Authentication and Authorisation for Research and Collaboration

What is maturing under the broad-leaved AARC-TREE

Supporting access for research communities with the BPA

Licia Florio, NORDUnet, licia@nordu.net
David Groep, Nikhef & Maastricht University, davidg@nikhef.nl
Christos Kanellopoulos, GEANT, christos.kanellopoulos@geant.org

TNC24 Rennes
"The Trust Roots That Make Research Grow"

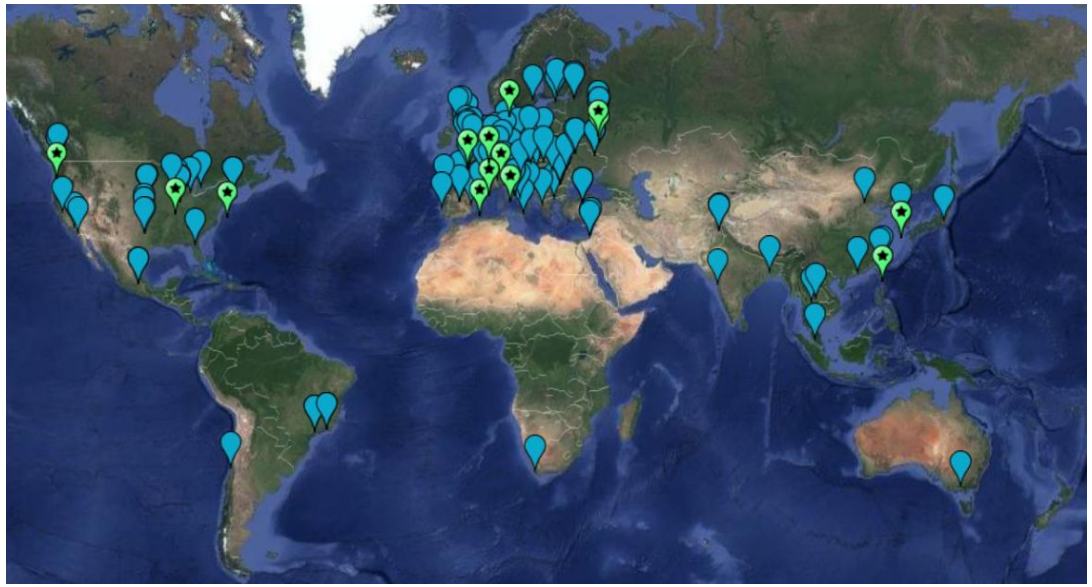
We live in a federated world! With researchers collaborating across borders

Collaboration: an inherently-cross-domain issue .. and an AARC solution?

Example from the LHC Computing infrastructure WLCG

170 sites
~50 countries & regions
~20000 users

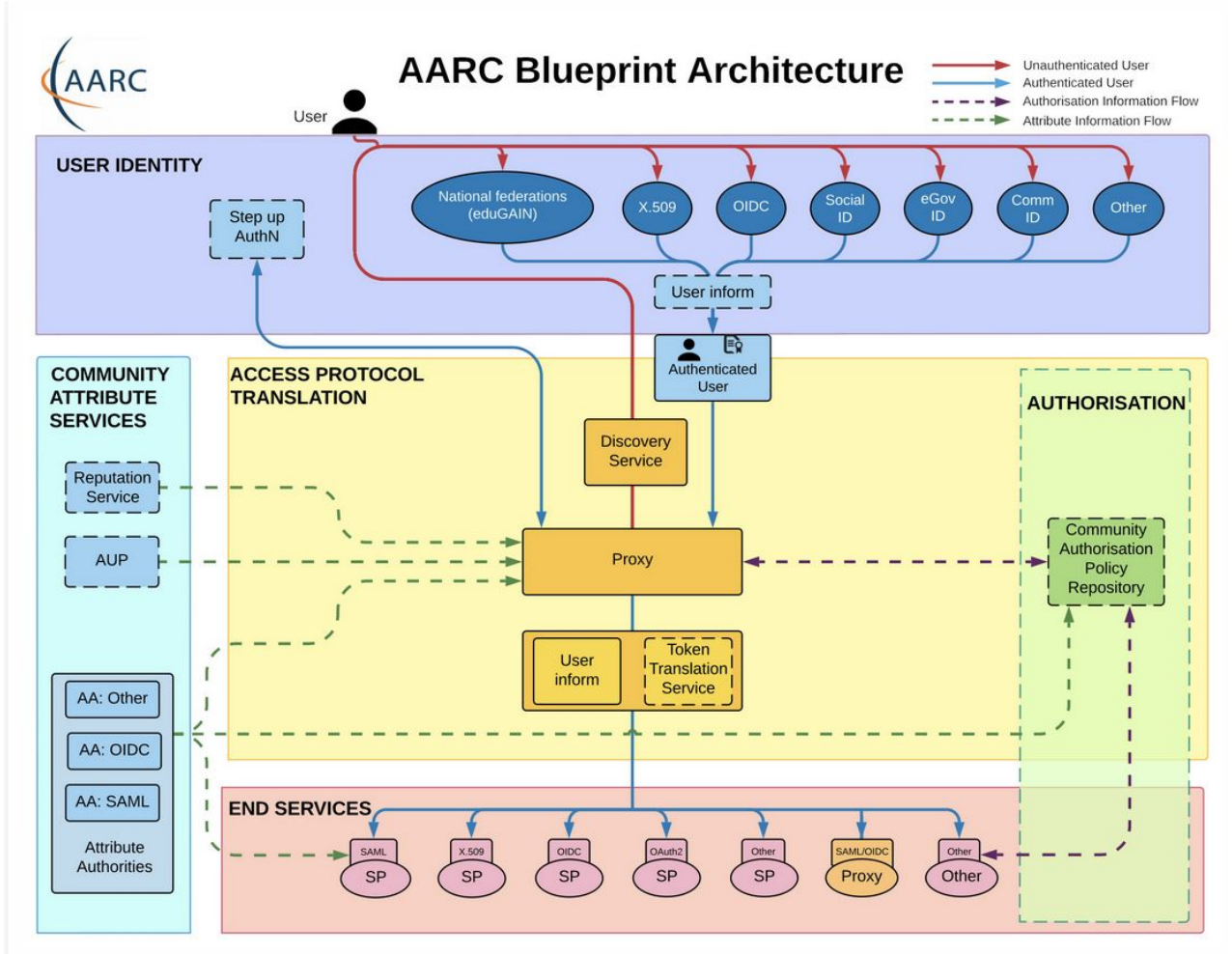
just *how* many interactions ??

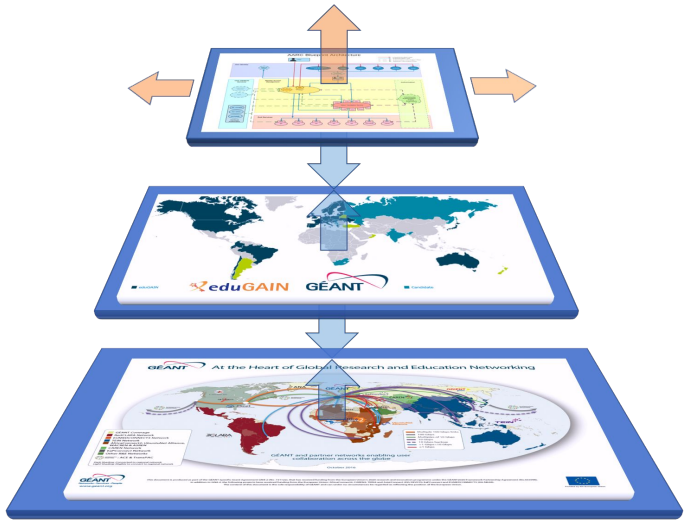


AuthN & AuthZ, **architecture and trust** should align with **collaboration structures**, and be **outward facing:** open, scalable, & multi-domain

people photo: a small part of the CMS collaboration in 2017, Credit: CMS-PHO-PUBLIC-2017-004-3; site map: WLCG sites from Maarten Litmaath (CERN) 2021

AARC Blueprint Architecture: one BPA many communities



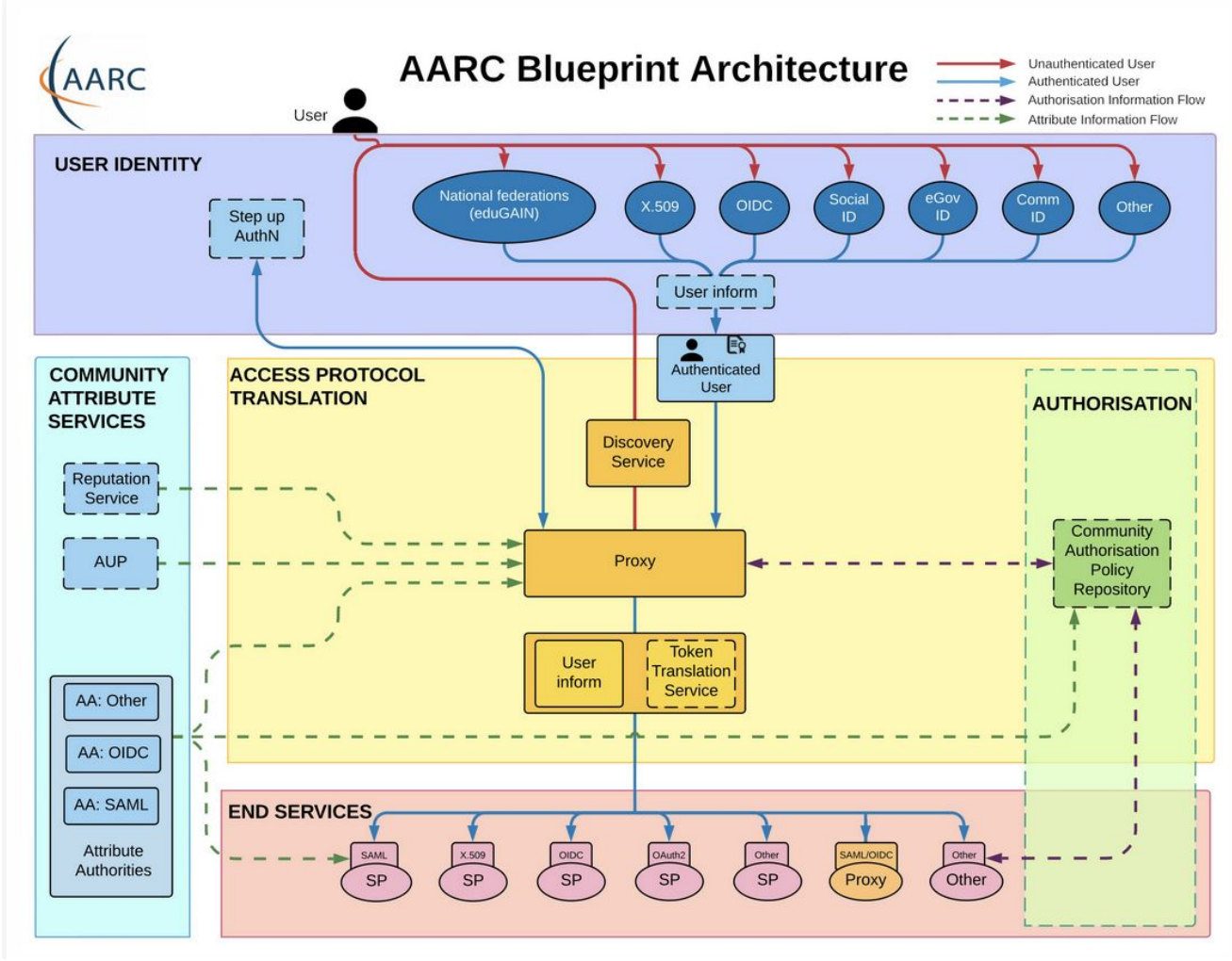


What is the AARC BPA?

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

Interoperability – more than just the nice colours



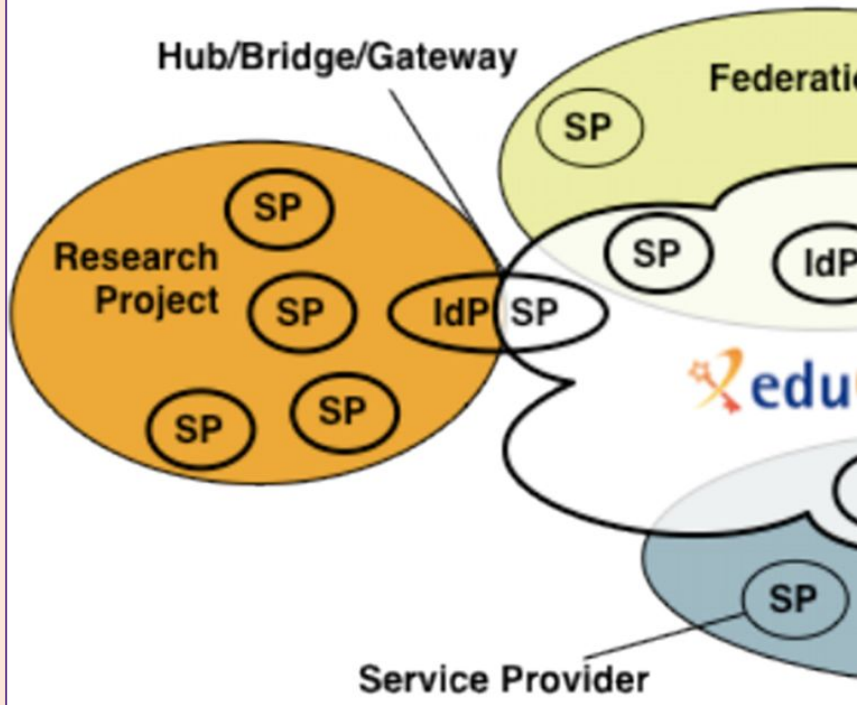
https://aarc-community.org/guidelines/

An AARC BPA to enable federated access for eScience

- Access services using **identities from users' Home Organizations**, but **hide complexity** of multiple IdPs, federations, AA technologies
- O**ne persistent identity** across all the community's services through **account linking**
- **Access** services **based on role(s)** users have **in the collaboration**.
- For both **web** and **non-web** resources
- Integration of **guest identity solutions**
- **Support for stronger authentication assurance** mechanisms

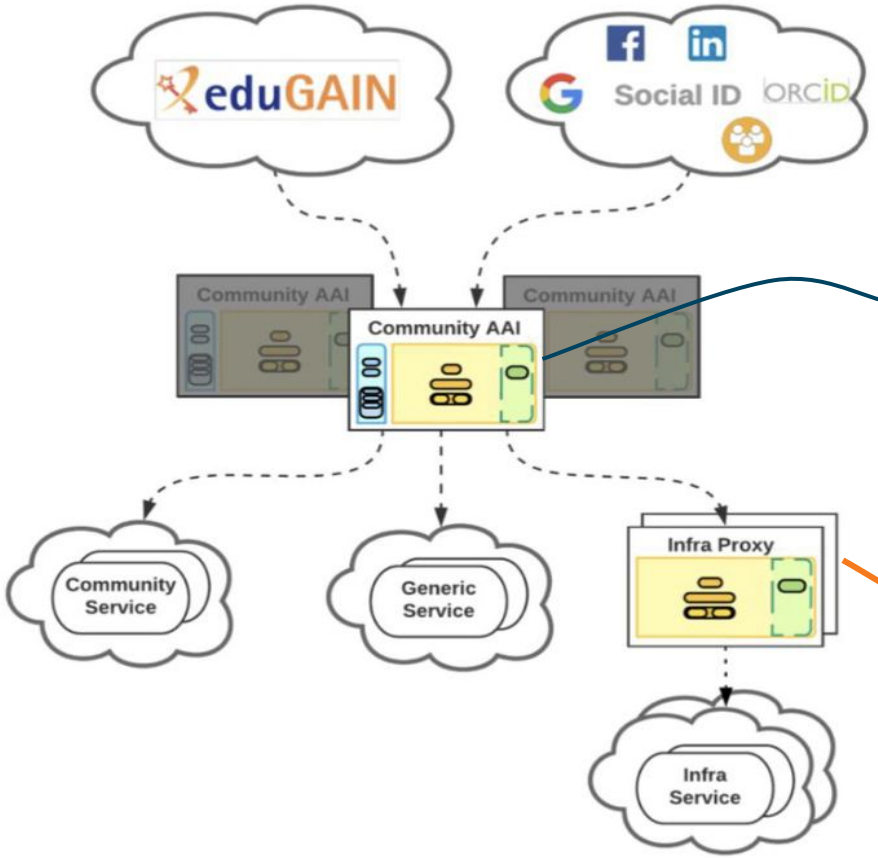
The AARC BPA: the IdP-SP proxy

- Access services using **identities from users' Home Organizations**, but **hide complexity** of multiple IdPs, federations, AA technologies
- One **persistent identity** across all the community's services through **account linking**
- **Access** services **based on role(s)** users have **in the collaboration**.
- For both **web** and **non-web** resources
- Integration of **guest identity solutions**
- **Support for stronger authentication assurance** mechanisms



Graphics: Ann Harding and Lukas Hammerle (SWITCH)– from a long time ago now!

The Community AAI and the Infrastructure Proxy – structuring elements



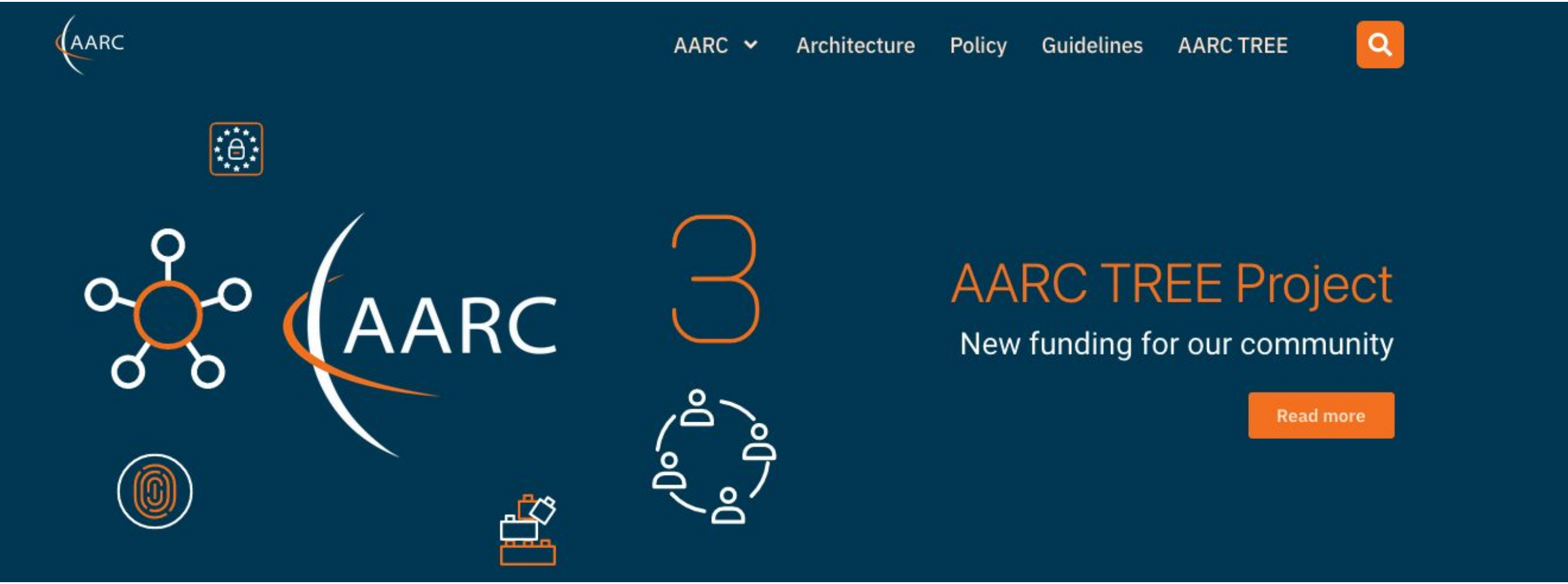
Community AAI

The purpose of the Community AAI is to streamline researchers' access to services, both those provided by their own infrastructure as well as the services provided by infrastructures that are shared with other communities.

Infrastructure Proxy

The Infrastructure Proxy, enables Infrastructures with a large number of resources, to provide them through a single integration point, where the Infrastructure can maintain centrally all the relevant Policies and business logic for making available these resources to multiple communities

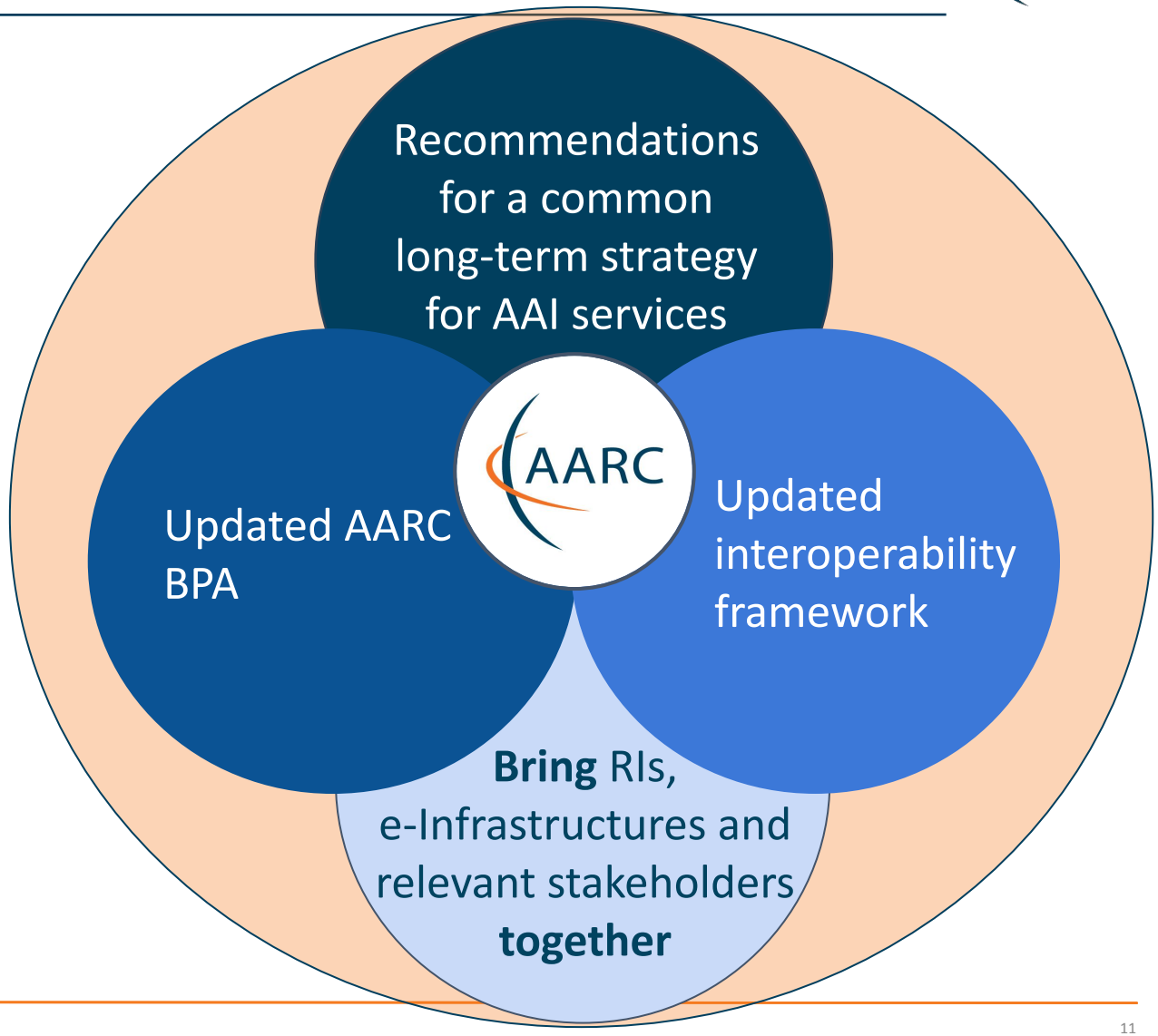
AARC TREE: new funding to enhance the impact of AARC



AARC Technical Revision to Enhance Effectiveness

AARC TREE Project Main Facts

Start date: March 2024
Duration: 24 M
22 Partners
NDN coordinator
2,5 M Euro

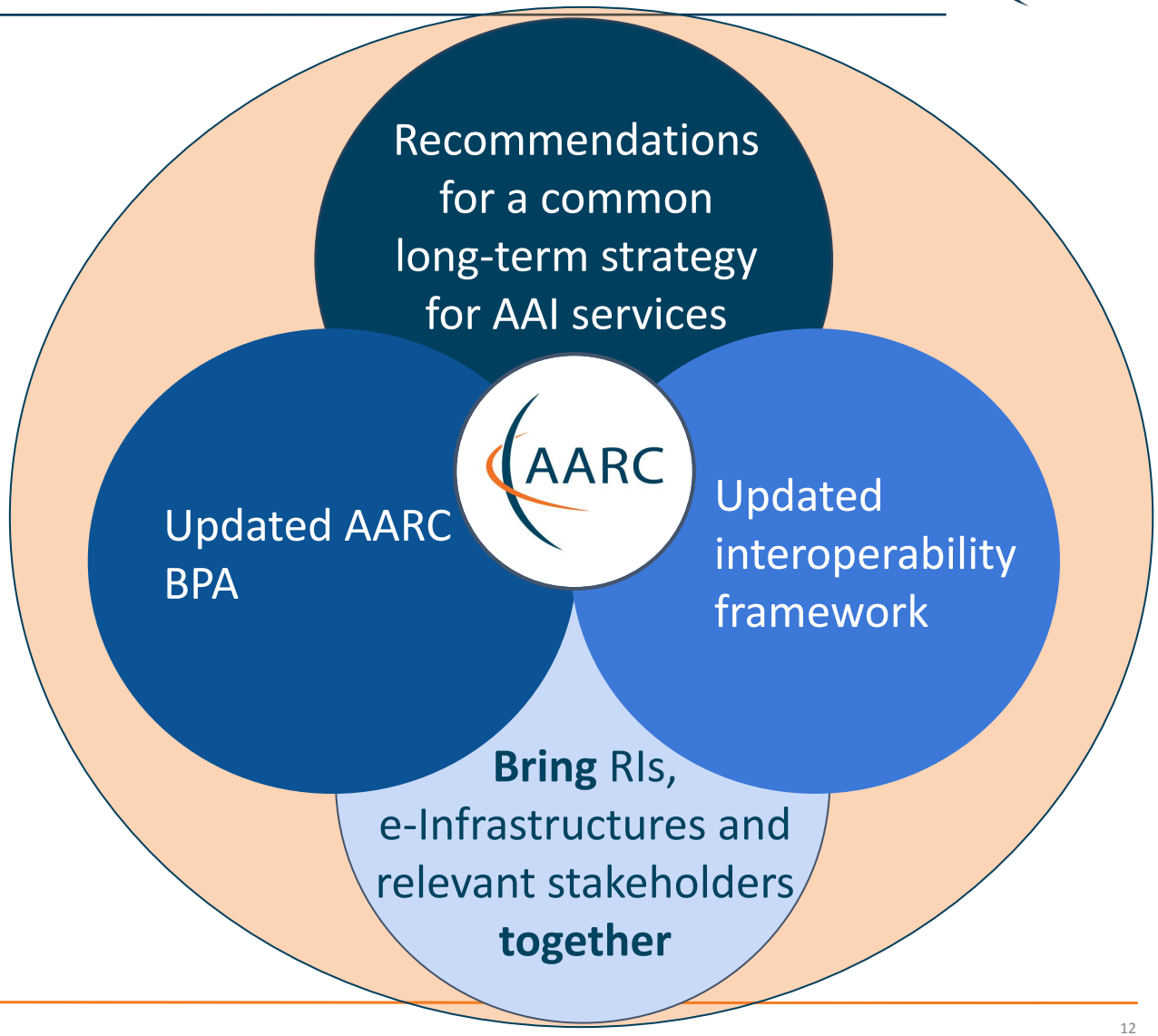


AARC Technical Revision to Enhance Effectiveness

AARC TREE Project Main Facts

Start date: March 2024
Duration: 24 M
22 Partners
NDN coordinator
2,5 M Euro

Make AARC3 a global activity to engage everyone interested in the evolution of AARC BPA



Challenges to address in AARC TREE

Interoperability with broader provider base (IdPs, eIDs, social IdPs)

Better uptake and integration of the BPA

Requirements for assurance

Service account information

Digital wallets

Proliferation of AARC Proxies

AARC Community - open for all

AARC Engagement Group for Infrastructures

The forum of e/r-Infras that operate an AARC BPA complaint AAI.
It's a closed group on purpose as we want to get feedback from the hands on group.
They approve the AARC guidelines.

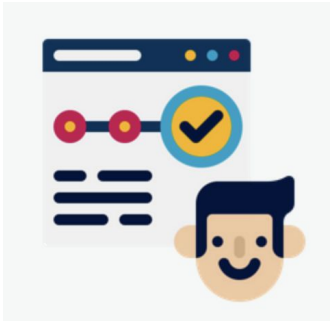
Technical WG

- Led by Nicolas and Christos
- Where technical guidelines are discussed
- Anybody can join the discussion: **https://lists.geant.org/sympa/info/aarc-architecture**

Policy WG

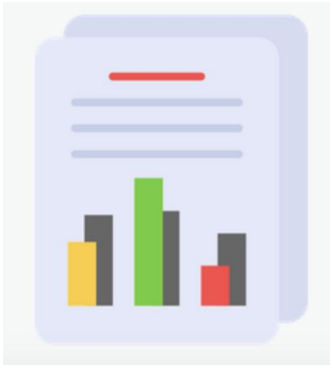
- Led by Dave and David
- Supported by EnCo and IGTF
- Anybody can join the discussion: **policy@aarc-community.org** https://lists.geant.org/sympa/info/aarc-na3

Right now in AARC TREE:
Time to engage ?



Use Cases Collection and Analysis

with the large ESFRI RIs, clusters, and national nodes to validate BPA effectiveness and act as a flywheel to increase its application



Compendium & Recommendations

Have the validators and use cases have a broader impact by promoting them as ‘community good practice’ examples – and telling the world about it.

Dedicated work package to collect requirements from (new) communities

Landscape analysis of AARC BPA adoption

- Conduct an AARC BPA **adoption survey** among the RIs,
  online survey accompanied by the arranged conversations with the individual RIs
- Collect information on current deployment of AARC BPA AAIs and adoption of guidelines

Result: **Landscape analysis of AARC BPA adoption (around December 2024)**

Use cases requirements & consultations

- Design and create survey (including technology and policy questions)
  based on FIM4Rv2 paper, Evolution, EOSC AAI TF requirements
- Engage FIM4R, AEGIS, EOSC AAI TF, National Ris, EU data spaces to capture requirements
- Discus with our ESFRIs to get expectations & requirements via consultations, workshops etc

Result: **Use cases requirements described in a white paper (target Q1 2025)**

Handover to Compendium

Compendium and Recommendations

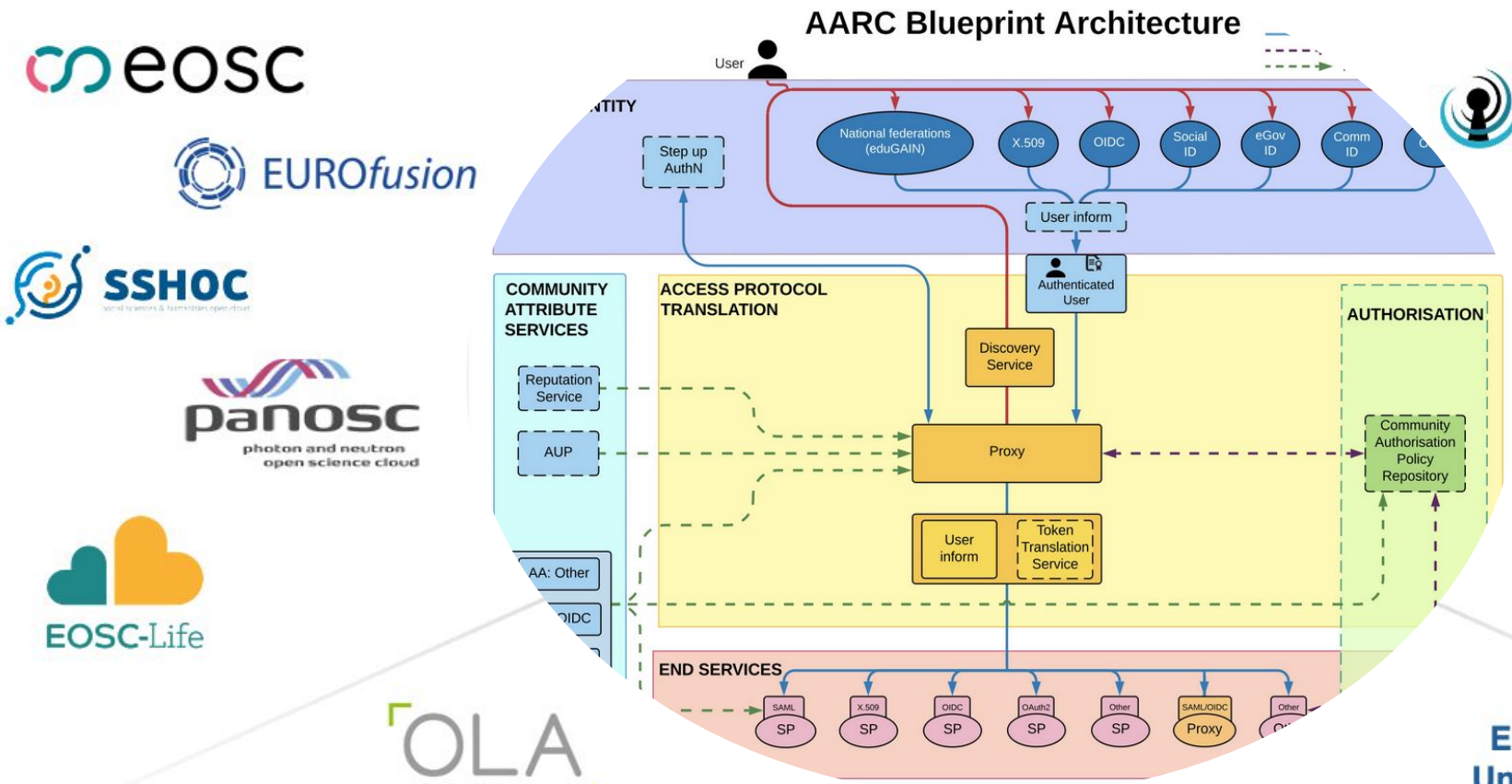
Key result in the '2nd year' (April 2025 - February 2026) is the **Compendium**

'**compendium of AARC best practices'** with **recommendations** for a common long-term strategy for AAI services in pan-European Research Infrastructures in Europe

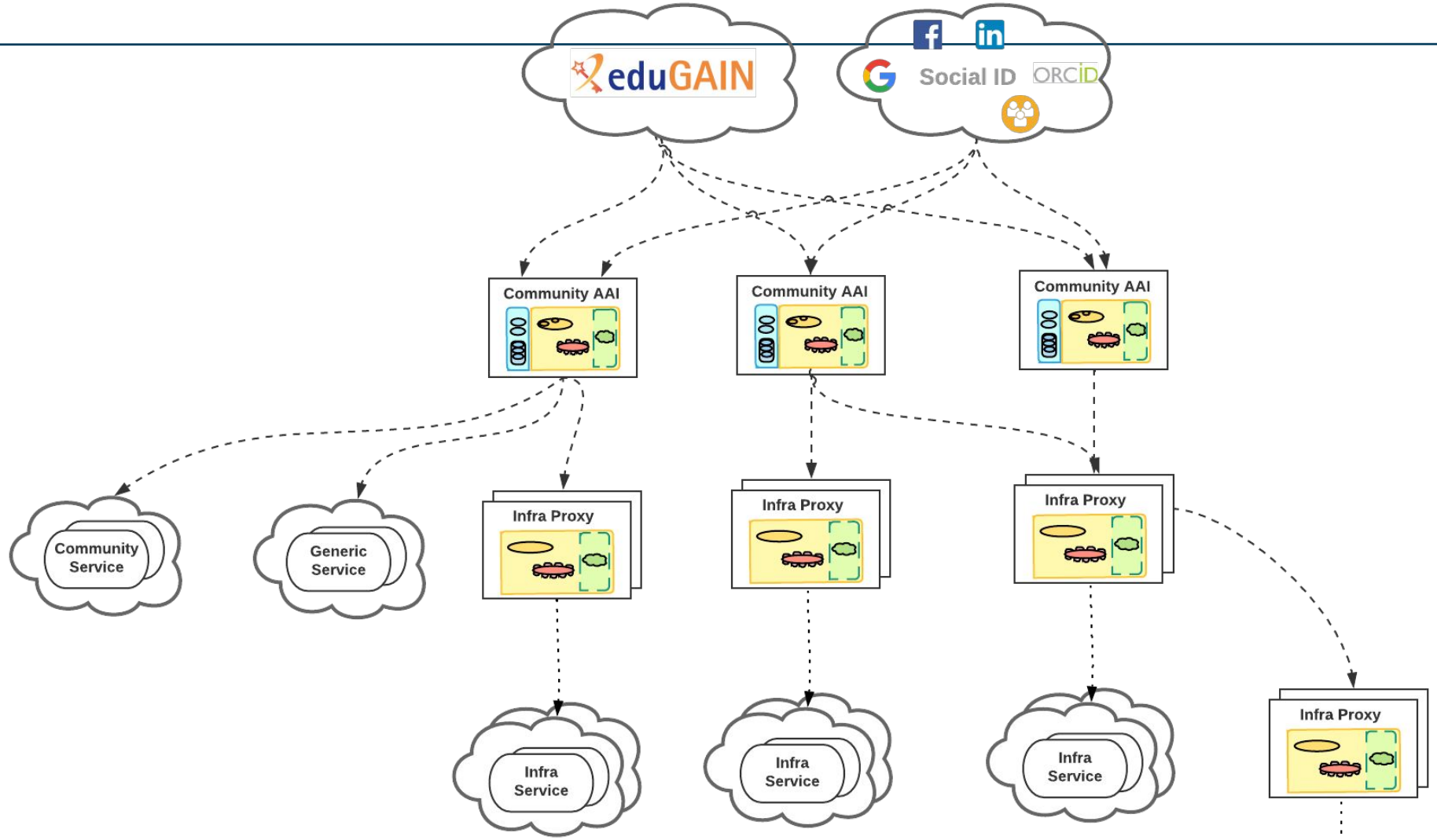
- based on the use case input and researcher requirements
- promotes coherent and interoperable architecture and policy
- **iterate and validate** with the infrastructures at large

describe the road that collaborative research infrastructure AAI will take!

Part II: AARC BPA Technical Guidelines


AARC Blueprint Architecture
User
Step up AuthN
National federations (eduGAIN)
X.509
OIDC
Social ID
eGov ID
Comm ID
User inform
Authenticated User
COMMUNITY ATTRIBUTE SERVICES
ACCESS PROTOCOL TRANSLATION
AUTHORISATION
Discovery Service
Reputation Service
AUP
Proxy
Community Authorisation Policy Repository
User inform
Token Translation Service
AA: Other
END SERVICES
SAML
SP
X.509
SP
OIDC
SP
OAuth2
SP
Other
SP
SAML/OIDC
Proxy
Other

And of course with more AARC Compliant AAIs come more proxies



… it's time for a Technical Revision to Enhance Effectiveness!

Community User Identifiers (CUID)

Problem

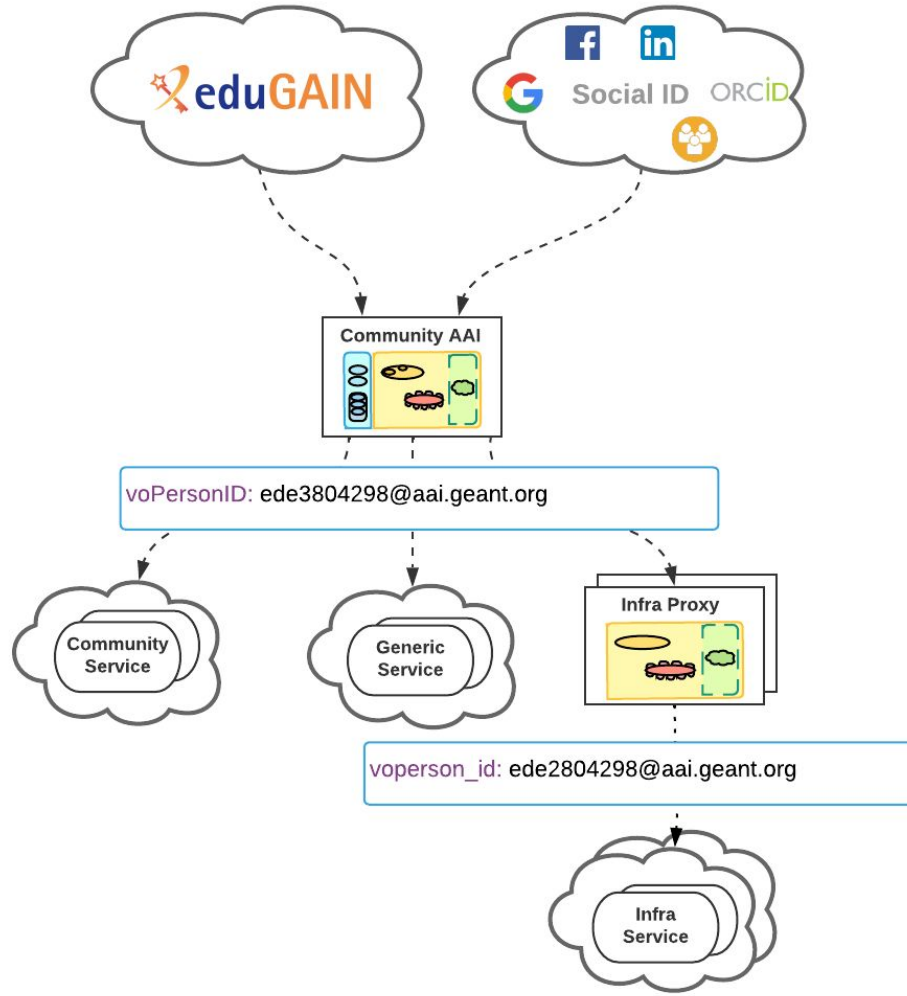
- How to identity the user uniquely and persistently across AAIs that implement the AARC BPA

Guidelines

- AARC-G026 - Guidelines for expressing community user identifiers

Summary

- A subject identifier, where the subjects are generally but not exclusively natural persons.
- Identifies the subject across AAIs
- Non-reassignable, persistent
- Managed by the Community AAI



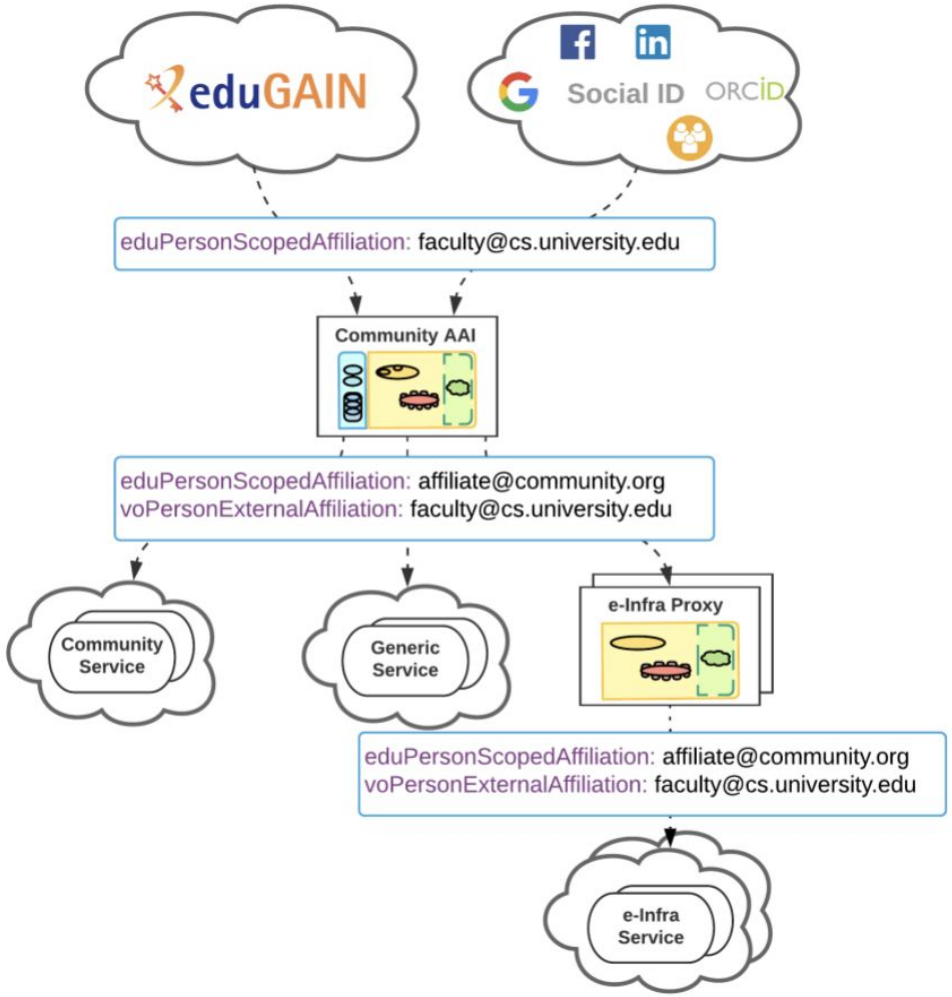
Authorisation and affiliation in community use cases

Problem

- How to communicate affiliation of a user with the community

Guidelines

- AARC-G025 - Guidelines for expressing affiliation information
- AARC-G057 - Inferring and constructing voPersonExternalAffiliation

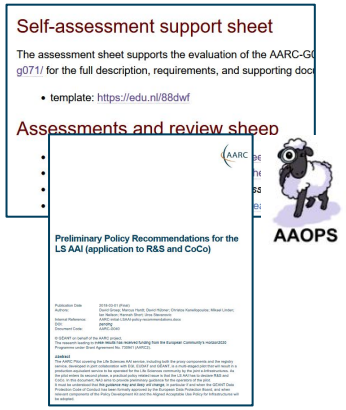


Parte III: How to Establish Trusted and Secure Operations

Policy and good practice underpinning the AARC Blueprint BPA

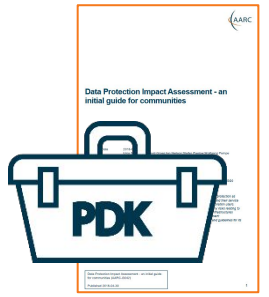
Infrastructure alignment and policy harmonisation: helping out the proxy

- **Operational Trust** for Community and Infrastructure BPA Proxies
- Increase acceptance of research proxies by identity providers through **common baselines**
- Review infrastructure models for **coordinated AUP, T&C, and privacy notices**, improving cross-infrastructure user experience (users need to click only once)



User-centric trust alignment and policy harmonization: helping out the community

- Lightweight community management policy template
- Guideline on cross-sectoral trust in novel federated access models
- Assurance in research services through (eIDAS) public identity assertion



How to establish secure operation for your (AARC BPA) proxy?

The Challenge

- How to securely operate proxies, attribute authorities and issuers of statements for entities?

Guideline

- AARC-G071 Guidelines for Secure Operation of Attribute Authorities

Summary

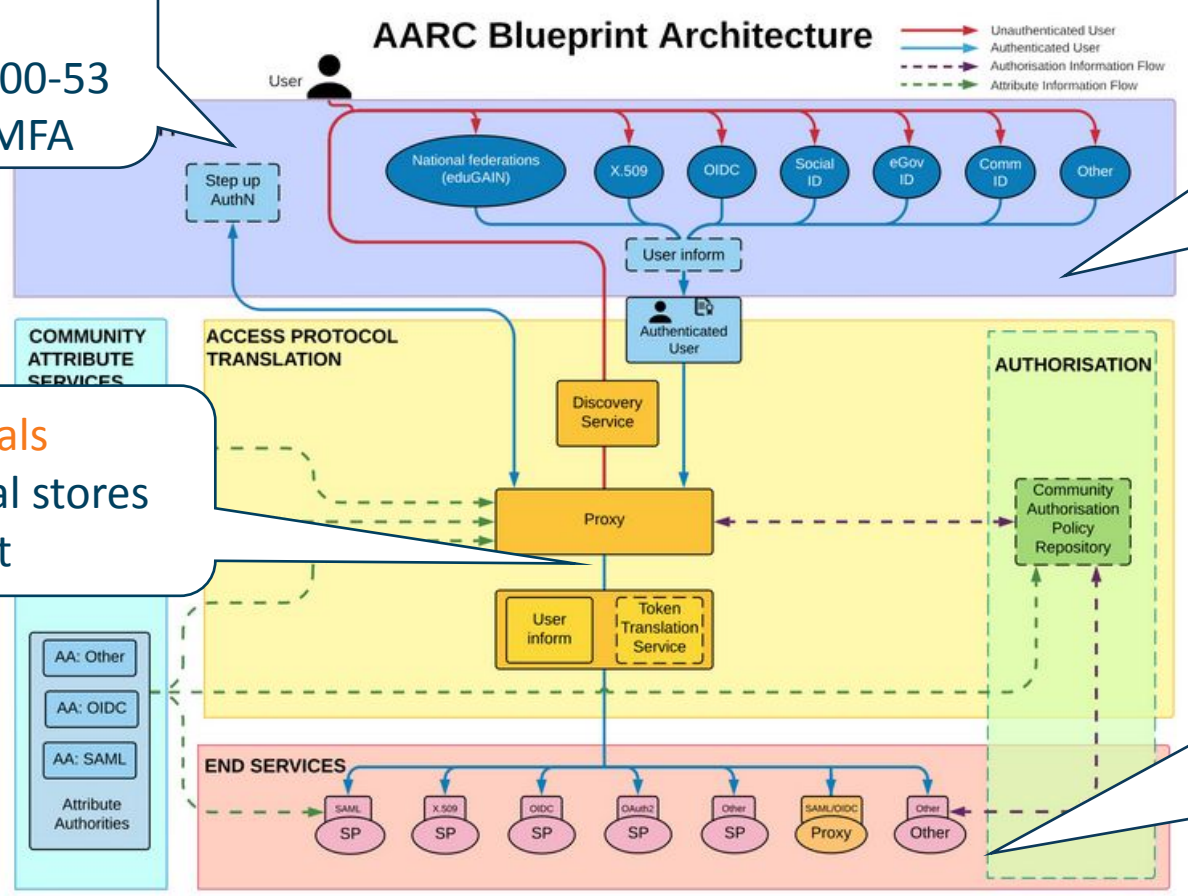
- Operational security processes and procedures
- Requirements on traceability, auditability, and logging
- Requirements on the secure operation
- Requirements on securing the interactions

Guidelines for Secure Operation of Attribute Authorities and issuers of statements for entities

Publication Date	2022-04-11
Authors:	Members of the IGTF and the AARC Community; David Groep; Ian Collier, Tom Dack; Jens Jensen; David Kelsey; Maarten Kremers; Ian Neilson; Stefan Paetow; Hannah Short; Mischa Sallé; Uros Stevanovic
With feedback from	Marina Adomeit; Sander Apweiler; Jim Basney; Christos Kanellopoulos; Johannes Reetz
AARC Document Code:	**AARC-G071**
Supported by:	*This guideline is a joint work of the International Global Trust Federation IGTF, the AARC community, and global partners. The research leading to these results has received funding from the European Community's Horizon2020 Programme by way of the AARC2 project (Grant Agreement No. 730941), EOSC-hub (Grant Agreement 777536), as part of the GÉANT 2020 Framework Partnership Agreement (FPA) under Grant Agreement No. 856726 (GN4-3), as well as from other sources*
Publishing Organisations:	IGTF and AARC Community
DOI:	https://doi.org/10.5281/zenodo.5927799

Operational guideline landscape for - proxy or source - AAI components

RFC6238/4226
FIPS140
NIST SP800-53
REFEDS MFA



Authentication/identity sources
Sirtfi
(eduGAIN) baselining, RAF
IGTF AP Profiles
NIST SP800-63
eduGAIN sec. team workflow

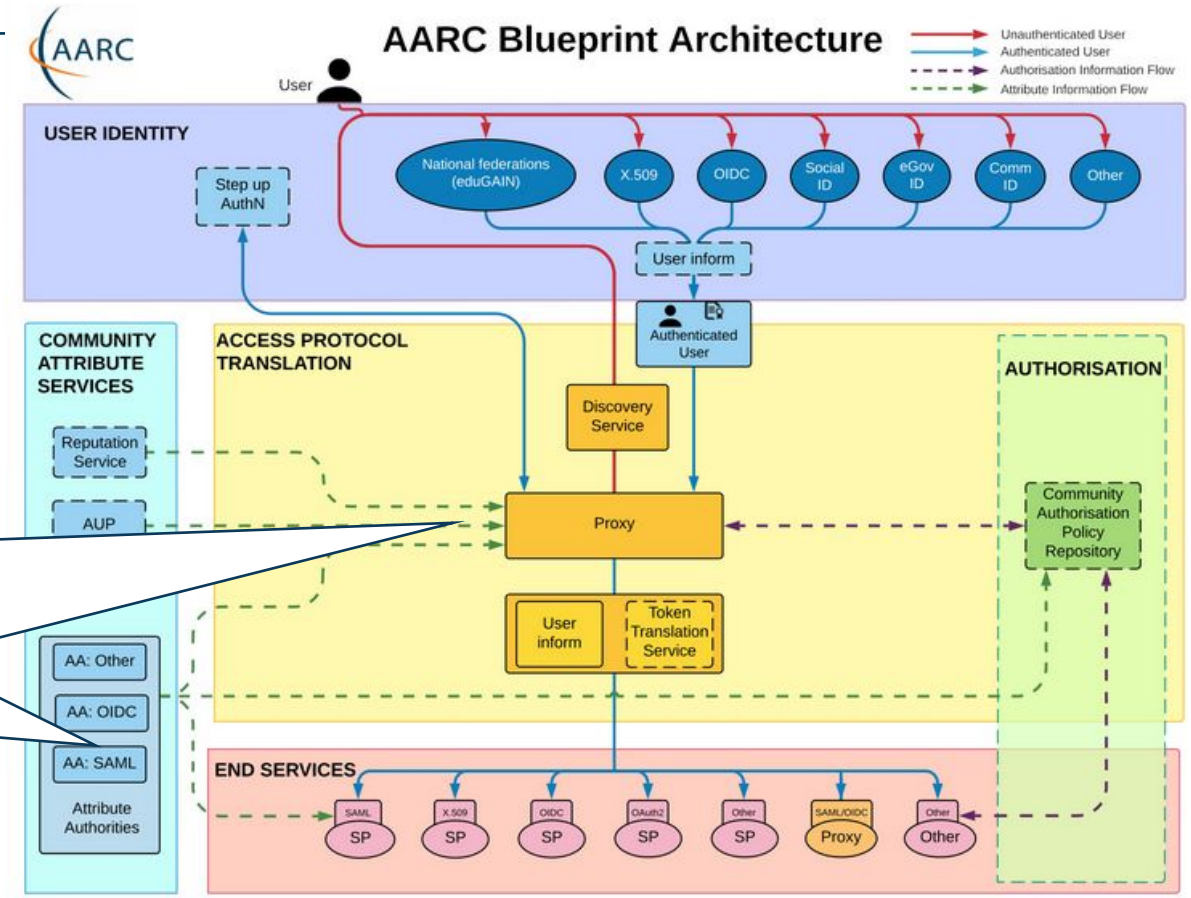
Ephemeral credentials
- trusted credential stores
- protection at rest

Service provider operations
ISO27k
Sirtfi
Infrastructure response plans

Operational security focus in the BPA: beyond just the IdPs

Community membership management directories and attribute authorities

- integrity of membership
- identification, naming and traceability
- site and service security
- protection on the network
- assertion integrity



Guidelines for Secure Operation of Attribute Authorities and other issuers of access-granting statements
(AARC-I048, in collaboration with IGTF AAOPS)

When the AA is in a managed environment …

Many of the recommendations are already implemented 'implicitly'

- because common software implements it: e.g. signing SAML assertions and JWTs
- because a good data centre already has network monitoring and central logging in place
- because you signed up to Sirtfi (didn't you?) – so you collaborate in incident response
- because you have trained IT operations personnel looking after the service

And some are intuitive best practice

- like assigning a unique and lasting name to a group
- because implemented controls ought to be those that have been documented

Some items contain reminders about appropriate values and recommendations that are good practice - based on the relevant standards involved

Deployment guidance included …

4.2. Attribute Management and Attribute Release

AMR-1

The Community must define and document the semantics, lifecycle, data protection, and release policy of attributes stored or asserted by the AA.

The community should follow the guidance from relevant policy documents. In particular, the Policy Development Kit has recommendations on Community Membership Management. It is recommended to use standardised attributes where possible, e.g. from eduPerson [EPSC] or SCHAC [SCHAC], and their semantics must be respected.

If Communities make modifications to the attribute set, their semantics, or release policies, it is recommended that they inform both their relying parties as well as the AA Operator thereof, since the AA operator may have implemented checks for schema consistency. The Community is ultimately responsible for the values and semantics of the attributes.

AMR-2

The AA Operator must implement the community definitions as defined and documented, for all the AAs it operates.

By implementing these requirements, the AA operator will support the chain of trust between Community and the RPs. An AA Operator must only host those communities for which it can implement the requirements.

AMR-3

It is recommended that the AA Operator provide a capability for the community to

AARC-G071 Example requirement: Attribute Assertions

AAS-3

If an AA Operator issues assertions containing a lifetime, this lifetime must be compliant with the Community policies, **as short as reasonably possible**, and the assertion must not be valid beyond the validity period of the attributes it contains. **The Community Management is responsible for the content of the assertion, as issued, during its entire lifetime**

AAS-4

Re-issuance of assertions must be based on information held in the AA at the time of re-issuance.

AARC-G071 example requirement: Operational Environment

OE-1

Through its personnel or by contractual measures, the AA Operator should ensure appropriate controls are in place over the security context.

OE-2

The AA must be located in a physically secure environment where access is controlled and limited to specific trained personnel.

OE-3

The protections on the AA and its operational environment, including the credentials of the AA administrators and operators, should **meet or exceed the requirements of all of the communities hosted in the AA**.

AARC-G071 Example requirement: Assessment and Peer Review

AR-5

The AA operator must **disclose and discuss**, on request, those aspects of their operational environment that are relevant to the evaluation of the security and trust by the Communities and Relying Parties.

AR-6

The AA Operator must be able and willing to **collaborate with affected organisations in the management of a security incident**.

AR-7

The AA Operator should review roles, rights, and access of its staff at least once per year.

AARC-G071 Example requirement: Relying Party Obligations “the other side”

RP-1

Relying Parties must, at the time of reliance, verify the integrity and validity of attribute assertions and any binding to a valid subject, to their satisfaction.

RP-2

Relying Parties must rely on assertions with an explicit lifetime only during their validity period.

RP-3

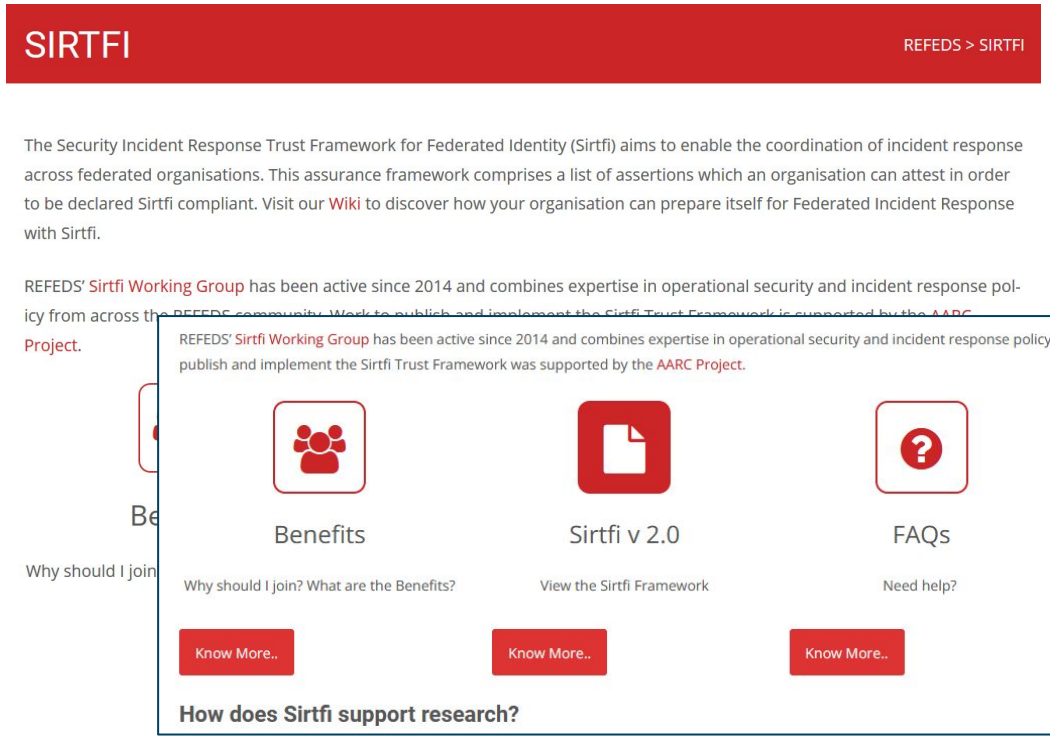
Relying Parties must assess the **risk of relying on assertions with no explicit lifetime** and should not rely on them for longer than the relevant industry standards for that type of assertion recommend.

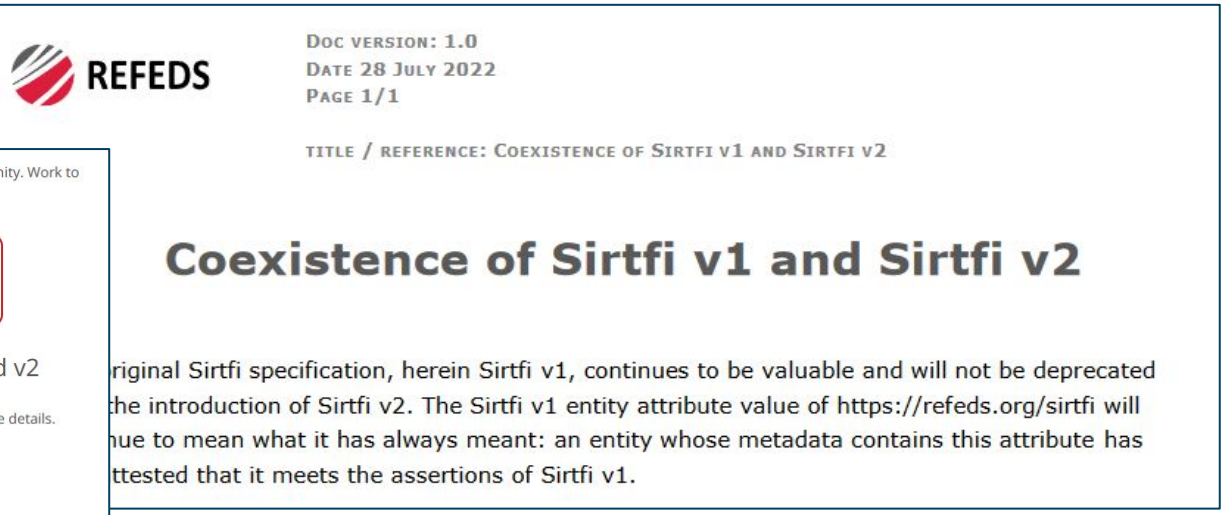
RP-4

Any long-lived, non-revocable statements received from an AA must be appropriately protected for confidentiality and integrity, by proxies and other intermediate entities.

Links to (probably) most well-known AARC outcome for security …

Security Incident Response Trust Framework for Federated Identity



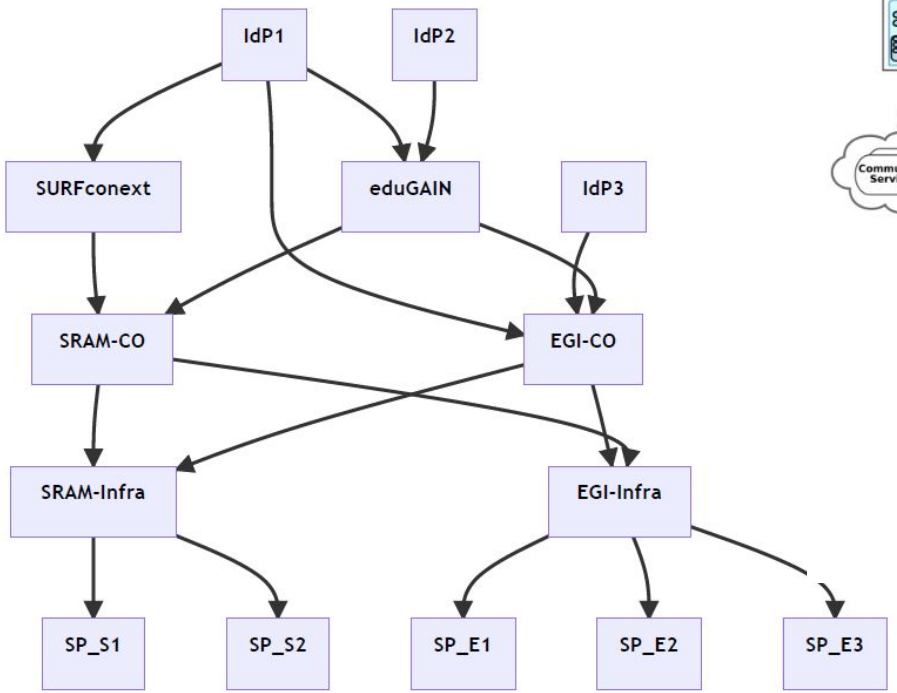


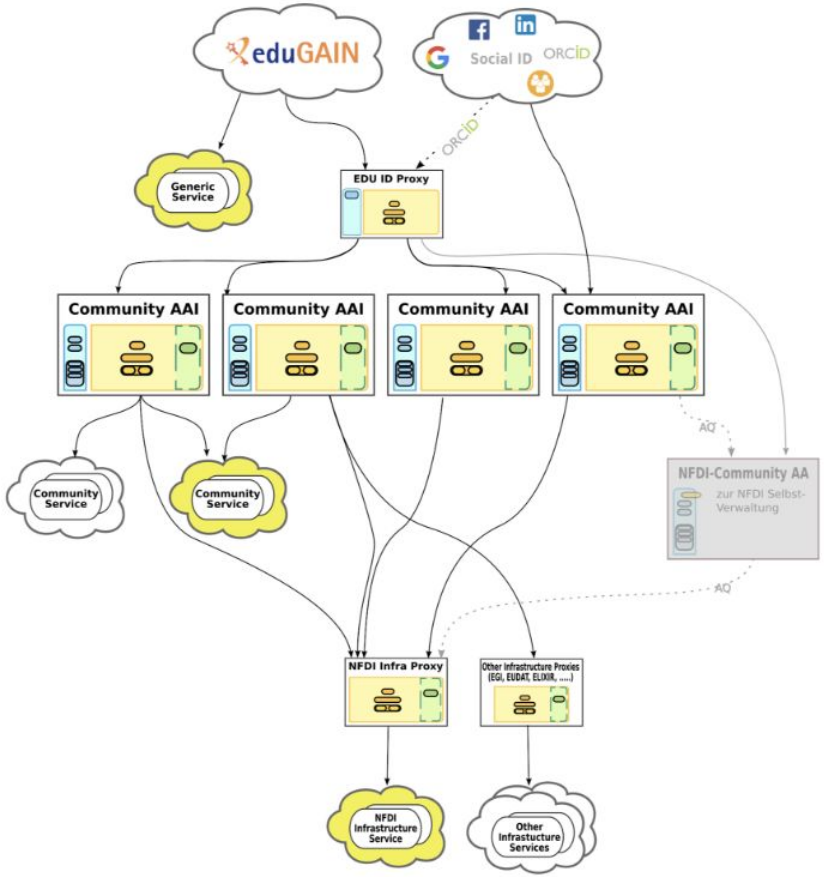
https://refeds.org/SIRTFI

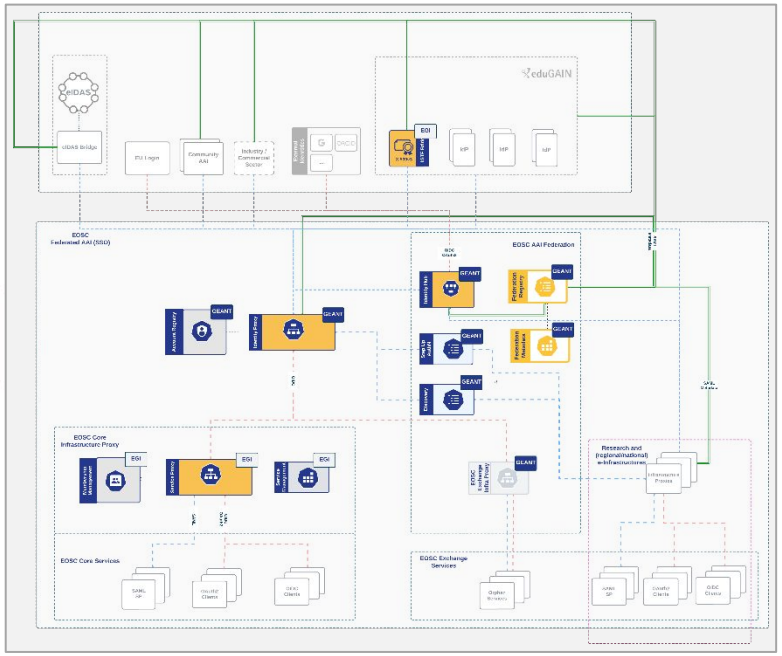
SIRTFI
Security Incident Response Trust Framework for Federated Identity

2. A new assertion, [IR3], was added that requires security contacts of entities participating in Sirtfi to be notified when a security incident investigation suggests that those entities are involved in the incident.

Our federated world is growing more complex

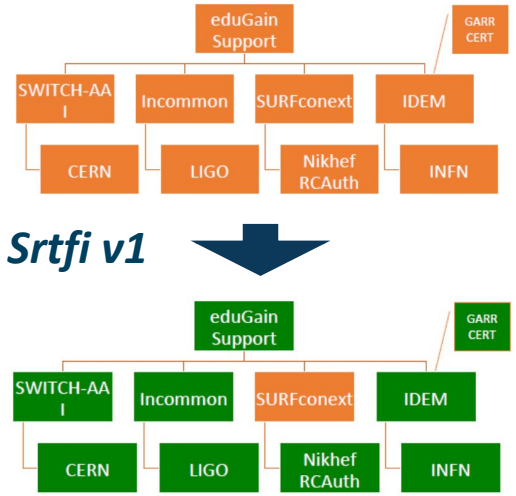


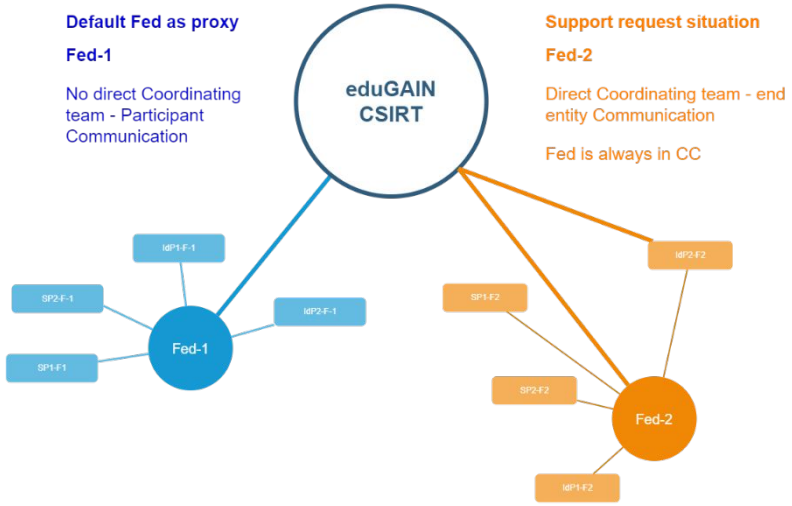


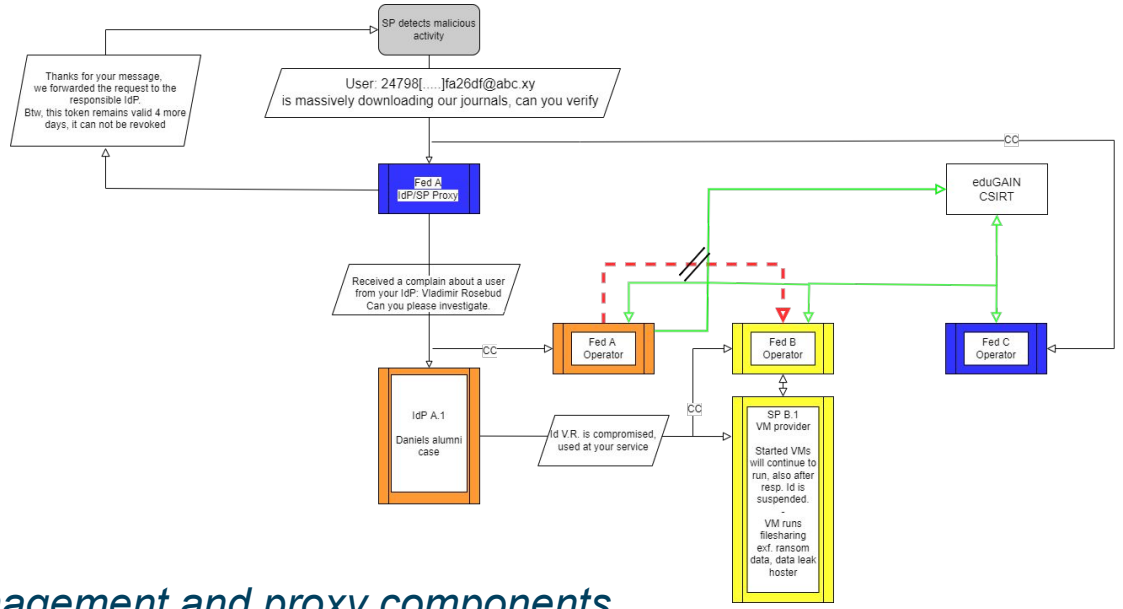


Images: SURF SSRAM and EGI by Maarten Kremers, NDFI AAI (Marcus Hardt), EOSC AAI for the EOSC Core and Exchange Federation for the EOSC European Node by Christos Kanellopoulos, Nicolas Liampotis, David Groep (June 2023 version)

Response and traceability across IdP-SP Proxies and the limits of Sirtfi







*Guidelines for a joint **operational trust baseline** for membership management and proxy components, supplemented by policy guidance for sectoral federations with more specific policies where needed*

- *'How can we **convey the trust in what is in and behind the proxy**?'*
- *'How to provide **timely traceability** between services and identities through the proxy?'*

Based on requirements from FIM4R, WISE, and the proxy operators in AEGIS.

Sirtfi

GÉANT | eduGAIN | CSIRT

joint work with GN5-1 EnCo and eduGAIN CSIRT

images: AARC Sirtfi v1 exercise (Hannah Short), eduGAIN security TTX (Sven Gabriel, eduGAIN CSIRT)

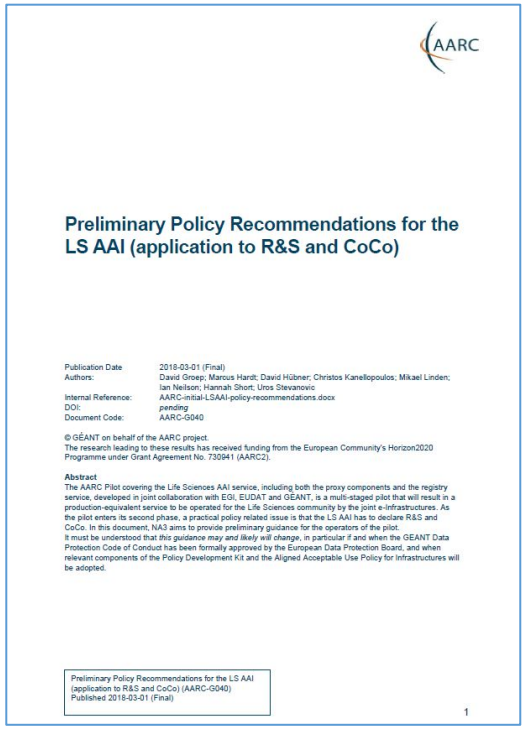
Proxies have more challenges as well: AUPs, T&Cs, Privacy notices, …

For large ‘multi-tenant’ proxies

- some subset users in some communities use a set of services –
  how to present their Terms and Conditions and their privacy policies, so that users
  - only see the T&Cs and notices for services they will access
  - this does not to need to be manually configured for each community
  - is automatically updated when services join

For community and dedicated proxies

- when new (sensitive) services join, who needs to see the new T&Cs?
- can we communicate existing acceptance of T&Cs to downstream services?


Preliminary Policy Recommendations for the LS AAI (application to R&S and CoCo)

Publication Date 2018-03-01 (Final)
Authors: David Groep; Marcus Hardt; David Hübner; Christos Kanellopoulos; Mikael Linden; Ian Neilson; Hannah Short; Uros Stevanovic
Internal Reference: AARC-initial-LSAAI-policy-recommendations.docx
DOI: pending
Document Code: AARC-G040

The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2).

Abstract
The AARC Pilot covering the Life Sciences AAI service, including both the proxy components and the registry service, developed in joint collaboration with EGI, EUDAT and GÉANT, is a multi-staged pilot that will result in a production-equivalent service to be operated for the Life Sciences community by the joint e-Infrastructures. As the pilot enters its second phase, a practical policy related issue is that the LS AAI has to declare R&S and CoCo. In this document, NA3 aims to provide preliminary guidance for the operators of the pilot.
It must be understood that *this guidance may and likely will change*, in particular if and when the GÉANT Data Protection Code of Conduct has been formally approved by the European Data Protection Board, and when relevant components of the Policy Development Kit and the Aligned Acceptable Use Policy for Infrastructures will be adopted.

beyond AARC-G040

What is an acceptable user experience in clicking through agreements?
What is effective in exploiting the WISE Baseline AUP? What do researchers need?

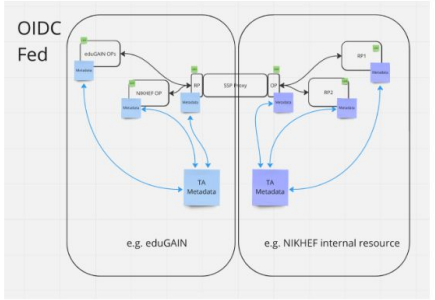
‘with fewer clicks to more resources’

Helping out the community: the policy toolkit for communities & trust

“small to mid-sized communities do not have the resources to maintain a bespoke community management policy”

this leaves communities *and SP operators* unclear about trust assurance level of members

Membership Management Policy	Infrastructure Management	Research Community (abides by)	This policy template defines how Research Communities should manage their members, including registration and expiration.
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.



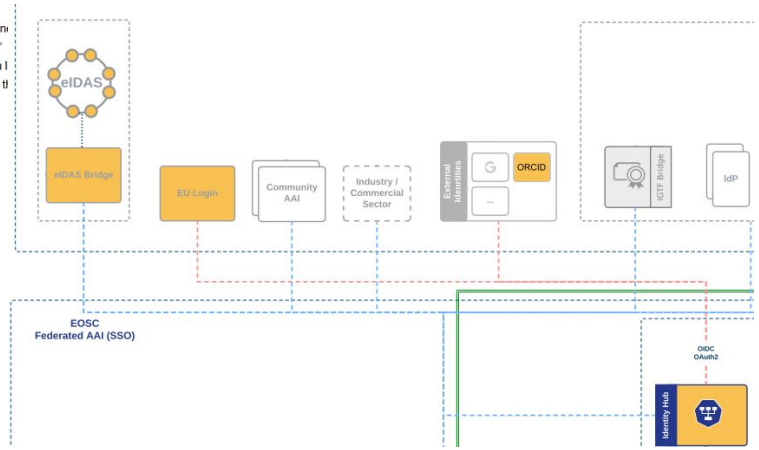
David Groep:
Raise of hands
Who knows about

- Proxy: most in the room
- OIDCfederation: few in the room
- Bridge PKI (public key infra): 1

What was the problem that triggered this session?
Proxies are wonderful, they can be opaque and expose things to the outside world..
Proxy into eduGAIN using SAML, token translation, attribute transformation, augmentation
Membership services?

OIDC world, to amalgamate a set of RPs
Essentially overloading the proxy with two roles, technical role of translating on
another (+ augment of claims), but also bridging trust between both “domains”
In OIDC federation, you can chain metadata statements not by publishing to a
hierarchies, trust anchors who can sign intermediates . multiple signatures on t

Today’s BPA proxy links attributes **as well as** trust



And what about assurance: we’ll have more, and maybe more reliable, sources of assurance in the near term?

Production Implementations of the AARC BPA

EOSC and MyAccessID as Real Life Examples

Production Implementations: EOSC

EOSC Access Federation

Registers, maintains, and publishes the trust anchors and the associated metadata for all the entities in the EOSC Federated AAI. Provides common horizontal functionalities.

Identity Hub

Provides user authentication and consistent user information to services in the EOSC Federated AAI.

EOSC Core Infrastructure Proxy

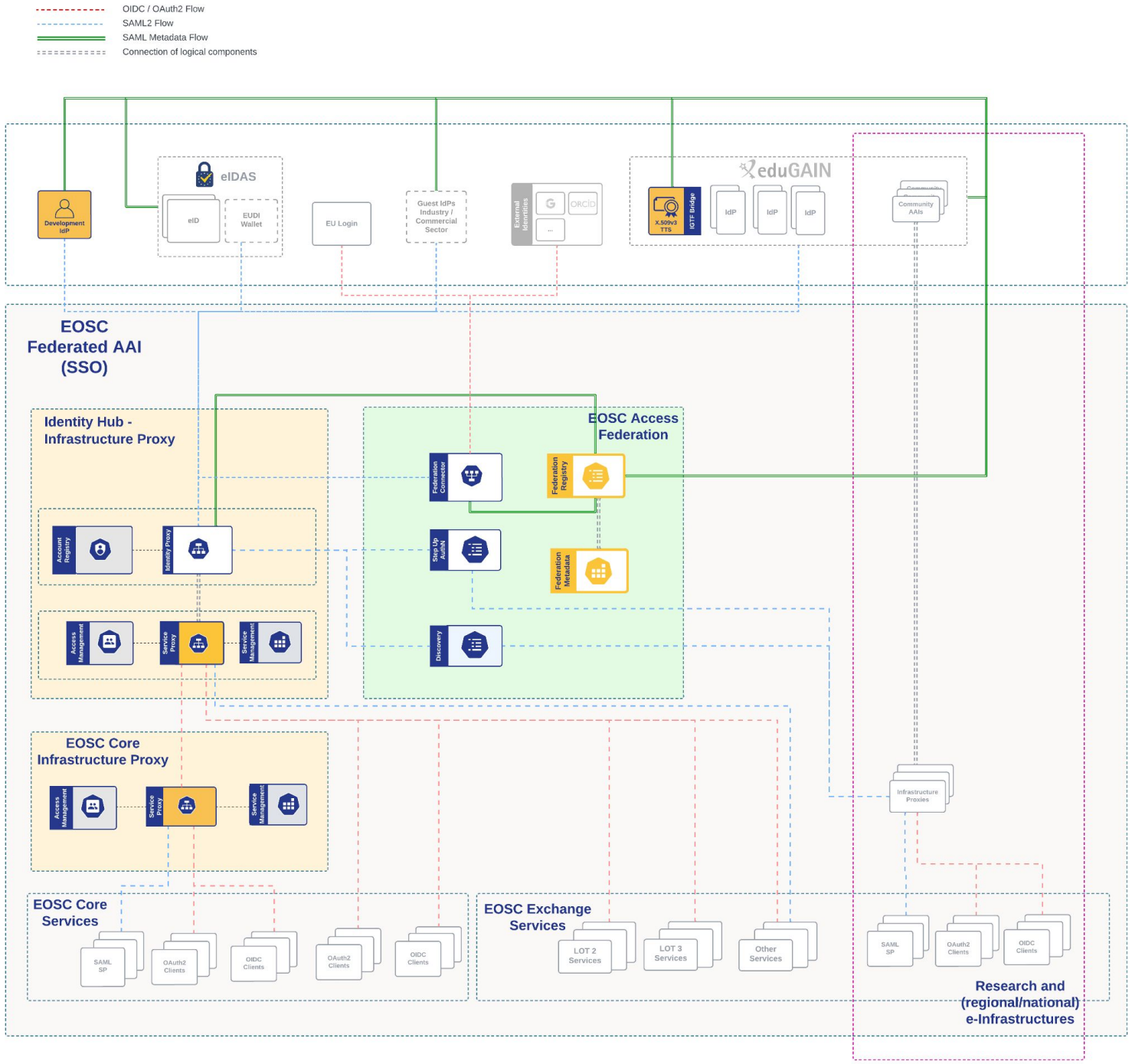
Connects the EOSC Core Services

EOSC Exchange Infrastructure Proxy

Connects the EOSC Exchange Services

X509v3 Token Translation Service (TTS)

Authenticates users with their X.509v3 credentials.



Production Implementations: MyAcademicID

MyAcademicID Service

The MyAcademicID Service was launched in November 2020 MyAcademicID Project

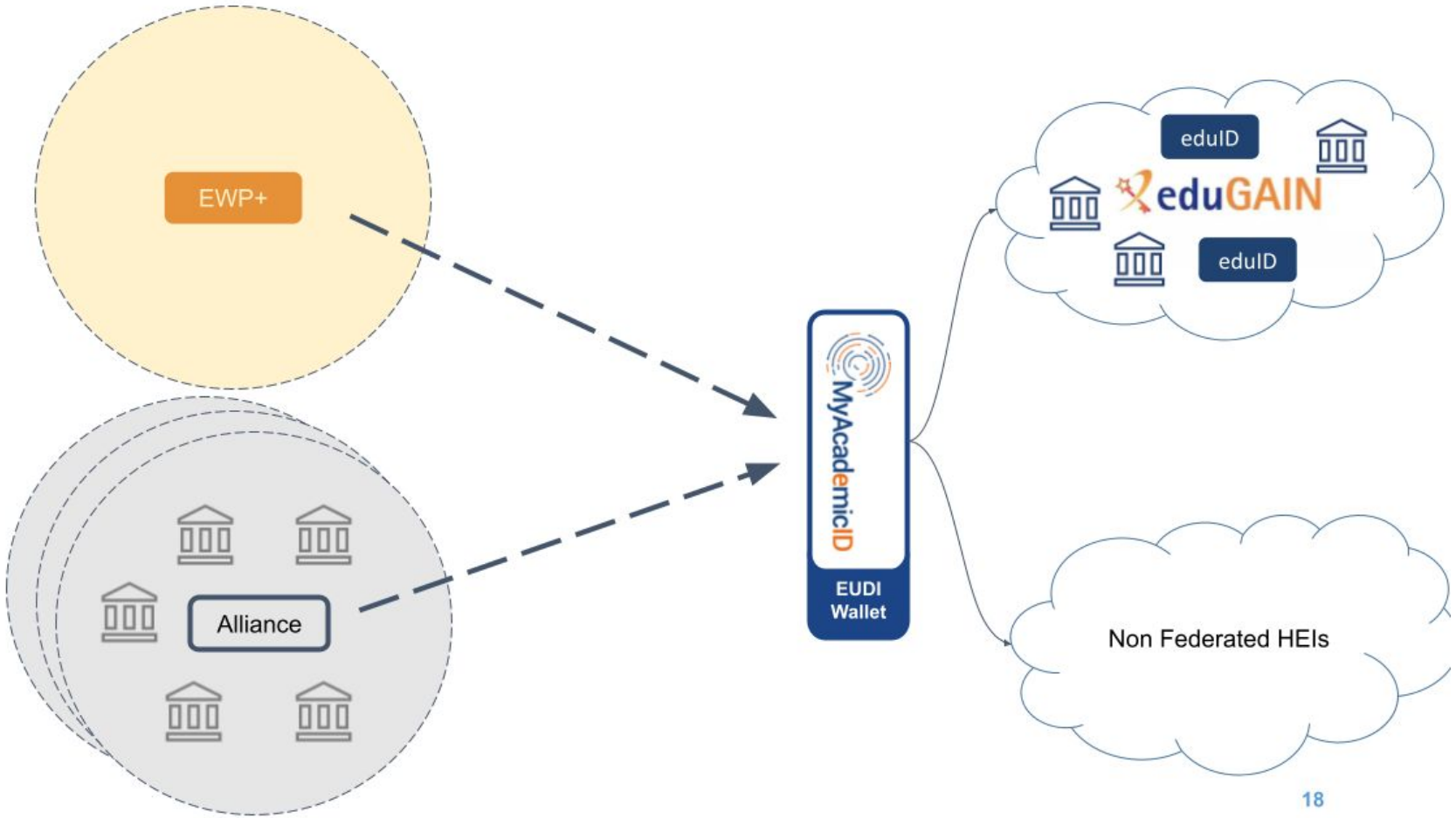
EWP+ / University Alliances

Provides an Authentication Proxy for the core Erasmus+ services (Online Learning Agreement, Dashboard, the Erasmus+ App).

eduGAIN, eIDAS & Google Authentication

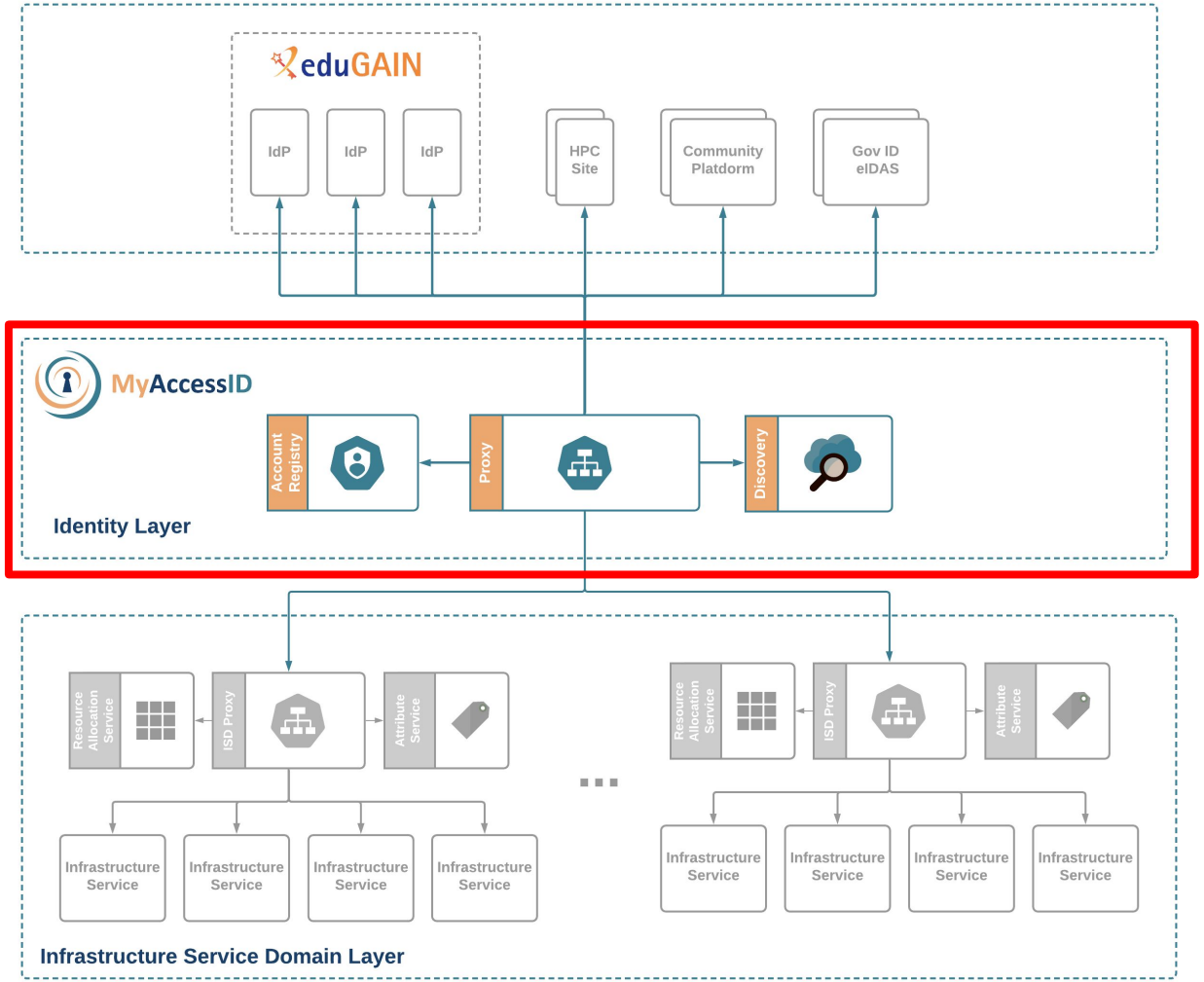
Supports authentication via eduGAIN, eIDAS and Google

Provides a catch-all IdP of Last Resort



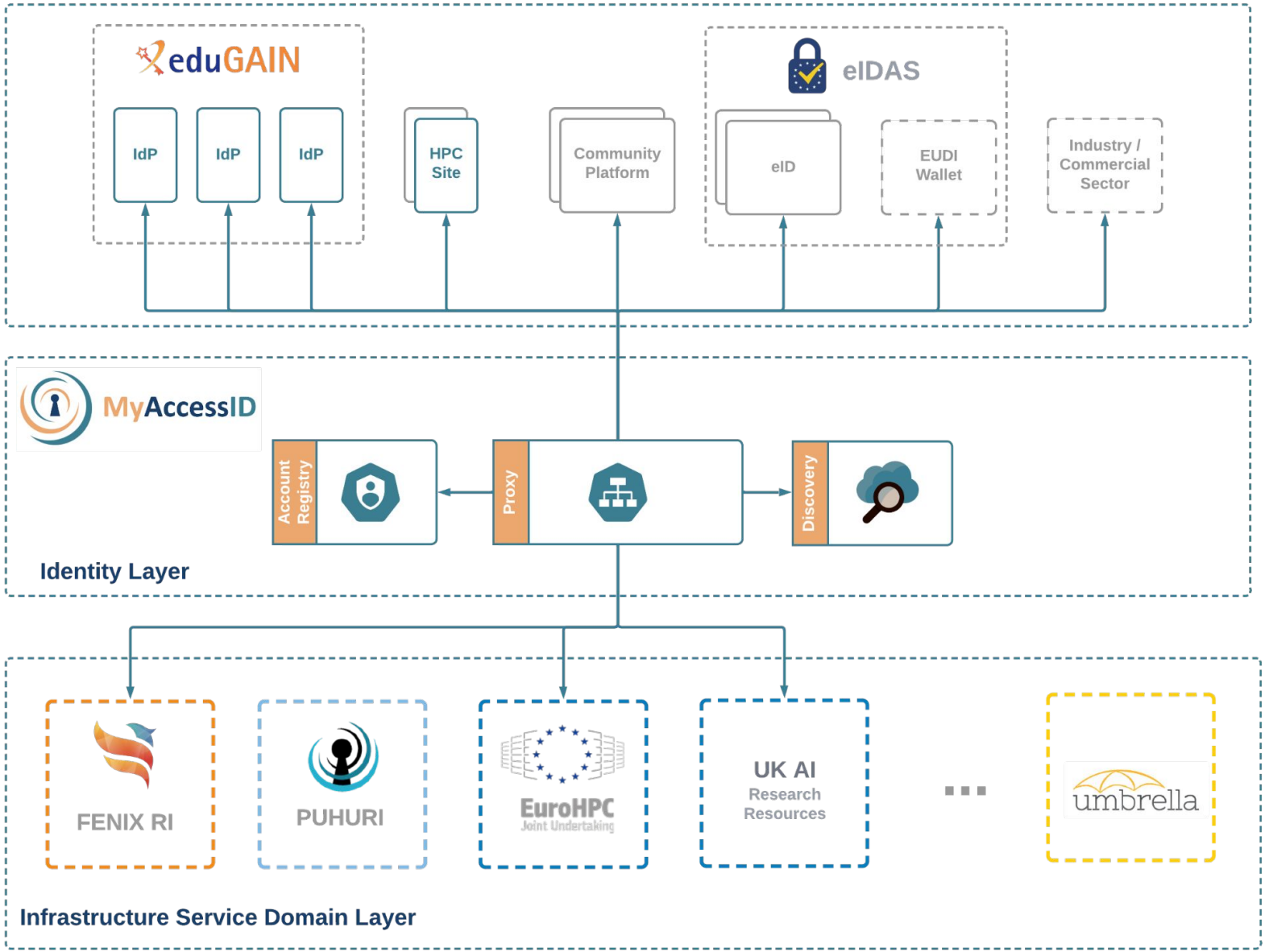
Production Implementations: MyAccessID

- HPC Datacenters are in the process of transforming to **Infrastructure Service Providers** with **a diverse Service Portfolio**
- These infrastructure services become available in different administrative and policy domains, which we call **Infrastructure Service Domains**
- **A common Authentication and Authorization Infrastructure** enables uniform accessibility to scientists and engineers at European scale

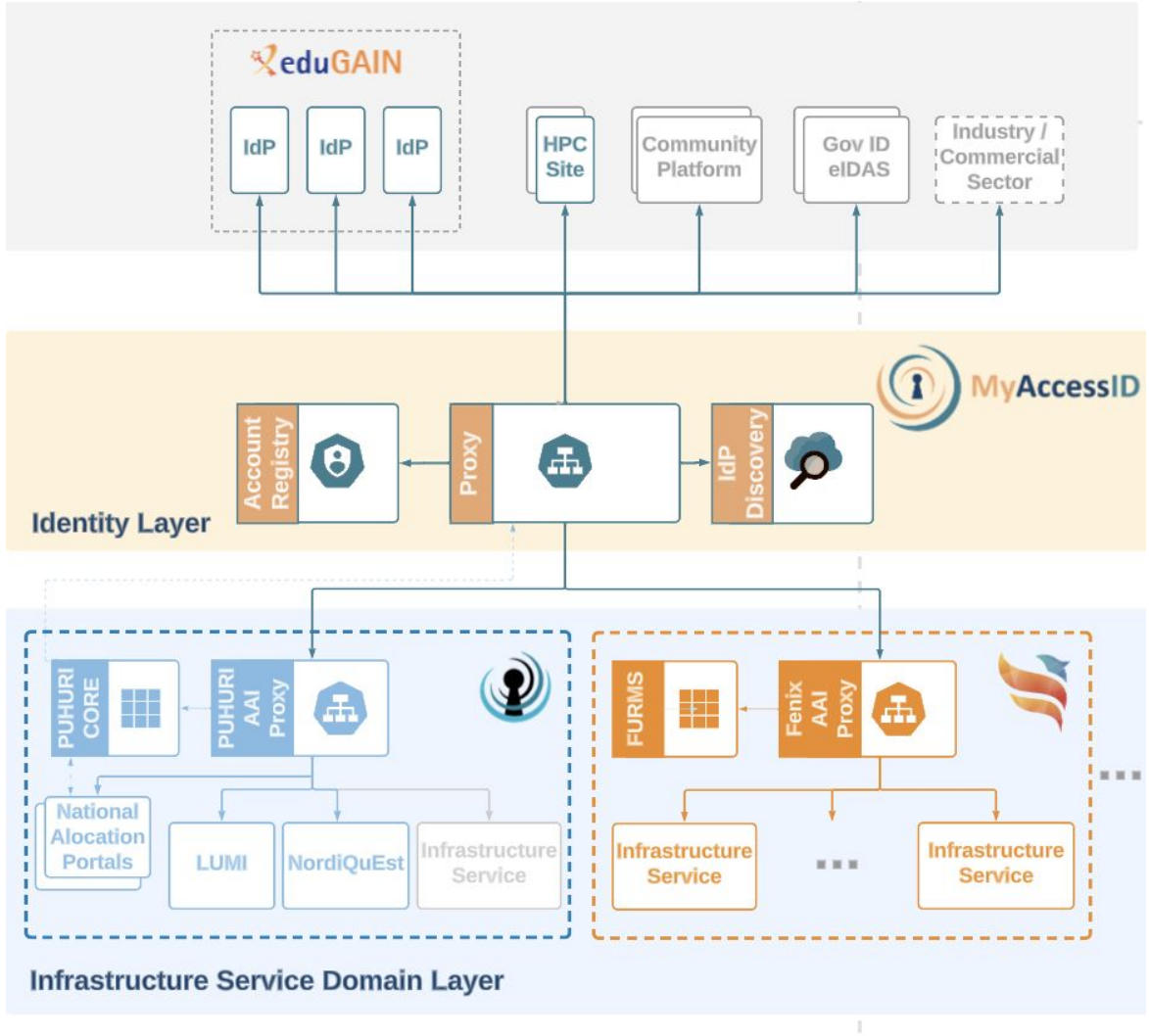


MyAccessID: A common AAI for ISDs in HPC

Production Implementations: MyAccessID



Authorisation and affiliation in MyAccessID/Fenix example

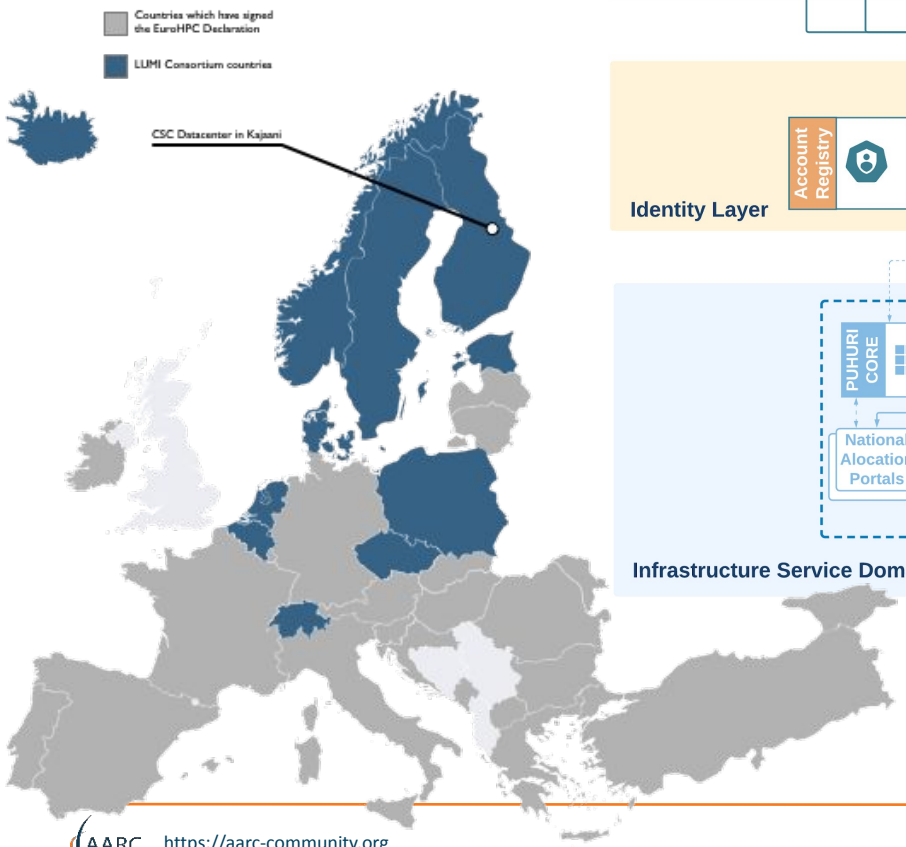


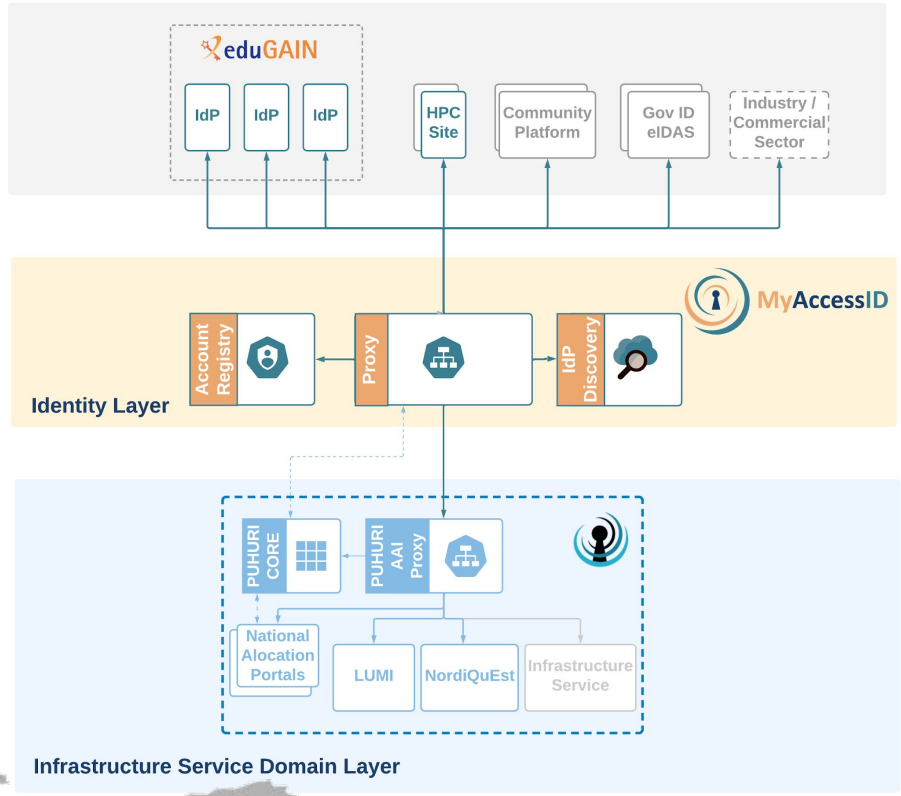
Complex Required Attributes

Affiliation

description	Specifies the person's affiliation. Possible values: • member@bsc.es • member@cineca.it • member@cscs.ch • member@fz-juelich.de • member@humanbrainproject.eu Access to many services connected through MyAccessID relies on authorizing member users based on affiliation with their home organization.
SAML attribute(s)	`urn:oid:1.3.6.1.4.1.5923.1.1.1.9`
OIDC claim	`eduperson_scoped_affiliation`
OIDC claim location	The claim is available in (select one or more) ☐ ID token ☑ Userinfo endpoint ☑ Introspection endpoint
OIDC scope	`eduperson_scoped_affiliation`
origin	Either: - Assigned by the Identity Provider based on the user's origin - Assigned by the MyAccessID based on the Identity Provider of the user
changes	Attribute values can change.
multiplicity	Multi-valued.
availability	Always Mandatory
example	member@community.example.org

Level of Assurance in MyAccessID/EuroHPC





2020
- PUHURI 1 project start
- MyAccessID & PUHURI Design
- MyAccessID & PUHURI Pilot

2021
- LUMI Pilots
- Policy for Quality of Identities/LoA
- MyAccessID & PUHURI Production

2022
- LUMI General Availability
- Community coordination on LoA

2023
- Implement policy on LoA
- External Identity Vetting Pilot

2024
- MFA - Strong Authentication Pilot

2025
- External Identity Vetting
- MFA - Strong Authentication

Assurance information in identity linking

Problem

- How to evaluate assurance information when linking identities

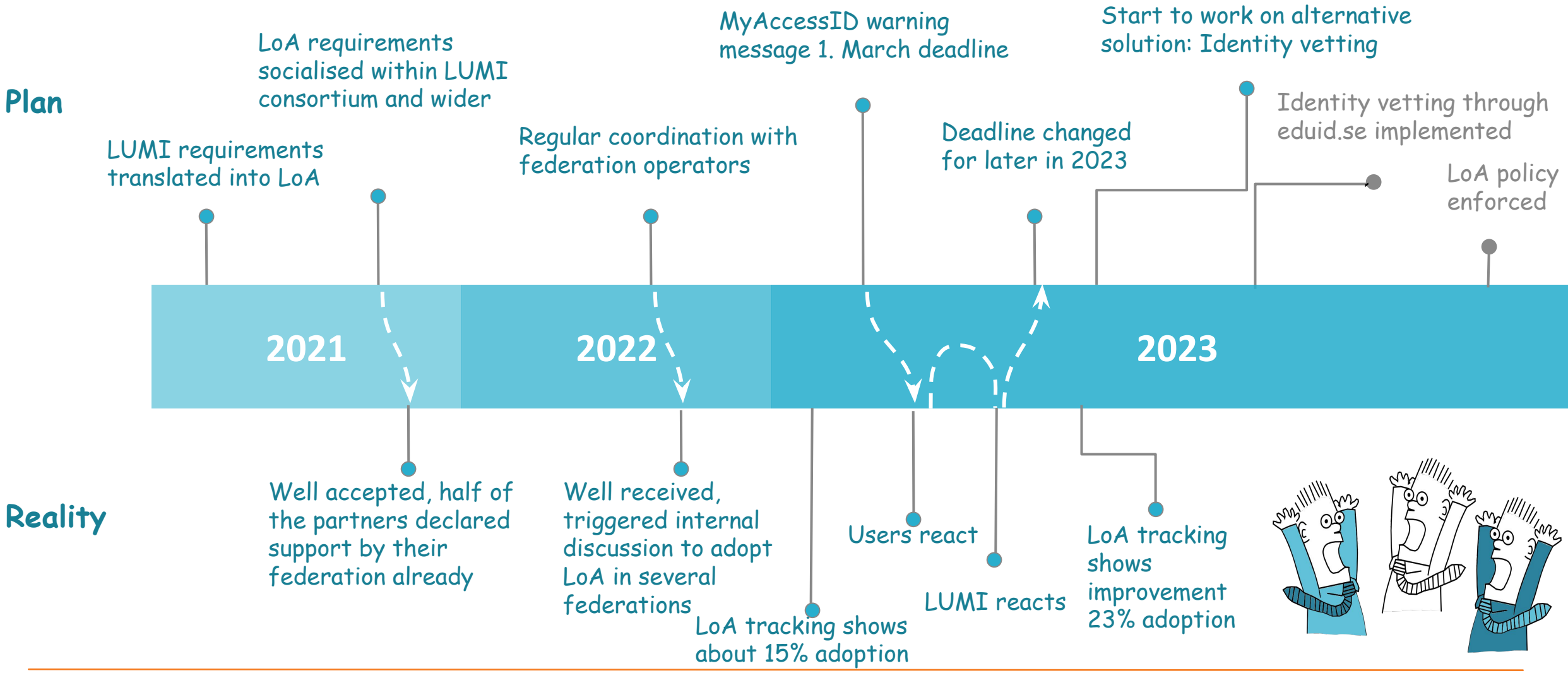
Guidelines

- AARC-G031 - Guidelines for evaluating the combined assurance of linked identities
- AARC-G009 - Account linking and LoA elevation use cases

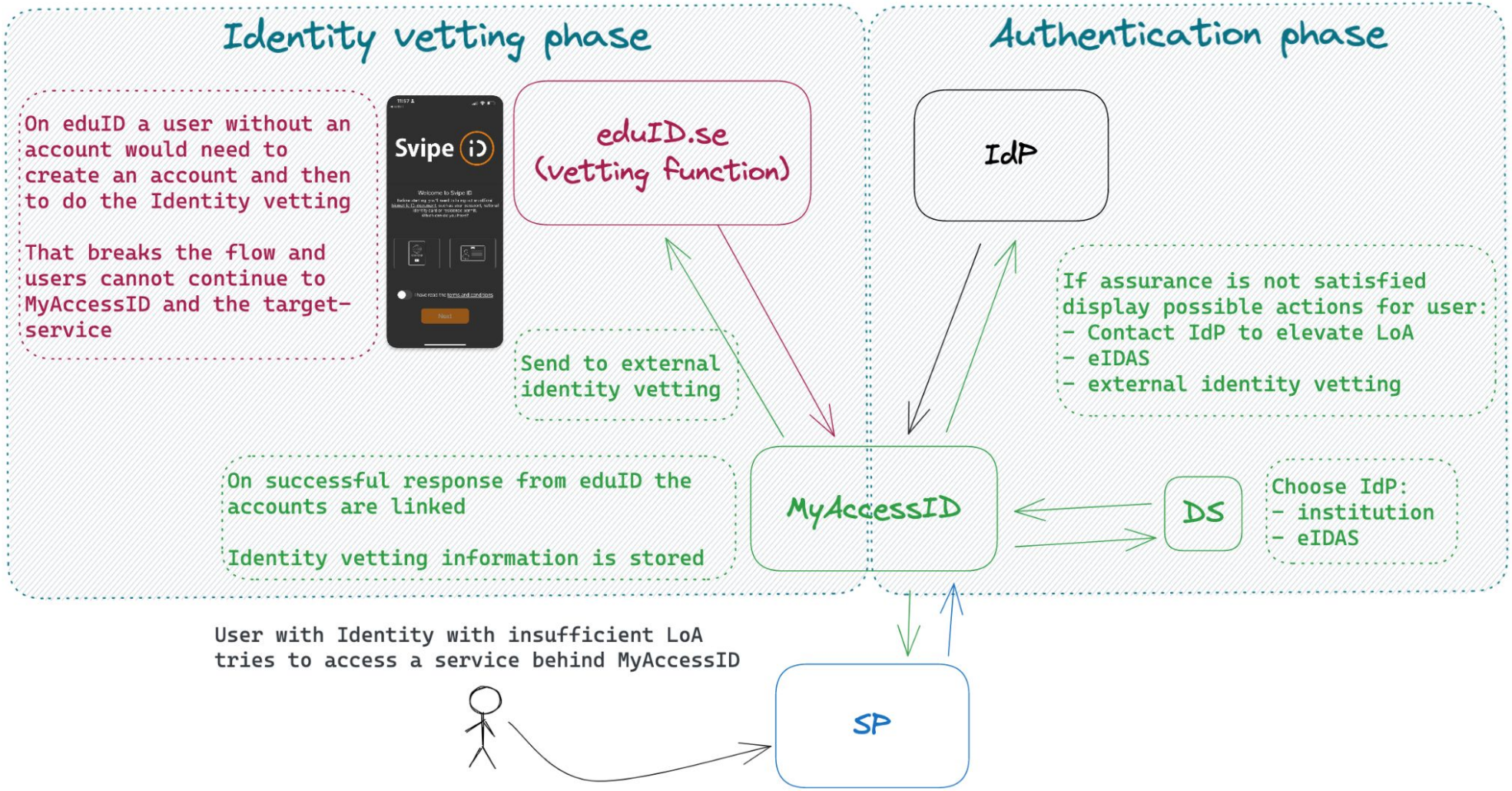
Summary

- Identifier uniqueness: AND function → Cannot assert unique ID for the combined evaluation when one of the linked identities lacks it
- Identity proofing: resolves to the effective identity used
- **Step-up Identity proofing: if the identifier uniqueness and level of authentication are the same, LoA can be assigned to the weaker identity**
- Step-up Authentication: user may register a second authentication factor to enhance the strength of the authentication method and effectively the associated LoA

Level of Assurance in MyAccessID/EuroHPC



Level of Assurance in MyAccessID/EuroHPC



Thanks to the AARC Community, including folk from whom we re-used graphics and material in this overview. In random order: Licia Florio, Nicolas Liampotis, Christos Kanellopoulos, Marina Adomeit, Janos Mohacsi, Ilaria Fava, Slavek Licehammer, Dave Kelsey, Ian Neilson, Marcus Hardt, Mischa Salle, Hannah Short, and Maarten Kremers.

Thank you

Any Questions?

https://aarc-community.org

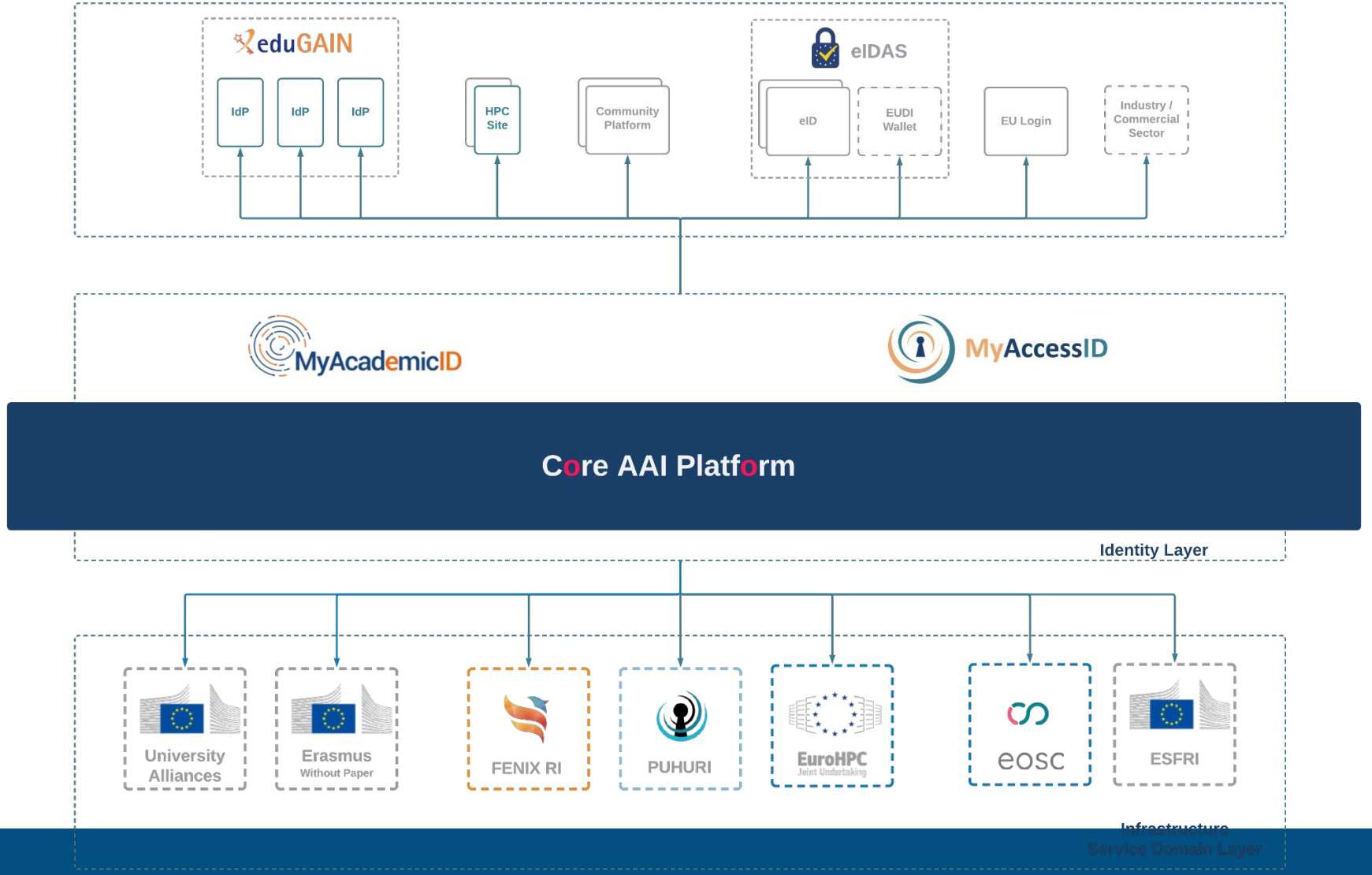
Co-funded by the European Union

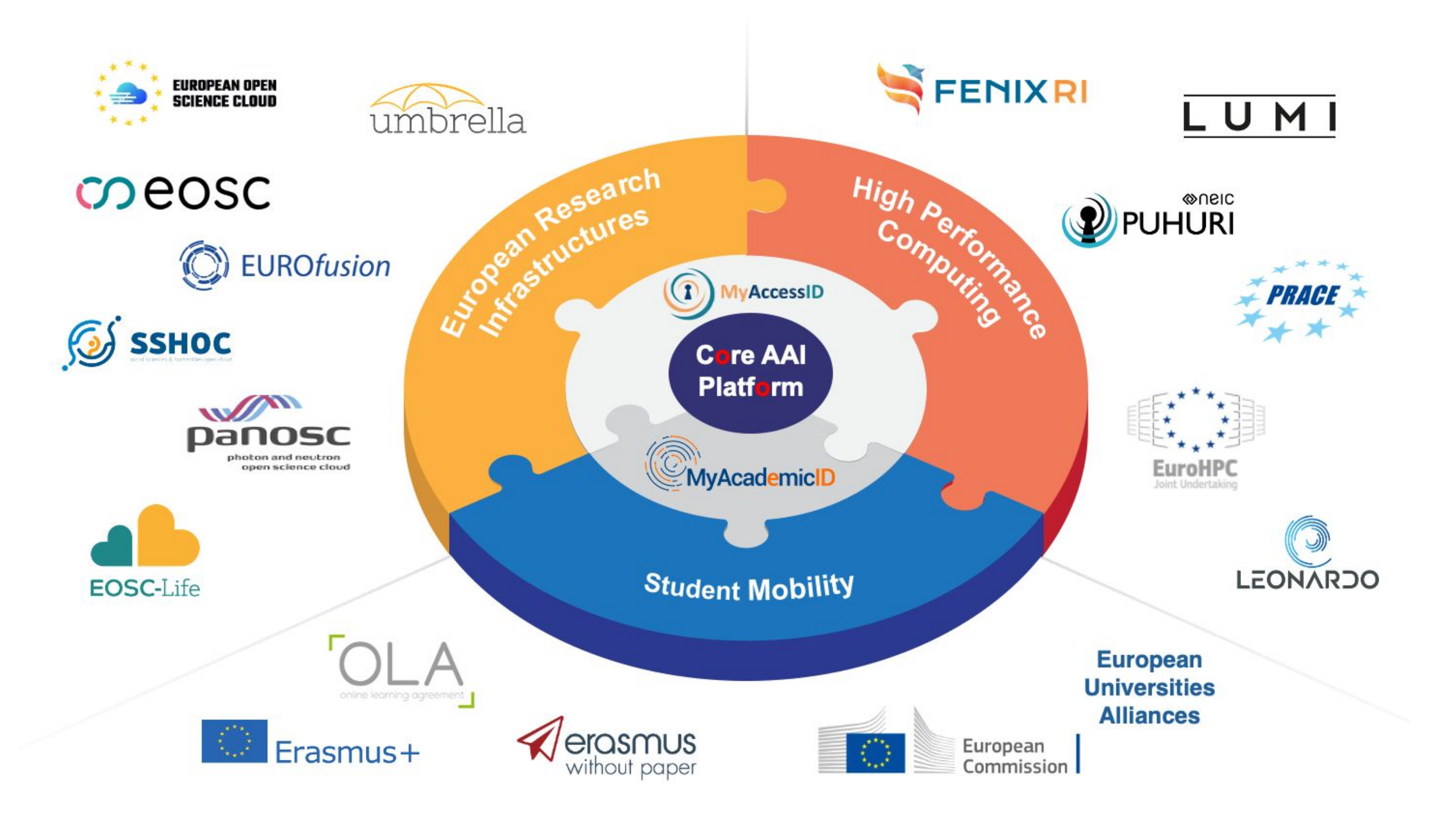
Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them. Grant Agreement No. 101131237 (AARC TREE).

Core AAI Platform Roadmap

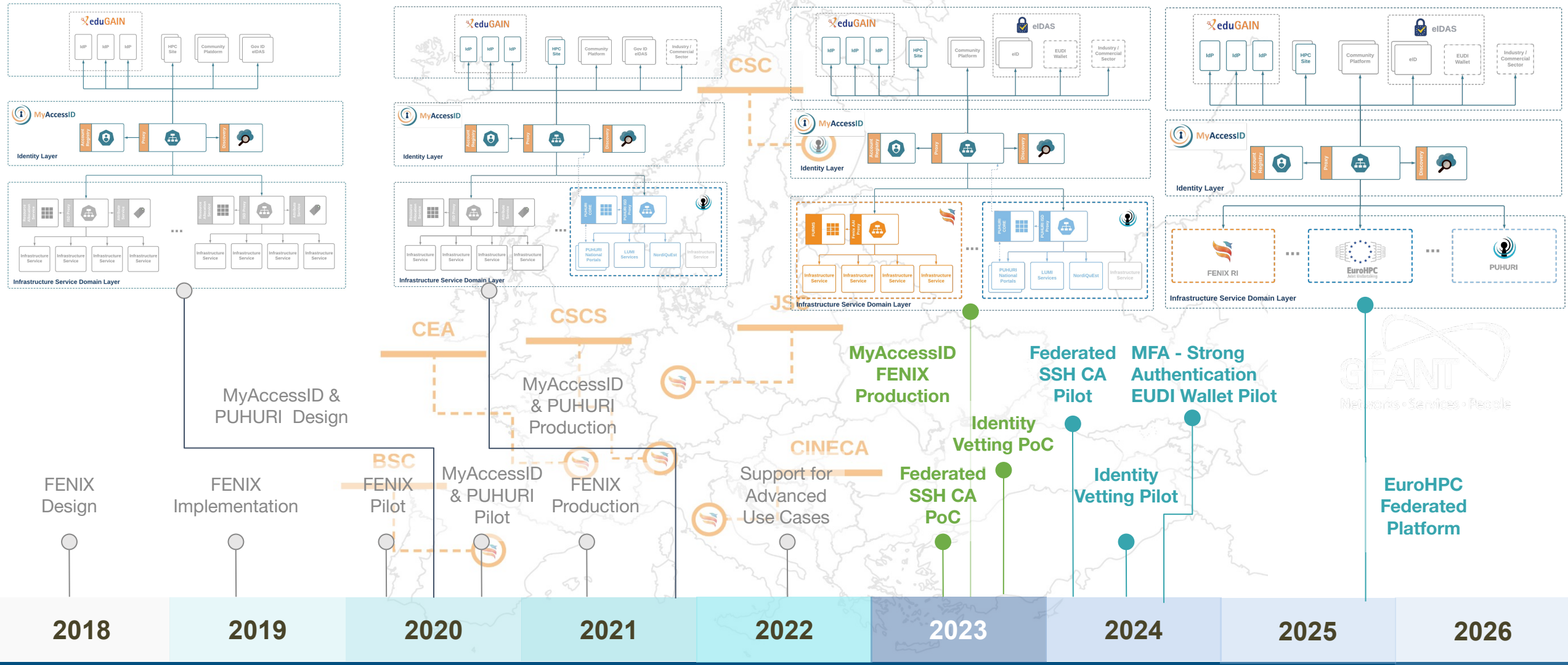
Christos Kanellopoulos (GEANT)

Core AAI Platform

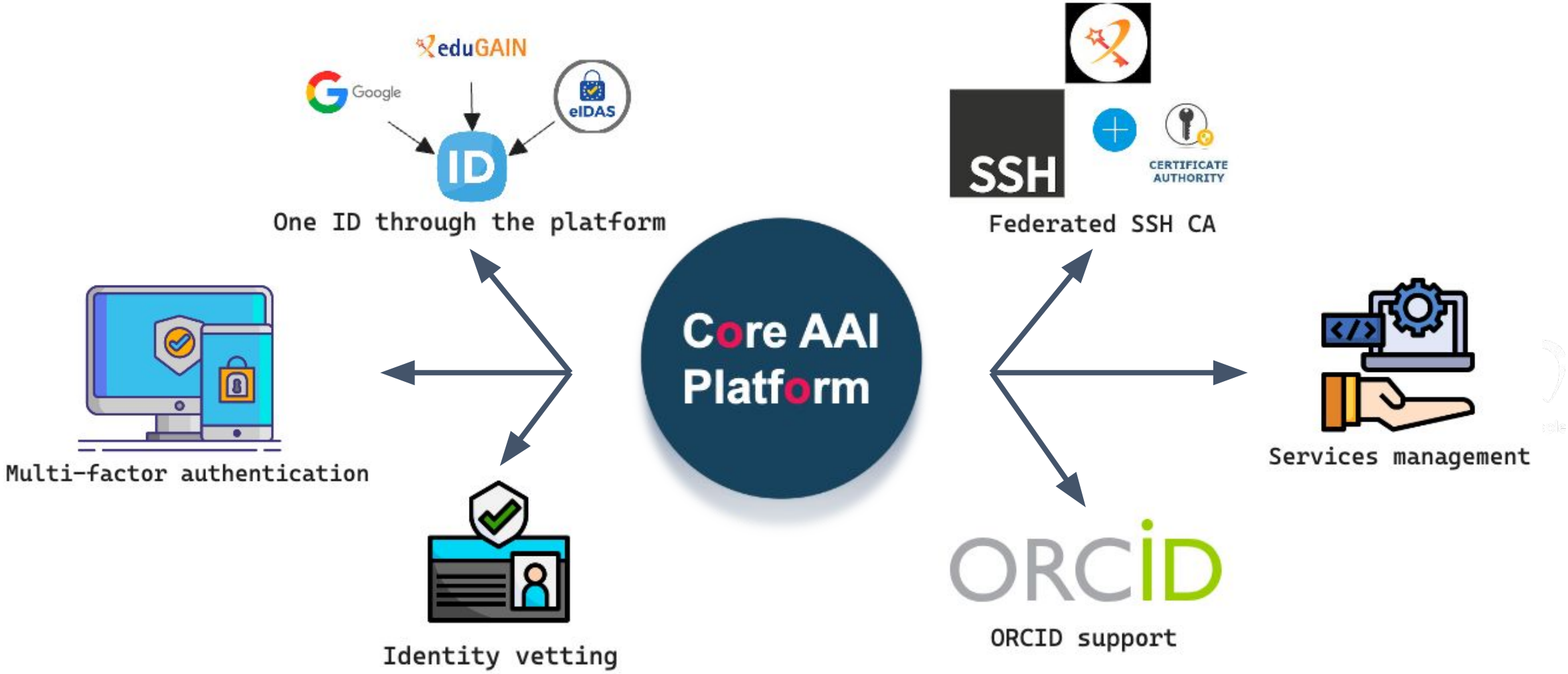



EUROPEAN OPEN SCIENCE CLOUD
umbrella
FENIX RI
LUMI
eosc
EUROfusion
neic PUHURI
PRACE
SSHOC
panosc
photon and neutron open science cloud
EuroHPC Joint Undertaking
EOSC-Life
LEONARDO
OLA
online learning agreement
Erasmus+
erasmus without paper
European Commission
European Universities Alliances
European Research Infrastructures
High Performance Computing
MyAccessID
Core AAI Platform
MyAcademicID
Student Mobility

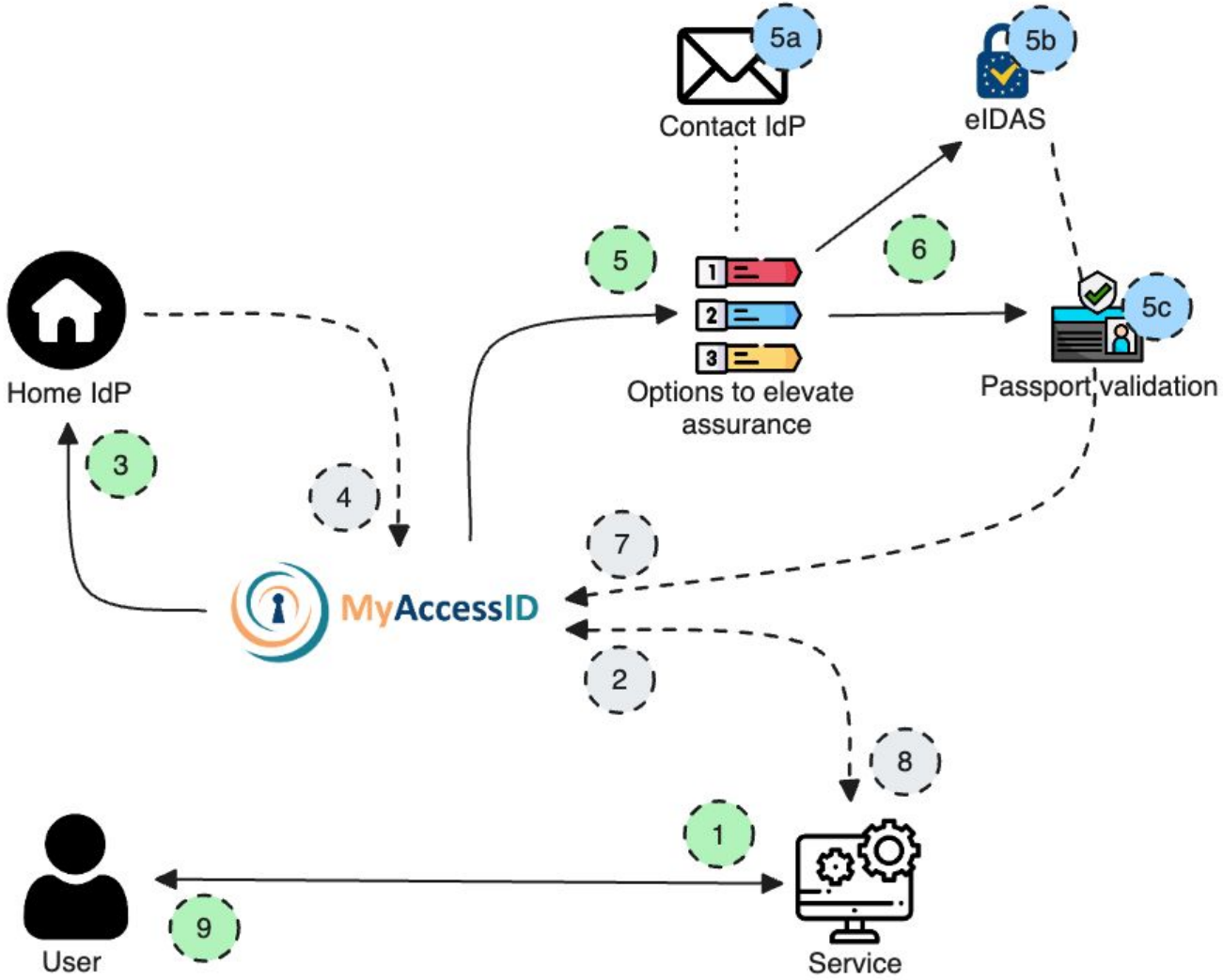
Core AAI Platform Roadmap



The Core AAI Platform - Features

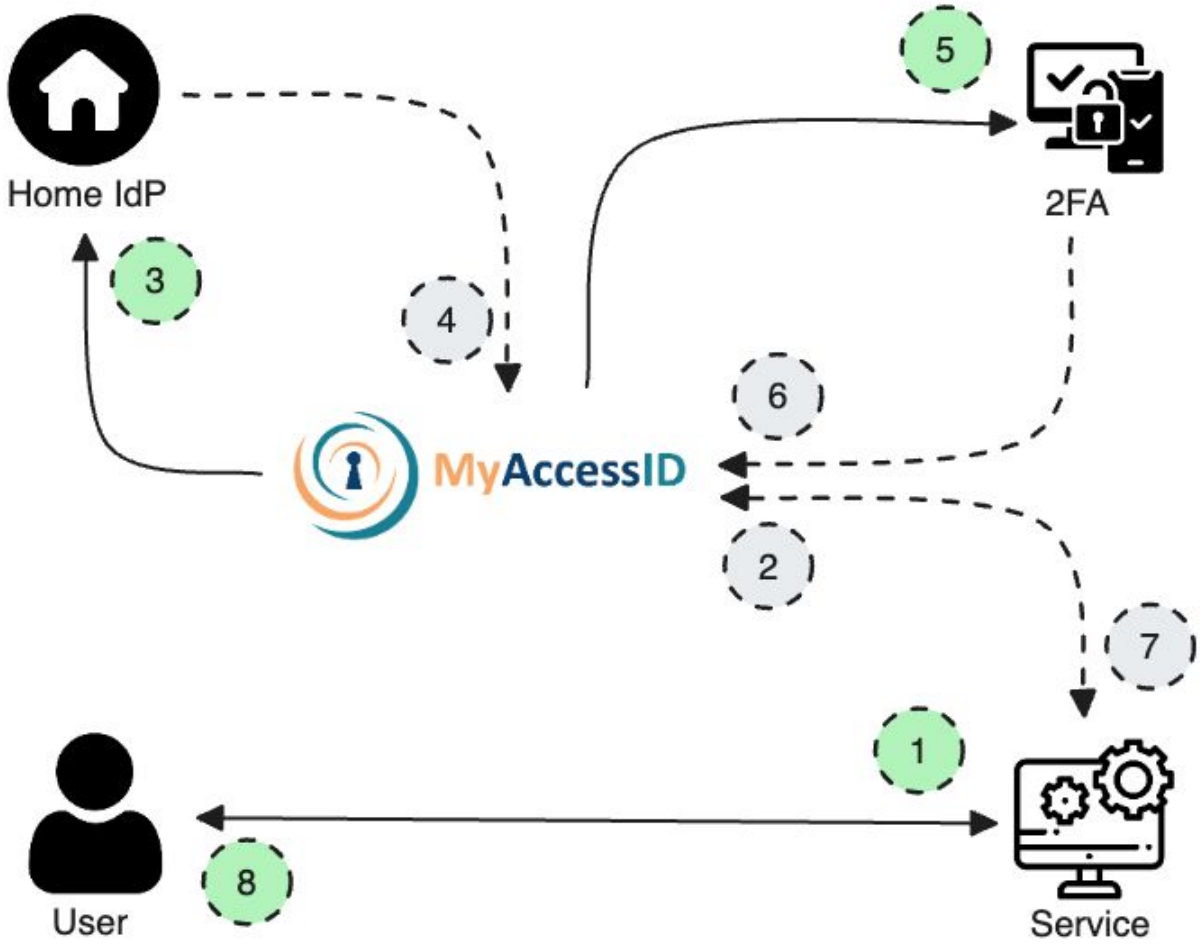


Identity vetting



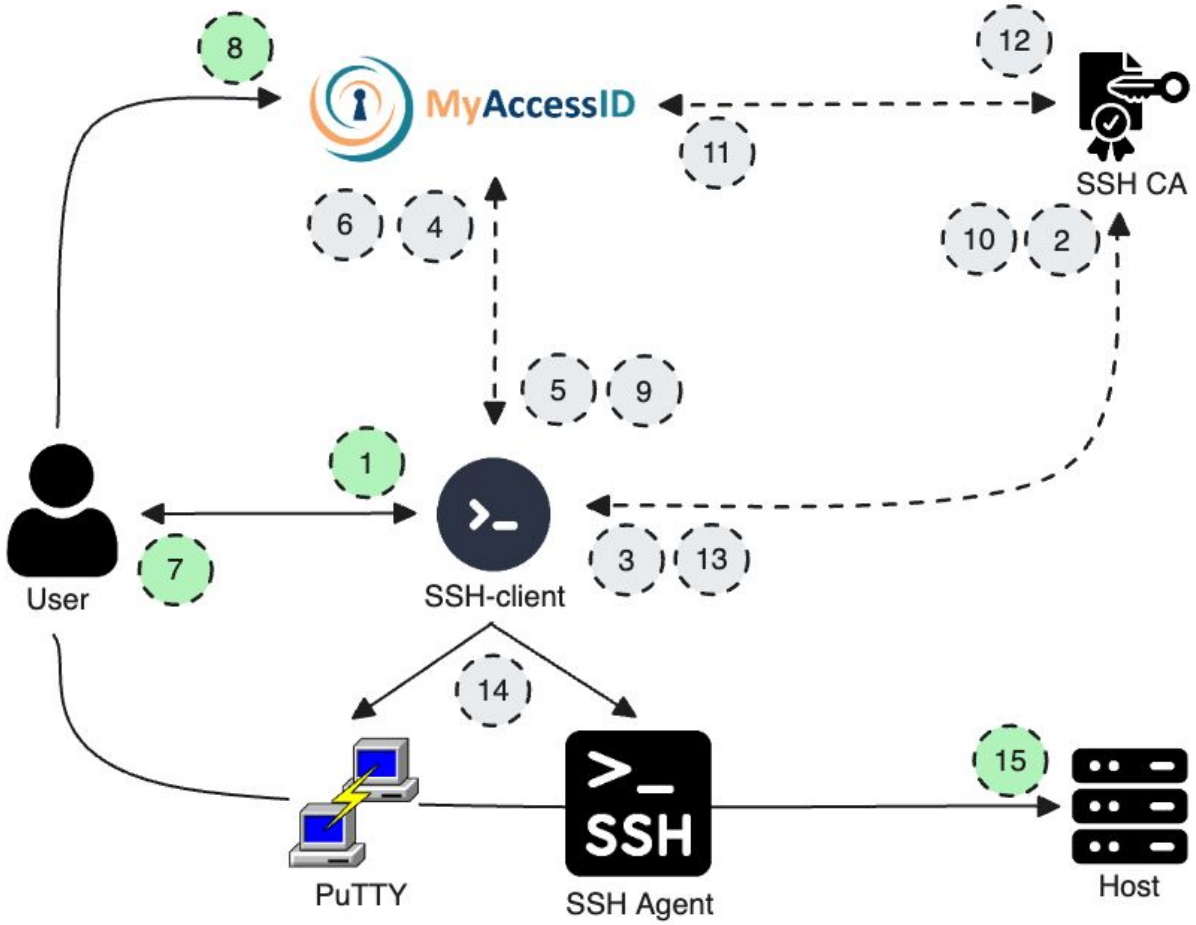
1. User accesses the target service
2. Service redirects the user to authenticate via MyAccessID expecting assured identity
3. MyAccessID lets the user to authenticate via user's home IdP
4. User authenticates to their home IdP with low assurance
5. MyAccessID redirects the user to options to elevate assurance of their identity
   a) contact the IdP to help with identity verificaiton
   b) use eIDAS
   c) use a governmental-issued certification
6. User chooses one mechanism and proceeds
7. MyAccessID verifies the assurance of the identity
8. MyAccessID provides assured identity information to the service
9. The target service lets user to access it

Multi-Factor Authentication



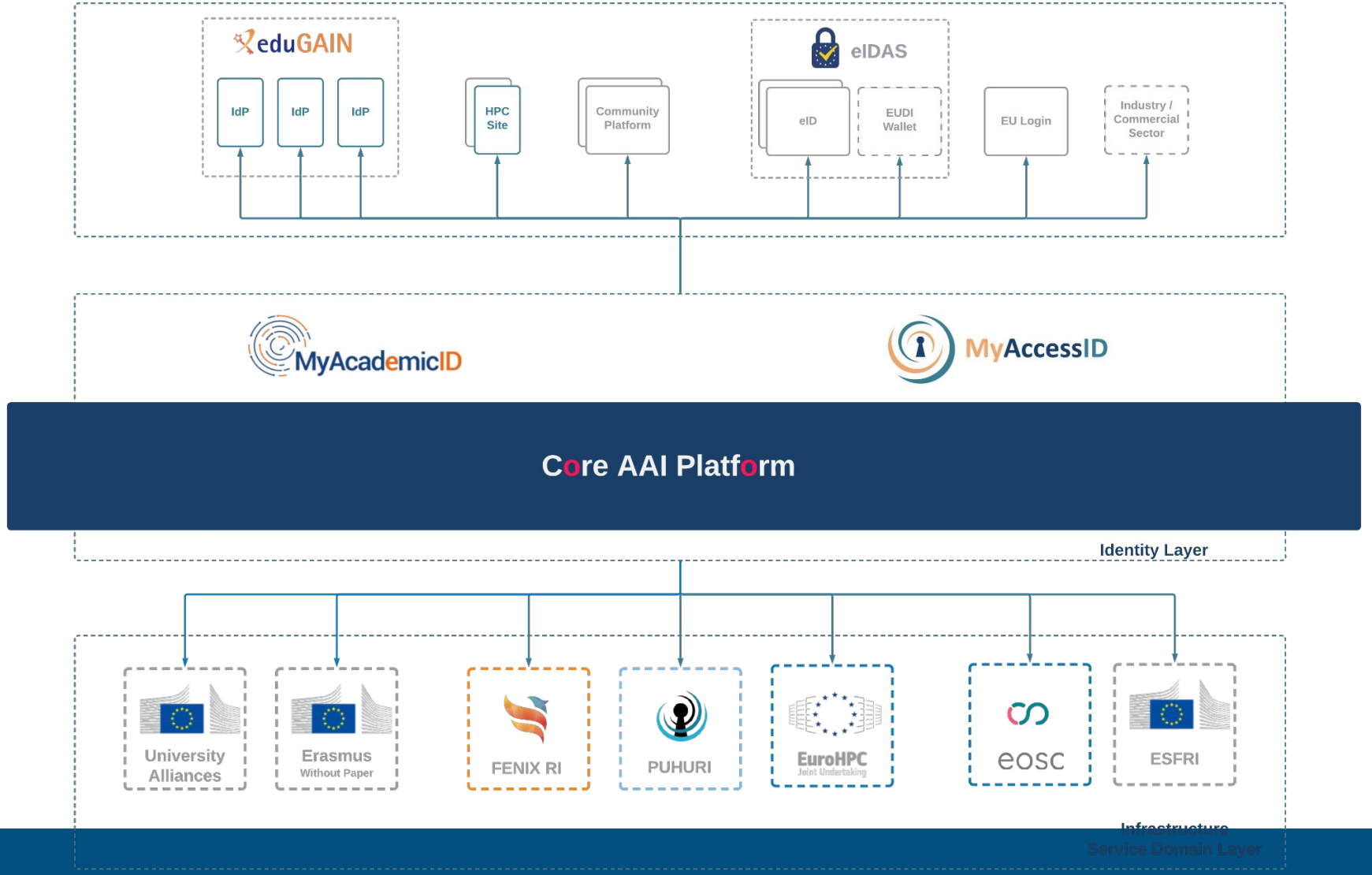
1. User accesses the target service
2. Service redirects the user to authenticate via MyAccessID requiring 2FA
3. MyAccessID lets the user to authenticate via user's home IdP
4. User authenticates to their home IdP without 2FA
5. MyAccessID checks if the 2FA has been provided so far and if not, it lets user to proceed with the 2FA through MyAccessID
6. MyAccessID verifies if 2FA was succesful
7. MyAccessID provides details about performed 2FA with the user's attributes to the service
8. The target service lets user to access it

The federated SSH CA

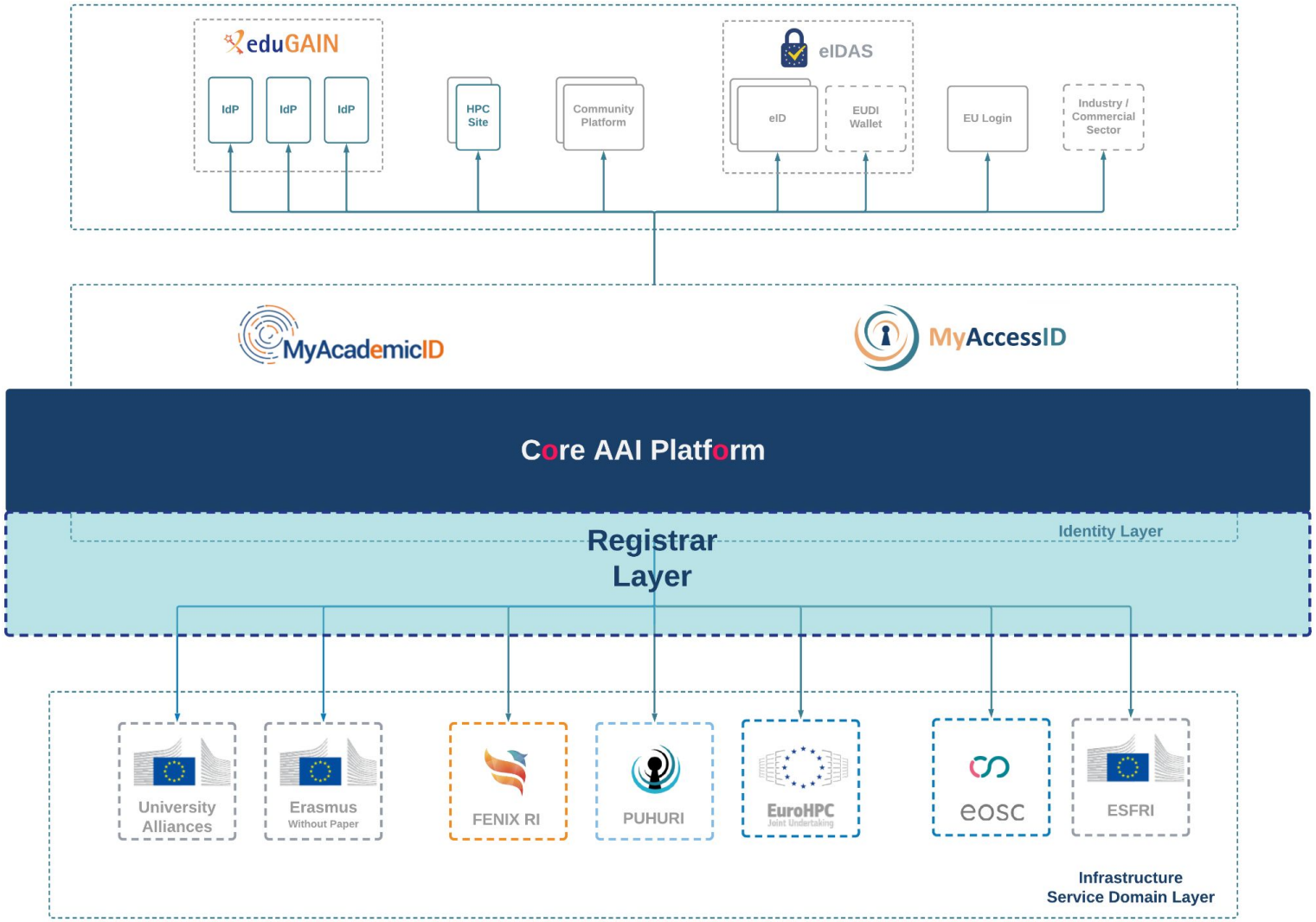


1. User uses the SSH-client
2. 3. SSH-client retrieves configuration details from the SSH CA
4. 5. SSH-client starts an OIDC device authorization flow
6. SSH-client starts polling MyAccessID waiting for user's authorization
7. SSH-client provides user with URL for authorization
8. User authenticates via MyAccessID and authorizes the operation
9. When authorized, MyAccessID polling returns access token to SSH-client
10. SSH-client provides SSH public key to SSH CA for signing it (send access token)
11. 12. SSH CA uses access token to get user's attributes
13. SSH CA provides a signed SSH certificate back to SSH-client
14. SSH-client sets up the environment (depends on the user's OS)
15. User accesses the host with the signed SSH certificate

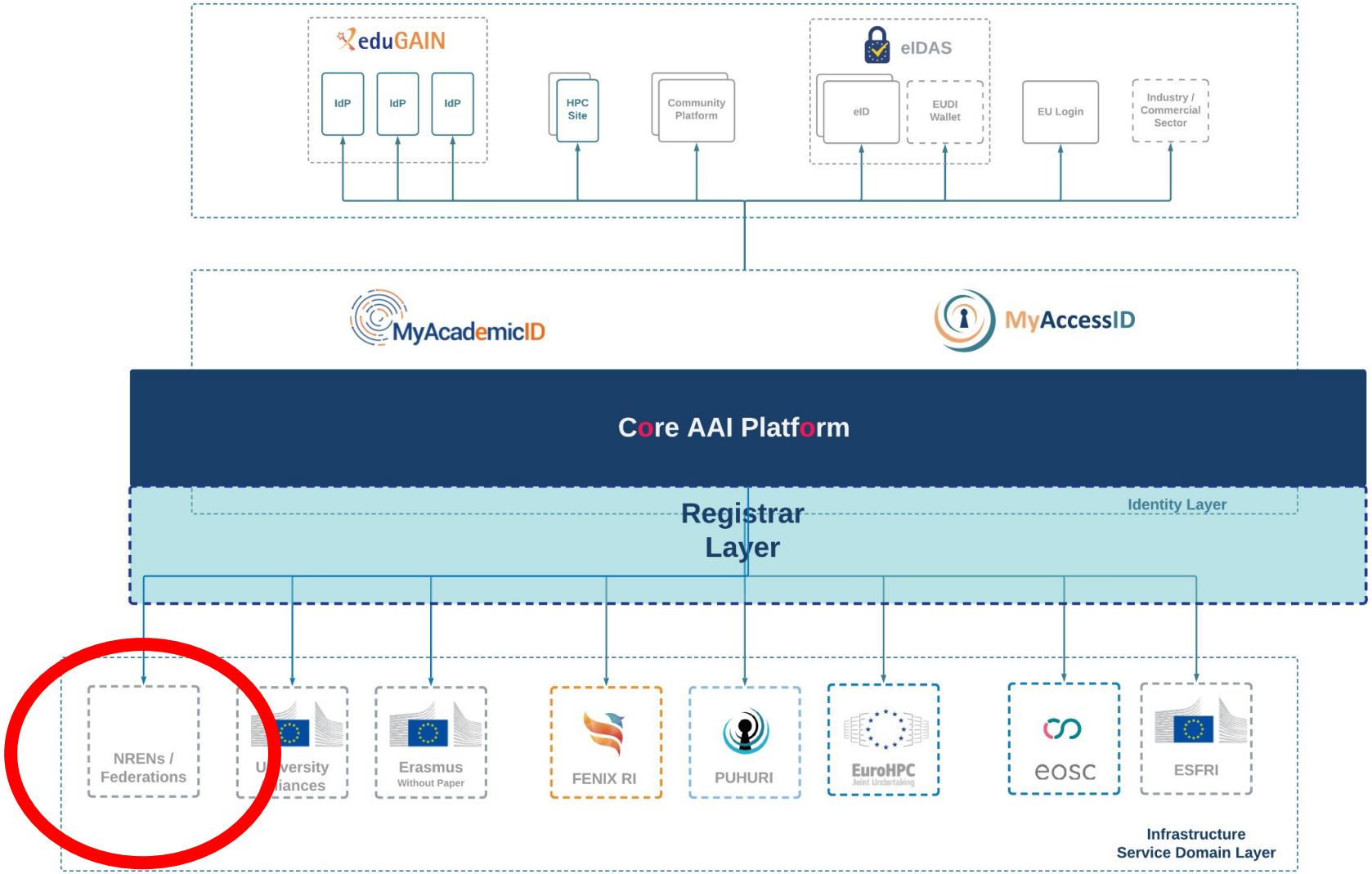
MyAccessID: A common AAI for ISDs in HPC



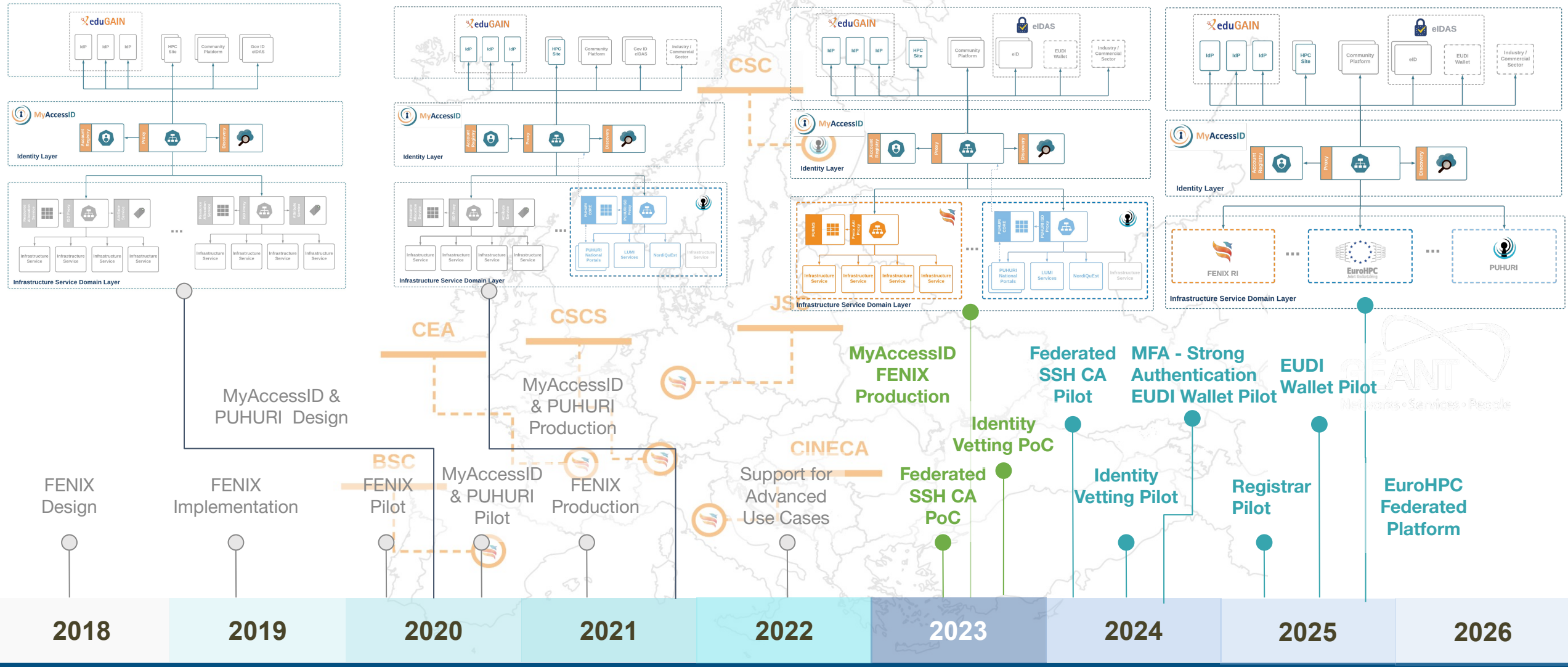
MyAccessID: A common AAI for ISDs in HPC



MyAccessID: A common AAI for ISDs in HPC



Core AAI Platform Roadmap

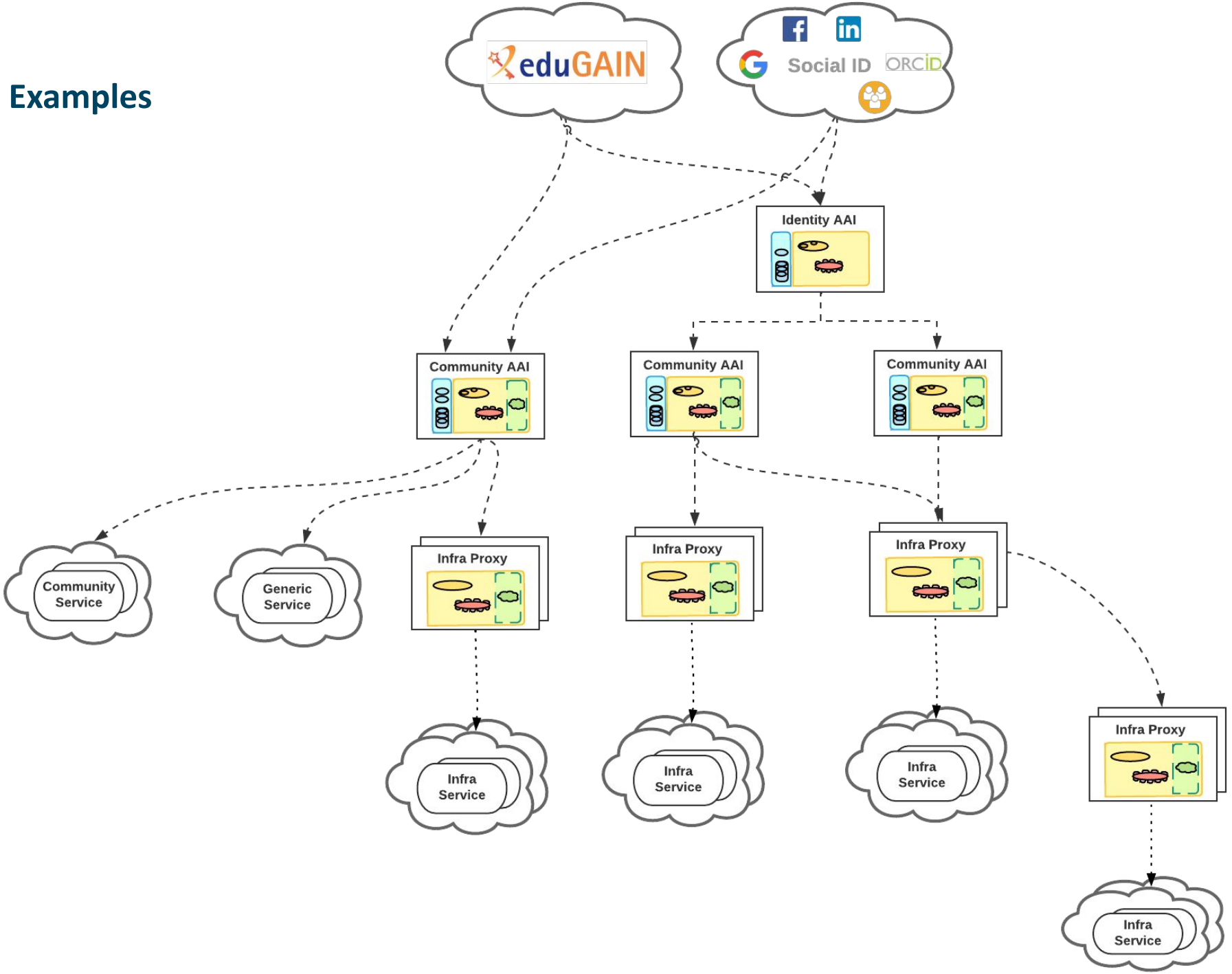


Thank you

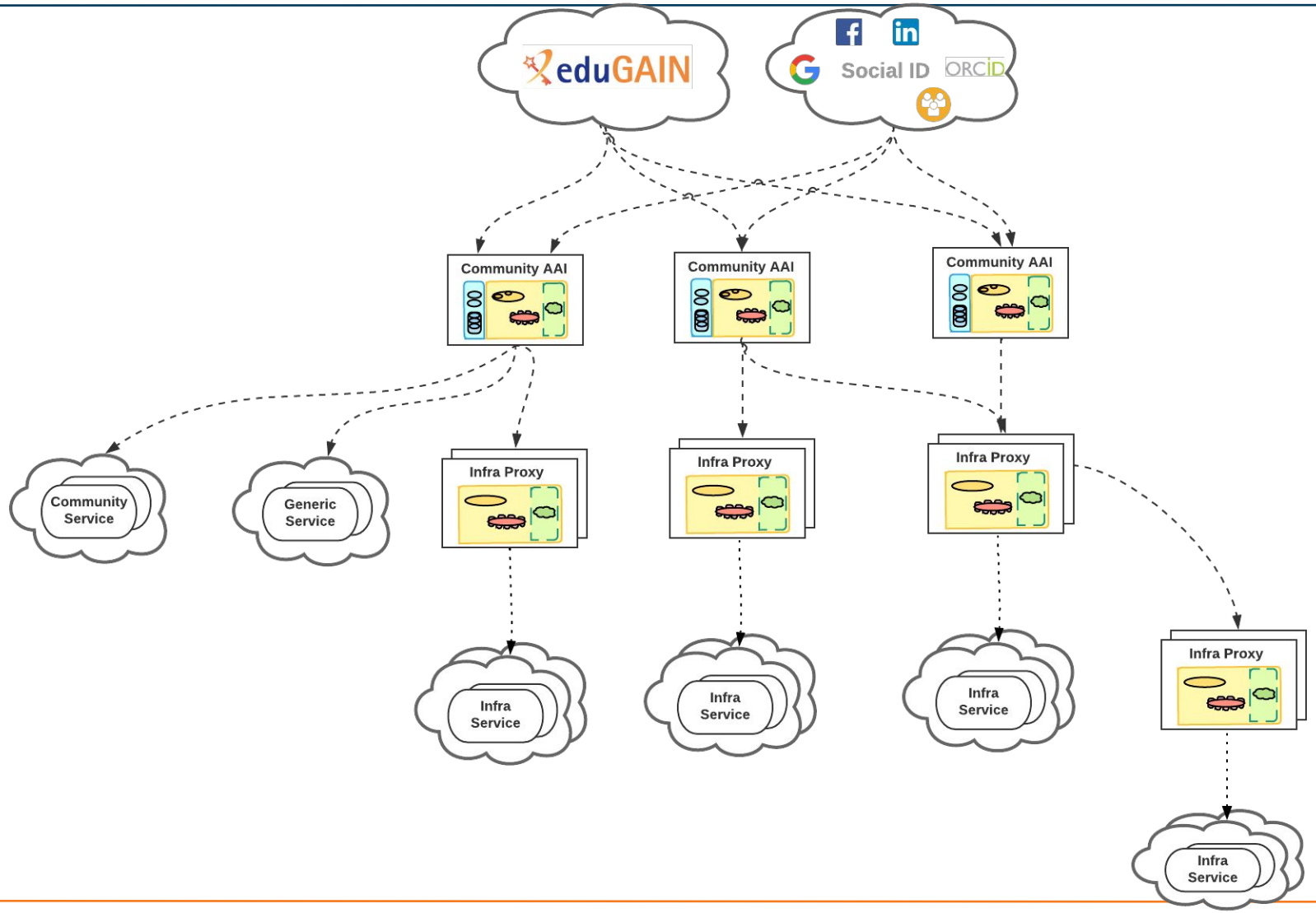
Christos Kanellopoulos (GEANT)

For Reference - Current Work in Progress

More complex Examples



OpenID connect - complex topologies, how do we enable trust



OpenID connect - complex topologies, how do we enable trust

Problem

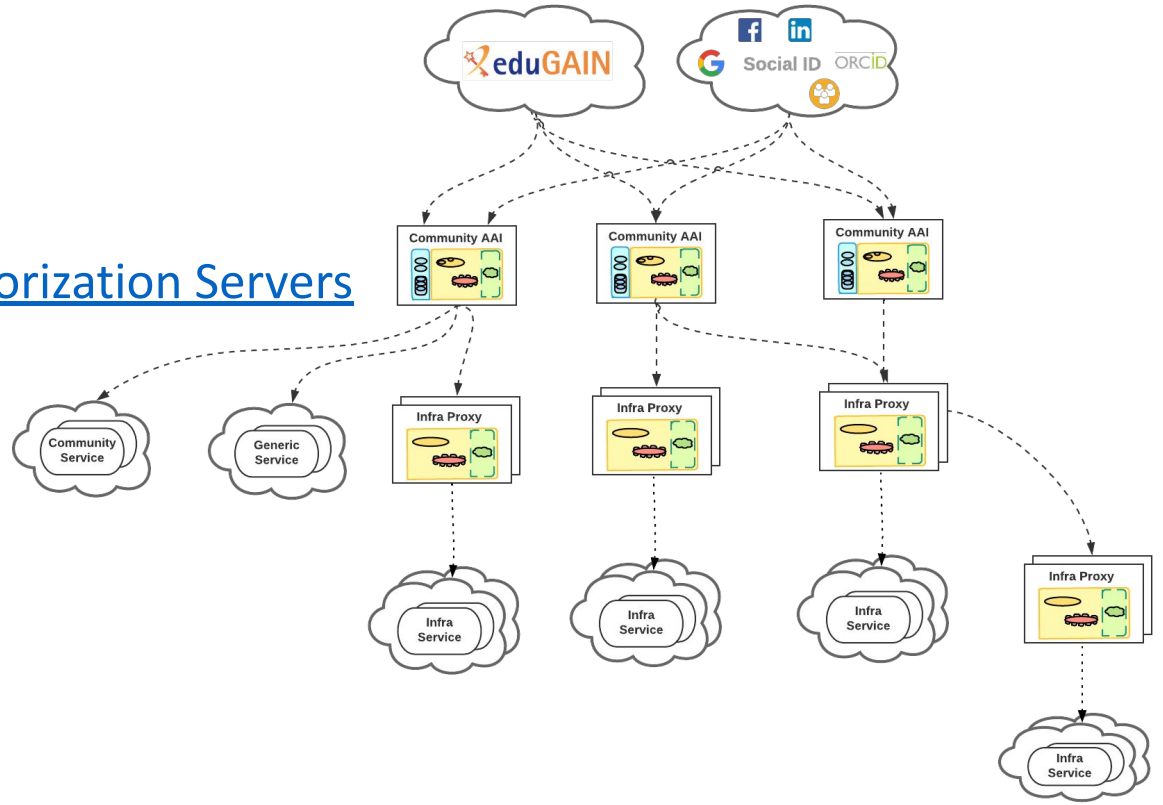
- How to convey meta-information about a token from an Authorization Server (AS) to the protected resource even when there is no direct trust relationship between the protected resource and the token issuer.

Guideline

LAST CALL [AARC-G052 OAuth 2.0 Proxied Token Introspection]

WIP [AARC-G058 Establishing trust between OAuth 2.0 Authorization Servers]

TODO AARC-GXXX OAuth2 Token Profile

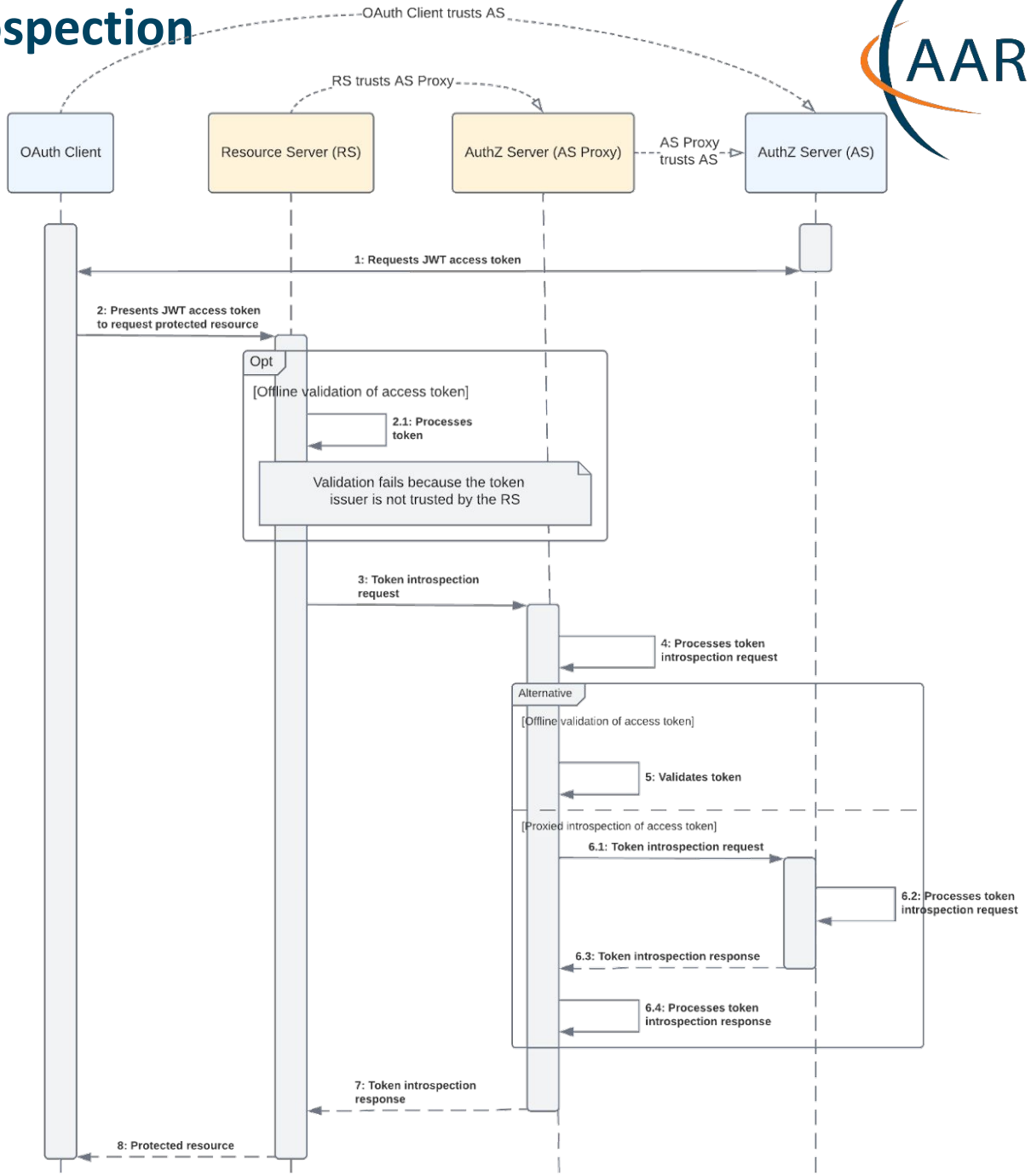


Summary

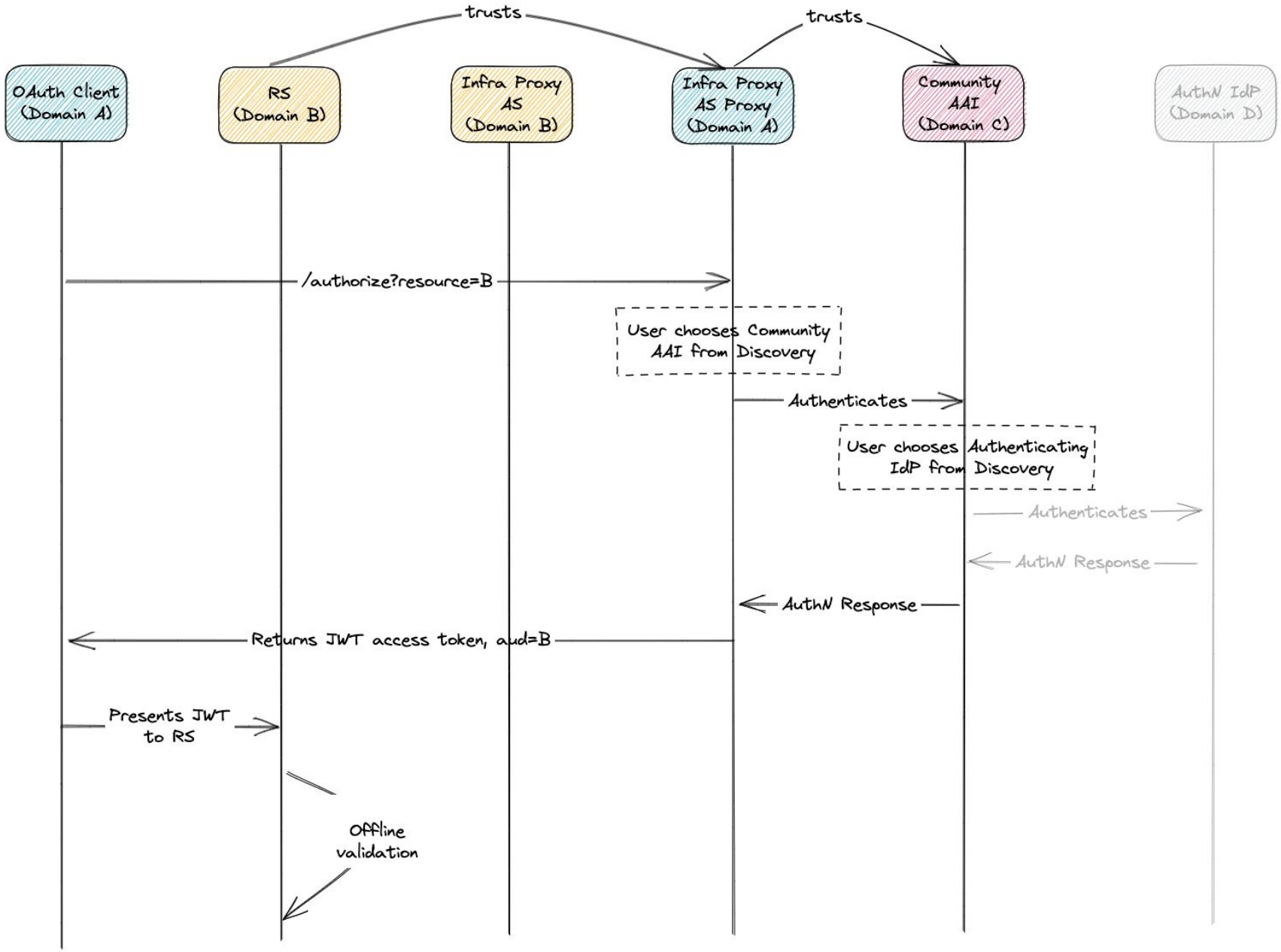
- Models for validating tokens across infrastructures
- Establishing trust across interfederations of AAIs
- Speaking the same language

AARC-G052 OAuth 2.0 Proxied Token Introspection

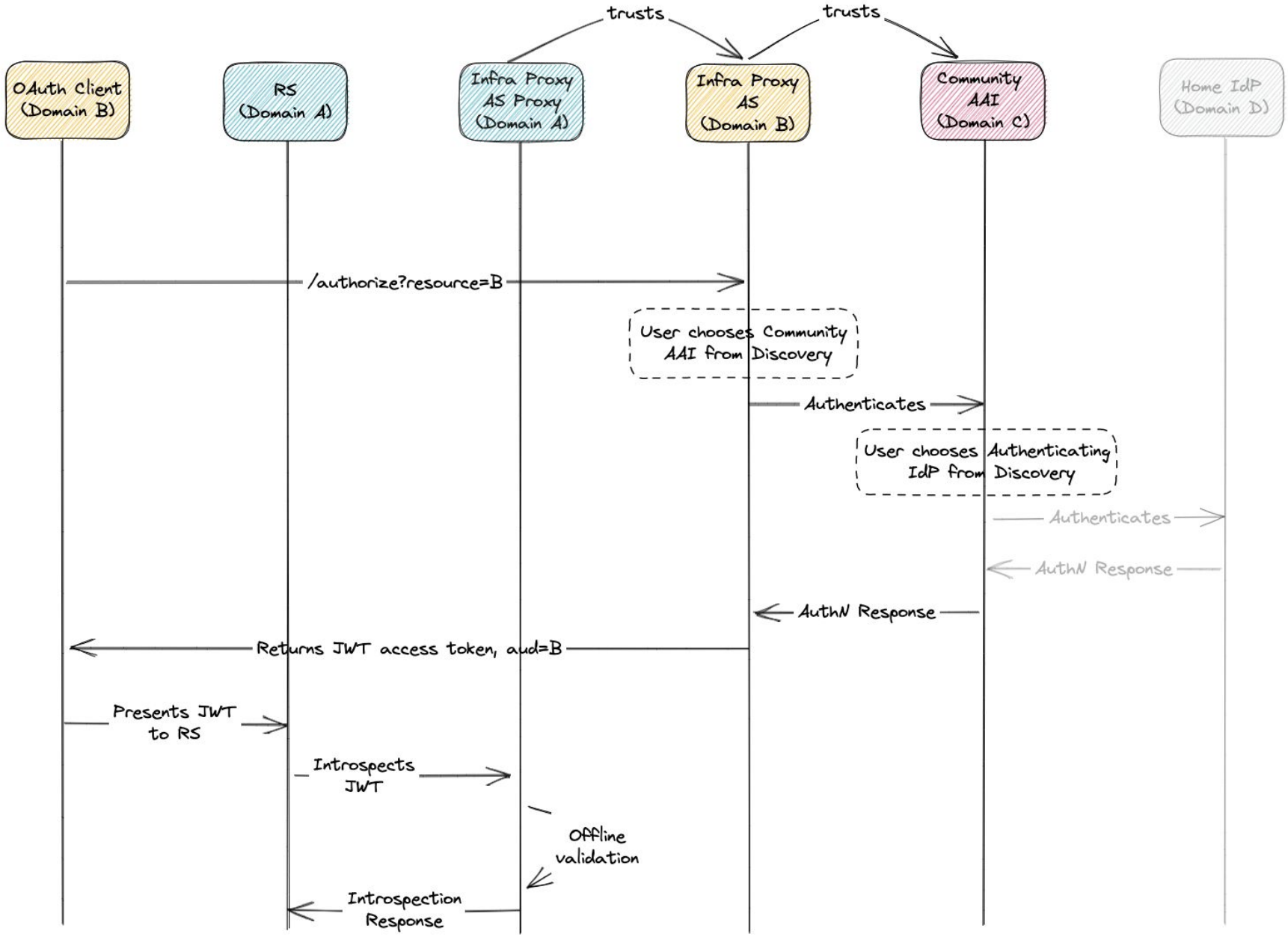
- Offline Token Validation by the RS
- Token introspection (RFC7662) invoked by RS, with offline token validation performed by AS
- Token introspection invoked by RS, with proxied token introspection performed by the AS



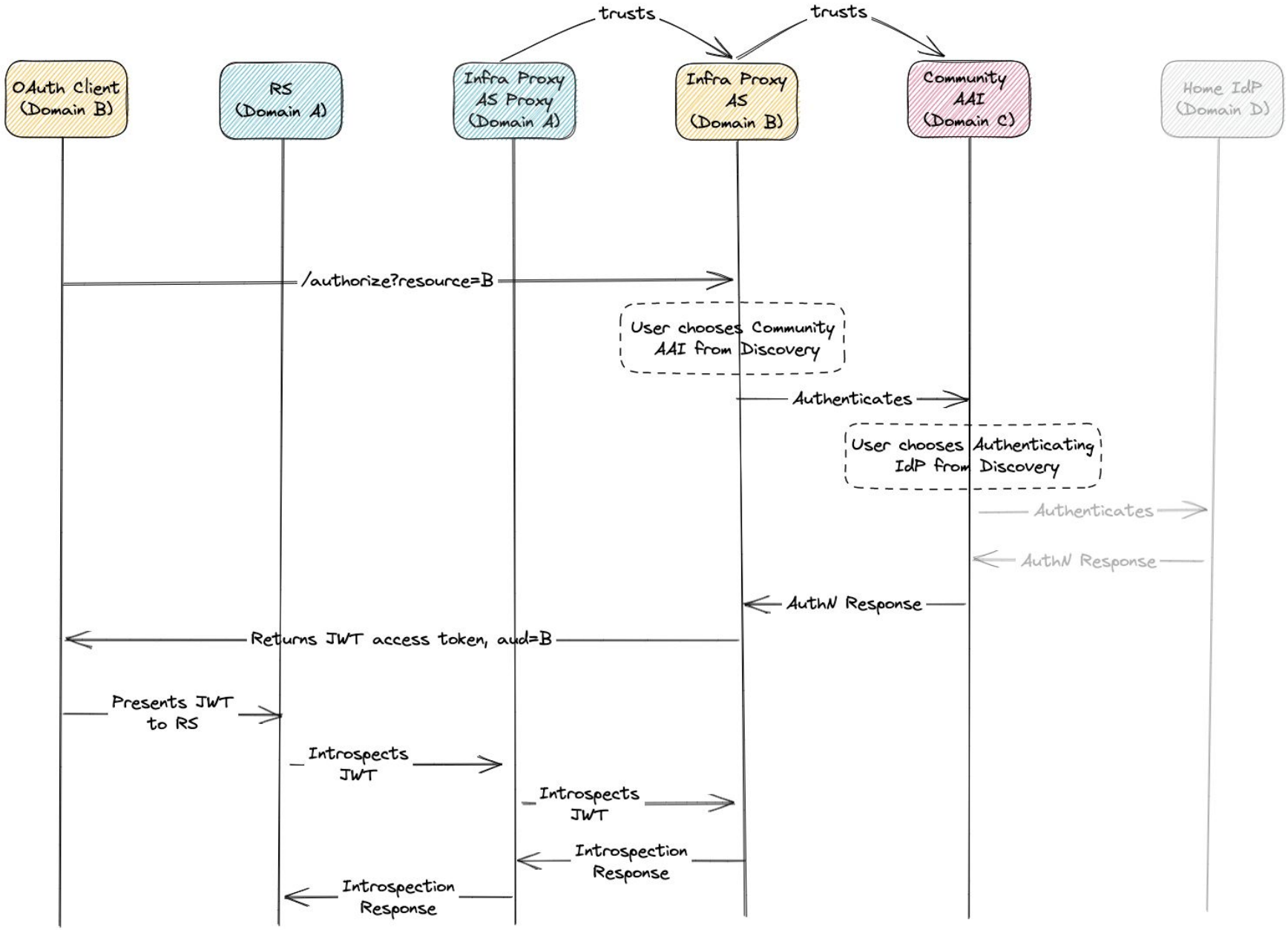
Offline token validation performed by the RS



Token introspection (RFC7662) invoked by RS, with offline token validation performed by AS

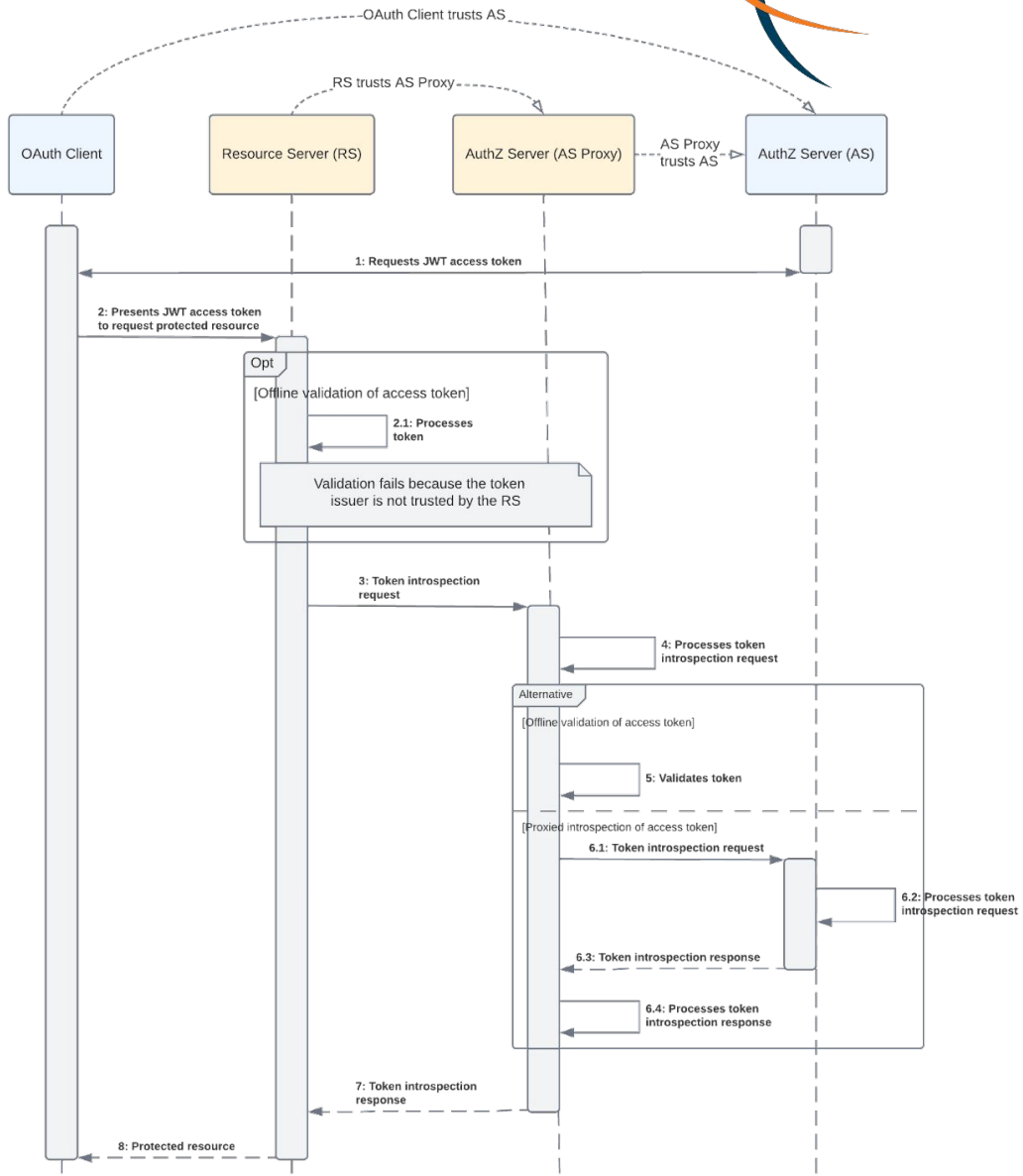


Token introspection invoked by RS, with proxied token introspection performed by the AS



AARC-G052 OAuth 2.0 Proxied Token Introspection

Approach	Advantages	Disadvantages
Offline token validation performed by RS	• Does not require callout to token issuer • Works with standard client and AS libraries	• Trust scalability: Each RS needs to trust all token issuers • Tokens MUST contain the authorisation claims • Does not support token revocation
Token introspection (RFC7662) invoked by RS, with offline token validation performed by AS	• Trust scalability: Only the AS Proxy needs to trust tokens issuers	• Requires callout from RS to AS Proxy • Tokens MUST contain the authorisation claims • Does not support token revocation • Requires modifications to AS libraries
Token introspection invoked by RS, with proxied token introspection performed by AS	• Trust scalability: Only the AS Proxy needs to trust tokens issuers • Supports token revocation	• Requires callout from RS to AS Proxy and from AS Proxy to token issuer • Requires modifications to AS libraries



Evolve the BPA to address the more complex (and the simpler) worlds

guidelines for **harmonising expression of community user attributes**

- **reduce inconsistencies** between implementations
- improve **interoperability** & **end-user usability** across research community communities and infrastructures

Extend AARC BPA

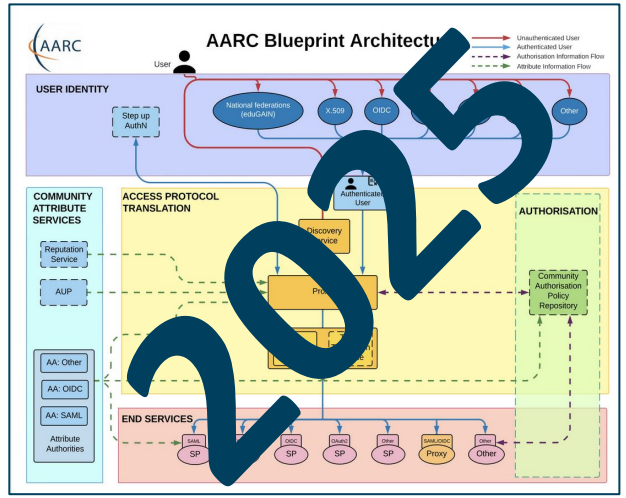
- improve **scalability**
- leverage emerging standards like **OpenID Federation**

Authorisation guidelines

- best practises to enable efficient & effective **sharing of federated resources**

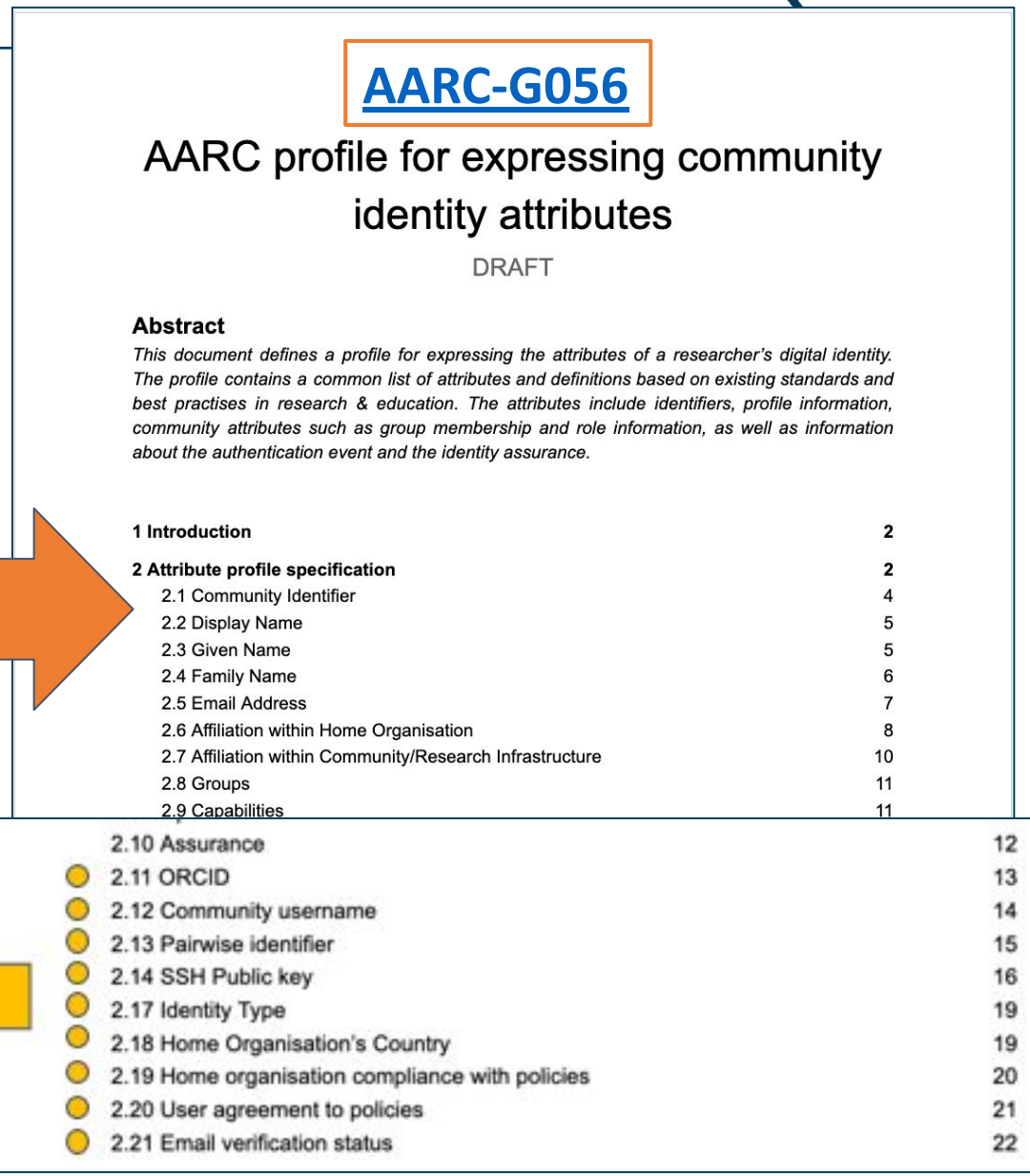
Decentralised identities

- guidance for **digital wallets** linked to BPA



How to *express* community identity attributes?

- *"How to express the **identifier** of a user?"*
  ⟶ AARC-G026
- *"How to express the **groups and roles** of a user?"*
  ⟶ AARC-G069 (was AARC-G002)
- *"How to express **resource capabilities** of a user?"*
  ⟶ AARC-G027
- *"How to express the **home institute** of a user?"*
  ⟶ AARC-G025
- *How to express user **assurance** information when interacting with another proxy?"*
  ⟶ RAF & AARC-G021



AARC-G056

AARC profile for expressing community identity attributes

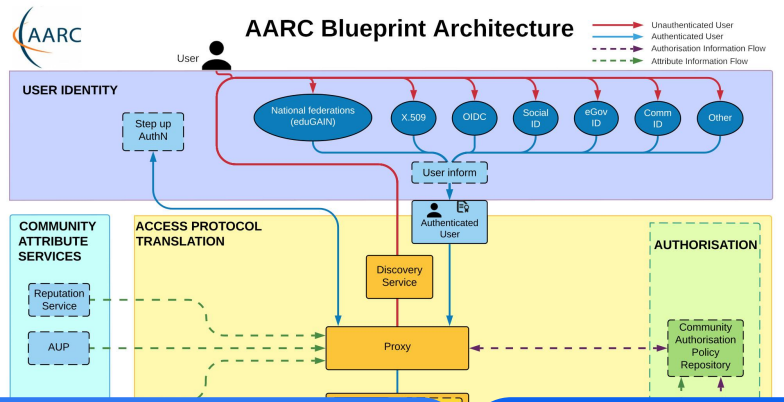
DRAFT

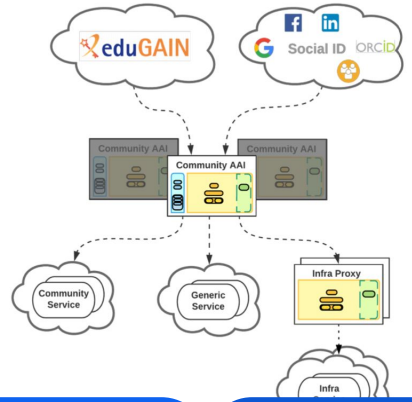
Abstract

This document defines a profile for expressing the attributes of a researcher's digital identity. The profile contains a common list of attributes and definitions based on existing standards and best practises in research & education. The attributes include identifiers, profile information, community attributes such as group membership and role information, as well as information about the authentication event and the identity assurance.

AARC Blueprint Architecture ‘BPA2025’!

AARC BPA 2019

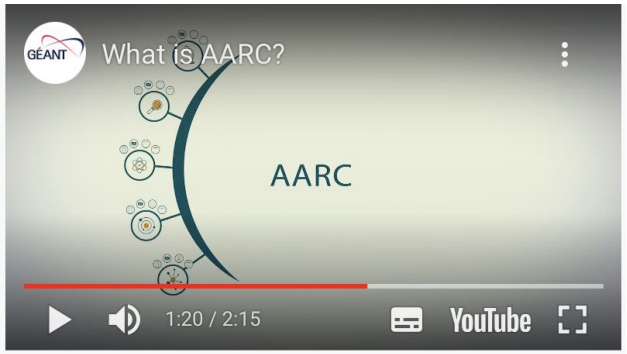




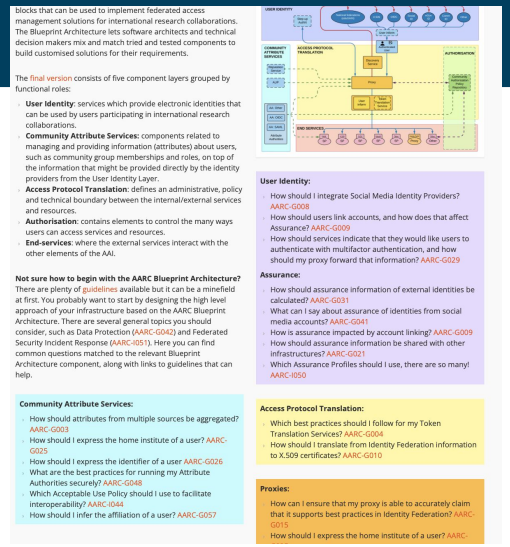
OpenID Federations + AuthZ for Federated Resources + Decentralised Identities & Wallets

AARC BPA 2025

Additional resources



https://youtu.be/Xpwb6BNxNW4



blocks that can be used to implement federated access management solutions for international research collaborations. The Blueprint Architecture lets software architects and technical decision makers mix and match tried and tested components to build customised solutions for their requirements.

The final version consists of five component layers grouped by functional roles:

- **User Identity**: services which provide electronic identities that can be used by users participating in international research collaborations.
- **Community Attribute Services**: components related to managing and providing information (attributes) about users, such as community group memberships and roles, on top of the information that might be provided directly by the identity providers from the User Identity Layer.
- **Access Protocol Translation**: defines an administrative, policy and technical boundary between the internal/external services and resources.
- **Authorisation**: contains elements to control the many ways users can access services and resources.
- **End-services**: where the external services interact with the other elements of the AAI.

Not sure how to begin with the AARC Blueprint Architecture?
There are plenty of guidelines available but it can be a minefield at first. You probably want to start by designing the high level approach of your infrastructure based on the AARC Blueprint Architecture. There are several general topics you should consider, such as Data Protection (AARC-G042) and Federated Security Incident Response (AARC-I051). Here you can find common questions matched to the relevant Blueprint Architecture component, along with links to guidelines that can help.

Community Attribute Services:
- How should attributes from multiple sources be aggregated? AARC-G003
- How should I express the home institute of a user? AARC-G025
- How should I express the identifier of a user AARC-G026
- What are the best practices for running my Attribute Authorities securely? AARC-G048
- Which Acceptable Use Policy should I use to facilitate interoperability? AARC-I044
- How should I infer the affiliation of a user? AARC-G057

User Identity:
- How should I integrate Social Media Identity Providers? AARC-G008
- How should users link accounts, and how does that affect Assurance? AARC-G009
- How should services indicate that they would like users to authenticate with multifactor authentication, and how should my proxy forward that information? AARC-G029

Assurance:
- How should assurance information of external identities be calculated? AARC-G031
- What can I say about assurance of identities from social media accounts? AARC-G041
- How is assurance impacted by account linking? AARC-G009
- How should assurance information be shared with other infrastructures? AARC-G021
- Which Assurance Profiles should I use, there are so many! AARC-I050

Access Protocol Translation:
- Which best practices should I follow for my Token Translation Services? AARC-G004
- How should I translate from Identity Federation information to X.509 certificates? AARC-G010

Proxies:
- How can I ensure that my proxy is able to accurately claim that it supports best practices in Identity Federation? AARC-G015
- How should I express the home institute of a user? AARC-

https://aarc-community.org/

Thanks to the AARC Community, including folk from whom we re-used graphics and material in this overview. In random order: Licia Florio, Nicolas Liampotis, Christos Kanellopoulos, Marina Adomeit, Janos Mohacsi, Ilaria Fava, Slavek Licehammer, Dave Kelsey, Ian Neilson, Marcus Hardt, Mischa Salle, Hannah Short, and Maarten Kremers.

Thank you

Any Questions?

https://aarc-community.org

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them. Grant Agreement No. 101131237 (AARC TREE).