Federation 101 Refresher

Identity Federation

Federation-as-a-Service Training
21./22. April 2015, Vienna

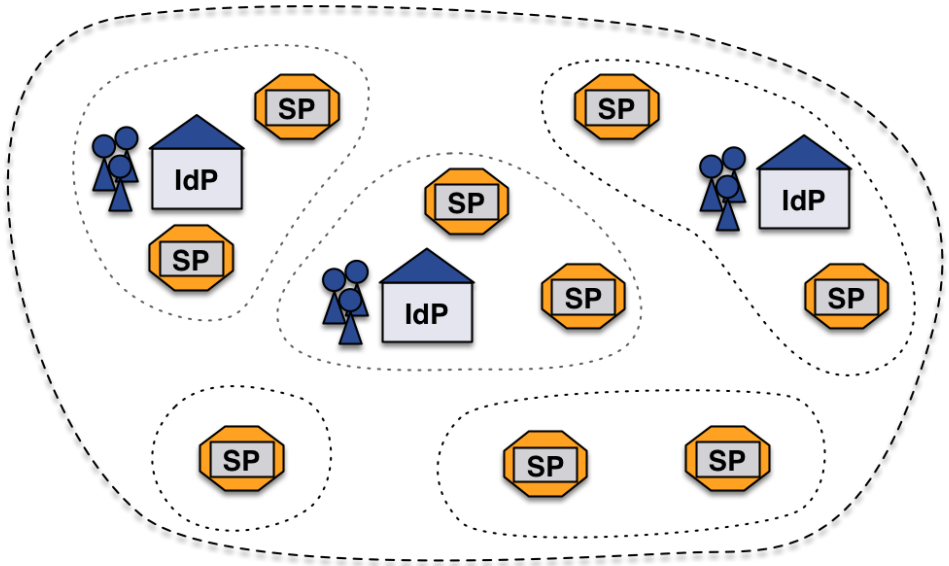
Lukas Hämmerle
lukas.haemmerle@switch.ch

Theory

- Definition of a Federation
- Trust
- Benefits

What is a Federation?

- A group of organizations running IdPs and SPs that agree on a **common set of rules and standards**
  - It's a label - to talk about such a collection of organizations
  - An organization may belong to more than one federation at a time
- The grouping can be on a regional level (e.g. SWITCHaai) or on a smaller scale
  (e.g. large campus)
- Note:
  IdPs and SPs 'know' nothing about federations, they only know metadata



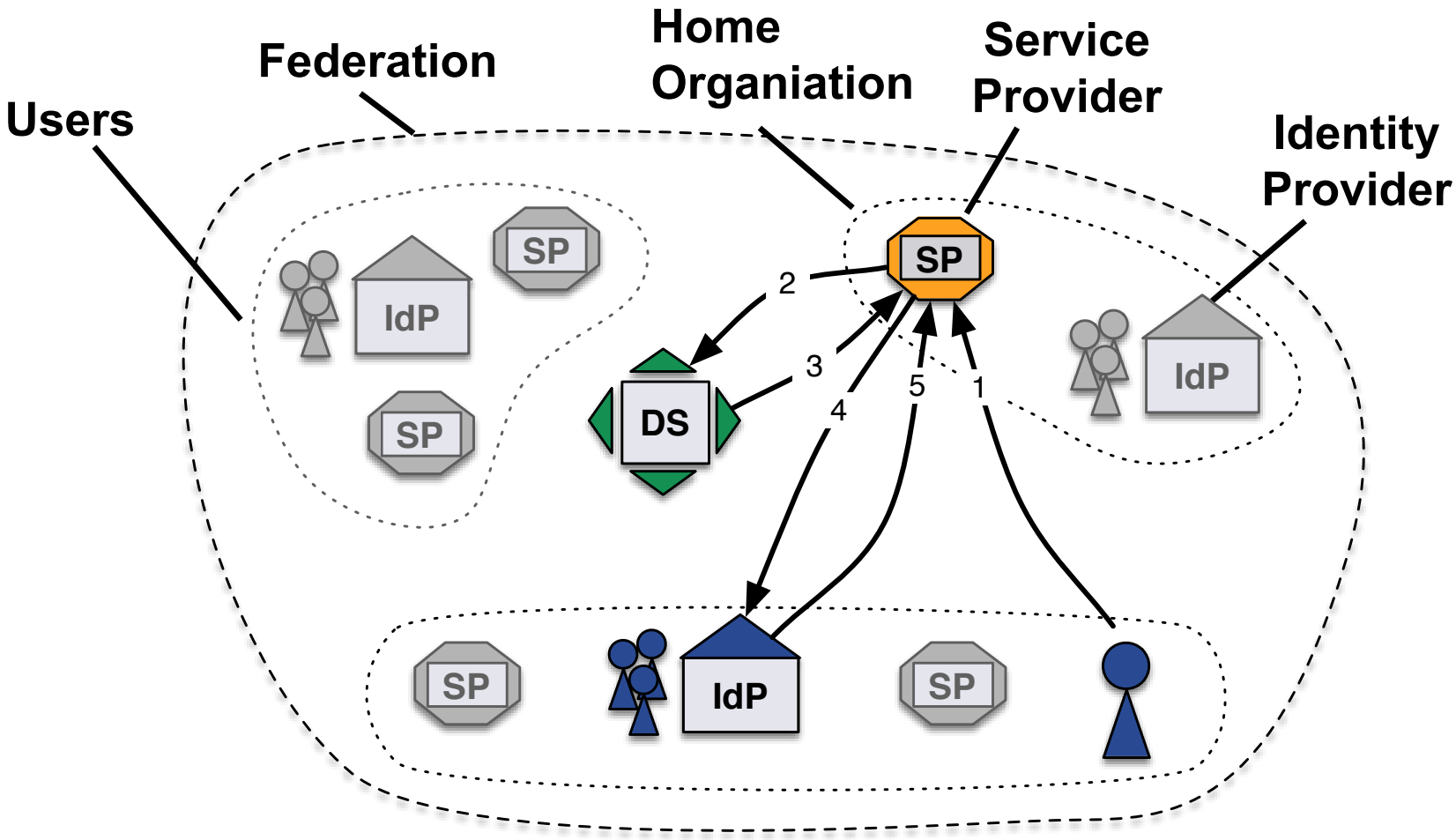
Evolution of Identity Management

- **Stone Age**
  Application maintains unique credential and identity information for each user locally

- **Bronze Age**
  Credentials are centralized (e.g. Kerberos, LDAP) but applications maintain all user identity information

- **Iron Age**
  Credentials and core identity information is centralized and application maintains only app-specific user data
  → Federated Identity Management

Typical Federated Login Flow



Benefits of Federated Identity Management

- **Reduces work**
  Authentication-related calls to Penn State University's helpdesk dropped by 85% after they installed Shibboleth.
- **Provides up-to-date data**
  Studies of applications that maintain user data show that the majority of data is out of date. Are you "protecting" your app with stale data?
- **Insulation from service compromises**
  With FIM data gets pushed to services as needed.
  An attacker can't get everyone's data on a compromised server.
- **Minimize attack surface area**
  Only the IdP needs to be able to contact user data stores.
  All effort can be focused on securing this single connection instead of one (or more) connection per service.

More Benefits

- **Saves clicks and Logins**
  Users generally find the resulting single sign-on experience to be nicer than logging in numerous times.
- **Consistent Login Process**
  Usability-focused individuals like that the authentication process is consistent regardless of the service accessed.
- **More efficient Service Integration**
  A properly maintained federation drastically simplifies the process of integrating new services.

Federated Identity Management

In Federated Identity Management:

- **Authentication** (AuthN) takes place where the user is known
  - An **Identity Provider** (IdP) publishes authentication and identity information about its users
- **Authorization** (AuthZ) happens on the service's side
  - A **Service Provider** (SP) relies on the AuthN at the IdP, consumes the information the IdP provided and makes it available to the application
- An **entity** is a generic term for IdP or SP

Federated Identity Principles

The first principle within federated identity management is the active protection of user information

- **Protect the user's credentials**
  Only the IdP ever handles the credentials

- **Protect the user's personal data, including the identifier**
  A customized set of information (in form of attributes) gets released to each SP

How to benefit from Federations

- Watch clip "How to benefit form eduGAIN" on: https://www.youtube.com/watch?v=x1YhuFPxMz8

Questions

- What do you think is the main or most important role of a federation?
- What alternatives are there?
- What are the (dis-)advantages of NREN federations over the alternatives?