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

Secure Authentication with OpenID Connect

Prof. Dr. Christoph Meinel

Hasso Plattner Institute
University of Potsdam, Germany

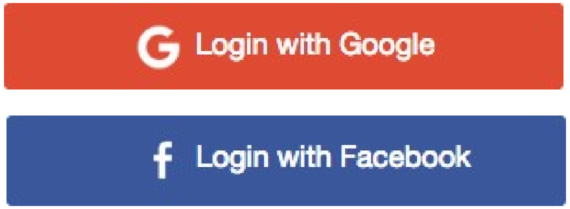
Authentication for Online Services

- Have already used Kerberos to learn about a protocol that can be used **to outsource the authentication process** for services
- However, Kerberos is usually only used within companies, and is not well suited for external online services
- Especially for online services, another authentication protocol is widely used:

OpenID Connect (OIDC)

OpenID®

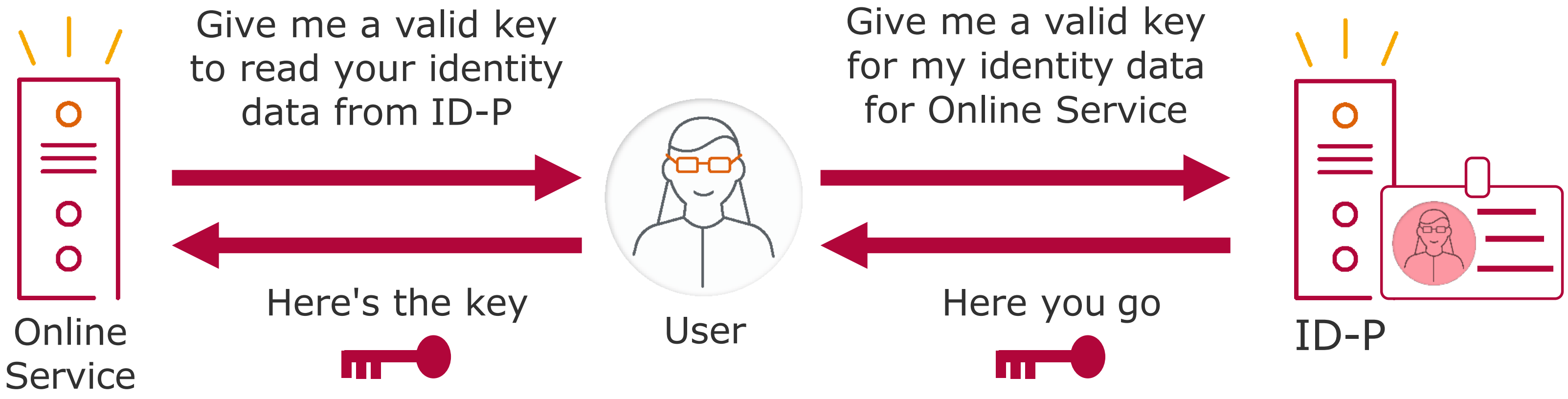
- OpenID Connect allows online services to outsource authentication to a third service
  - □ this service may belong to other companies
  - □ users can use already existing identities



Authentication for Online Services

Idea of OpenID Connect: Online service receives identity information about the user from the ID provider

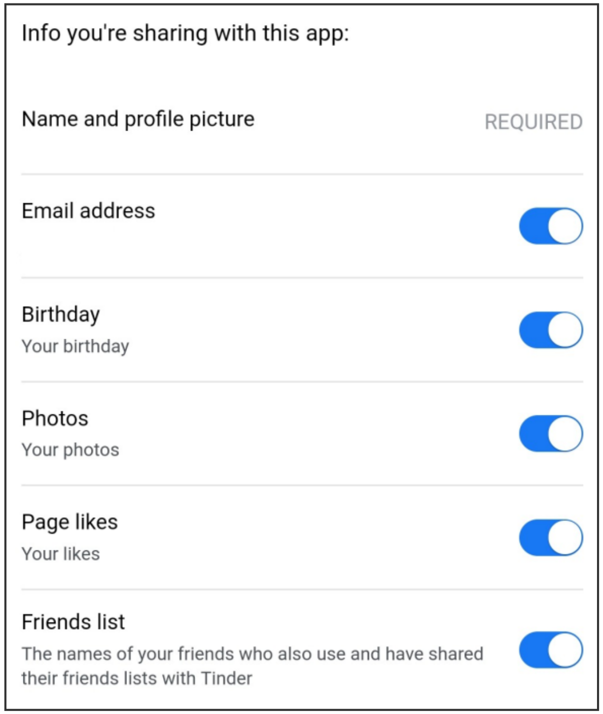
- There are 3 rolls: User, online service and ID provider
  - □ user must authorize on the ID provider for the service


Give me a valid key to read your identity data from ID-P
Give me a valid key for my identity data for Online Service
Here's the key
Here you go
Online Service
User
ID-P

With this key, the service can then read the required identity attributes directly from the ID provider

Access Control for Attributes of a Digital Identity

- Before users request keys from the ID provider, they see what attributes are needed
- User can agree to this, but can also reject (then online service will not or only partially be usable)
- **Example**: **Tinder via Facebook**
  - □ Attributes: name and profile picture, friends, birthday, photos
  - □ Some of the attributes can be deactivated. Tinder then does not get access to these attributes, but does get access to the ones still activated
  - □ Some attributes can not be deactivated



Info you're sharing with this app:

Name and profile picture REQUIRED

Email address

Birthday
Your birthday

Photos
Your photos

Page likes
Your likes

Friends list
The names of your friends who also use and have shared their friends lists with Tinder

OpenID Connect
Advantages and Disadvantages

Advantages:

- Easy to understand
- Easy to implement
- Fewer digital identities
- Single sign on
- User sees which attributes are requested

Disadvantages:

- Online service must add each ID provider to be used separately
- User can only use ID providers that are offered
- Often users can only see which attributes are requested, but cannot deactivate them

OpenID Connect
Summary

- OpenID Connect is a protocol for authentication via an external ID provider
- Online service asks for an access key to the identity data it requires
- User authorizes it
- ID provider generates a key and transmits this key to online service