Identity Management Session

Agenda
16:15 – 18:00

- 10 Min: General FIM intro (Lukas Hämmerle, SWITCH)

- IdM/FIM Overview Presentations:
  - 10 Min: EGI (Peter Solagna, EGI.EU)
  - 10 Min: EUDAT (Johannes Reetz, Max Planck Gesellschaft)
  - 10 Min: GÉANT (Lukas Hämmerle, SWITCH)
  - 10 Min: PRACE (Jules Wolfrat, SurfSARA)

- 50 Min: Discussion

- 5 Min: Wrap-up

(Federated) Identity Management Introduction

e-Infrastructures for Earth Sciences Workshop
22./23. January 2015, Amsterdam

Lukas Hämmerle, SWITCH
lukas.haemmerle@switch.ch

A brief history of Identity Management

Primordial Soup

- Nothing yet!

Stone Age

- Application holds all info

Bronze Age

- Centralised credential e.g. LDAP
- Identity in app

Iron Age

- Central user directory, credentials and identity
- App only has specific user data

Diamond Age

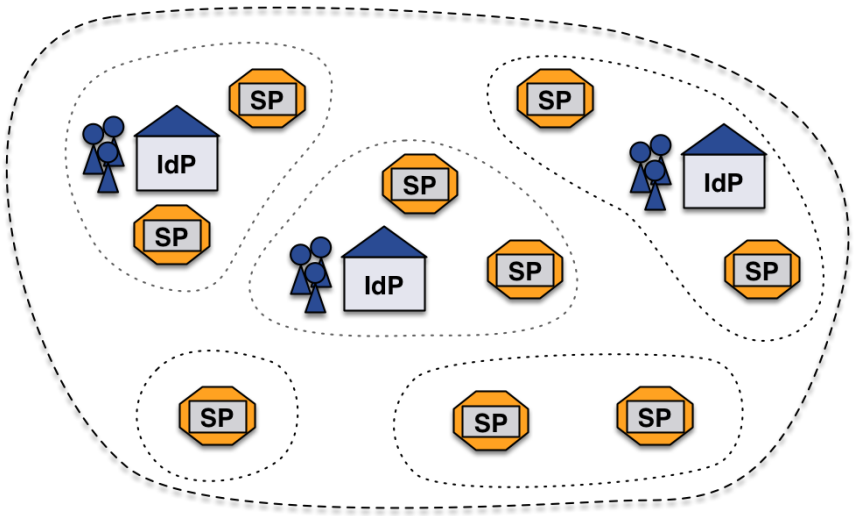
- Federated identity
- Share information outside one domain
- App only has specific user data

Credentials not provided to App anymore

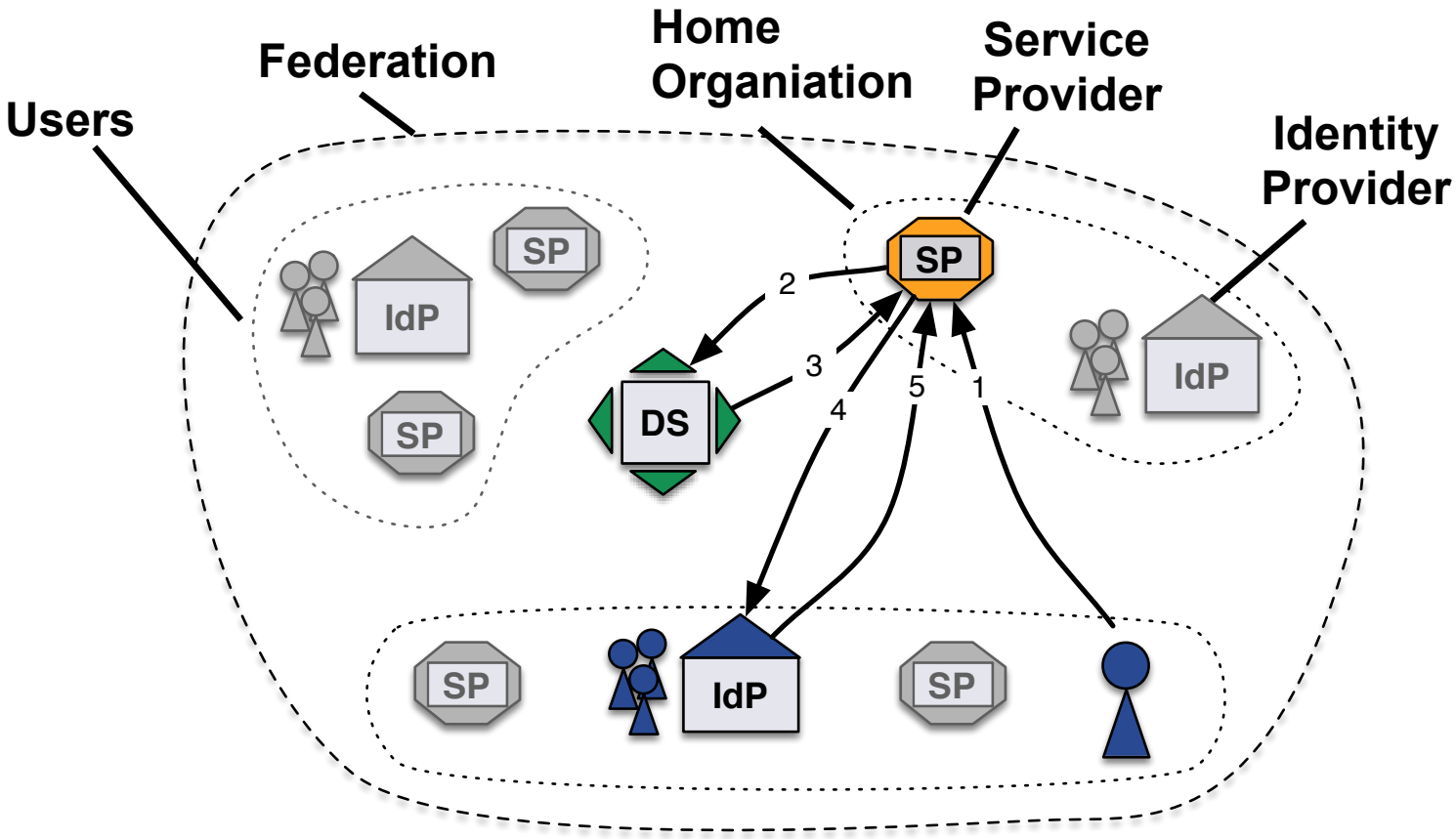
Where are you? Where do you need to be?

What is a Federation?

- A group of organizations running Identity Providers (IdP) and Service Providers (SP) 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. national identity federation) or on a smaller scale (e.g. large campus)
- **Note**: IdPs and SPs typically 'know' nothing about federations, they only know metadata (description about other SPs IdPs).



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  Studies of applications that maintain user data show that the majority of data is out of date.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 unless (identity) data is stored there.
- **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

- **One Login**
  Number of (academic) user credentials can be reduced to one single login issued, managed and protected by the user's home institution (e.g. university).

- **Single Sign-On 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 relatively 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
- AAI = **Authentication and Authorisation Infrastructure**
- 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 checks 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