAP, Kerberos, …

The central ID provider model is increasingly found on the Internet

- There are websites that do not offer their own registration, but rely on login via third-party, e.g.
  - Facebook, Google, Twitter are used as identity provider



Isolated and Centralized ID Provider Model
Summary

Isolated ID provider model:

- Each services manages its own digital identities
- Users have many digital identities, one for each service

Centralized ID provider model:

- An identity provider that takes care of digital identities
- Other services rely on the digital identity provided by one ID provider
- Users have only one (or few) digital identity