SEE Identity Federation Training

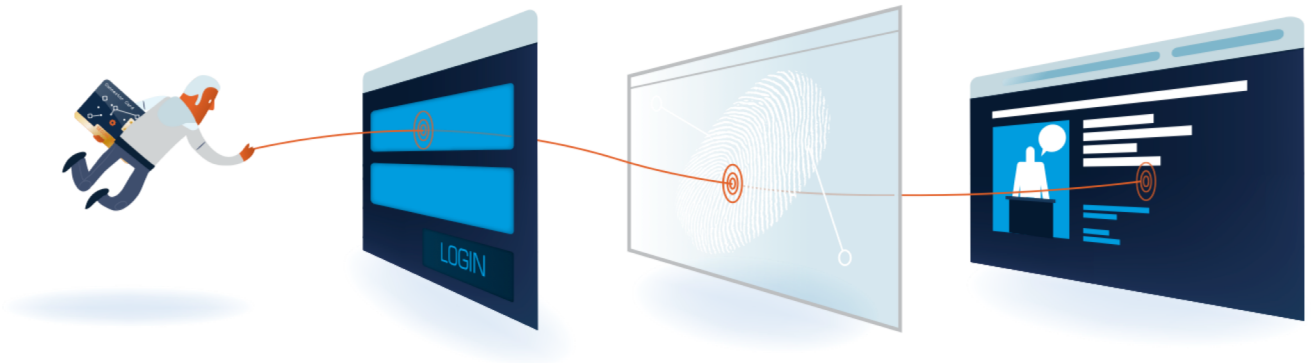
Introduction to Federated Identity Management

April 1st , 2021

Slides v1.0

www.geant.org

Learning Objectives



What is Federated Identity Management?

What is a Federation?
- Full mesh example
- Hub and spoke federation example
- eduroam example

What is Interfederation?
- eduGAIN example
- Positioning Federation as a Service

Evolution of Identity Management

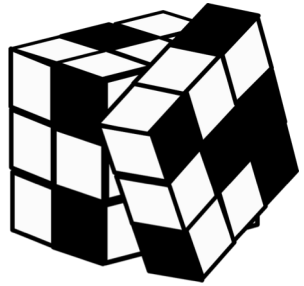
				
Primordial Soup • Nothing yet!	Stone Age • Application holds all info	Bronze Age • Centralised credential e.g. LDAP • Identity in app	Iron Age • Central credentials and Identity • App only has specific user data	Diamond Age • Federated Identity • Share information outside one domain

Different levels of identity management

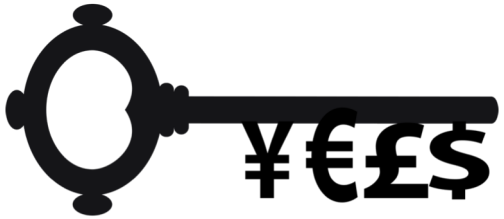
- Local authentication

- Centralized or delegated authentication to 1 Identity Provider

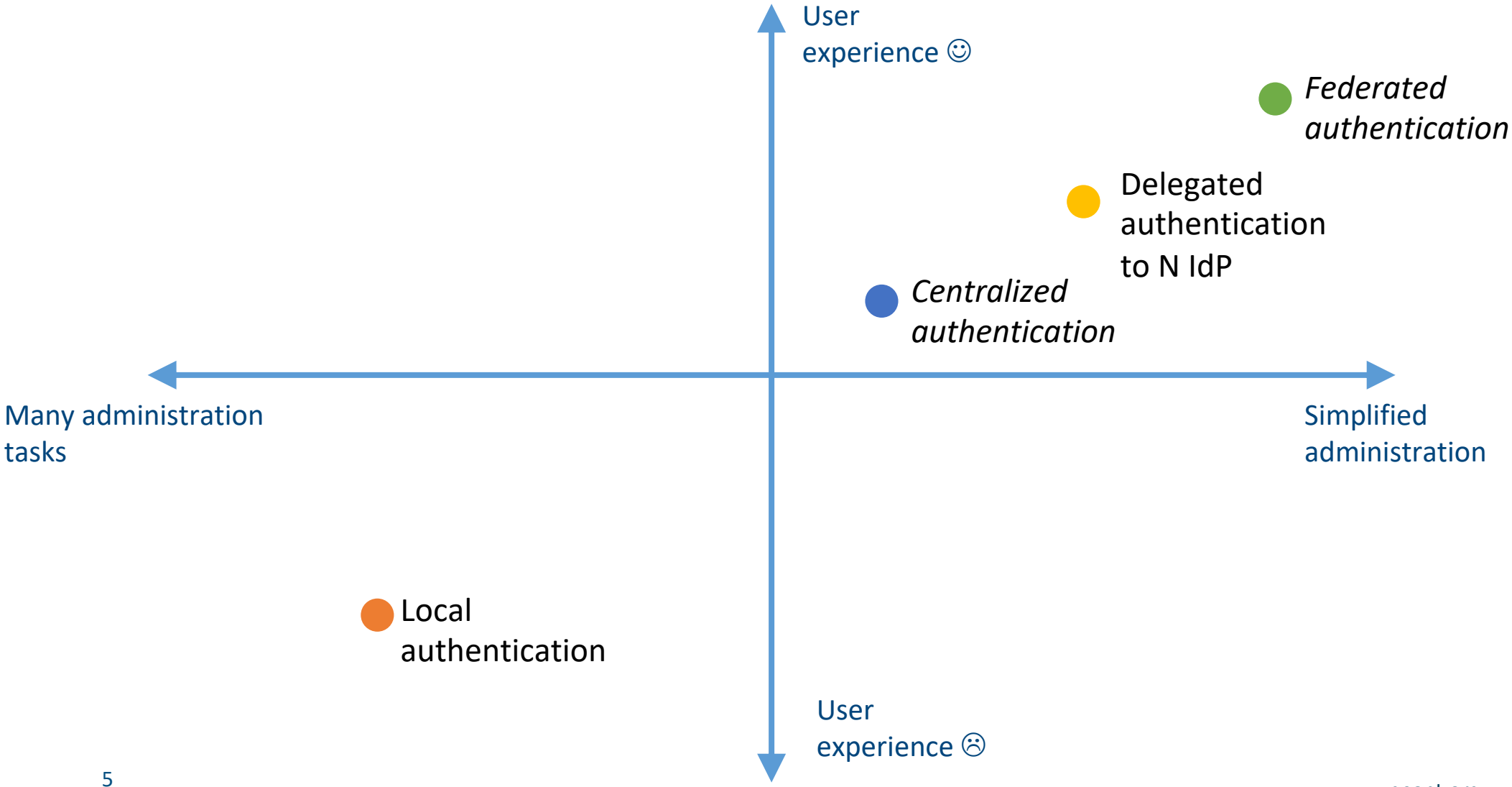
- Delegated authentication to N identity providers



- Federated authentication



Comparison of the different levels

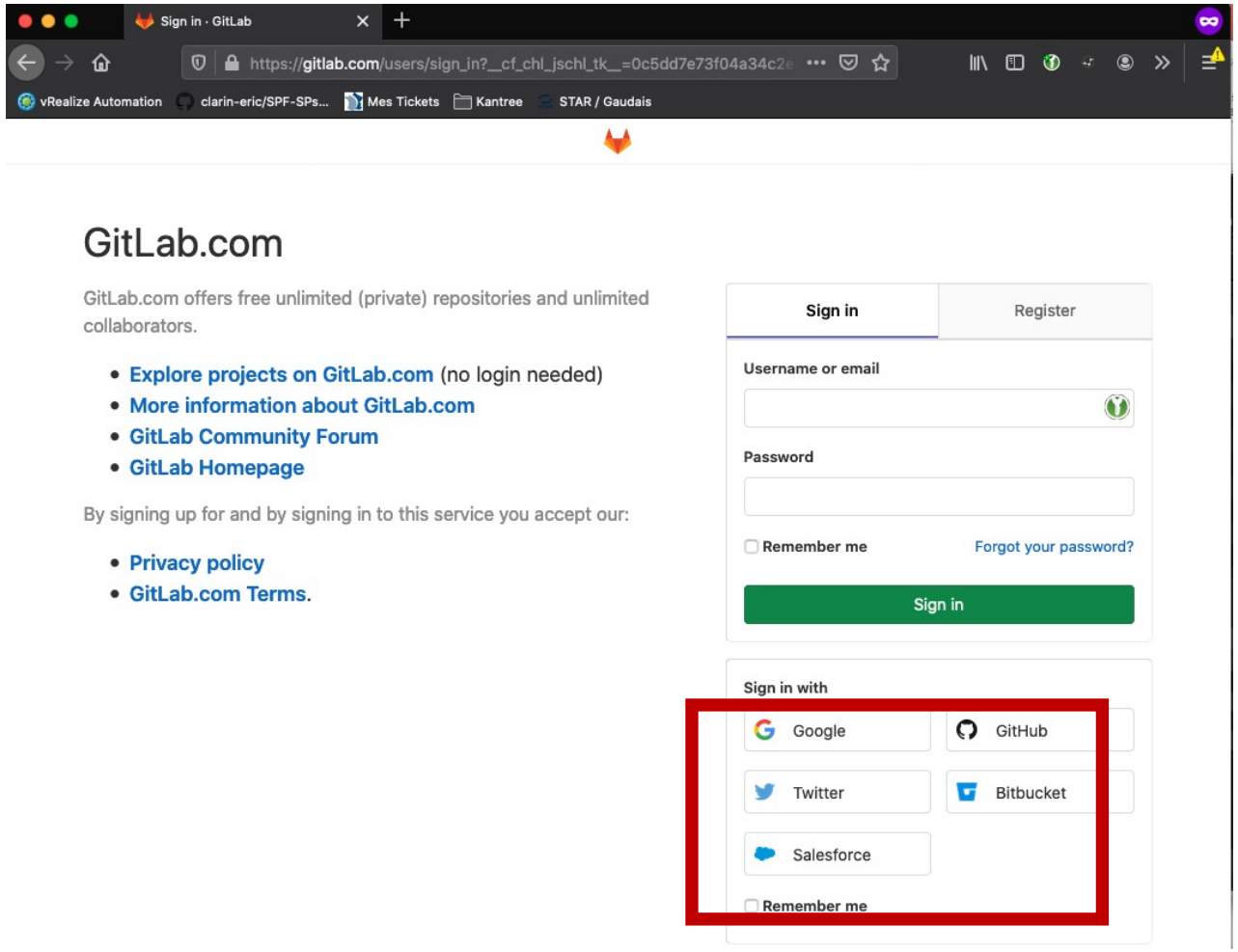


Delegation of authentication

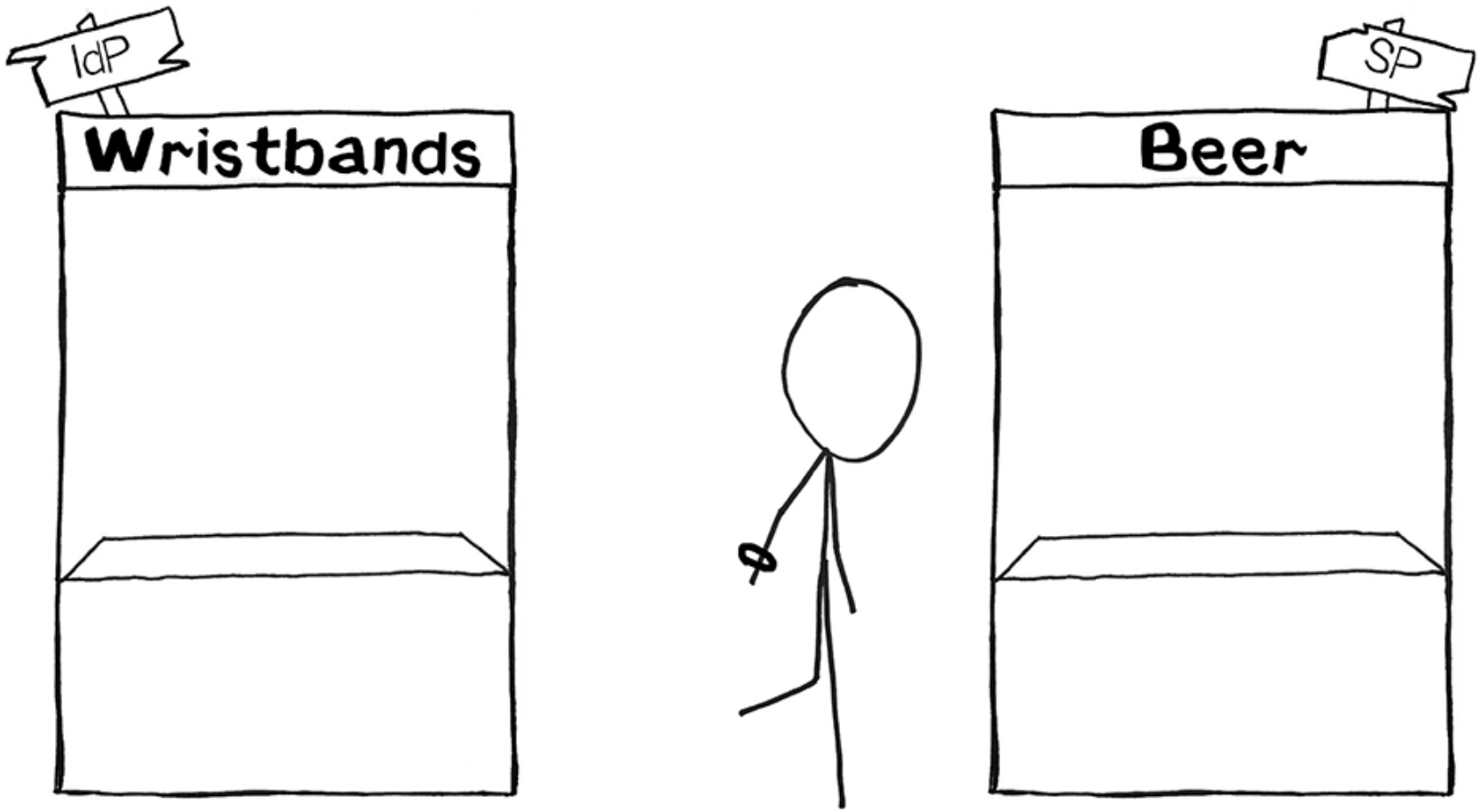
- Before talking about "federation", let's talk about delegation of authentication

Why and How ?

Example

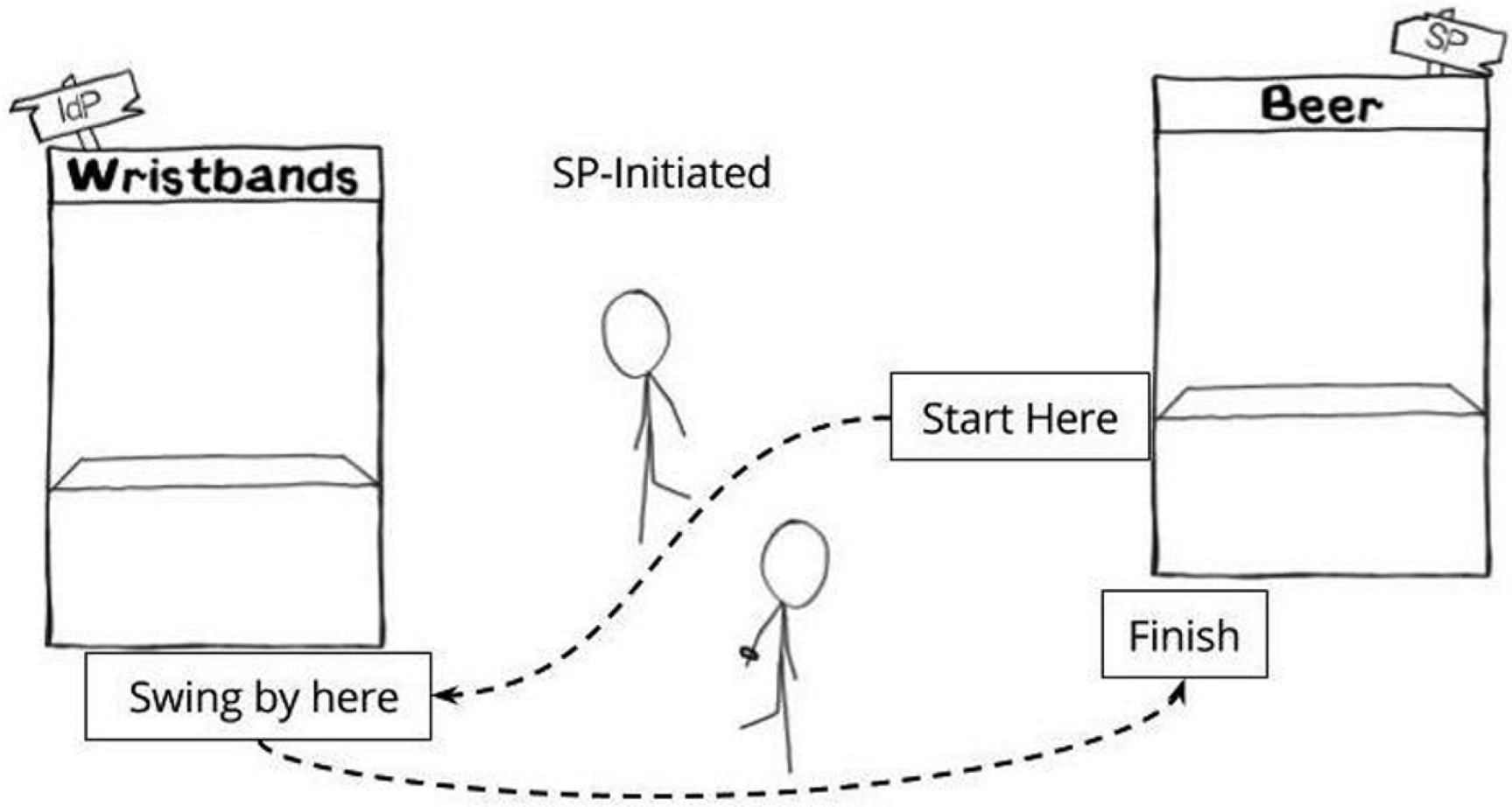

Sign in · GitLab
https://gitlab.com/users/sign_in?__cf_chl_jschl_tk__=0c5dd7e73f04a34c2e
vRealize Automation
clarin-eric/SPF-SPs...
Mes Tickets
Kantree
STAR / Gaudais
GitLab.com
GitLab.com offers free unlimited (private) repositories and unlimited collaborators.
Explore projects on GitLab.com (no login 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



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

Example in real life



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

How to delegate the authentication ?

- Use of a protocol (SAML, OIDC, CAS ...)

- For a SP to agree to delegate to an IDP, this IdP must be trusted
- For an IDP to accept authentication request from a third party (SP), this SP must be trusted

- Trust can be built in several ways:
  - Via agreement between SP / IDP administrators (bilateral relationship)
  - Via a trusted third party (federation)

Identity Management concepts

Identity management is the organizational process for identifying, authenticating and authorizing individuals or groups of people to have access to services, by associating user rights and restrictions with established identities.

- **Authentication:** Process of confirming an identity
- **Authorization:** Process of confirming access rights to a specific service (access control)

Identity Management concepts

- **Attributes:** Information about users, for example: name, email address ...
  They are used for:
  - **Identification:** Is subject the same as last time
  - **Authorization:** Access decision based on attribute values,Identity or Role based access control
  - **Profile data:** Personalization, identification “for humans”, name,email address, etc.

Federated Identity

Identity Provider (IdP) asserts authentication and identity information about users.

Home organisation (HO) a related term

Service Providers (SP) check and consume this information for authorization and make it available to an application

Relying Party (RP) a related term

Identity Providers and Service Providers are collectively called entities

Federated Identity

- In Federated Identity Management:
  - **Authentication** takes place where the user is known, the Identity Provider (IdP) publishes authentication and identity information about its users.
  - **Authorization** happens on the service's side, where the Service Provider (SP) consumes and relies on the information provided by the IdP, then make it available to the application that can as well authorize the user based on his profile for example.
  - **Metadata:** The Metadata providers the technical trust between IdPs ans SPs ! It is only and XML file based on SAML standards that define its layout and contents.

Federated Identity

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

Protect the user's credentials - *only the IdP ever handles the credential*

Protect the user's identity information, including identifier - *customized set of information released to each SP*

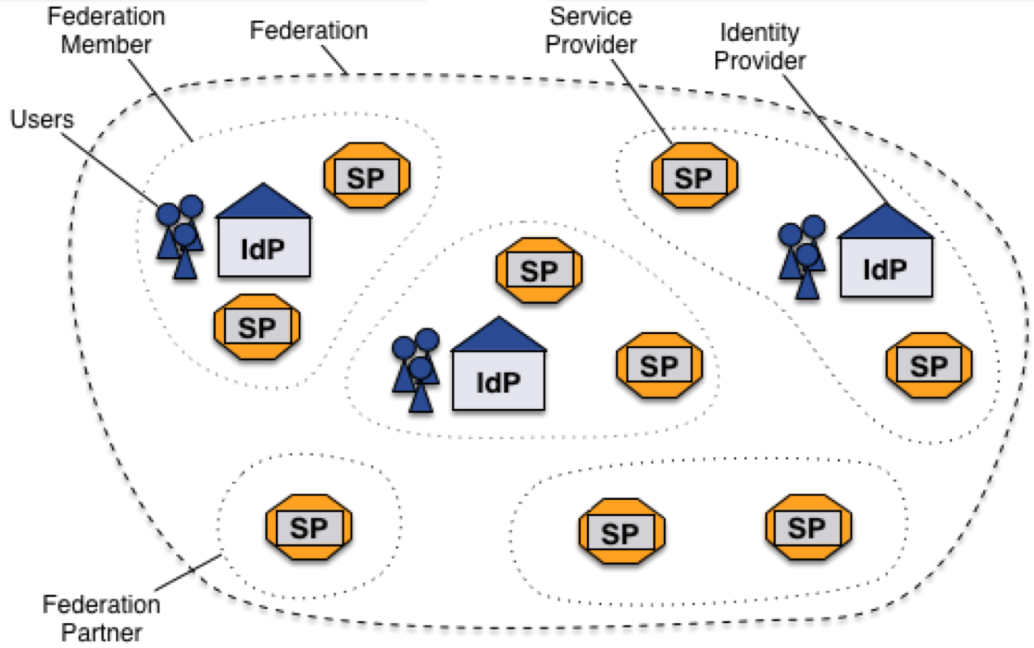
Benefits/Compelling Reason to Act

Reduces work	• Authentication-related calls to Penn State University's helpdesk dropped by 85% after they installed Shibboleth
Provides current 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	• In FIM data is pushed to services as needed. If those services are compromised the attacker can't get everyone's data.
Minimize attack surface area	• Only the IdP needs to be able to contact user data stores. All effort can be focused on securing this one connection instead of one or more connections per service.

What is a Federation?

A group of organizations running IdPs and SPs that agree on a common set of rules and standards

The grouping can be on a regional level or on a smaller scale (e.g. large campus)



IdPs and SPs "know" nothing about federations
They read metadata!

An organization may belong to more than one federation at a time

What do Federations do?

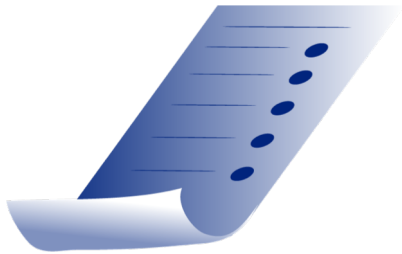
At a minimum a federation maintains the list of which IdPs and SPs are in the federation

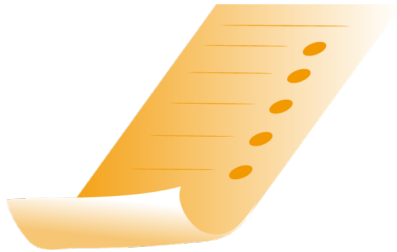
Most federations also
- Define agreements, rules, and policies
- Provide some user support (documentation, email list, etc.)
- Operate a central discovery service and test infrastructure

Some federations
- Provide self-service tools for managing IdP and SP data (Resource Registry)
- Provide application integration support
- Host or help with outsourced IdPs (IdP in the Cloud, hosted IdP
- Provide tools for managing "guest" users
- Develop custom tools for the community

Federation Rules?

Technical Interoperability	Legal Interoperability	Others
• Supported protocols • User authentication mechanisms • User attribute specifications • Accepted X.509 server certificates	• Membership agreement or contract • Federation operation policies • Requirements on identity management practices	• Common/best operational practices



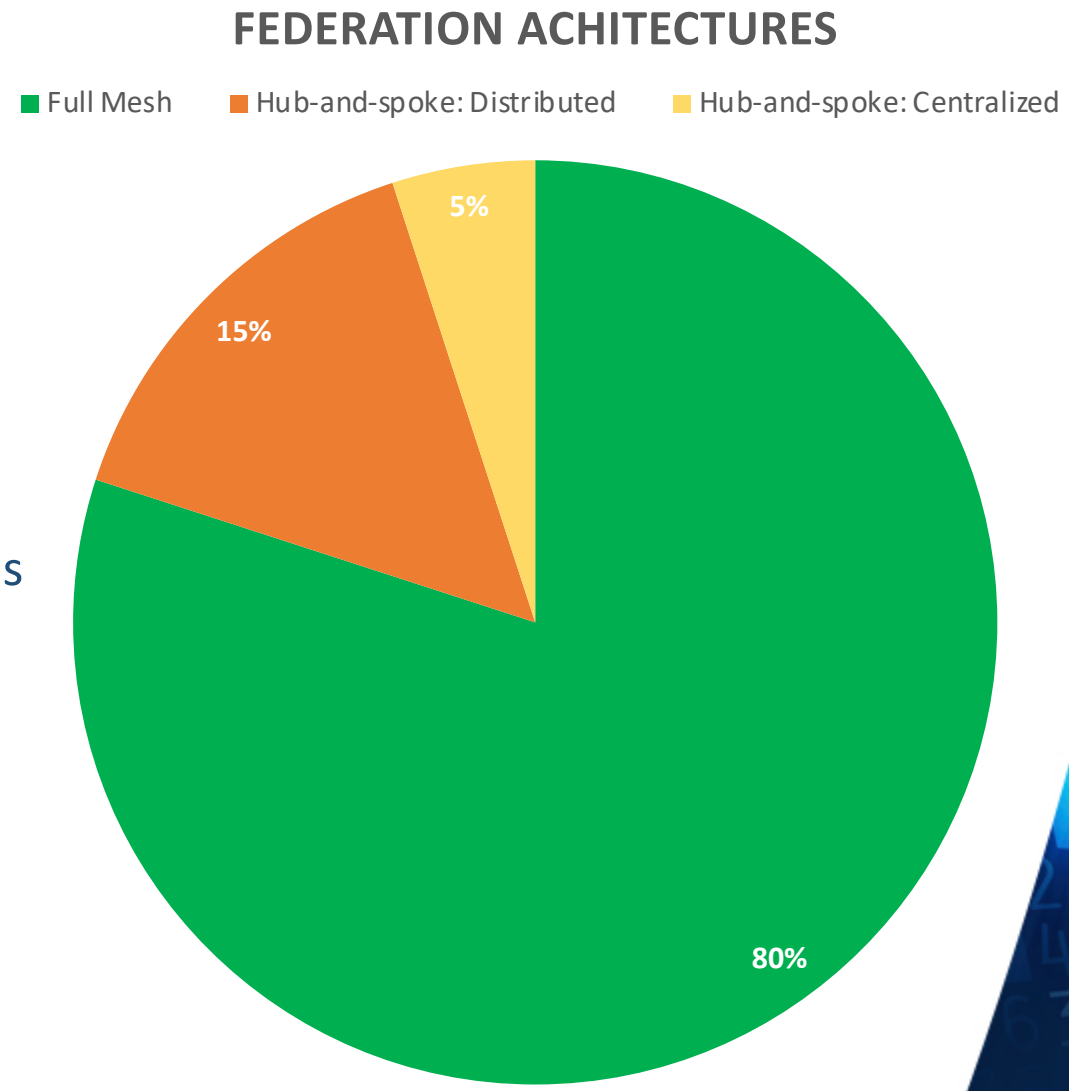


Common Federation Architectures

Full Mesh: Full mesh federations are the most common and straight forward to implement federations because everything is distributed and there is no need for a central component that has to be protected specifically against failover.

Hub-and-spoke Distributed: Hub & Spoke federations with distributed login rely on a central hub or proxy via which all SAML assertions are sent.

Hub & Spoke Centralized: Hub & Spoke federations with central login are a special case in the sense as there is only one single Identity Provider in the federation.

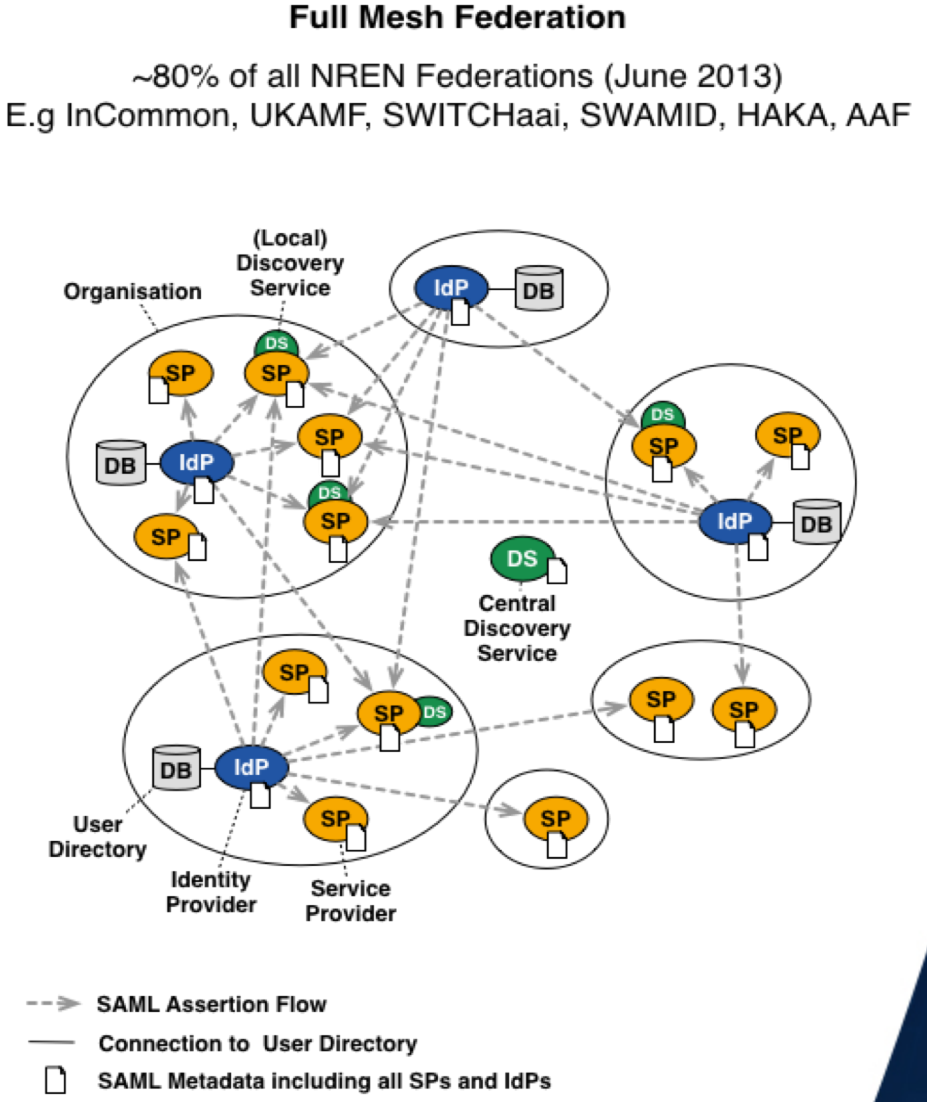


Full Mesh Federation

Full mesh federations are the most common and straight forward to implement federations because everything is distributed and there is **no need for a central component** that has to be protected specifically against failover (that duty is distributed as well).

Every organisation in mesh federations (IdP) connected to a local user data **operates their own Identity Provider** base and an arbitrary number of Service Providers (SP).

All these **entities are listed in a centrally distributed SAML metadata file**, which is consumed by all entities.

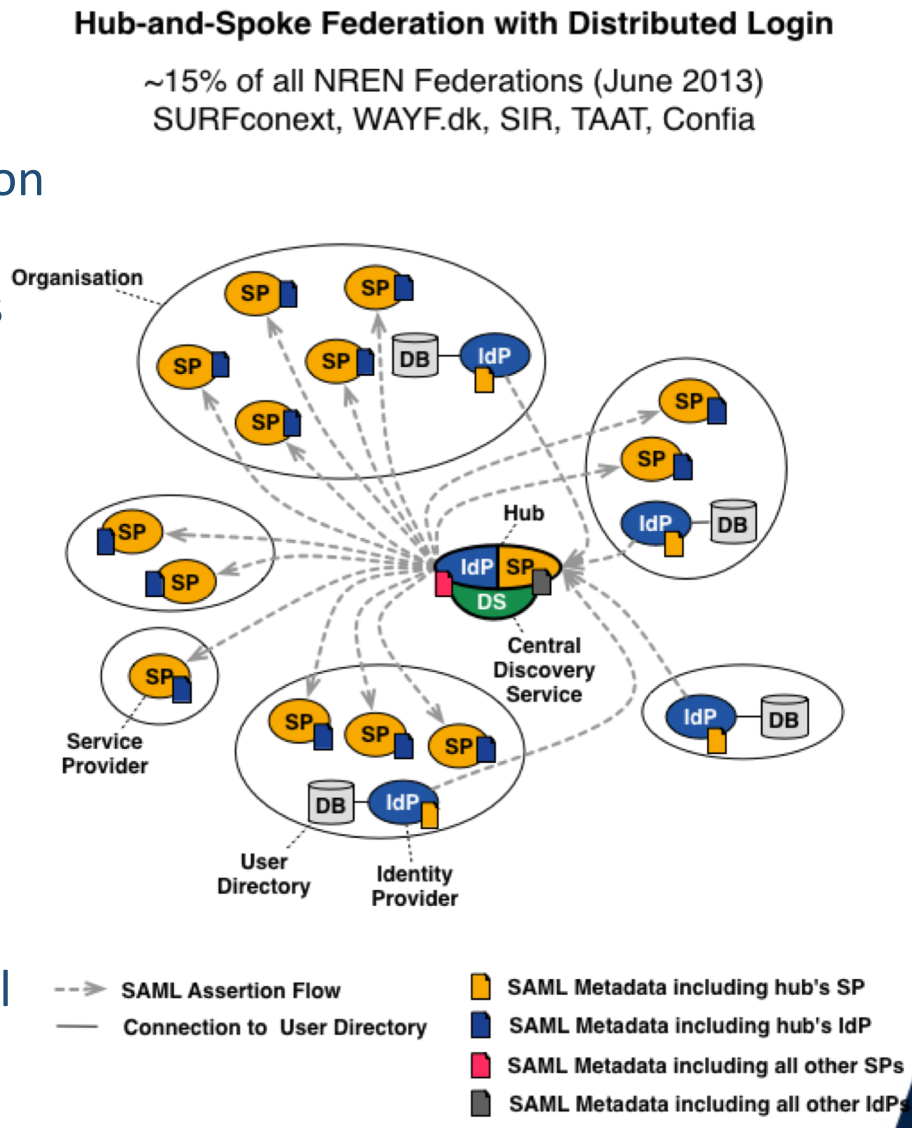


Hub-and-Spoke Federation

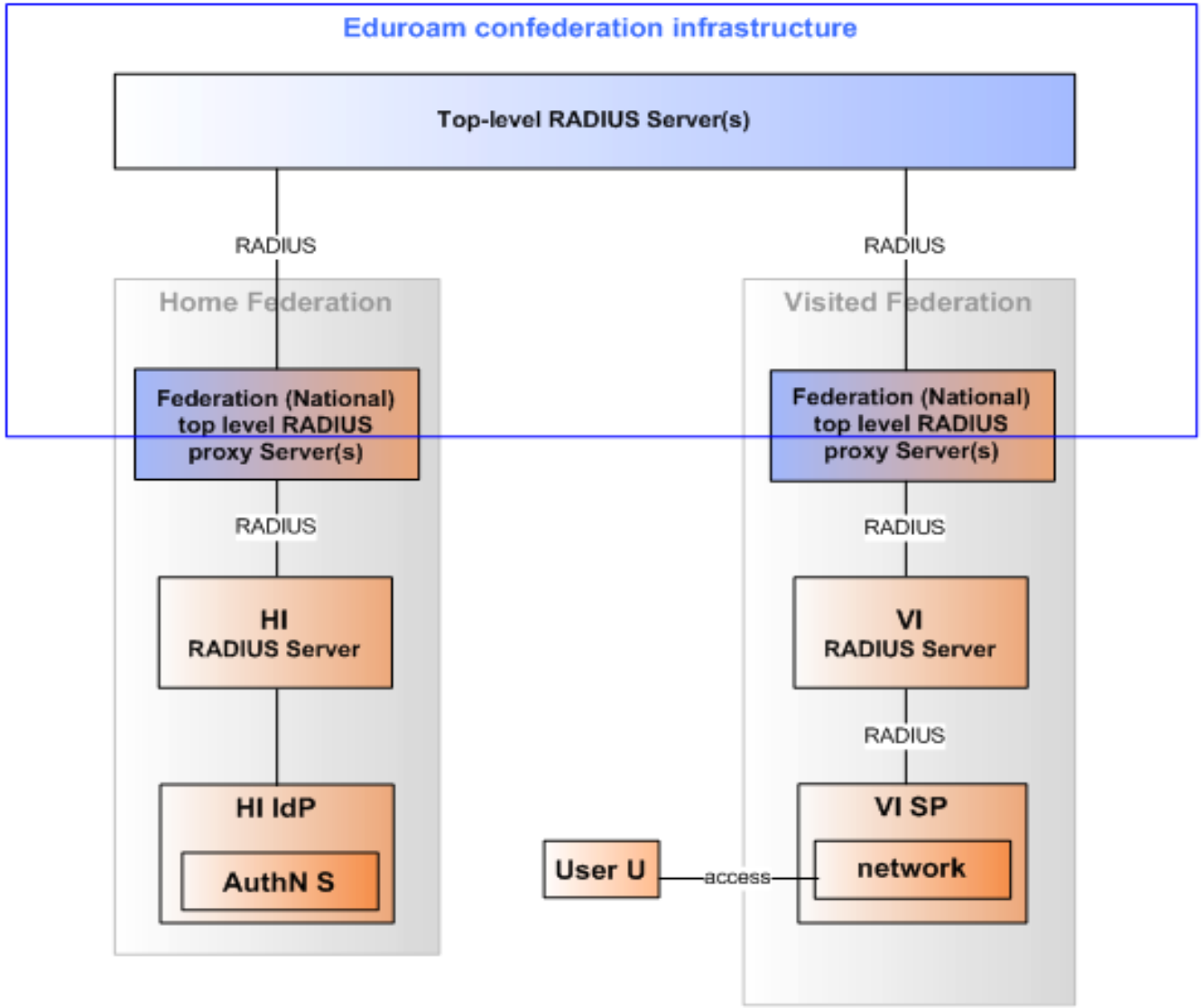
Hub & Spoke federations with distributed login rely on a central hub or proxy via which all SAML assertions are sent. The hub serves as a Service Provider versus the Identity Providers and as an Identity Provider versus the Service Providers in the federation.

Each organisation still operates their own Identity Provider connected to a local user database but the Identity Provider only needs metadata of the hub. Vice versa the Service Providers only need metadata for the hub.

On the hub there is a central Discovery Service for all users. Because the hub is a single-point of failure, it has to be carefully secured and protected.



Other technology example - eduroam



- HI = Home Institution
- VI = Visited Institution
- IdP = Identity Provider
- SP = Service Provider

Interfederation

- Interconnecting national federations
- eduGAIN → Interfederation, eduroam → Confederation

No longer a single legal or policy framework
Each federation has its own eduGAIN has one as well

Different sets of attributes used internationally

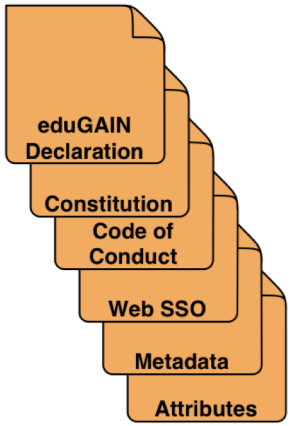
No single 'interfederation helpdesk' in case of problems
Debugging involves probably more parties
Involved parties will generally know less about each other

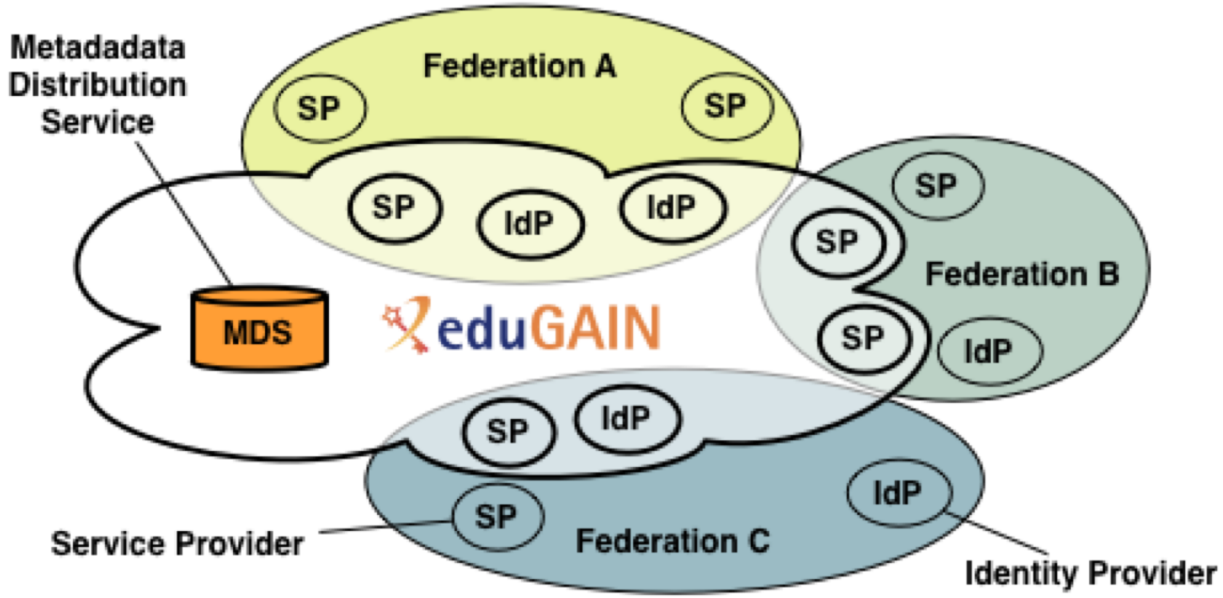
eduGAIN Example

eduGAIN provides policy framework and standards to build trust

SPs and IdPs of participating federations **opt-in** for eduGAIN
- Various local processes for what this means
- Opt out being piloted by some

MDS fetches, aggregates and republishes metadata



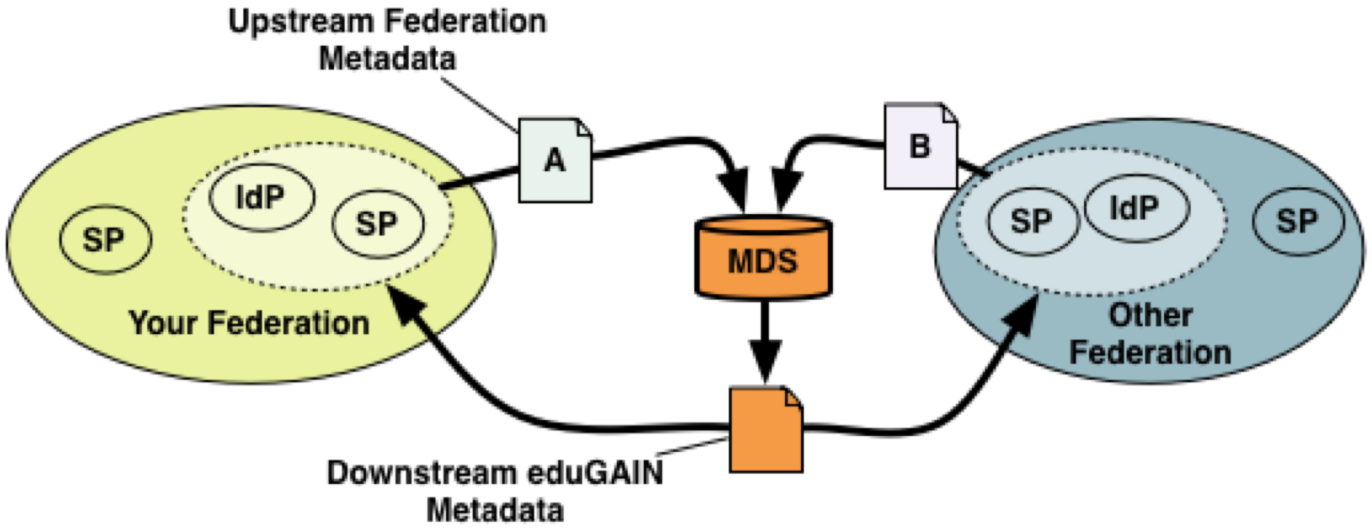


Metadata Exchange for eduGAIN

Each Federation publishes a Metadata file with the entities that want to interfederate.

The eduGAIN Metadata Data Service fetches them

eduGAIN MDS aggregates all metadata and republishes it



Federations fetch it and filter-out their own entities

Entities consume the filtered eduGAIN metadata file
in addition to the one from the federation

eduGAIN Constitution and Policy

Governance and Governing Bodies

- eduGAIN Executive Committee (eEC)
- eduGAIN Steering Group (eSG)
- Operational Team (OT)

Participant Federations MUST:

- Primarily serve the interests of the education and research sector.
- Provide a point of contact for their Members for dealing with technical issues.
- Provide processes for handling complaints and incidents involving their Members.
- Have a published Metadata registration practice statement.
- Follow the eduGAIN SAML 2.0 Metadata Profile

No express right of communication

- For an Entity registered in an eduGAIN Participant Federation it does not imply any right of communication with any other Entity exchanged through eduGAIN.

GÉANT
Networks • Services • People

Thank you

Any questions?

www.geant.org

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).