



Introduction to Federated Identity Management

Click to edit subtitle

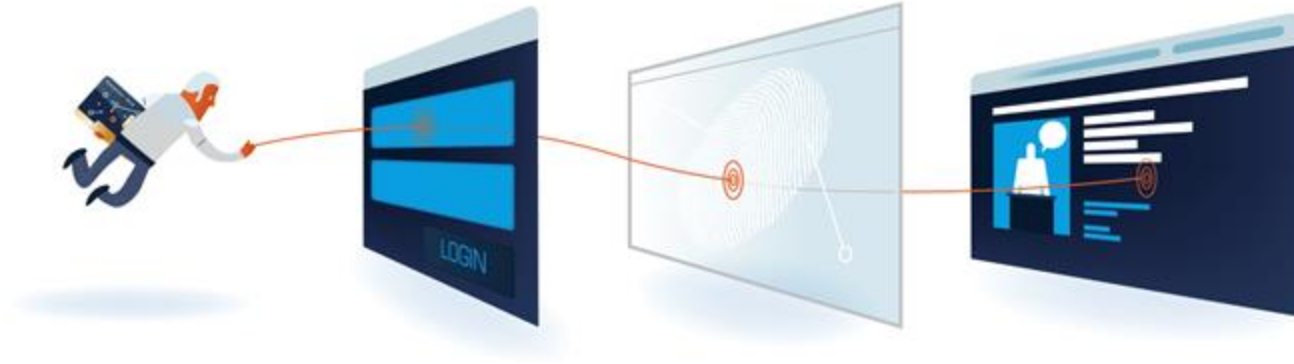
eduGAIN Training Team

GÉANT GN5-2

eduGAIN training for ngREN
April 2025

<Click to edit label> Public (PU) / Project Participants Sensitive (SEN)

Learning Objectives



01

What is Federated Identity Management?



02

What is a Federation?



03

What types of federation exist?



Identity Management processes

- Identification
- Authentication
- Authorization



Example

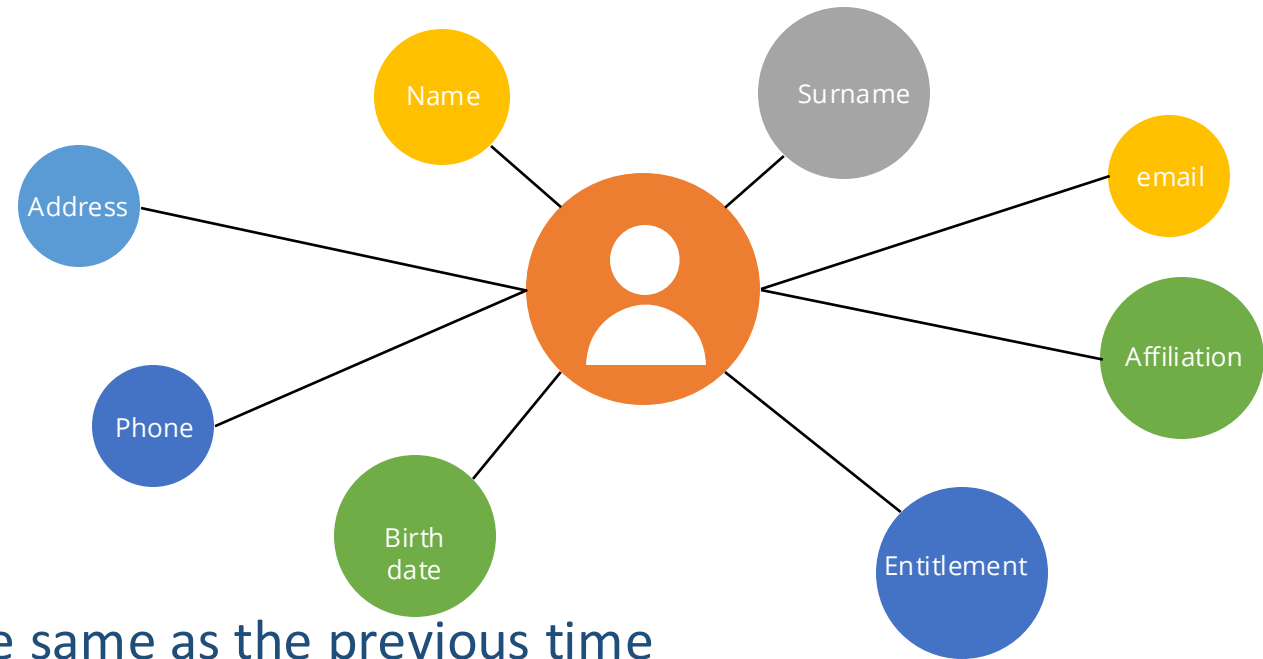


Digital Identity

- **Set of Attributes**

- **Purpose:**

- **Identification:** Prove that subject is the same as the previous time
- **Authorization:** Access decision based on attribute values, Identity or Role based access control
- **Profile data:** Personalization, identification “for humans”, name, email address, etc.



Delegation of authentication



Why and How ?

Example

GitLab.com

GitLab.com offers free unlimited (private) repositories and unlimited collaborators.

- [Explore projects on GitLab.com](#) (no login needed)
- [More information about GitLab.com](#)
- [GitLab Community Forum](#)
- [GitLab Homepage](#)

By signing up for and by signing in to this service you accept our:

- [Privacy policy](#)
- [GitLab.com Terms.](#)

Sign in | **Register**

Username or email

Password

☐ Remember me | [Forgot your password?](#)

Sign in

Sign in with

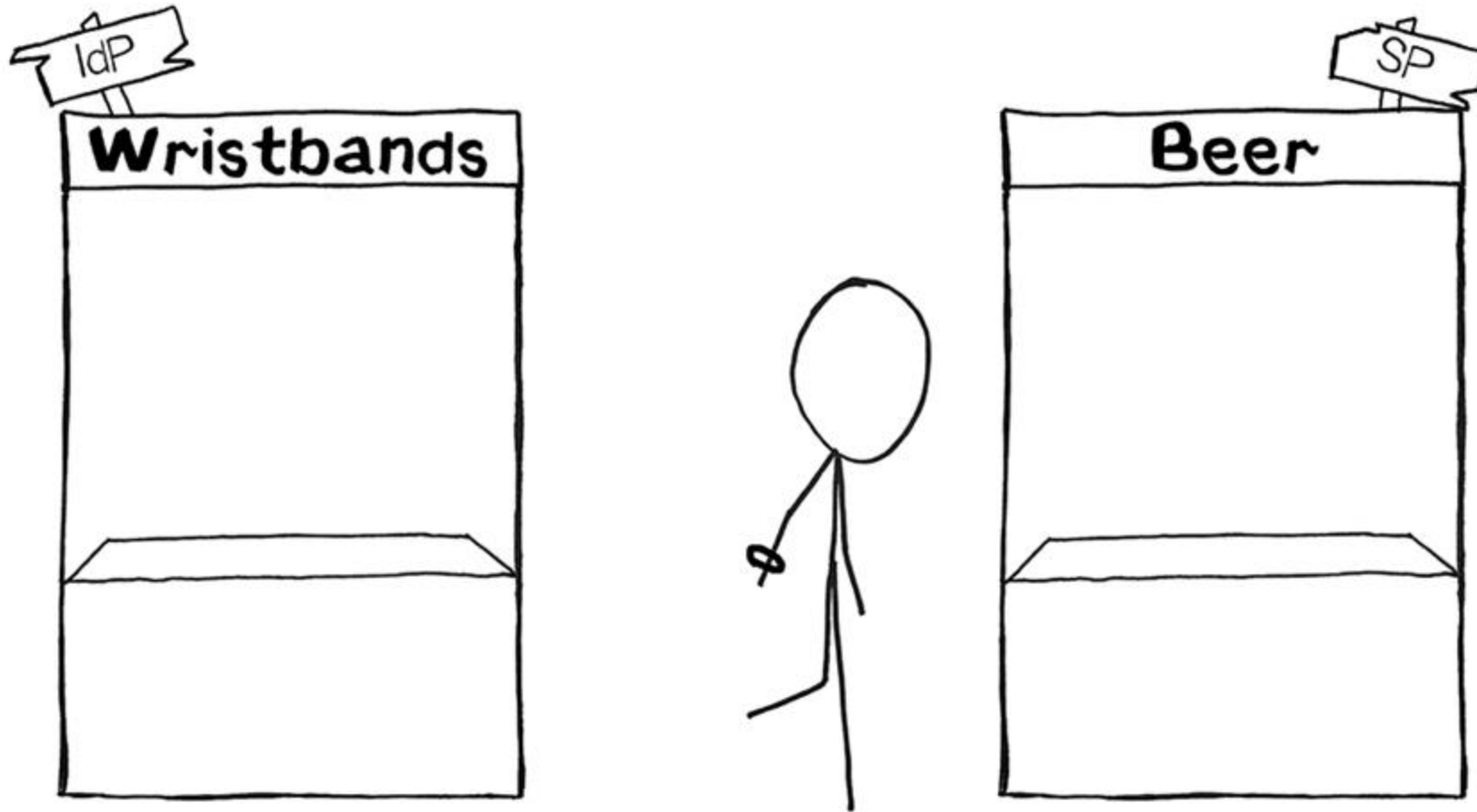
Google | GitHub

Twitter | Bitbucket

Salesforce

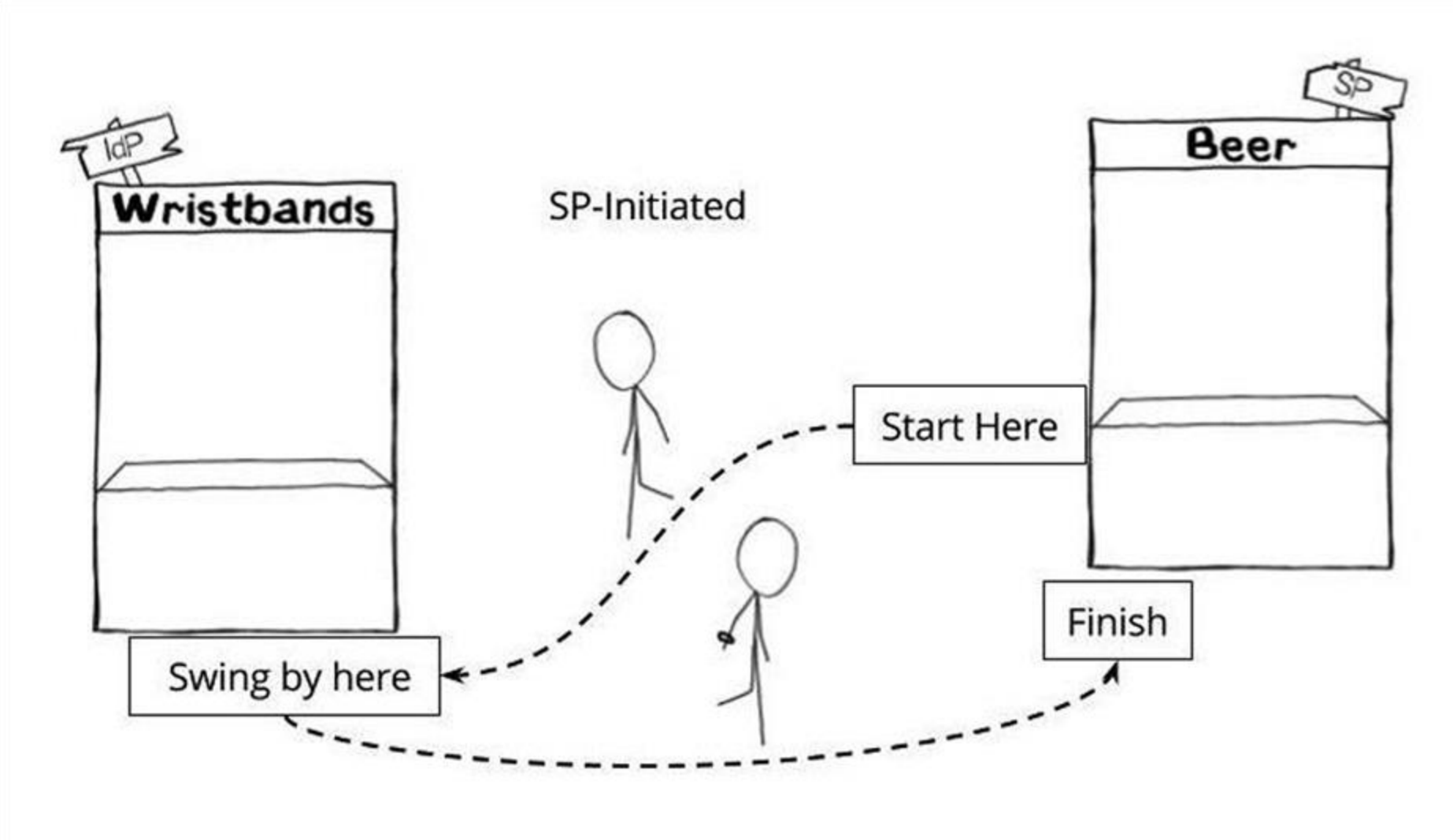
☐ Remember me

Example in real life: Beer as a Service



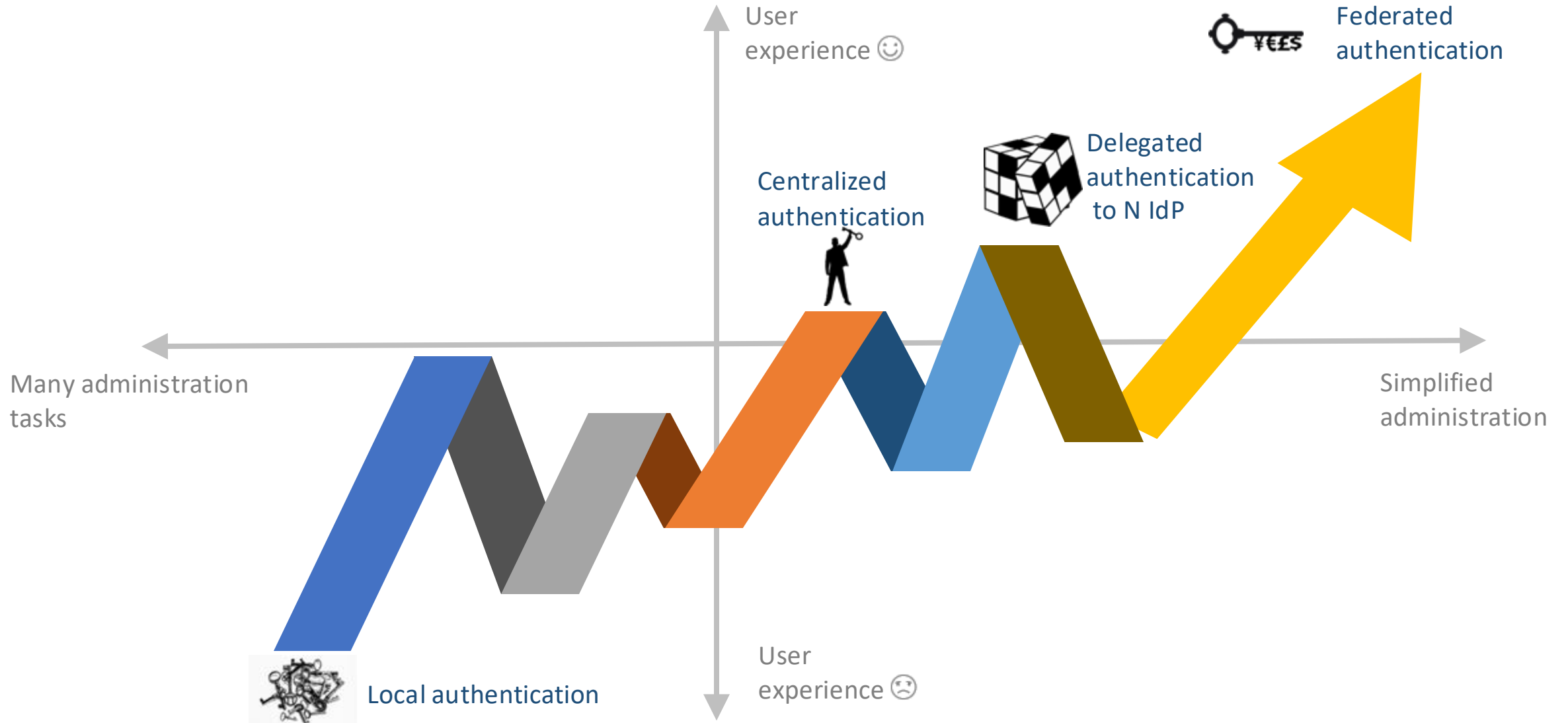
Crédit: <https://duo.com/blog/the-beer-drinkers-guide-to-saml>

Example in real life: Beer as a Service



Crédit: <https://duo.com/blog/the-beer-drinkers-guide-to-saml>

Different levels of Identity Management



Identity Federations are made of entities



Identity Provider (IdP) ~ Home organization (HO)



Service Provider (SP) ~ Relying Party (RP)

Discovery Service (DS)

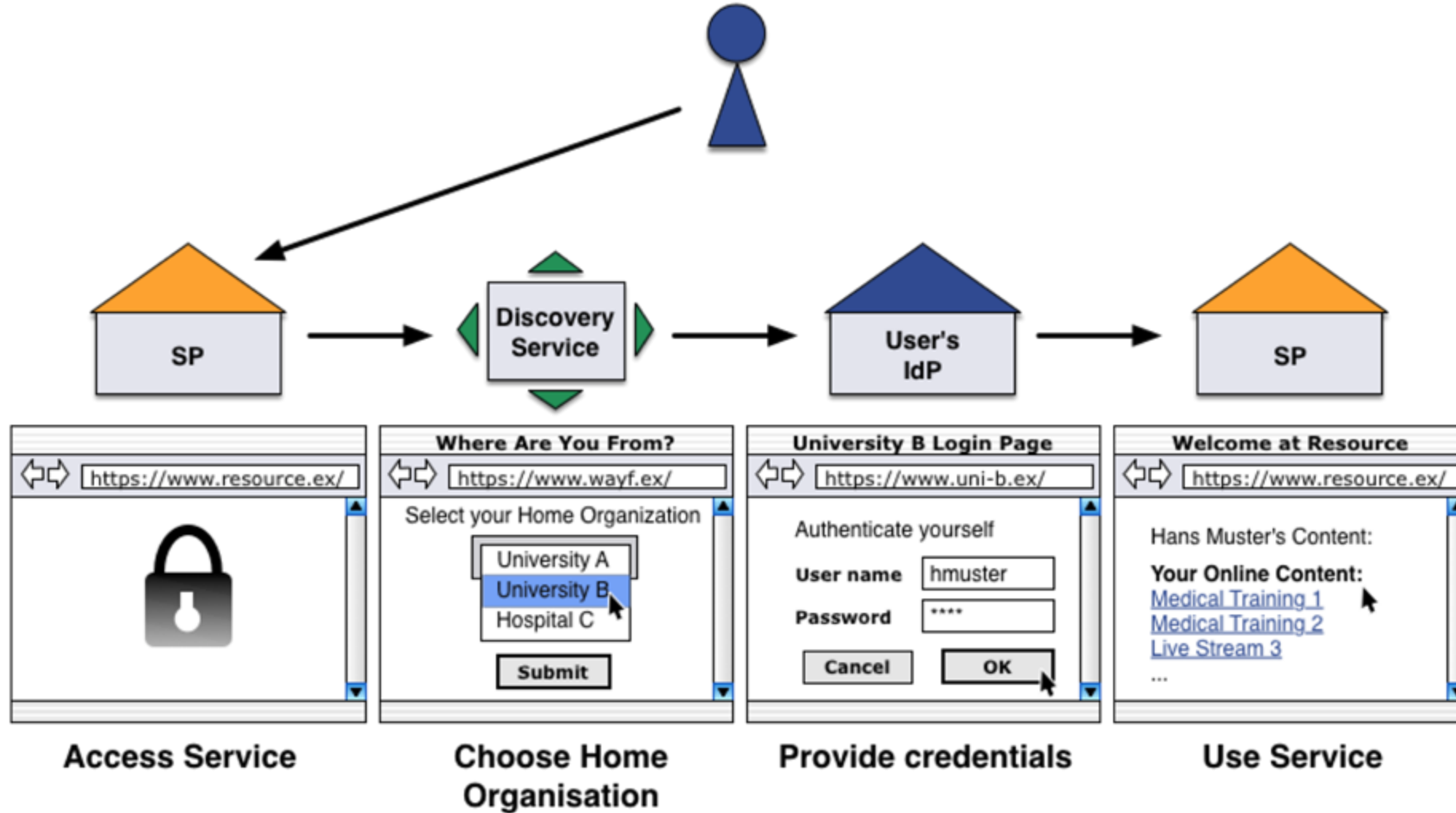
Identity Providers and Service Providers are collectively called **entities**

Identity Federations are built on trust



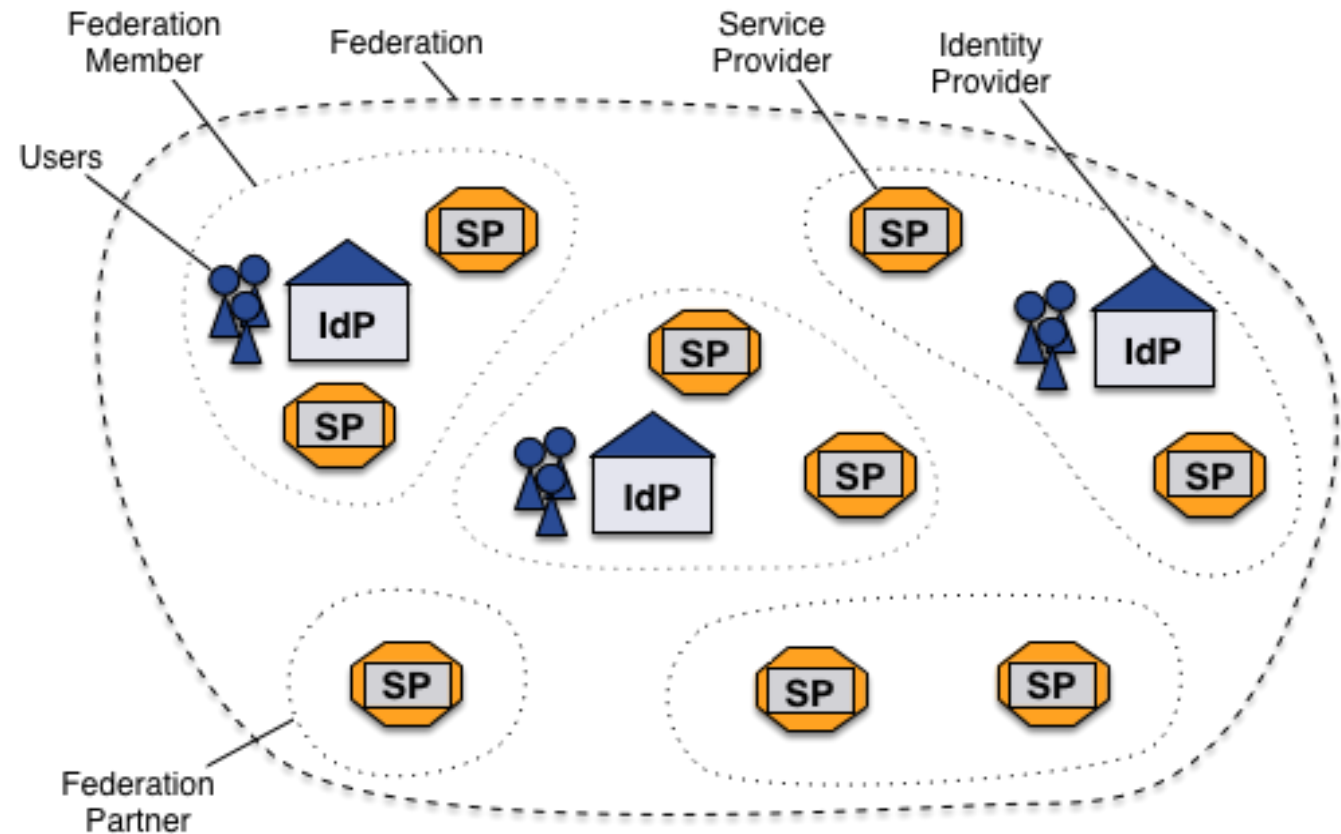
- Use of a protocol (SAML, OIDC, CAS, etc.)
- Trust can be built in several ways:
 - Via agreement between SP/IdP administrators (bilateral relationship)
 - Via a trusted third party (federation)

A simple authentication flow



What is an Identity Federation?

An Identity Federation is a collection of organizations that agree to interoperate under a certain rule set.



What do Identity Federations do?

- Maintain the list of entities
- Define policies, rules and legal frameworks
- Operate a central Discovery Service and test infrastructure
- Provide self-service Registry
- Provide hosted entities
- Provide tools for guest access
- Developing custom tools for the community
- Guidelines and deployment instructions to operate services in the federation
- Helpdesk to assist with deploying services and debugging issues
- Workshops and Trainings

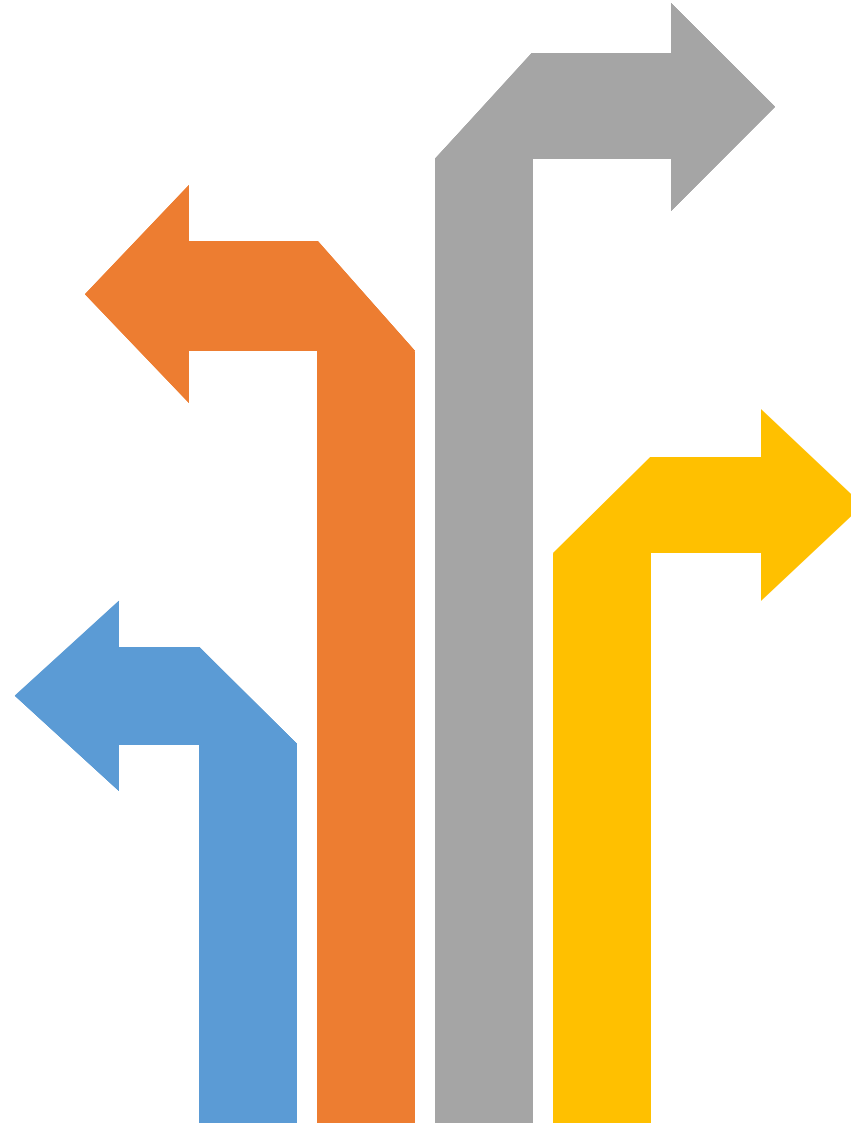
A Federation Operator is an organization that operates an identity federation.



Benefits that the Federated Identity Management brings

Provides current data

Minimizes attack
surface area



Reduces work

Insulates from
compromised service

Interoperability

Technical

- Supported protocols
- User authentication mechanisms
- User attribute specifications
- Accepted X.509 server certificates



Legal

- Membership agreement or contract
- Federation operation policies
- Requirements on identity management practices



Others

- Common/best operational practices

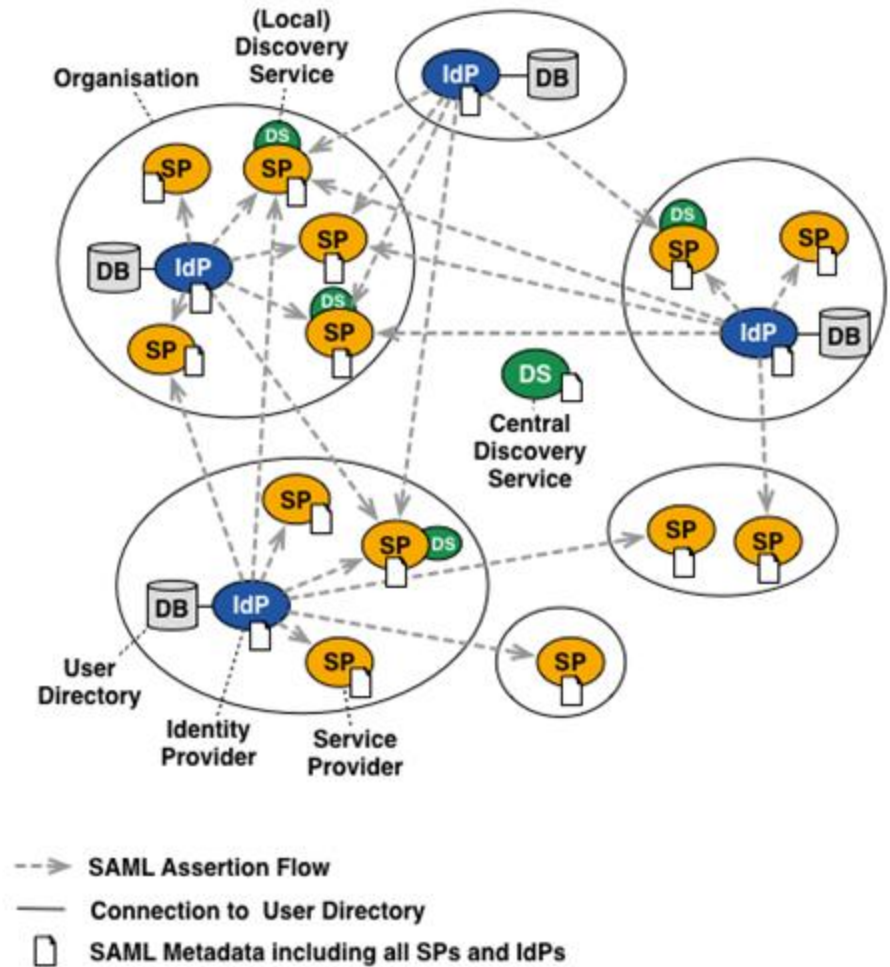


Common Identity Federation Architectures

- Full mesh federations
- Hub & Spoke with distributed login
- Hub & Spoke with central login

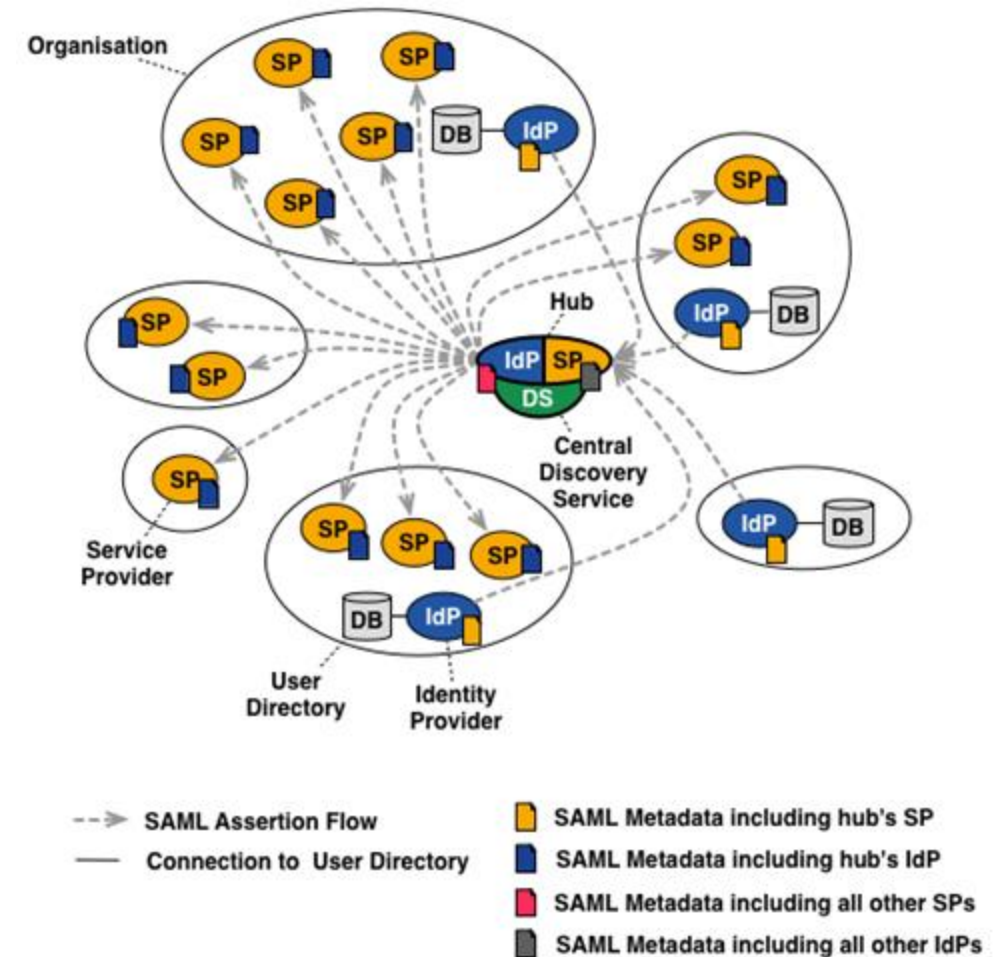
Full Mesh Identity Federation

- Entities are distributed
- There is no need for a central component



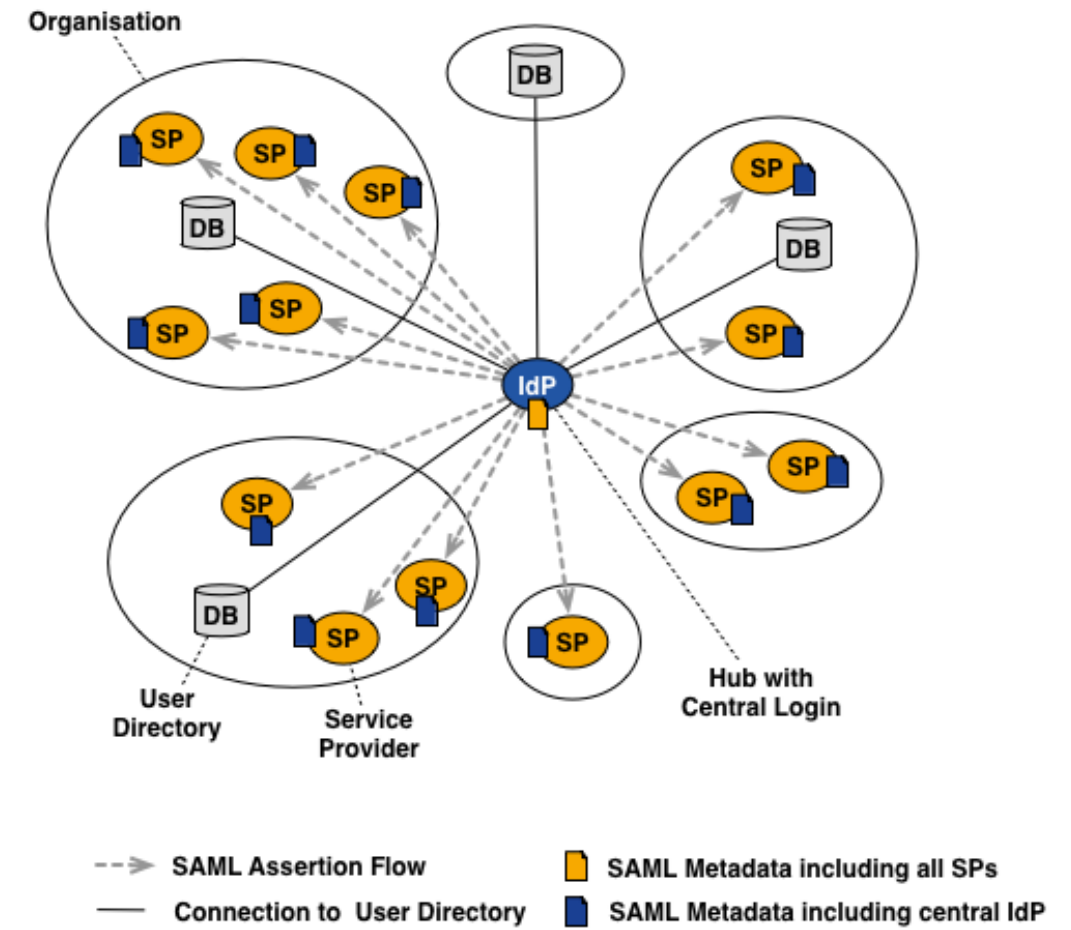
Hub-and-Spoke Identity Federation with distributed login

- Central hub: an SP for IdPs, an IdP for SPs
- Each organization still operates their own Identity Provider
- Central hub = Central Discovery Service

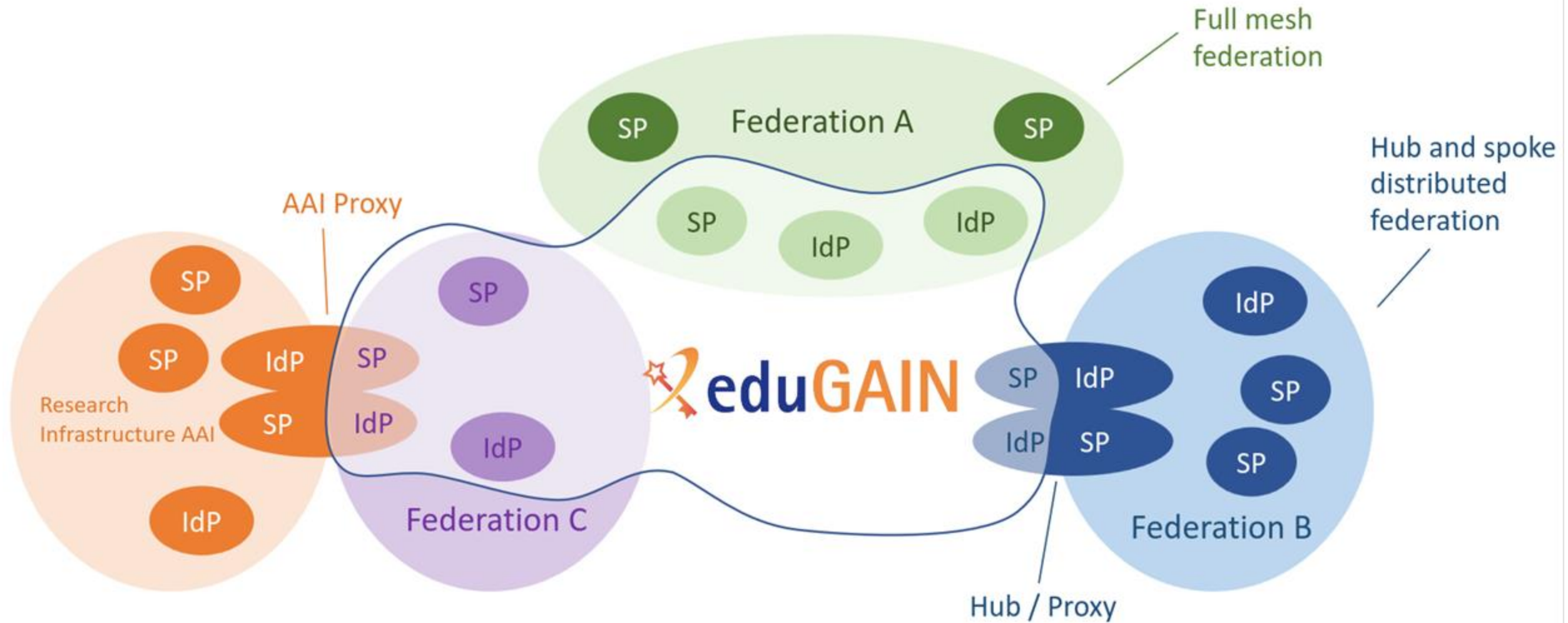


Hub & Spoke Identity Federation with central login

- A special case in the sense as there is only one single Identity Provider in the federation



eduGAIN is interfederation





Thank You

www.geant.org



Co-funded by
the European Union