Sunet dagarna

Trust and identity for international research

Marina Adomet, SUNET

Sunetdagarna, 5.November 2024

A story about how...

- **Research infrastructures** - facilities that provide resources and services for the research communities*
- **Science clusters** - RIs in Europe are organised in five major Science Clusters to link European and other world-class RIs to the European Open Science Cloud (EOSC)
- **e-Infrastructures** - computing, data and AAI infrastructures in support for research in Europe

Make use of federated identities and what are the challenges

*https://roadmap2021.esfri.eu/projects-and-landmarks/view-the-table/

Requirements for access to RIs - federated identity

- Global coverage, typically scatered
- Attribute release - identifier, name, email, affiliation, organisation
- Identity assurance
- Multifactor Authentication

Requirements for access to RIs - AAI

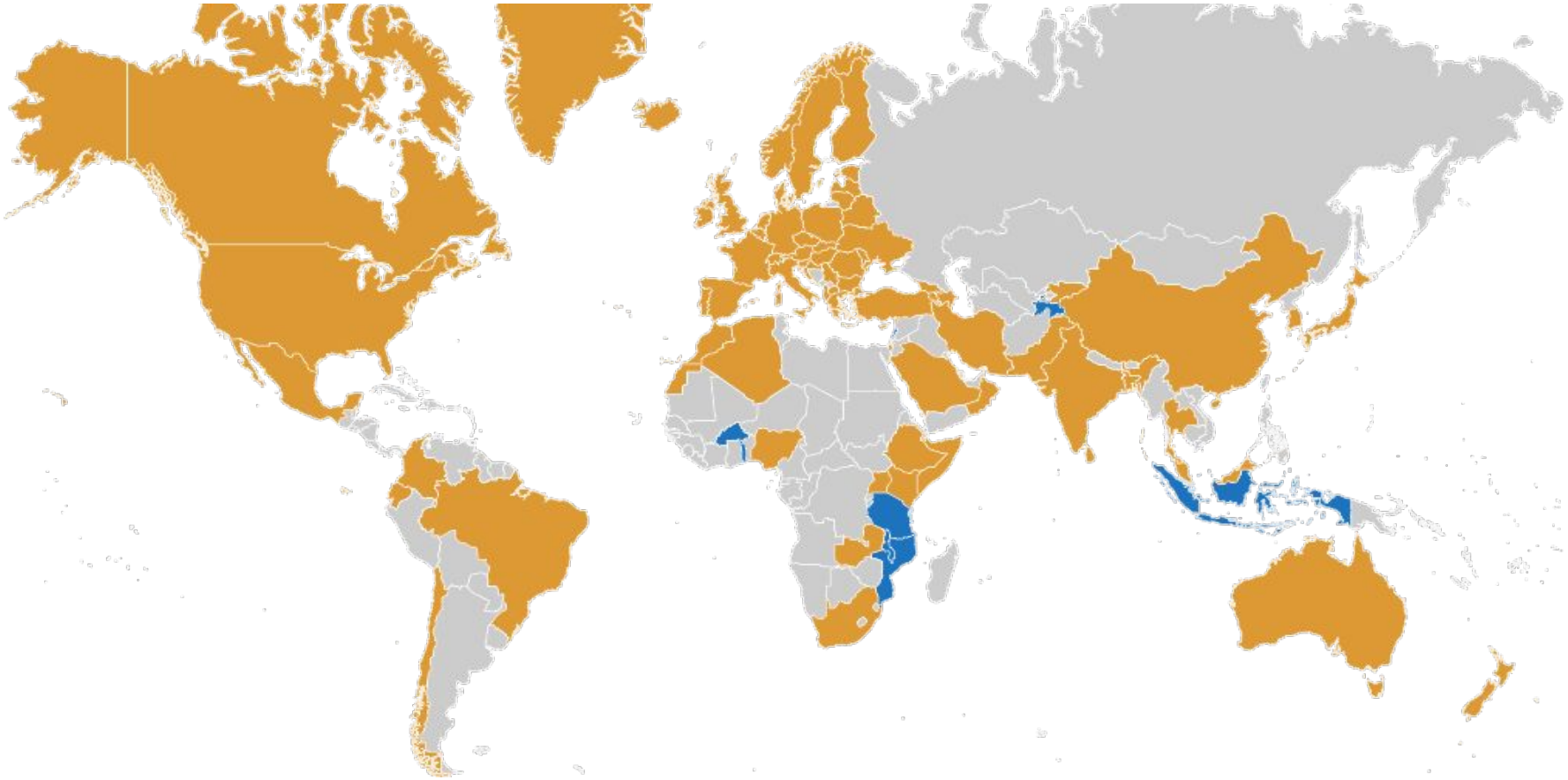
- Connect multiple services
- Connecting not federated IdPs (e-ID, industry, guests)
- Protocol translation (OpenID)
- Manage access policies
- Membership management system
- Discovery service (adapted for the RI)
- Linking identities
- Federated SSH access
- MFA
- Seamless user experience

About attribute release and assurance...

Federated Identities in R&E

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

eduGAIN Global Coverage



78 Federations

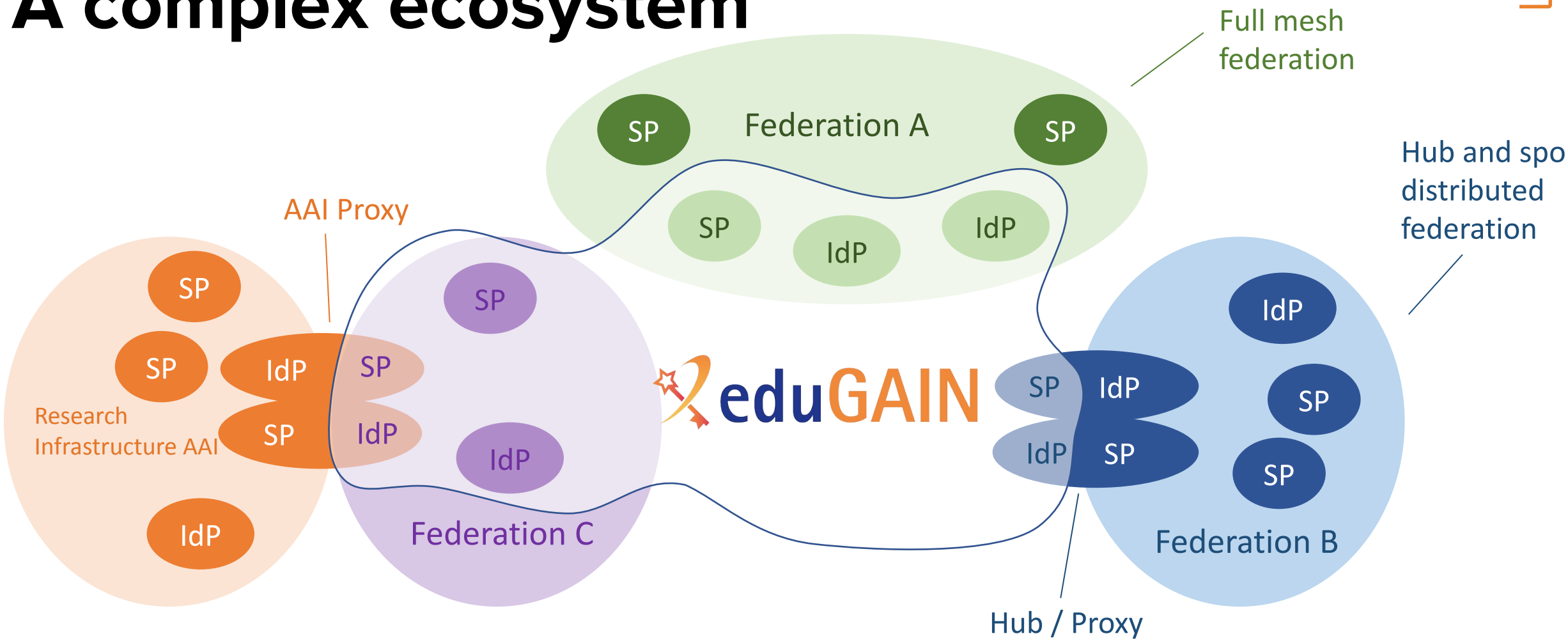
9535 Entities

5753 Identity Providers

3800 Service Providers

Last update November 4th 2024

A complex ecosystem



eduGAIN provides trust framework for metadata exchange

Other trust e.g for IdPs to release attributes and SPs to trust the data breaks on the federation borders

Compensating measures to establish trust

Attribute release:

- Anonymous Access entity category - organization, scoped affiliation
- Pseudonymous Access entity category - above + assurance, identifier
- Personalised Access entity category- above + name, email
- R&S entity category - identifier, name, email, scoped affiliation
- Code of conduct

Identity assurance:

- REFEDS Assurance framework

Security:

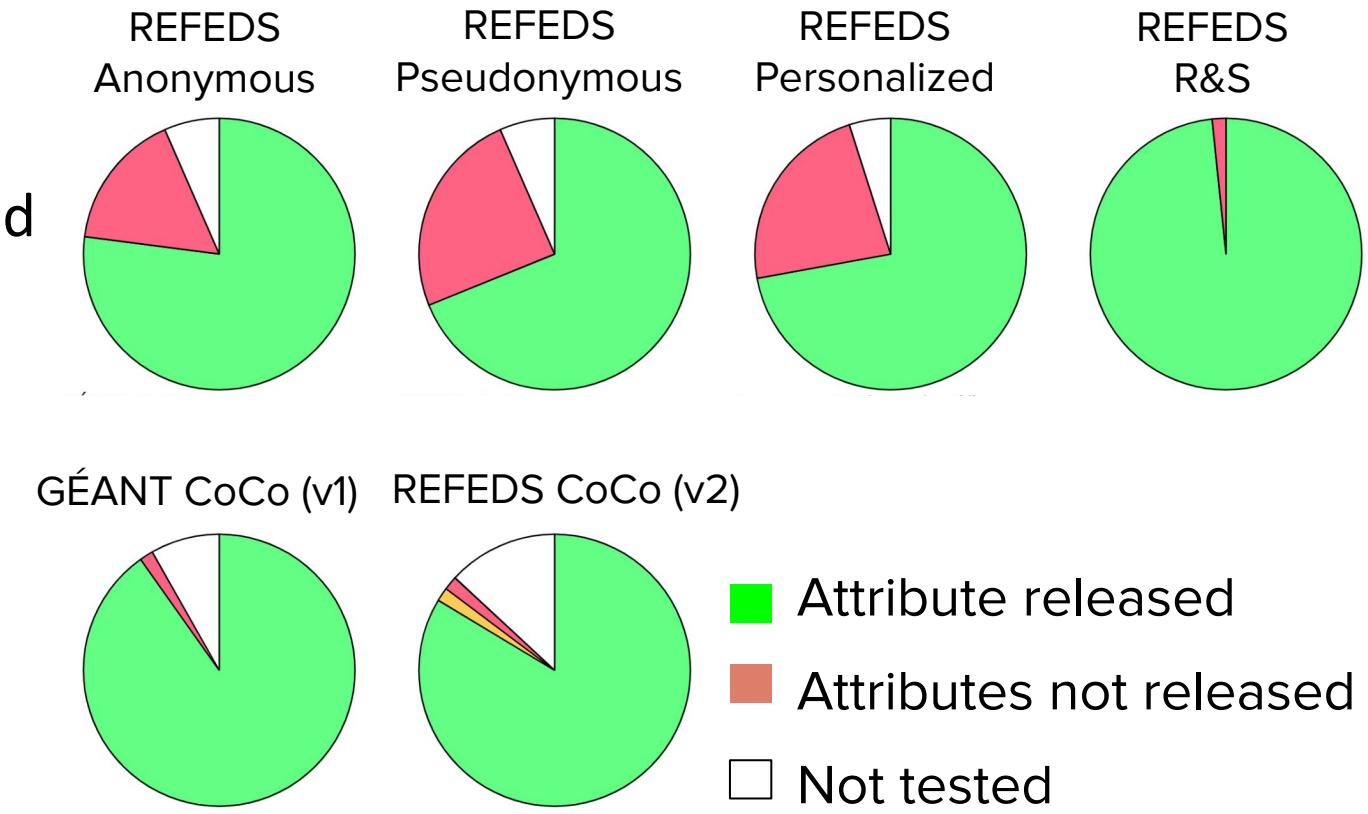
- Sirtfi framework

Implementation in Sweden

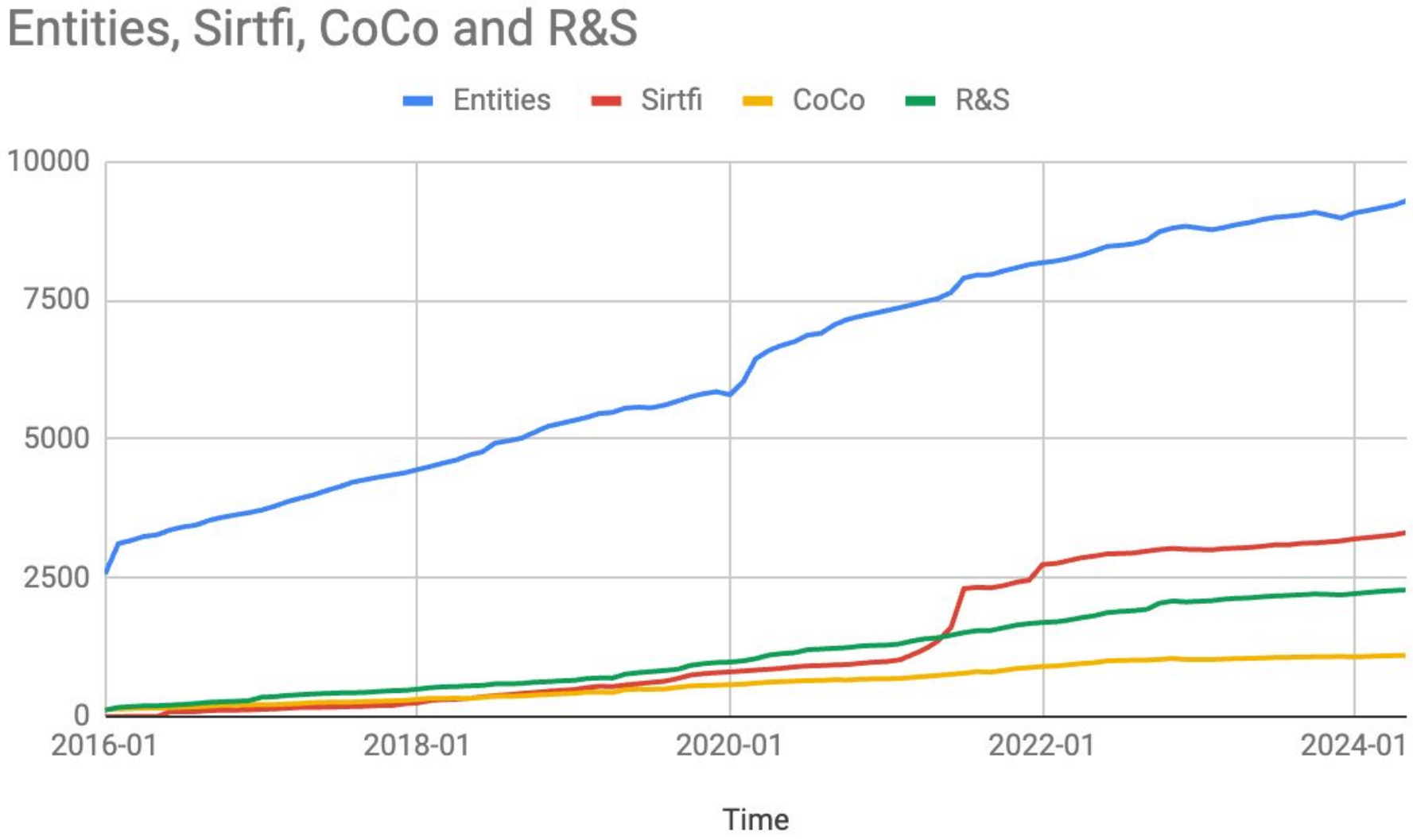
SWAMID

Identity Provider attribute release is based on REFEDS and GÉANT Entity Categories

Rules are employed automatically or by manual personal data release decisions

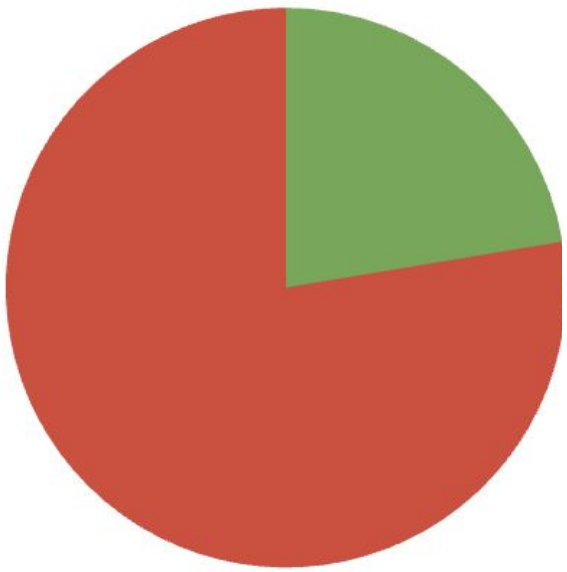


Global implementation

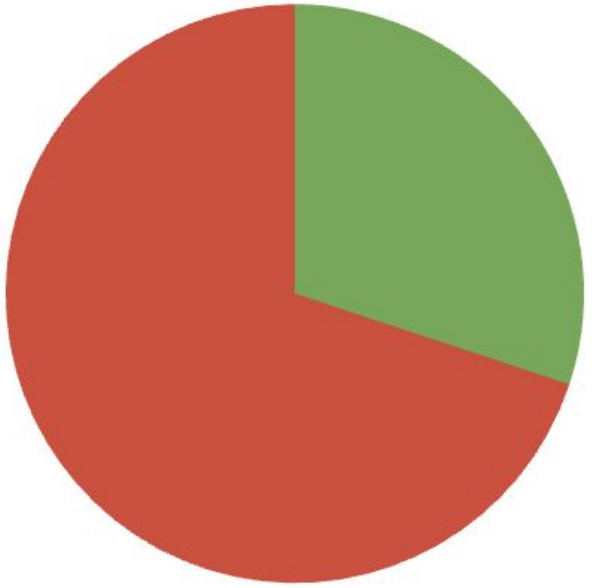


Adoption in Europe

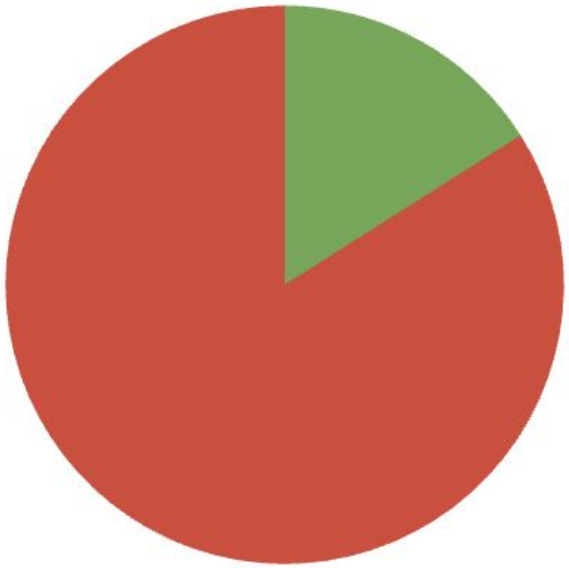
CoCo in Europe



R&S in Europe

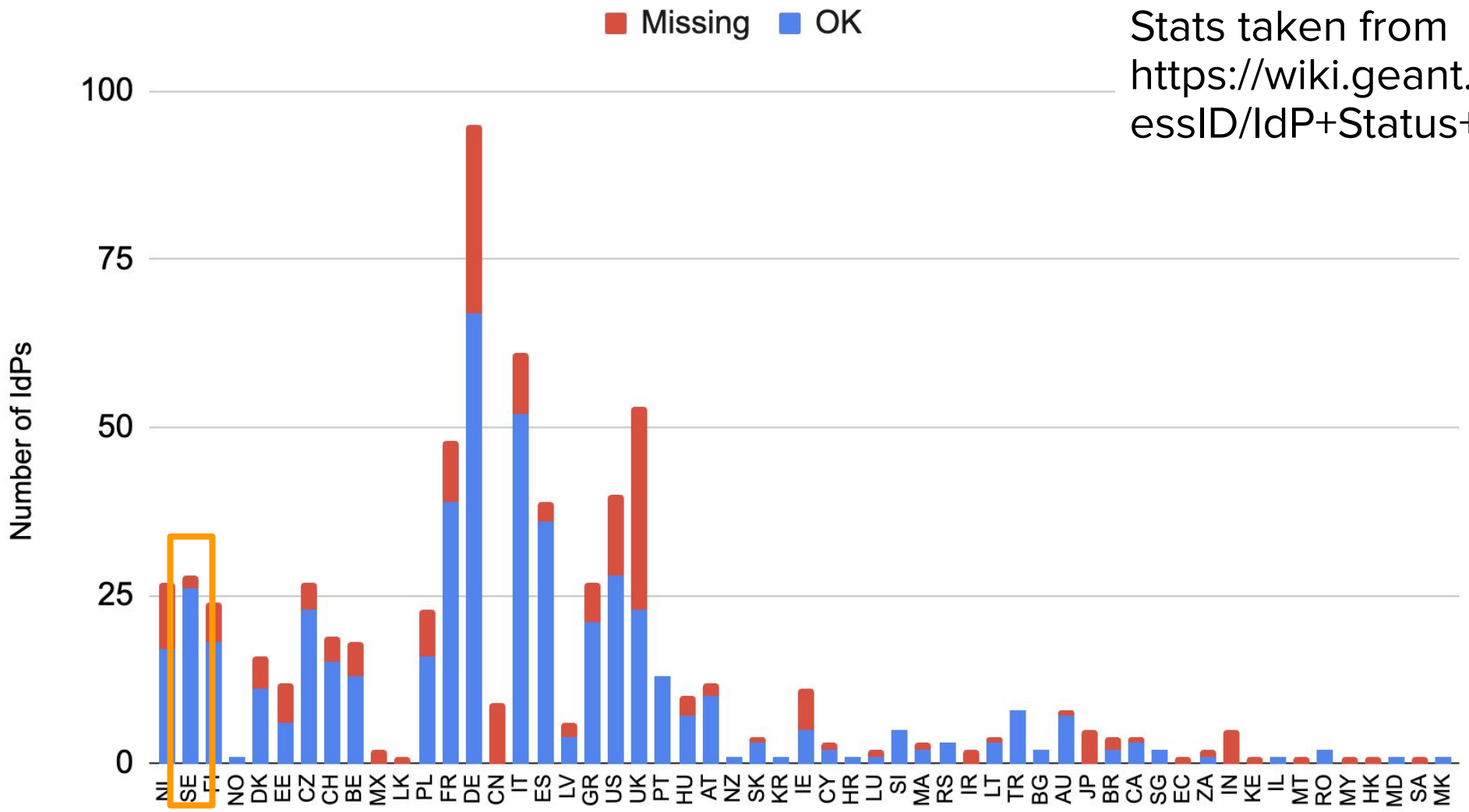


Sirtfi in Europe



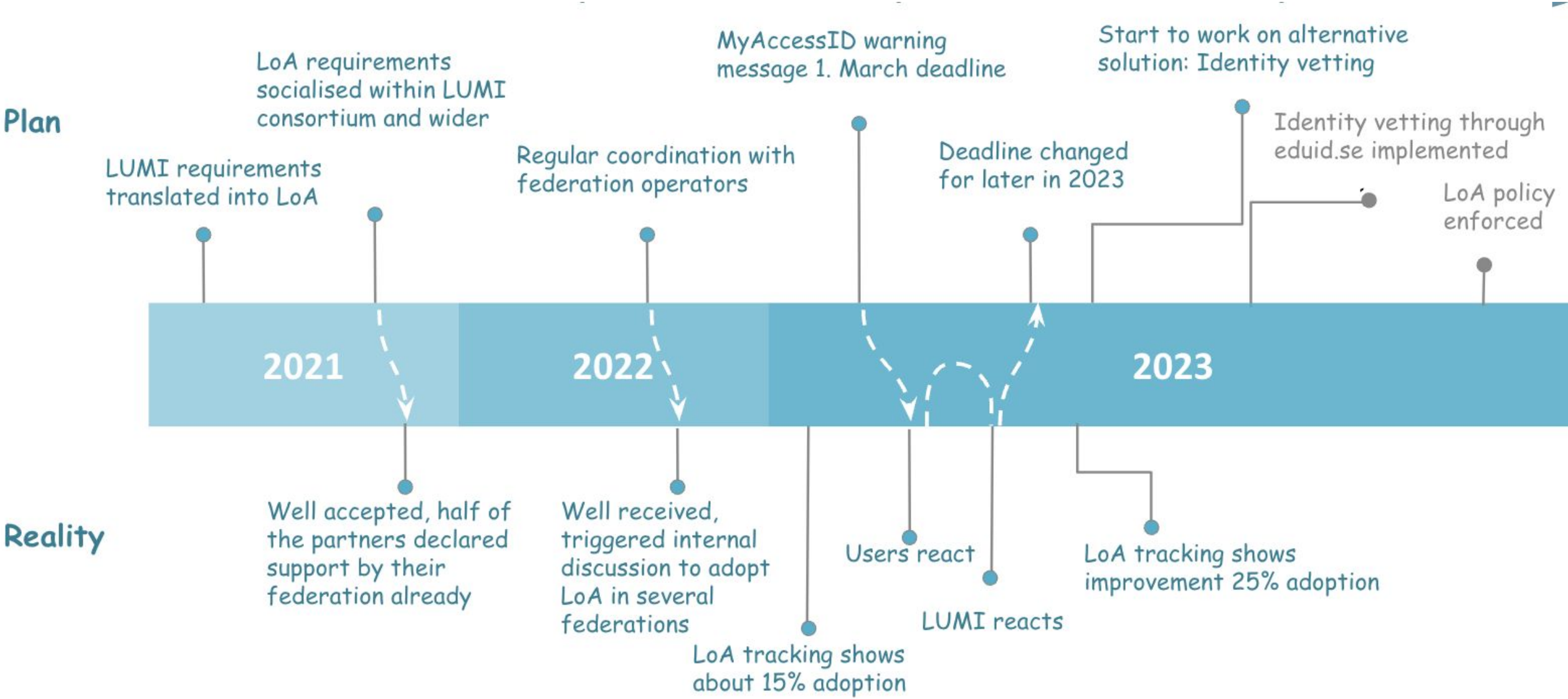
- Entities not signaling implementation
- Entities signaling implemention

Practice shows not so grim results - example with Name attribute release



Stats taken from https://wiki.geant.org/display/MyAccessID/IdP+Status+Report

Identity Assurance - LUMI story



eduGAIN Futures Working Group

REFEDS Baseline Expectations

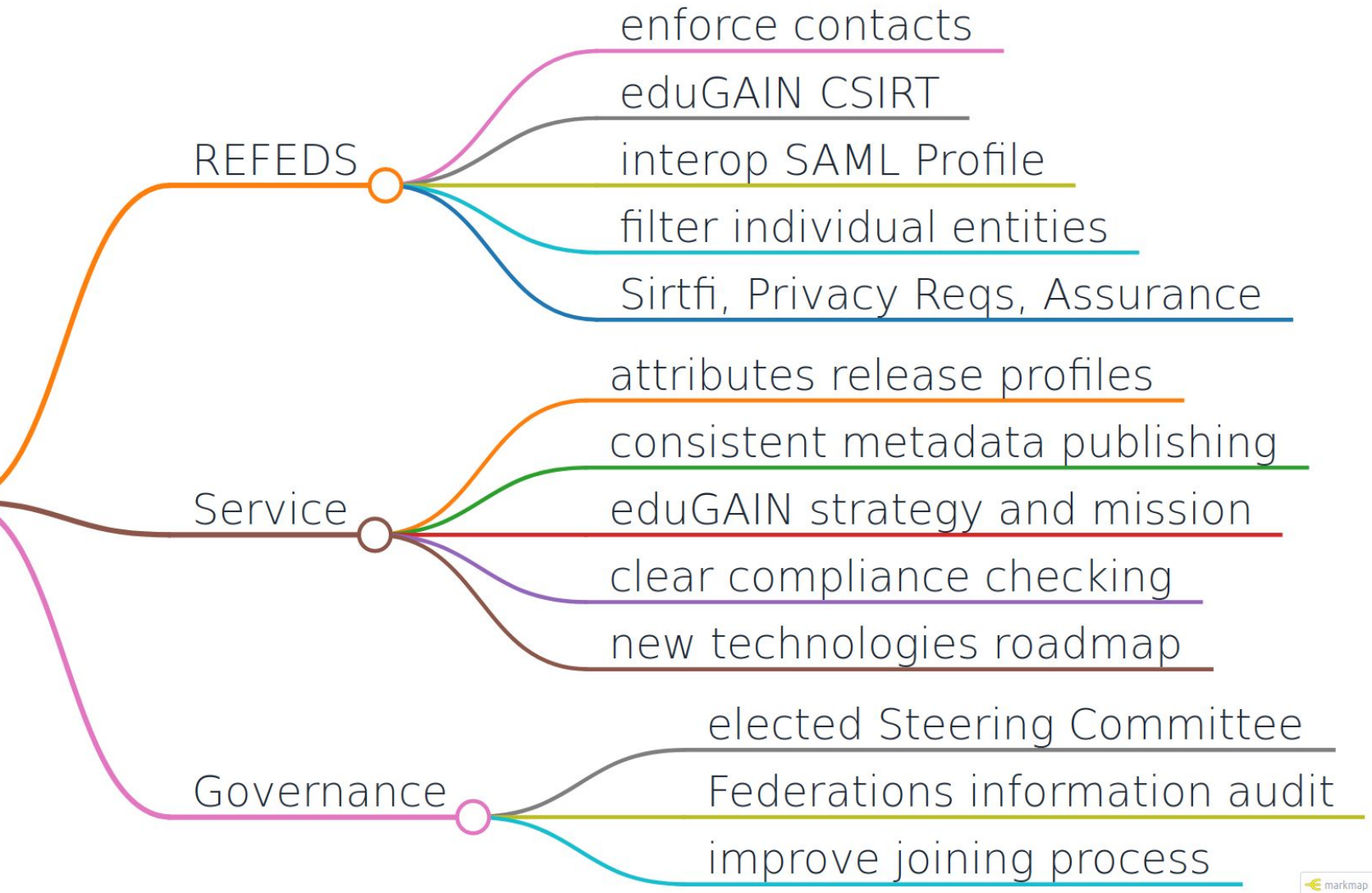
Identify key issues with current eduGAIN service

Review the governance model

https://nordu.net/ndn2024/talks/#62e5db88-729a-4c0c-9d97-0dda159419e5

eduGAIN Futures WG Problem Statements and Recommendations

01	Complex service experience
02	Low predictability
03	Diverse policies and processes
04	Variable service offerings
05	Slow response to change
06	Delays on decision and new Technologies
07	Unclear mission and branding strategy



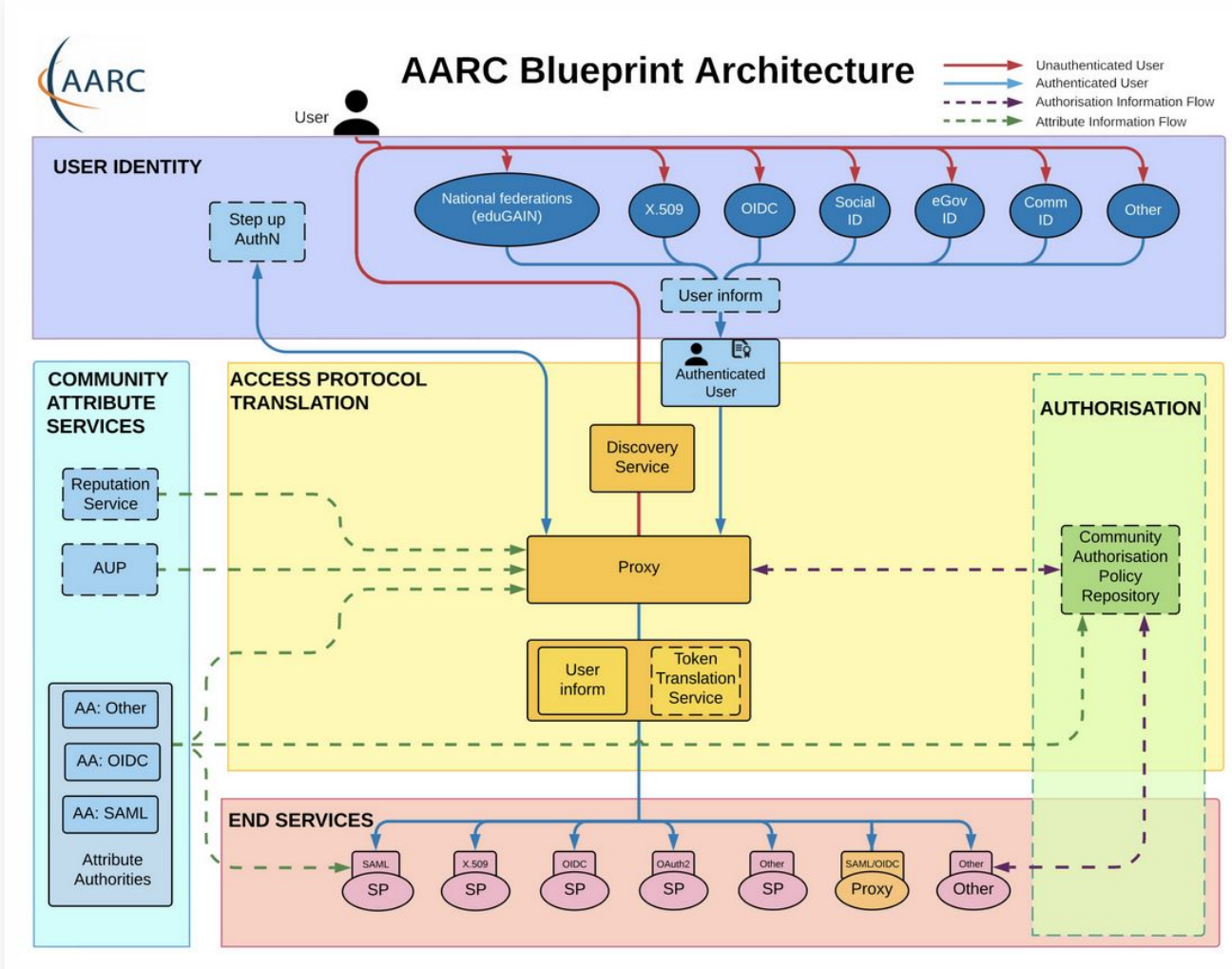
About other requirements for RI AAIs...

What is the AARC BPA?

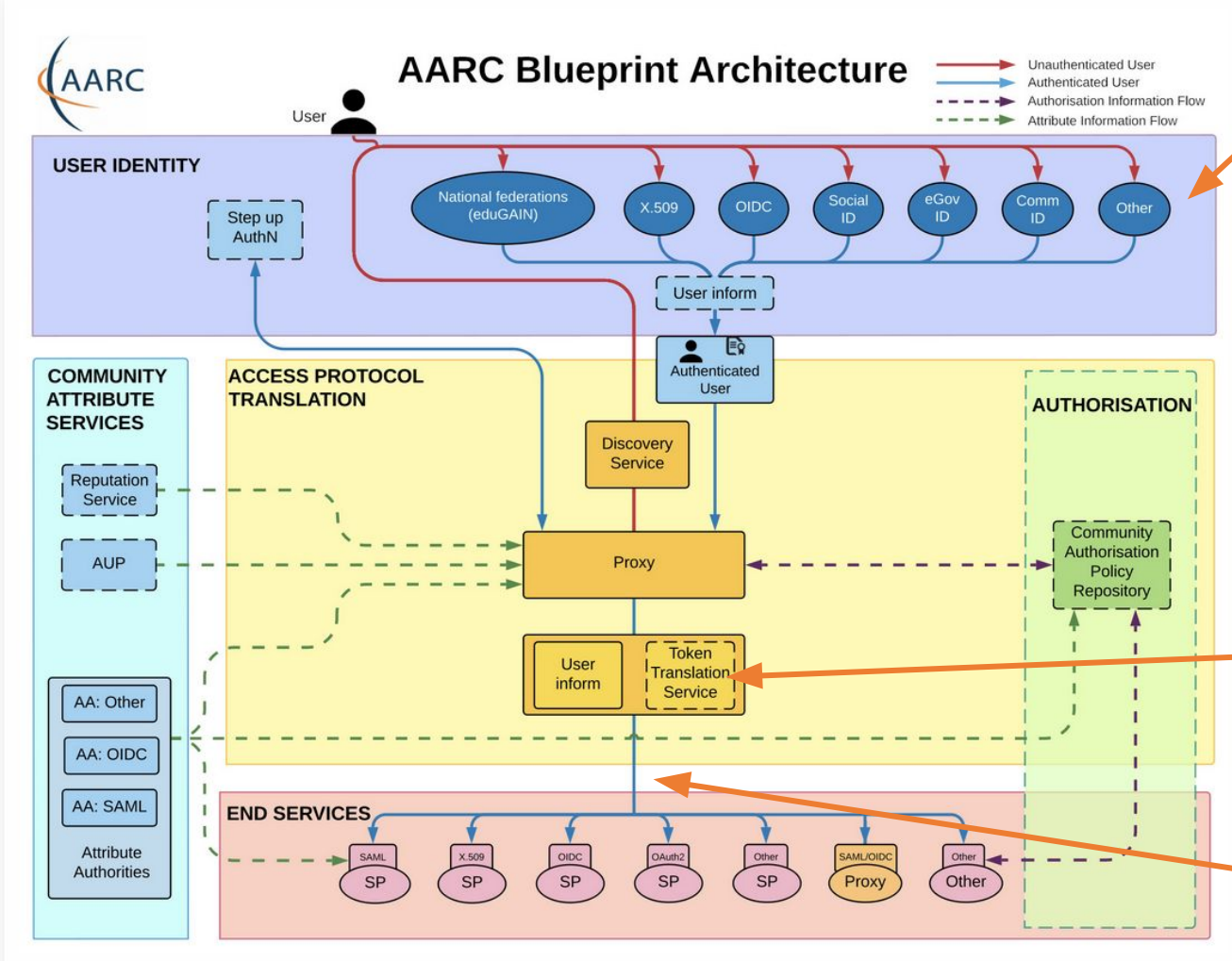
The Authentication and Authorization For Research and Collaborations BluePrint Architecture provides a set of building blocks for software architects and technical decision makers who are designing and implementing access management solutions for international research collaborations. By design the AARC BPA is technology agnostic and provides an architectural design for those the deploy AAIs.

Science Clusters, Research Infrastructures and e-Infrastructure Providers have been been implementing their AAIs using the AARC Blueprint Architecture in order to manage their users and the access rights to resources

AARC BPA overview



AARC BPA overview

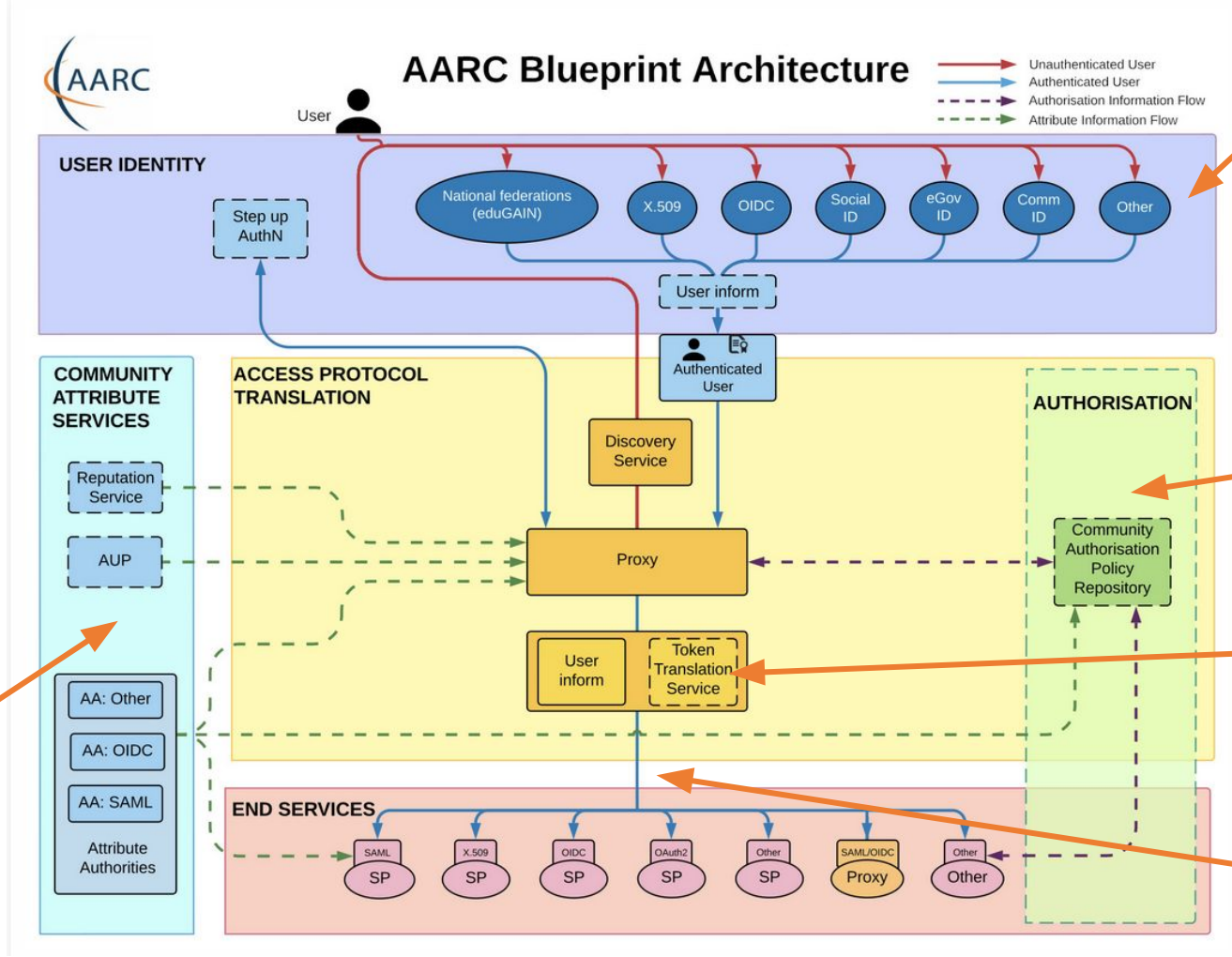


Connecting not federated IdPs

Protocol translation (OpenID to SAML)

Connect multiple services

AARC BPA overview



Connecting not federated IdPs

Access Policies

Membership management system

Protocol translation (OpenID to SAML)

Linking identities

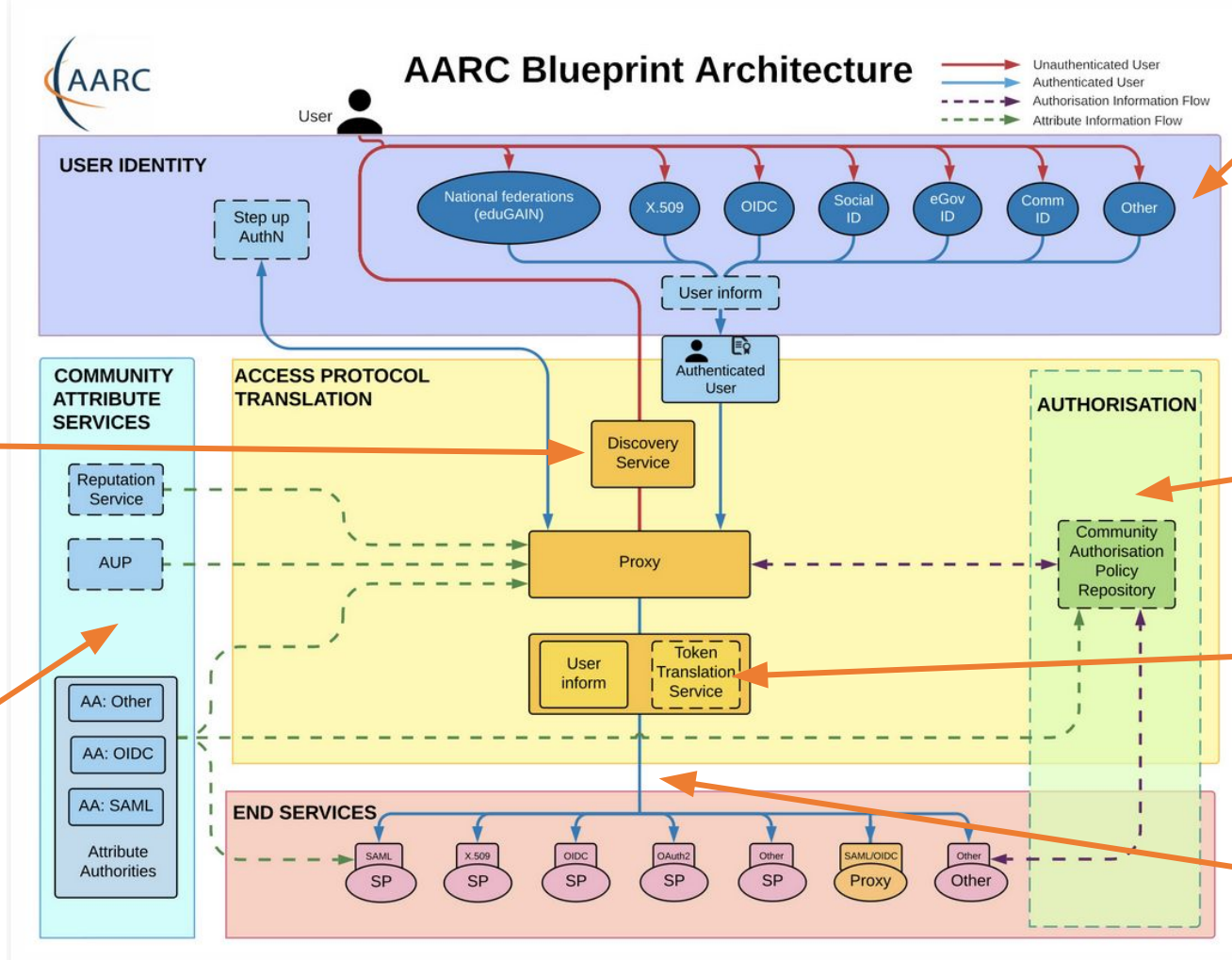
Connect multiple services

AARC BPA overview

Federated SSH access

MFA

Seamless User experience



Connecting not federated IdPs

Discovery service adapted for the RI

Access Policies

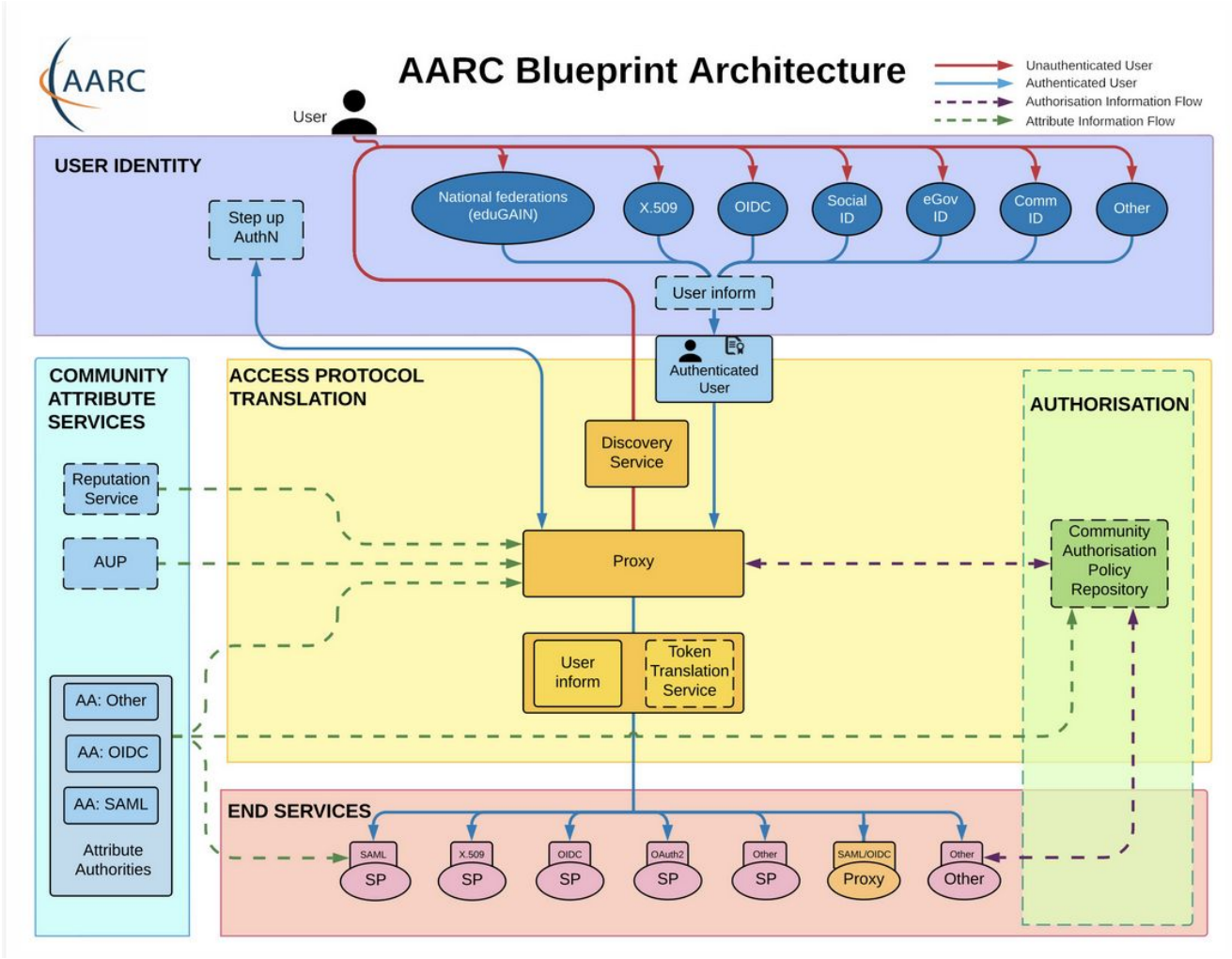
Membership management system

Protocol translation (OpenID to SAML)

Linking identities

Connect multiple services

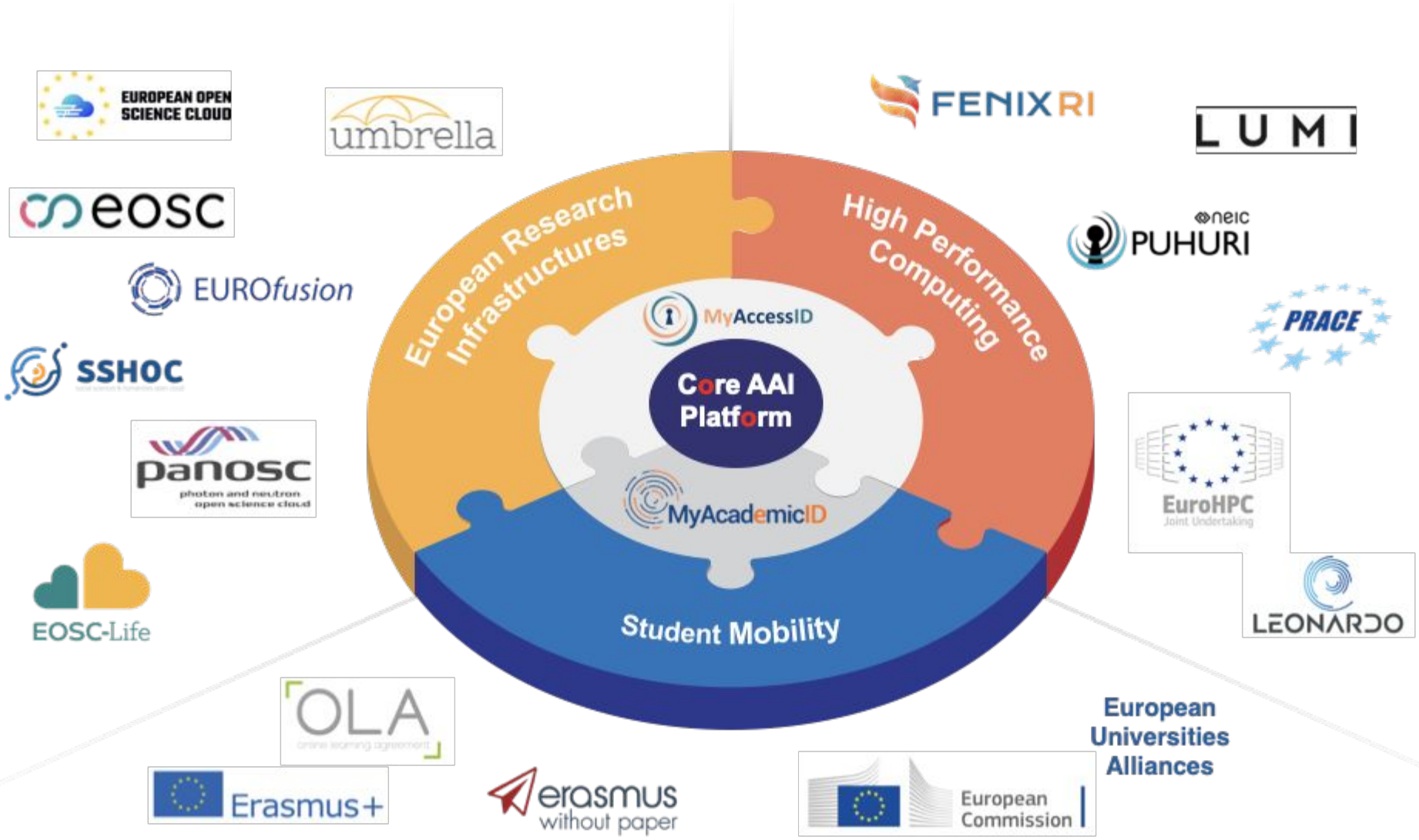
Interoperability in the AARC BPA: the AARC GUIDELINES



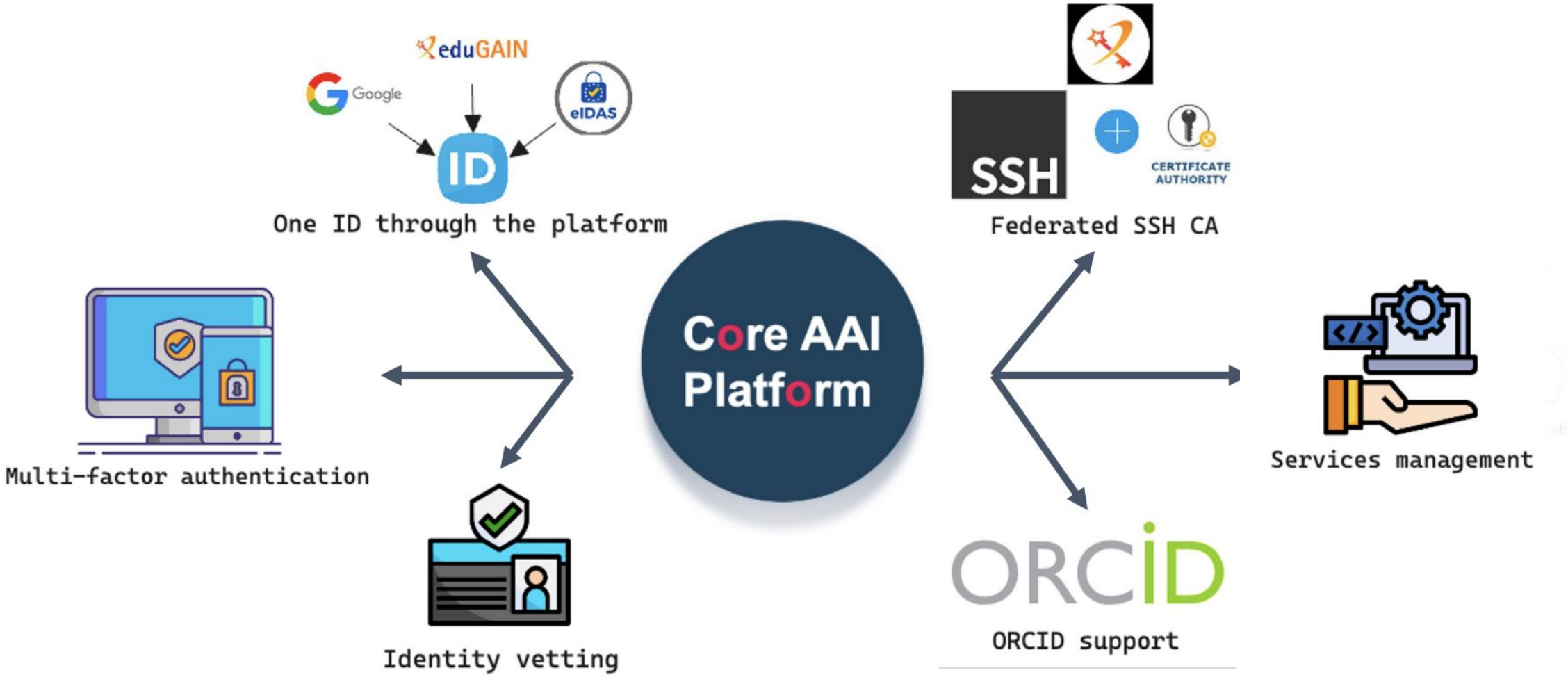
Document	Who should complete the template?	Audience	Description	Link
Top Level Infrastructure Policy	Infrastructure Management	All Infrastructure Participants (abides by)	This policy template defines the roles of actors in the Research Infrastructure and binds the policy set together	Google Doc
Incident Response Procedure	Infrastructure Management & Security Contact	Infrastructure Security Contact, Services (abides by)	This template procedure provides a step-by-step breakdown of actions to take following a security incident.	Google Doc
Membership Management Policy	Infrastructure Management	Research Community (abides by)	This policy template defines how Research Communities should manage their members, including registration and expiration.	Google Doc
Acceptable Authentication Assurance	Infrastructure Management	Research Community, Services (abide by)	This is a placeholder for the Infrastructure to determine rules for the acceptable assurance profiles of user credentials.	Google Doc
Risk Assessment	Infrastructure Management, Services & Security Contact	Infrastructure Management (completes)	This table can be used as a starting point for identifying whether a full Data Protection Impact Assessment is required.	Google Doc
Policy on the Processing of Personal Data	Infrastructure Management & Data Protection Contact	Research Community, Services (abide by)	This document defines the obligations on Infrastructure Participants when processing personal data.	Google Doc
Privacy Policy	Infrastructure Management (for general policy) & Services (for service specific policies)	Users (view)	This can be used to document the data collected and processed by the Infrastructure and its participants. Each service in the infrastructure, as well as the infrastructure itself, should complete the template.	Google Doc
Service Operati…	…tructure …gement	Services (abide by)	This policy defines requirements for running a service within the Infrastructure.	Google Doc
		Users (abide by)	This is a template for the acceptable use policy that users must accept to use the Research Infrastructure. It should be augmented by the Research Community.	Google Doc

Previous Next

Common solution for AAI for RIs



Complementing features



Conclusions

Research infrastructures have some requirements that are commont to international SPs (attribute release, identity assurance and authenticaiton characteristics)

However, they have a number of other requirements for which they need to use additional solutions, either to run them by themselves or use services provided by e-infrastructure providers

What can we do to make it better

All

- **Participate in the SIRTFI framework**, use Entity Categories to express attribute release requirements and capabilities

IdPs

- Release Attributes and identity assurance (medium, **high**), **support MFA**

RIs

- Adopt AARC BPA, **consider using common services such as MyAccessID (get in touch with marina@sunet.se)**

Questions?

marina@sunet.se