Federated Identity for Research

Marina Adomeit, SUNET

TDI 2025, 3. February 2025

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

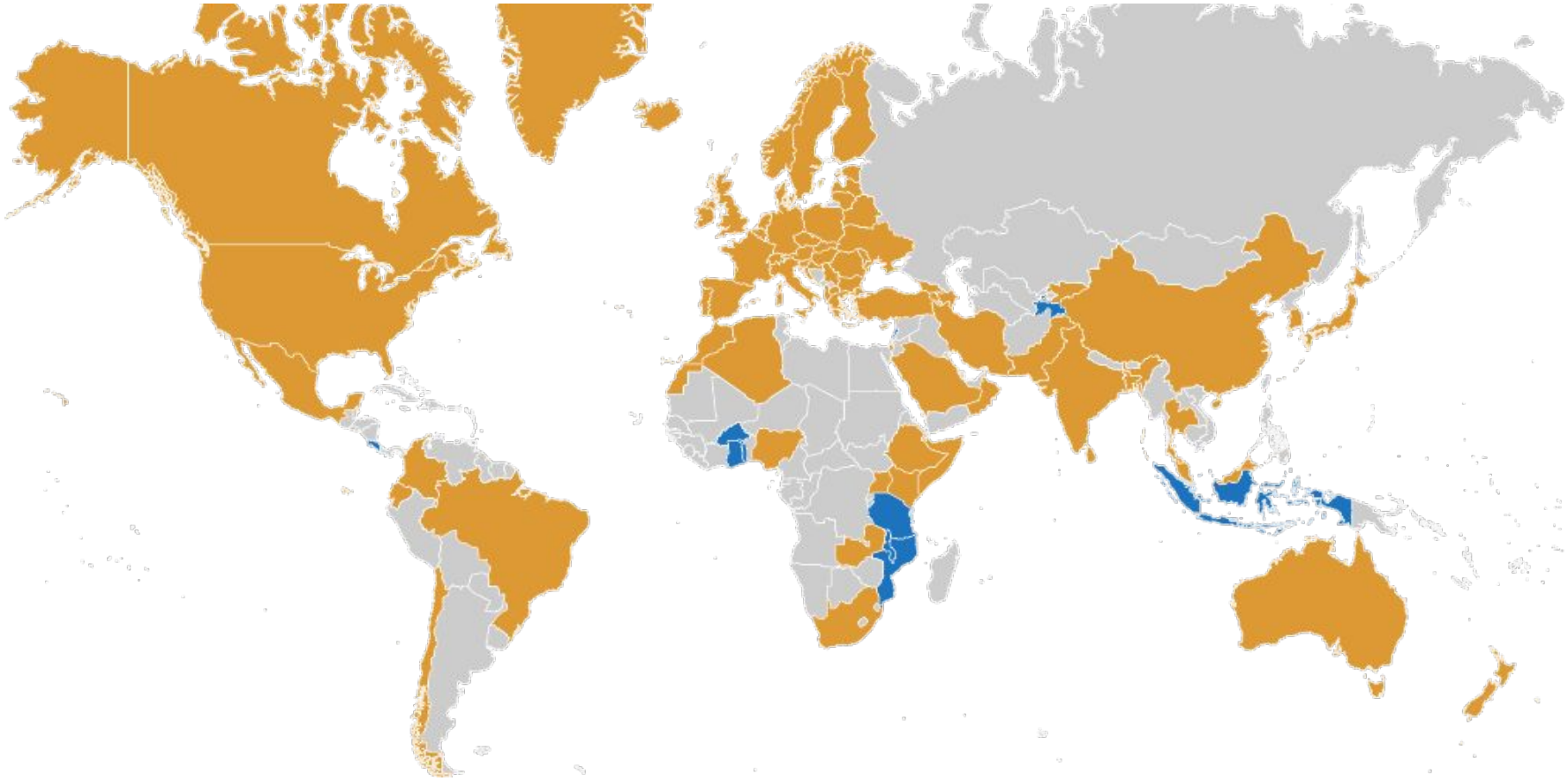
*https://roadmap2021.esfri.eu/projects-and-landmarks/view-the-table/

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"*

https://st.fbk.eu/assets/areas/events/TDI2024/slides/3_1_VaghettiDavide.pdf

eduGAIN Global Coverage



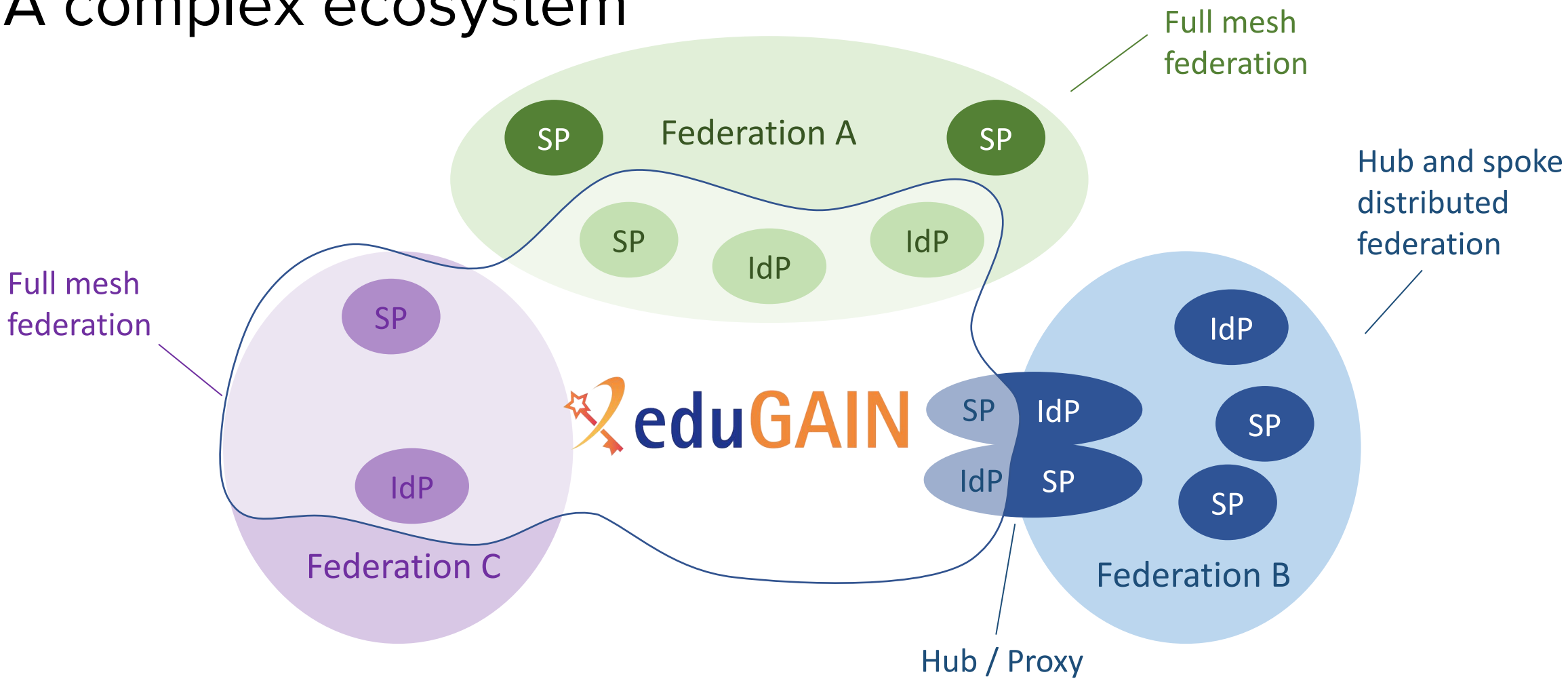
78 Federations

9698 Entities

5911 Identity Providers

3805 Service Providers

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

Additional 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

Requirements for access to RIs

Federated Identity

Global coverage

Attribute release

Identity assurance

Multi-factor Authentication

Functionalities

Connect multiple services

Non-federated/R&E IdPs

Protocol translation

Manage access policies

Membership management system

Discovery service

Linking identities

Federated SSH access

MFA

Seamless user experience

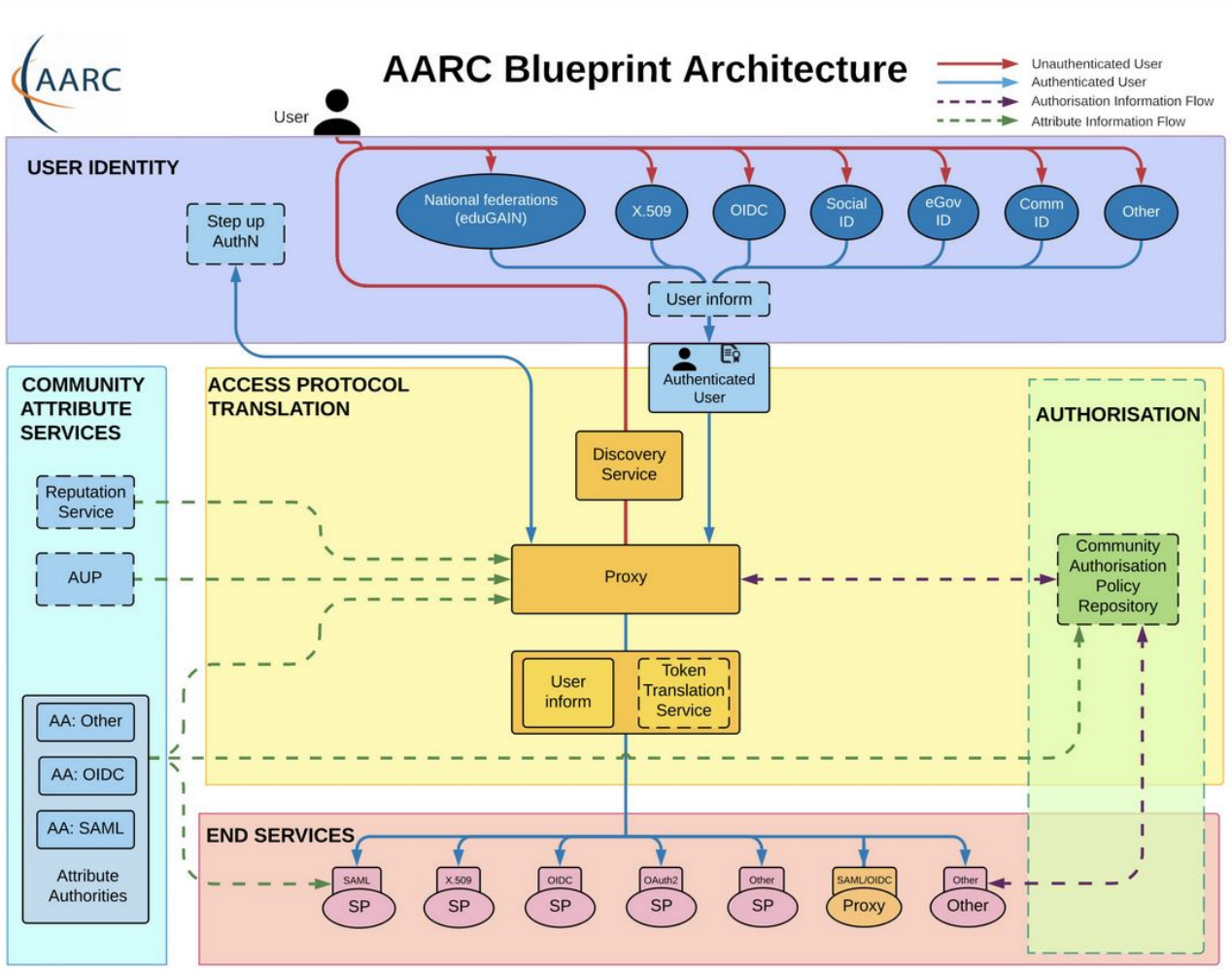
AARC BPA

Authentication and **A**uthorization for **R**esearch and **C**ollaborations

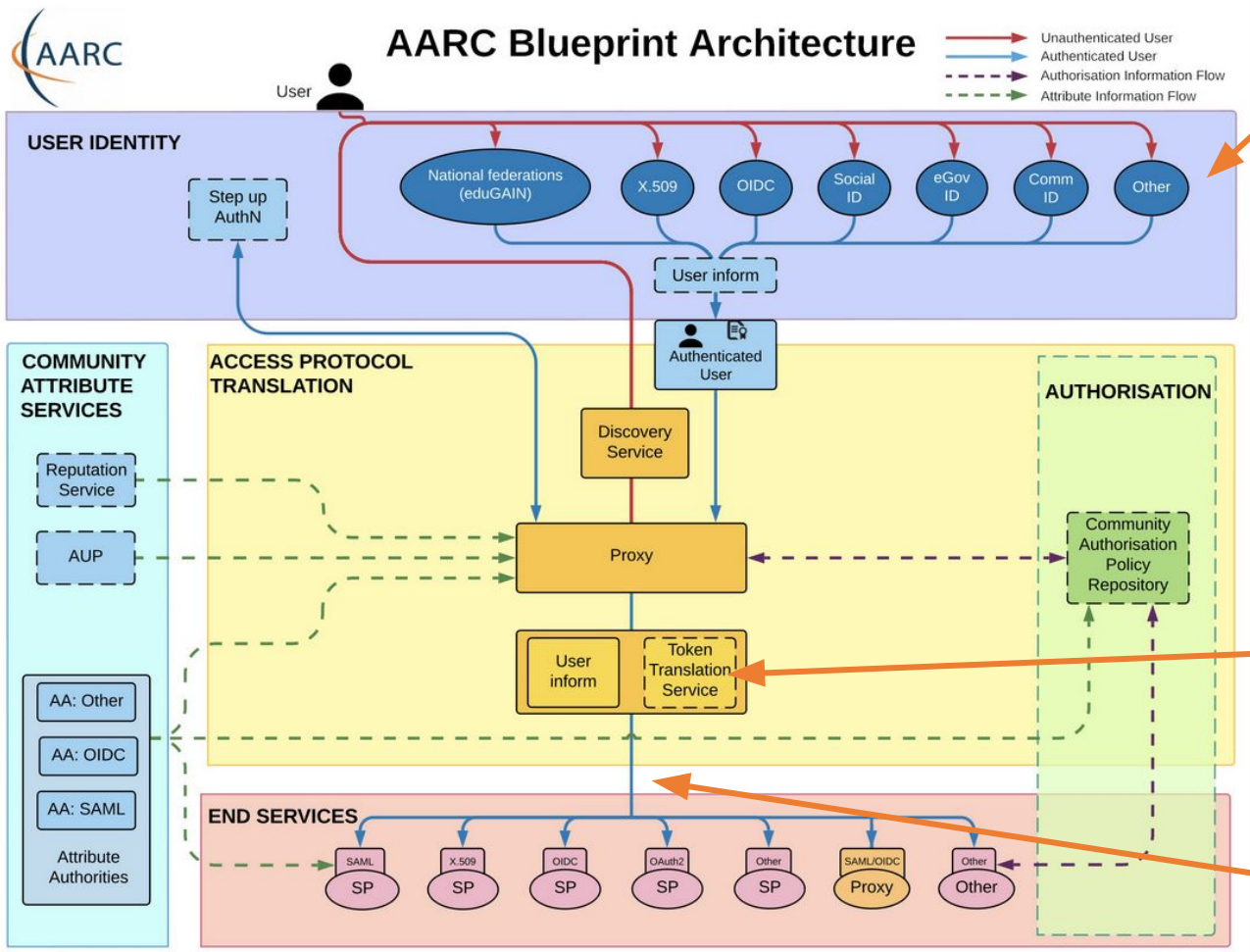
Blue**P**rint **A**rchitecture

Provides a set of building blocks for solution architects and technical decision makers who are designing and implementing access management solutions for international research collaborations

AARC BPA overview



AARC BPA overview

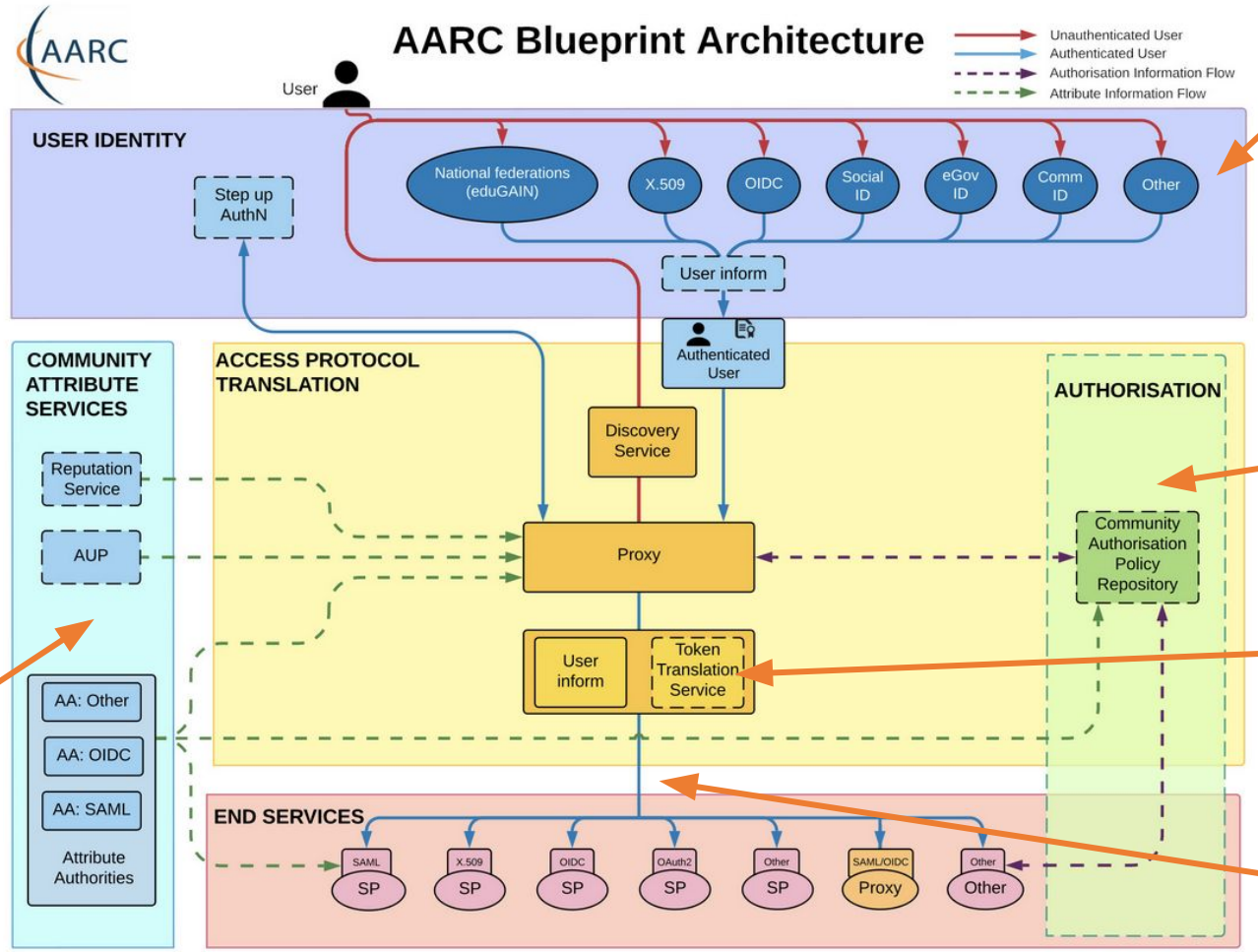


Non-federated /R&E IdPs

Protocol translation (OpenID to SAML)

Connect multiple services

AARC BPA overview



Non-federated /R&E IdPs

Access Policies

Membership management system

Protocol translation (OpenID to SAML)

Linking identities

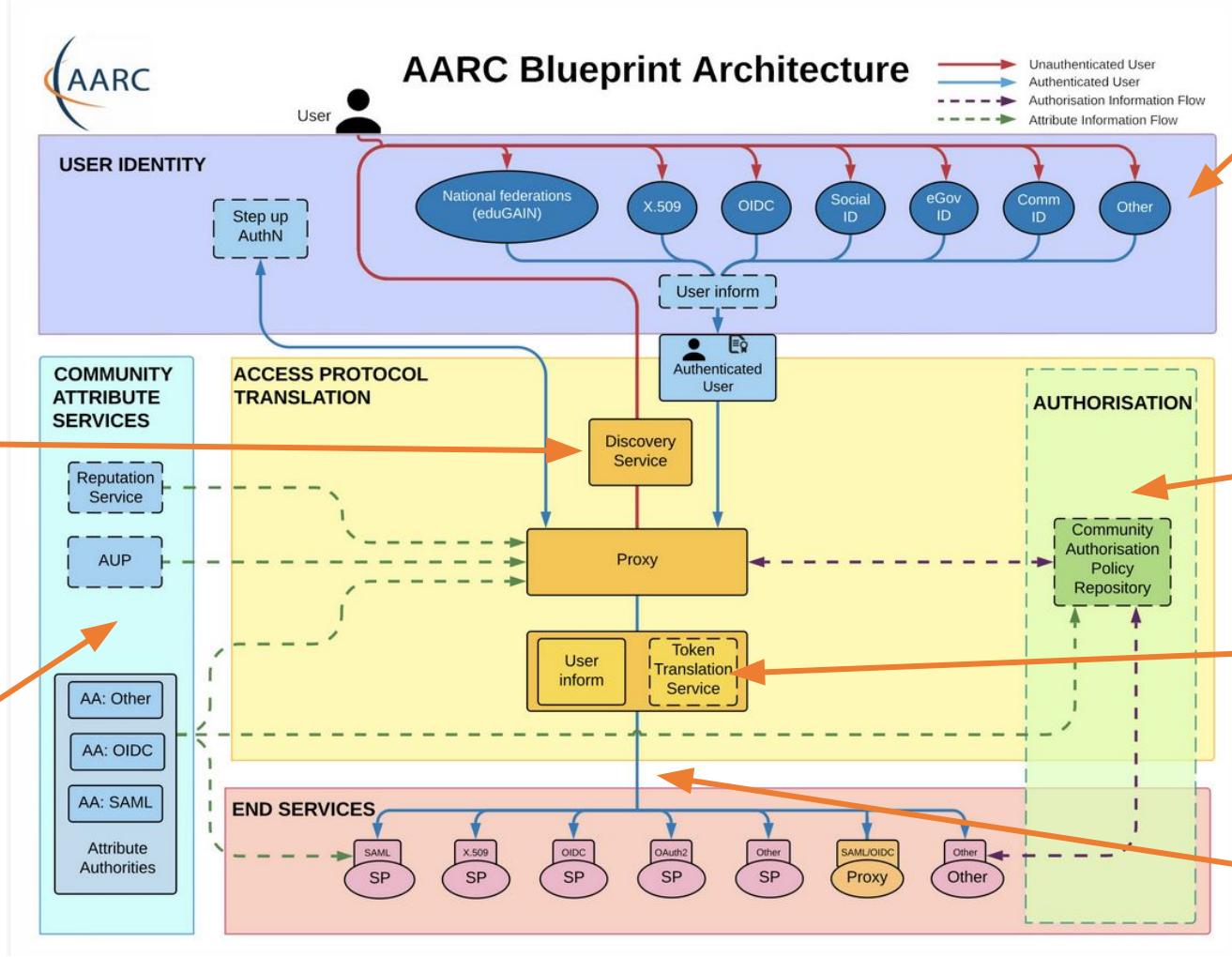
Connect multiple services

AARC BPA overview

Federated SSH access

MFA

Seamless User experience



Non-federated /R&E IdPs

Discovery service adapted for the RI

Access Policies

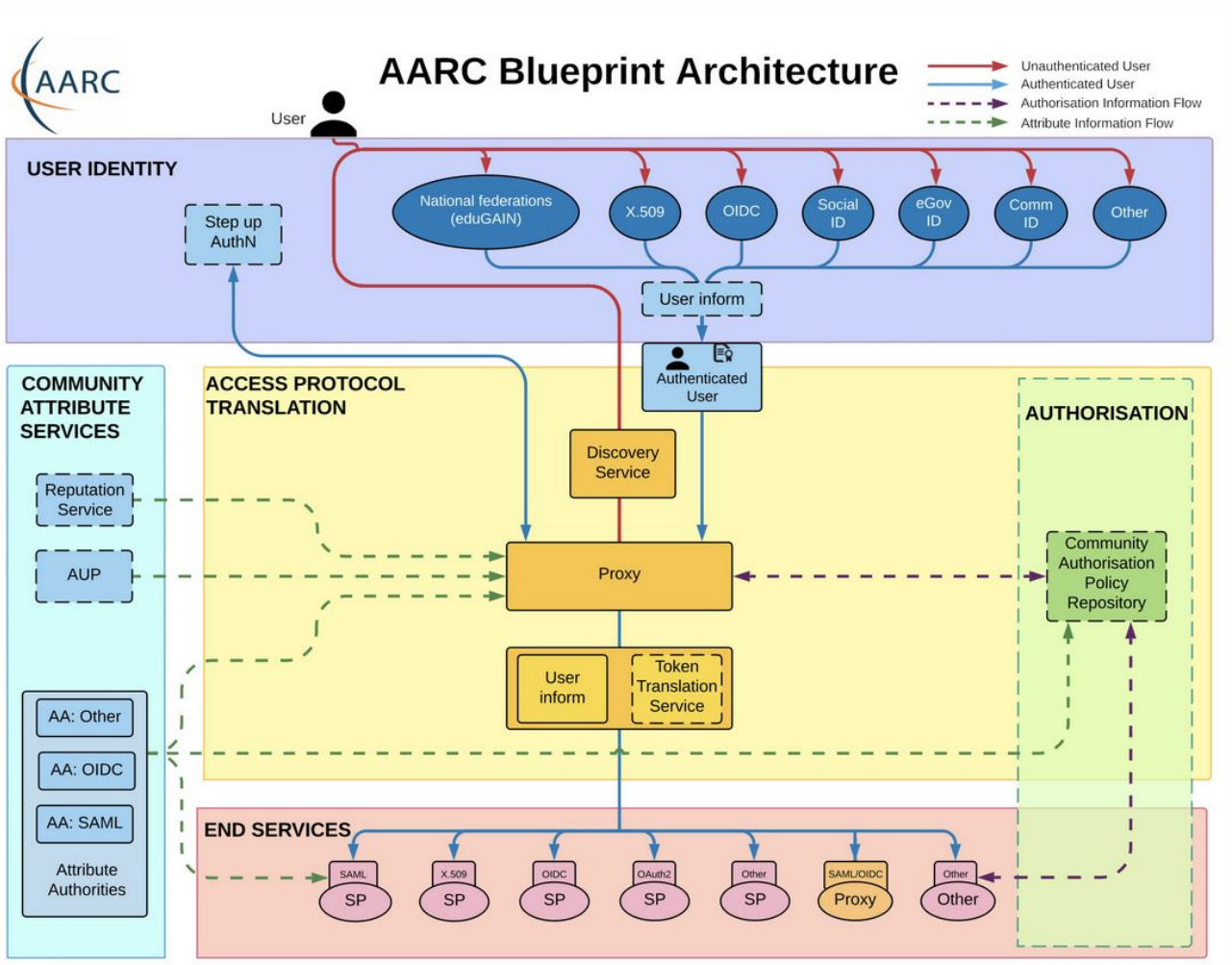
Membership management system

Protocol translation (OpenID to SAML)

Linking identities

Connect multiple services

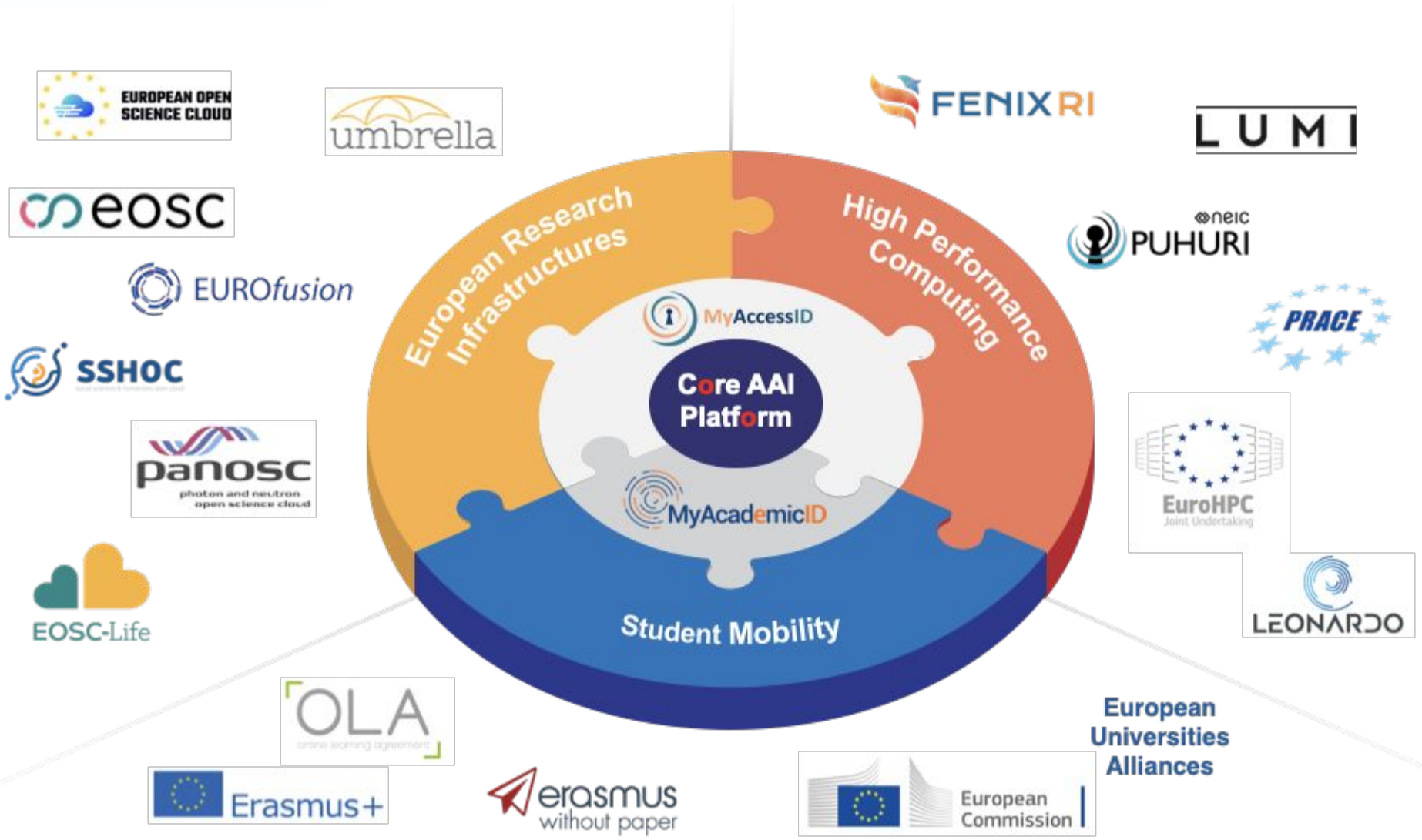
Interoperability in the AARC BPA: the AARC GUIDELINES



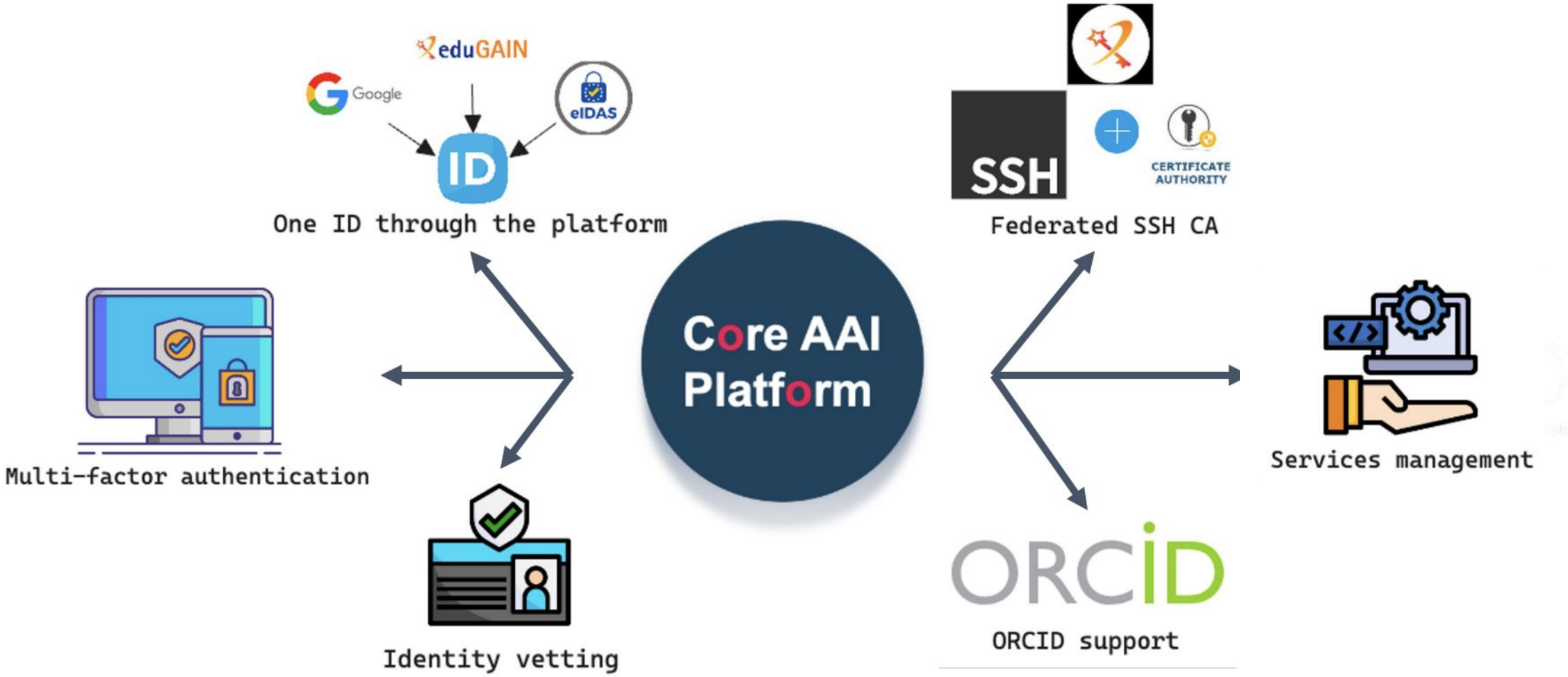
Document	Who should complete the template?	Audience	Description	Link
Top Level Infrastructure Policy	Infrastructure Management	All Infrastructure Participants (abides by)	This policy template defines the roles of actors in the Research Infrastructure and binds the policy set together	Google Doc
Incident 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

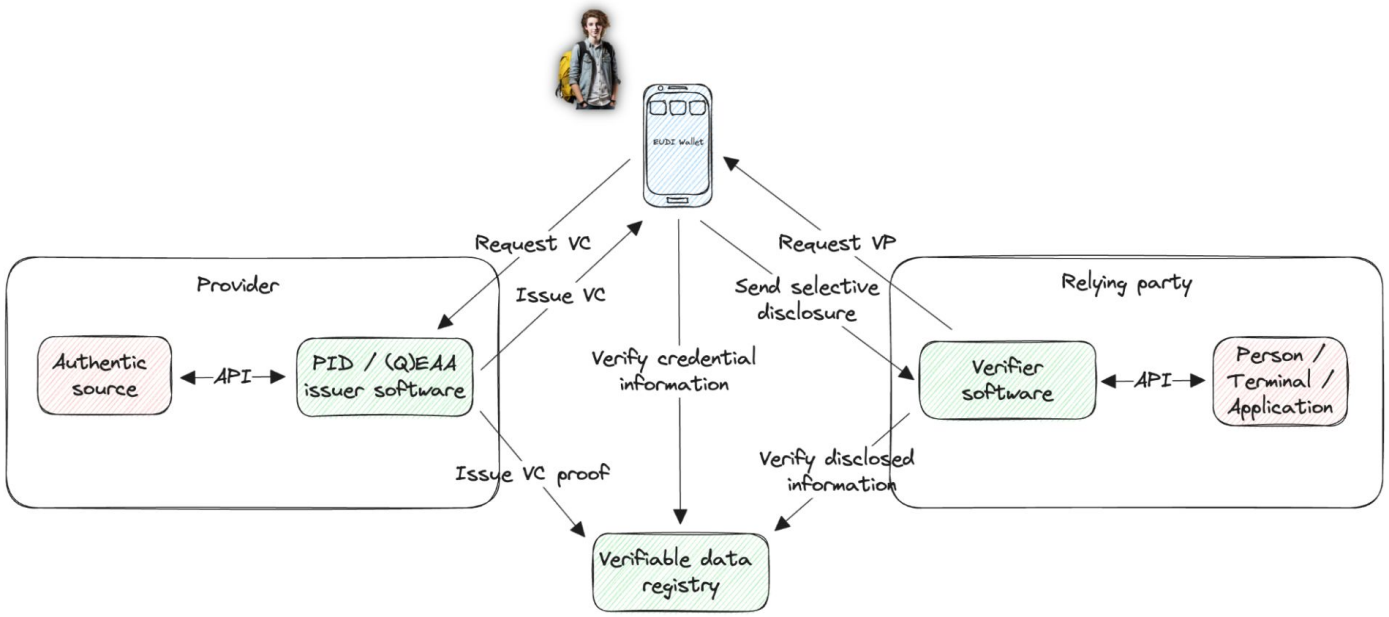
Identity and Access Management Solution for RIs



Complementing features



Looking forward - Wallets for research use cases



Researcher identity

Attestations of organisational affiliations

Entitlements, group membership or resources capabilities

Researcher accomplishments

Questions?

marina@sunet.se