Multilateral Federations

Why we've built research and education identity federations and how they differ from enterprise federations

Davide Vaghetti <davide.vaghetti@garr.it>

CNAF, Bologna 26/01/2024

Agenda

- Authentication: Local, Centralized, Single Sign On
- Federated Authentication
- Research and Education Identity Federations
- R&E federated identity standards
- AARC Blueprint Architecture

Single Sign On

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

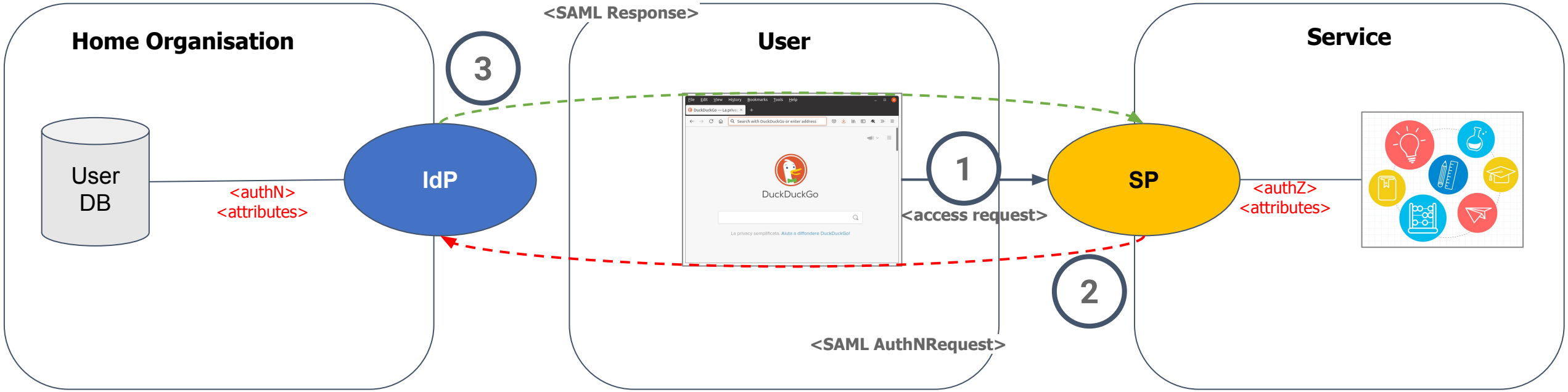
Diamond Age

- Federated Identity
- Share information outside one domain

Local, Centralized and SSO identity management

	Local	Centralized	Single Sign On
Users	Each application has its own user database.	One database or directory for the entire organization.	Users' database and authentication systems are separated.
Credentials	Each application assigns a set of credentials to its users.	Applications collect user's credentials and send them to centralized systems for authentication.	Applications access and authentication are completely decoupled. Credentials are managed only by the SSO system.

Federated Authentication in action

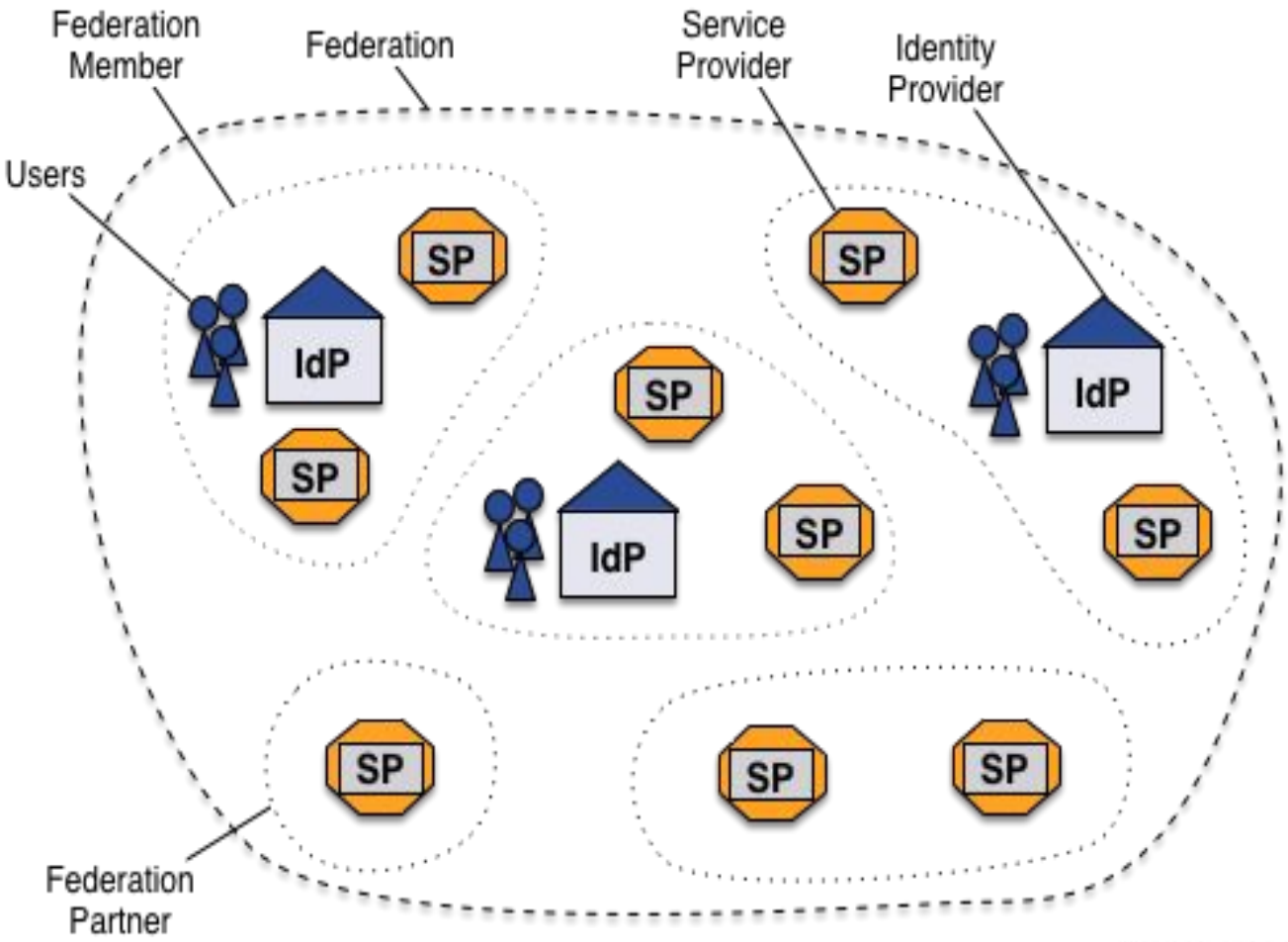


Identity Federation

An identity federation is a collection of organizations that agree to interoperate under a certain rule set.

This rule set typically consists of **legal frameworks**, **policies** and **technical profiles** and standards.

It provides the necessary **trust** and **security** to exchange home organizations' **identity** information to **access services** within the federation.



Identity Provider, Service Provider, Discovery Service

Identity Provider

The system component that authenticates a user (e.g. with username and passwords) and issues identity assertions on behalf of the user who wants to access a service protected by a Service Provider.

Service Provider

The system component that evaluates identity assertions from an Identity Provider and uses the information from the assertion for controlling access to protected services.

Discovery Service

The Discovery Service service, also known as "Where Are You From (WAYF)" service, lets the user choose his home institution from a list and then redirects the user to the login page of the selected institution for authentication.

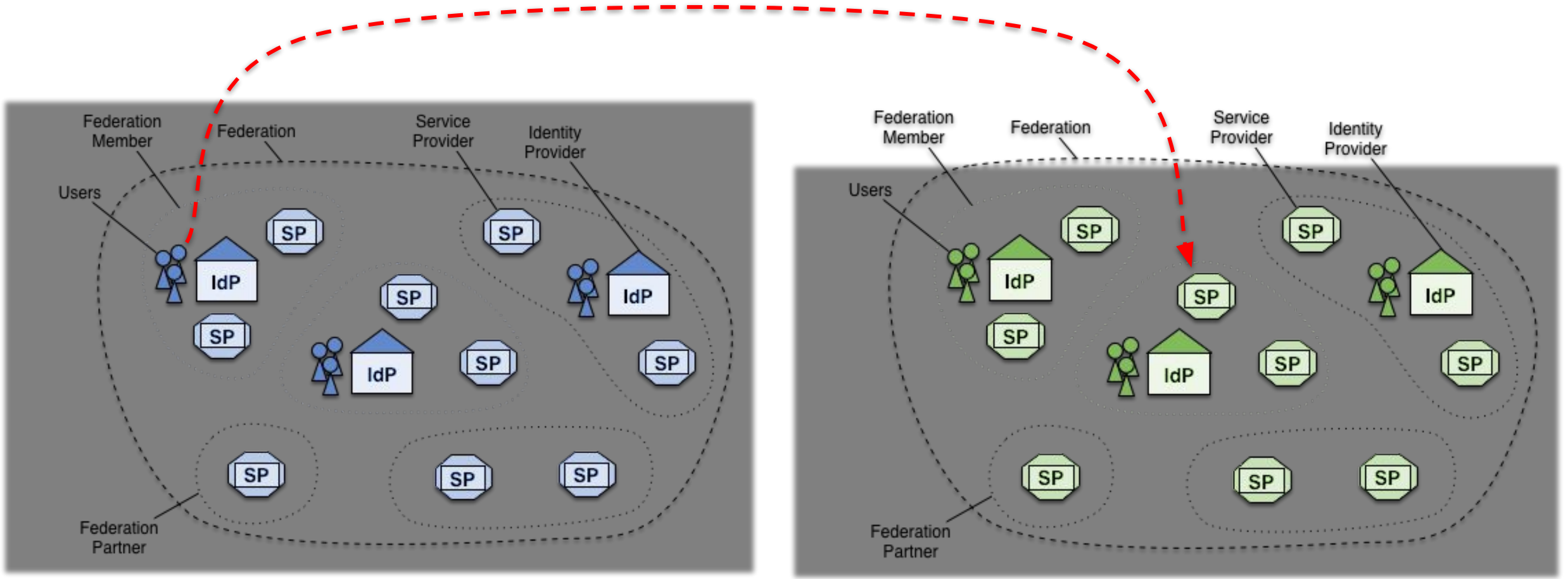
The Federation Operator

The Federation Operator is the **trusted third party** that manages and signs the metadata about the federation entities


```
<?xml version='1.0' encoding='UTF-8'?>
<md:EntityDescriptor
        xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
        xmlns:mdrpi="urn:oasis:names:tc:SAML:metadata:rpi"
        xmlns:mdui="urn:oasis:names:tc:SAML:metadata:ui"
        xmlns:ds="http://www.w3.org/2000/09/xmldsig#" entityID="https://wiki.idem.garr.it/rp" ID="_20240126T080128Z"
validUntil="2024-01-28T08:01:28Z" cacheDuration="PT1H">
        <ds:Signature>
                <ds:SignedInfo>
                        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                        <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
                        <ds:Reference URI="#_20240126T080128Z">
                                <ds:Transforms>
                                        <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                                        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#WithComments"/>
                                </ds:Transforms>
                                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                                <ds:DigestValue>QjwmkEVDQd1b5e/lbuSb3beCjWhg0GwyD6ruoxl0XKA=</ds:DigestValue>
                        </ds:Reference>
                </ds:SignedInfo>
                <ds:SignatureValue>LlR2nhB6nN/5iipkkWPyyypBJDDXSLFnK3zFMNCgOJU6eBrifhUx8vJGmk6aZIS73NwRwHjl4XXyxIcxQDuN/83x9i
uPqs9wz8WLN6kG2VGsKHVMhGisGGaNBliU1jUvvwUxc/Btmmi9/iIsgyRshfEtno34Vapcb8q8eZ+RsUJE57QUzdJYPR9desdHoezO3JXGi3XGn8x
CnHbo4uya1t9JiTUhinovupXlcYIOsEV1p5Bf1gAVUy2j3Md1posyYIf7X+utc5GDaImHRsPhuZRNLnQ2soPm5kJqVaUUsz+NnDHYIinuTHtRAPzfB
Duy+Zg+v8IVPbRqFOCASmmMmjkcs7kqrvPSWFI8aoMcVm0tNafl3/y0UssEi+ljAYEmDz2LDhGwPVOY4OcCS1ifub/o9Y1g/NRHqsPwoMTiPBXR
Nihwr3hbPl6nLOucvpYvwDLl5w4k0gdg+PznHWfLG0AmFsp8Itwaxp2ZBkKIOVOShd76WIJ7zny2SDnMrtmT</ds:SignatureValue>
                <...>
```

*"eduGAIN **interfederation service** connects identity federations around the world, simplifying **access** to content, services and resources for the **global** research and education community"*

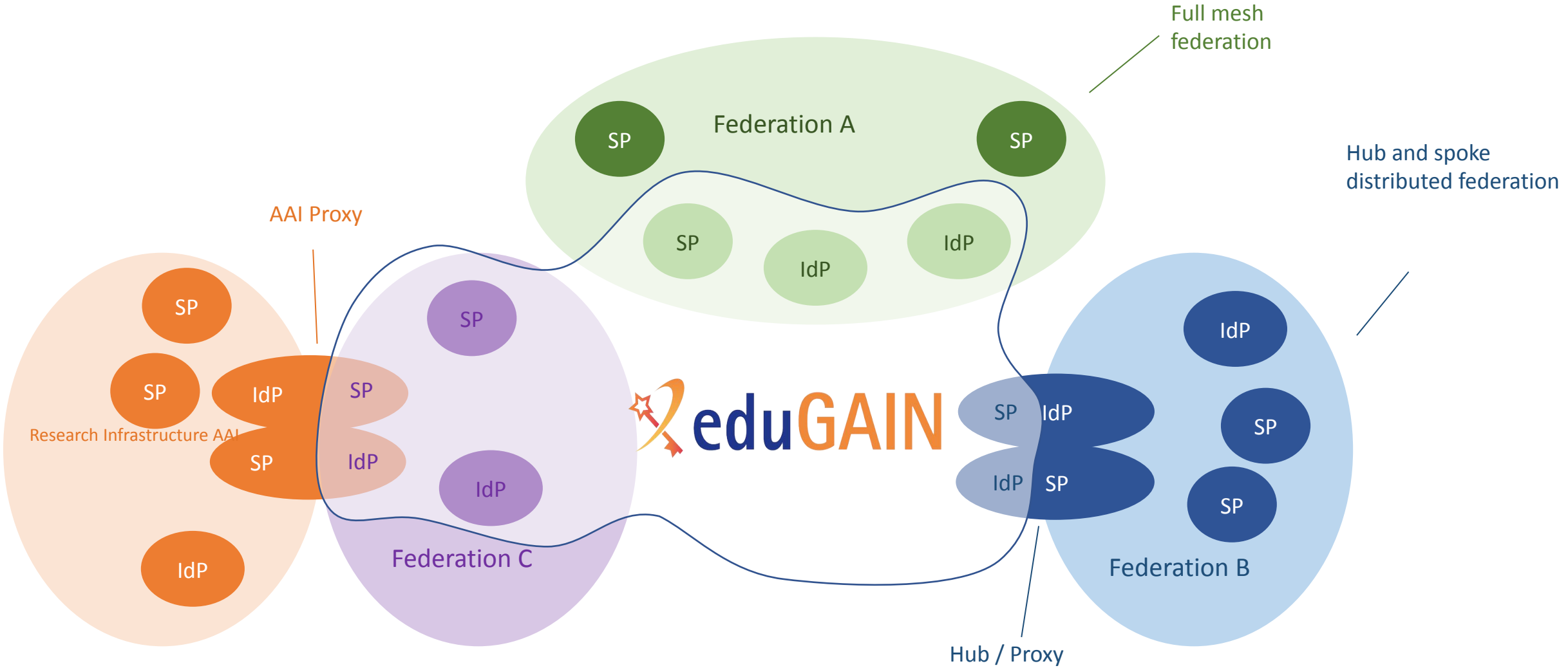
Interfederated access



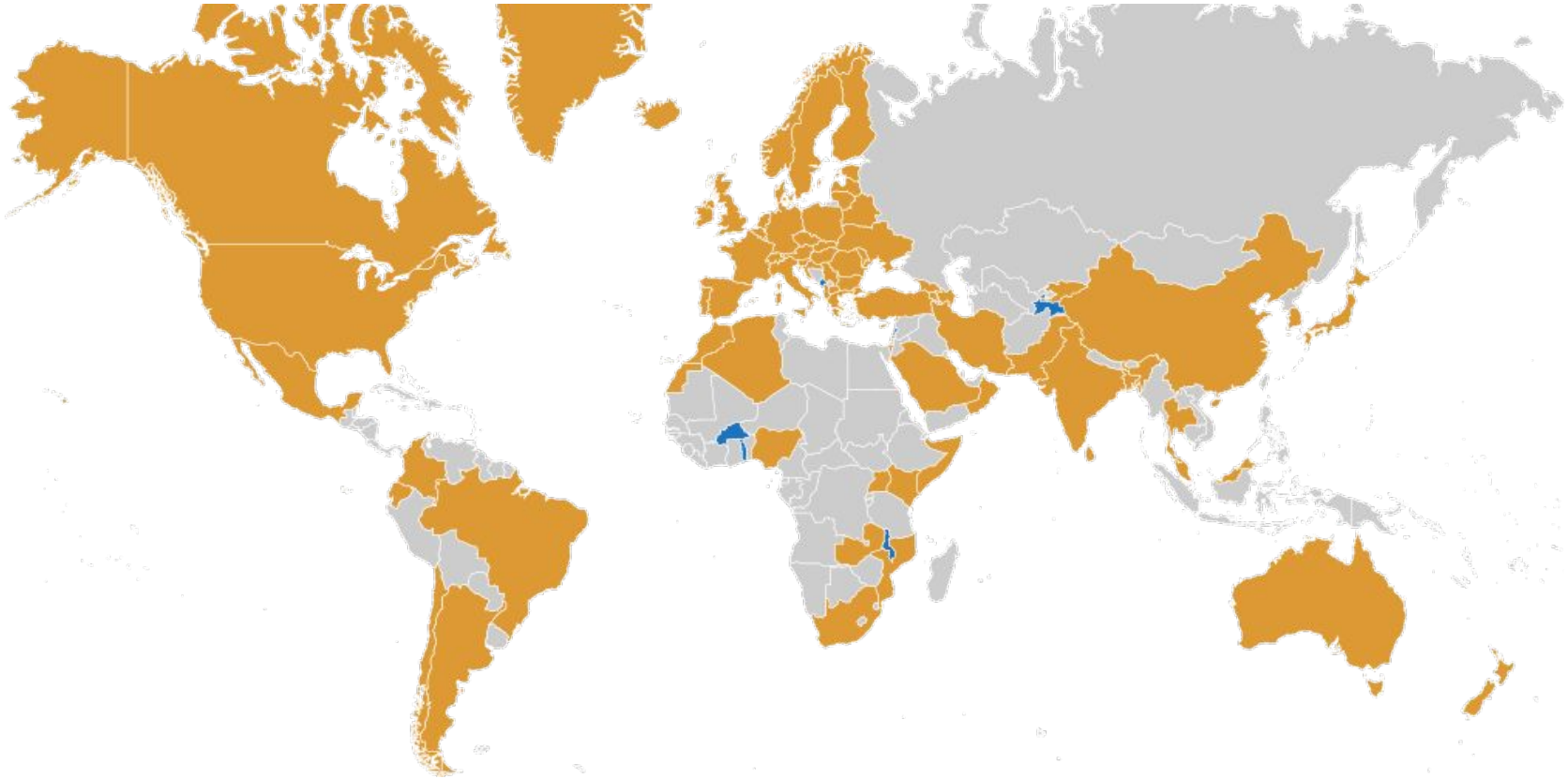
Federation Blue

Federation Green

A complex ecosystem



eduGAIN Global Coverage



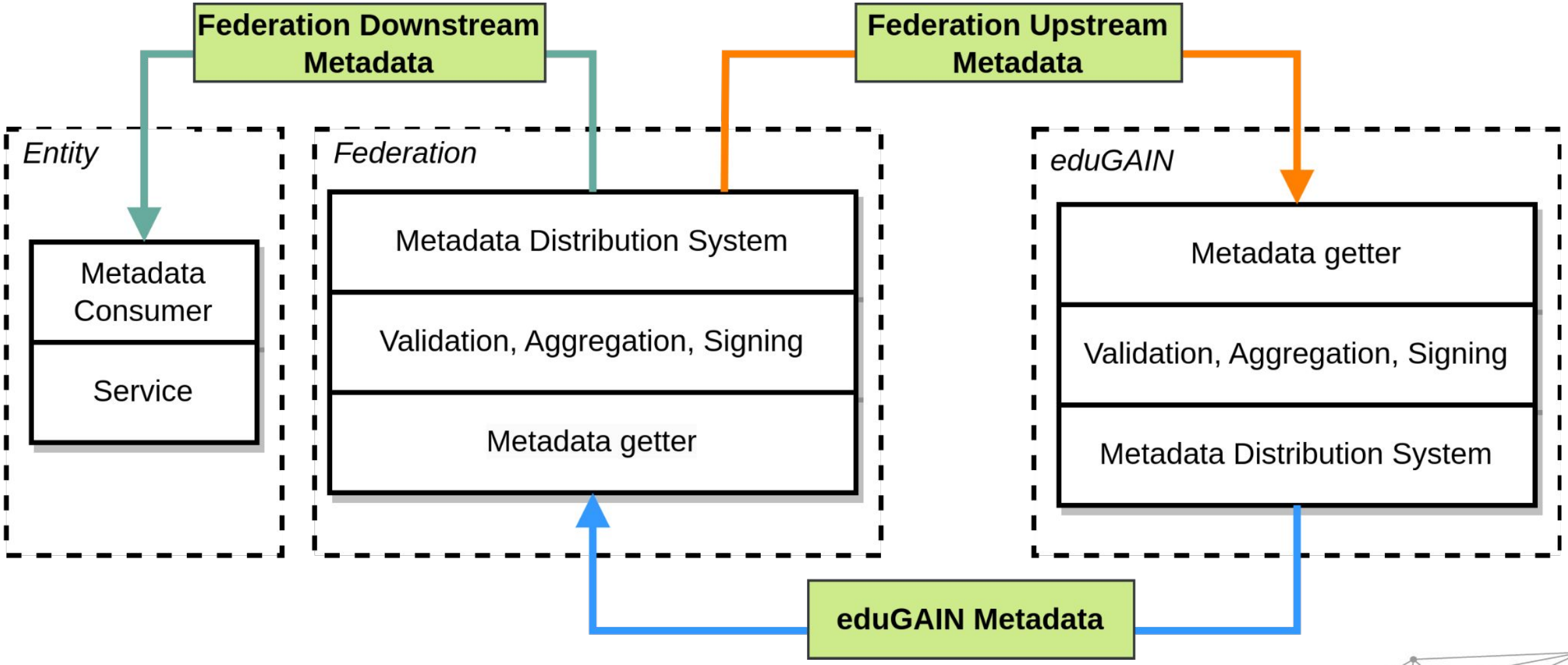
79 Federations

9109 Entities

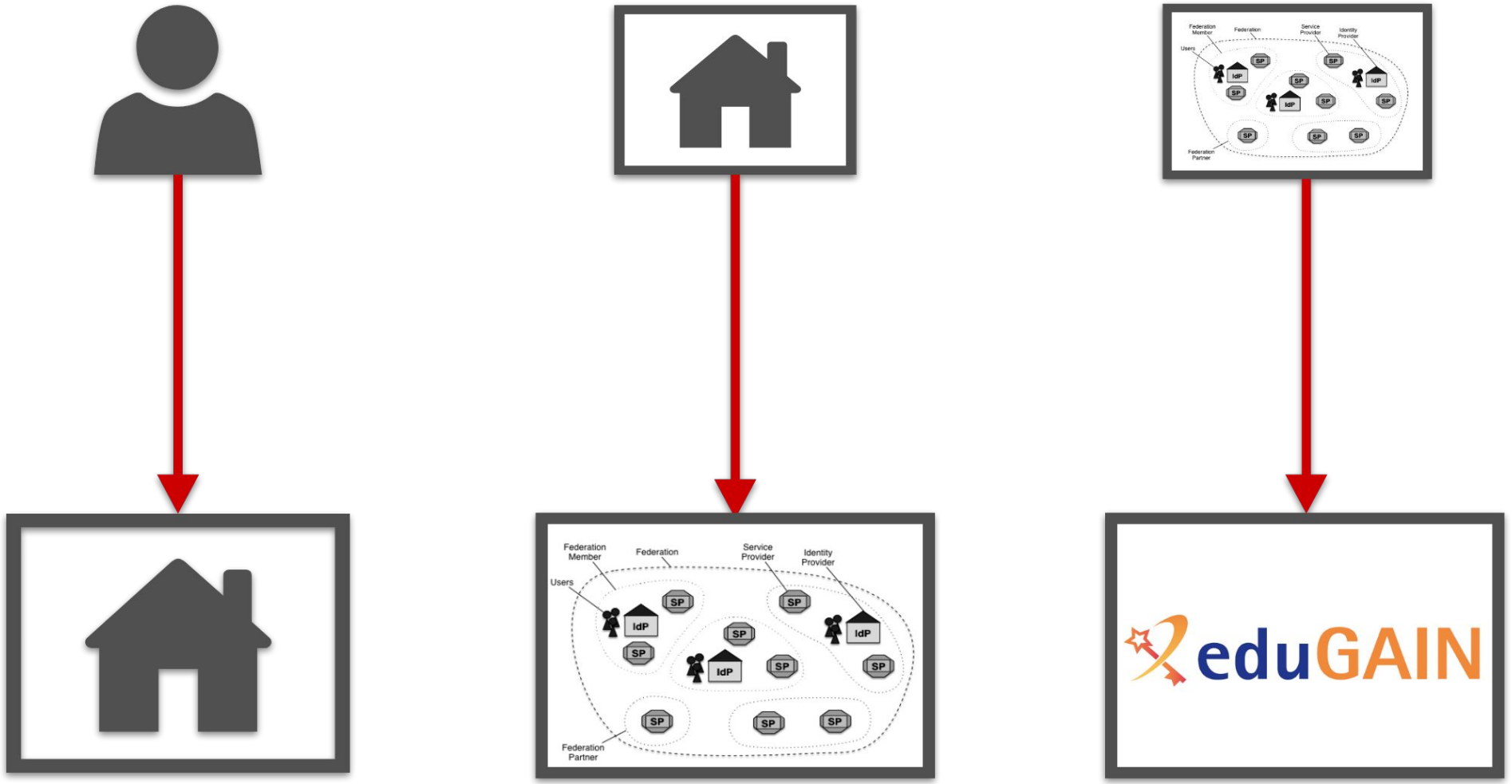
5525 Identity Providers

3604 Service Providers

eduGAIN Metadata Creation and Distribution



eduGAIN Trust Flow



Users trust Home Organisation

HomeOrg/Providers trust Federations

Federations trust eduGAIN

Do users trust eduGAIN?

Do users even know eduGAIN?

eduGAIN Policy Framework

Policy requirements	Metadata Registration Practice Statement
Metadata Requirements	SAML V2.0 Metadata Extensions for Registration and Publication Information Version 1.0, SAML V2.0 Metadata Extensions for Login and Discovery User Interface Version 1.0
Metadata Signing	Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0, SAML V2.0 Metadata Interoperability Profile Version 1.0
Metadata Publication	*Federations MUST provide their members with trustworthy SAML Metadata about eduGAIN Entities, signed with their own signing key [..]*
Participant requirements	*Produce and register a URL to the (participant) SAML Metadata export* *Register a signing certificate and an* `mdrpi:registrationAuthority`

ref https://technical.edugain.org/documents

eduGAIN Contributors

REFEDS

AARC

FIM4R

kantara INITIATIVE

eduGAIN

REFEDS Specifications

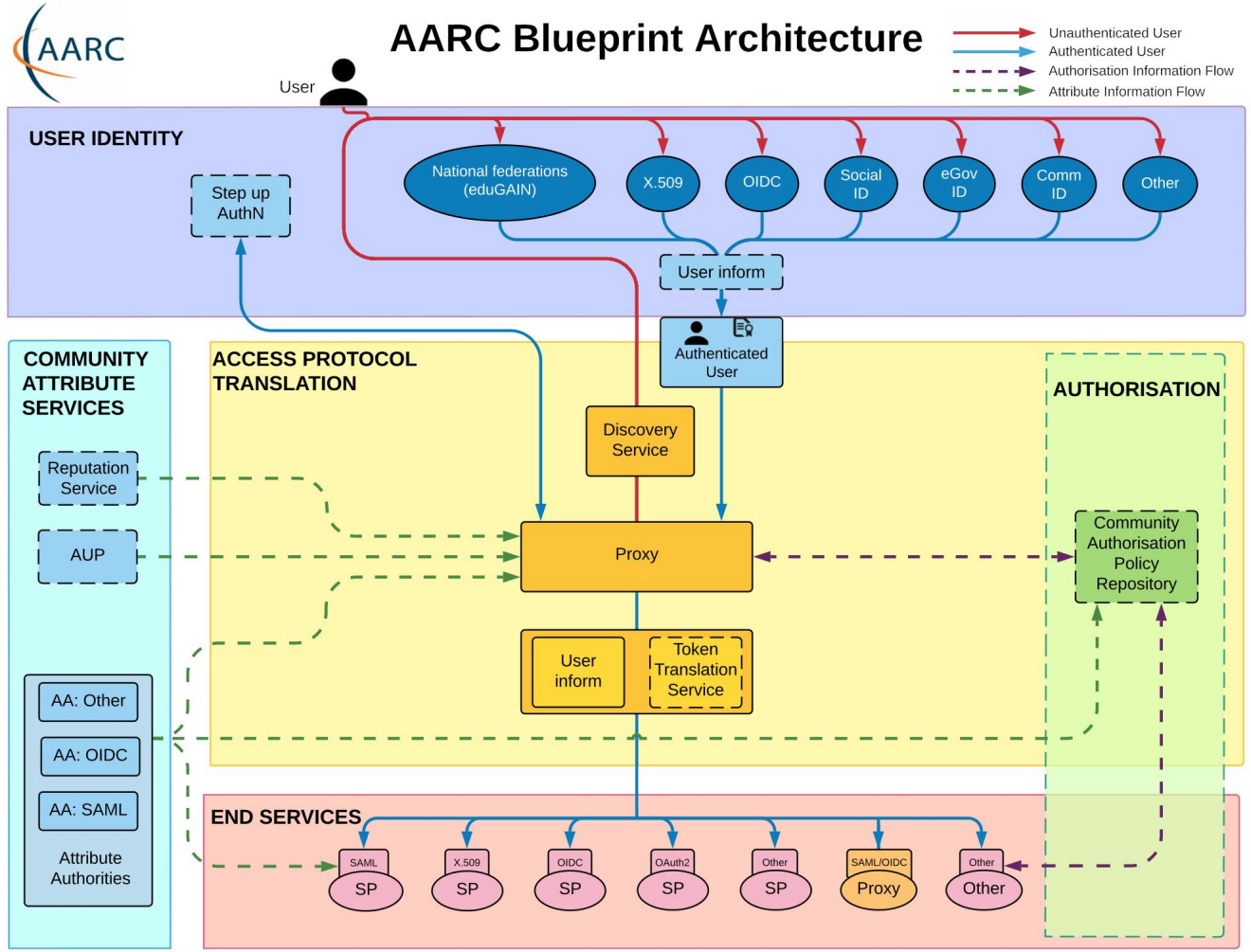
The mission of REFEDS (the Research and Education FEDerations group) is to be the voice that articulates the mutual needs of research and education identity federations worldwide. The group represents the requirements of research and education.

Research and Scholarship (R&S) v1.3	Entity Category	http://refeds.org/category/research-and-scholarship		https://wiki.refeds.org/display/ENT/Research+and+Scholarship
Hide From Discovery v.1	Entity Category	http://refeds.org/category/hide-from-discovery		https://wiki.refeds.org/display/ENT/Hide+From+Discovery
Anonymous Access v.2	Entity Category	https://refeds.org/category/anonymous		https://wiki.refeds.org/x/aQA2B
Pseudonymous Access v.2	Entity Category	https://refeds.org/category/pseudonymous		https://wiki.refeds.org/x/aQA2B
Personalized Access v.2	Entity Category	https://refeds.org/category/personalized		https://wiki.refeds.org/x/aQA2B
MFA Profile v.1.2	Profile	https://refeds.org/profile/mfa		https://wiki.refeds.org/display/PRO/MFA
SFA Profile v.1	Profile	https://refeds/org/profile/sfa		https://wiki.refeds.org/display/PRO/SFA
Security Contact	Metadata Extension	http://refeds.org/metadata/contactType/security		https://wiki.refeds.org/display/SIRTFI/SIRTFI+Home
Sirtfi v1 & v2	Entity Attribute	https://refeds.org/sirtfi https://refeds.org/sirtfi2		https://wiki.refeds.org/display/SIRTFI/SIRTFI+Home
Error Handling v.1	Profile	https://refeds.org/specifications/errorurl-v1		https://wiki.refeds.org/display/PRO/Error+Handling+URL+Profile
Baseline Expectations v.1	Framework	https://refeds.org/baseline-expectations		https://wiki.refeds.org/display/BASE
Assurance v.2	Framework	https://refeds.org/assurance		https://wiki.refeds.org/display/ASS/Assurance+Home
Code of Conduct v.2	Entity Category and Best Practice	https://refeds.org/category/code-of-conduct/v2		https://refeds.org/category/code-of-conduct/

https://refeds.org/specifications

AARC Blueprint Architecture

- Blueprint for Research Infrastructure (RI) AAIs
- RI AAI Specifics:
  - Manage roles and membership attributes that are in context of that research project
  - Connect specific SPs in context of that collaboration via one AAI Proxy
  - Integrate IdPs not available in context of eduGAIN



Thanks

Davide Vaghetti <davide.vaghetti@garr.it>