Authentication and Authorisation for Research and Collaboration

Introduction to the AARC Blueprint Architecture (AARC-BPA-2017)

Training by AARC

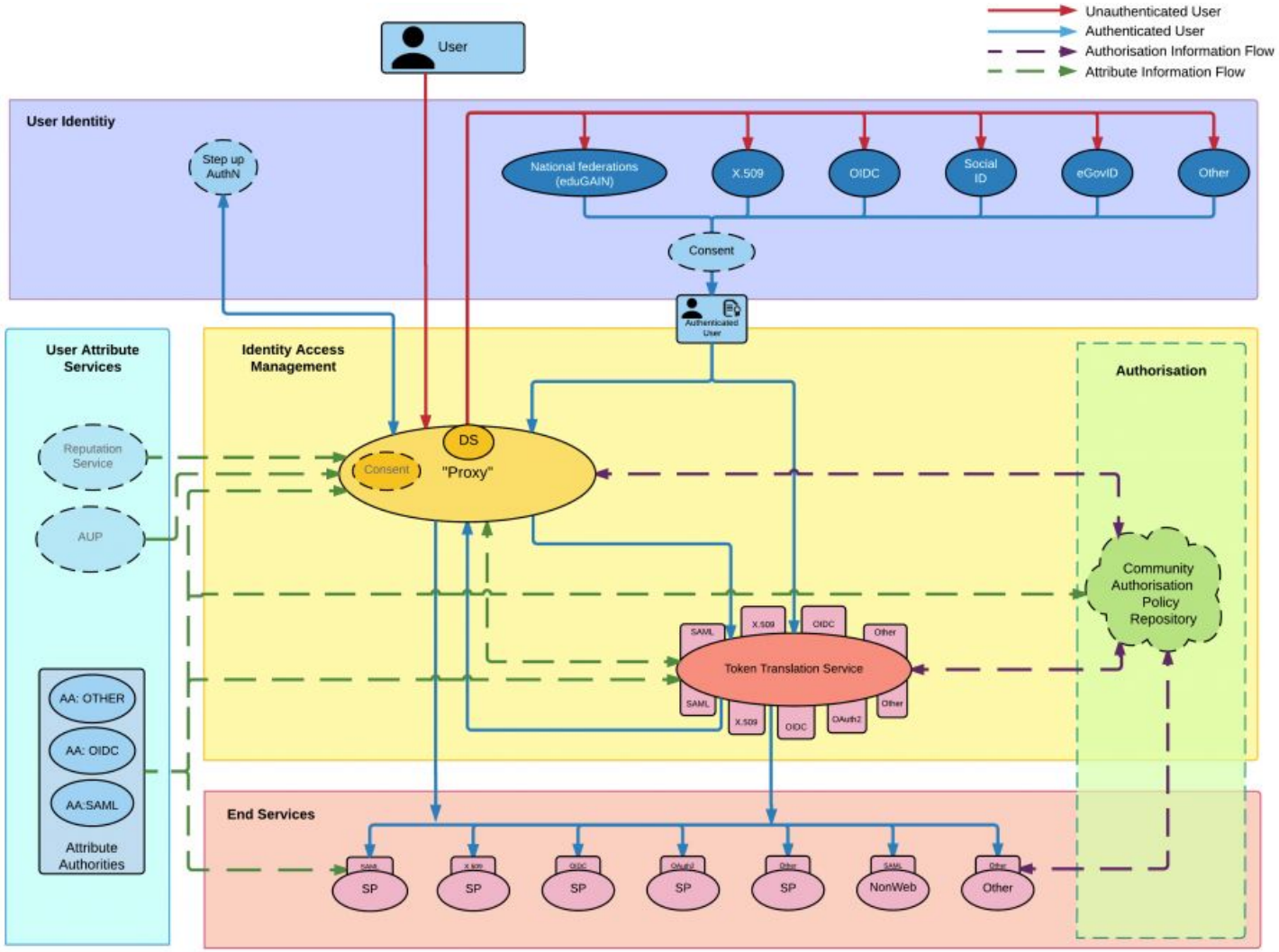
Agenda

- Goals of the BPA
- The AARC Blueprint Architecture schema
- eduGAIN as a foundation for the BPA

Introduction to the BPA
Goals

The purpose of the AARC Blueprint Architecture (BPA) is to provide **set of interoperable architectural building blocks** for software architects and technical decision makers, who are designing and implementing **access management solutions** for international research collaborations.

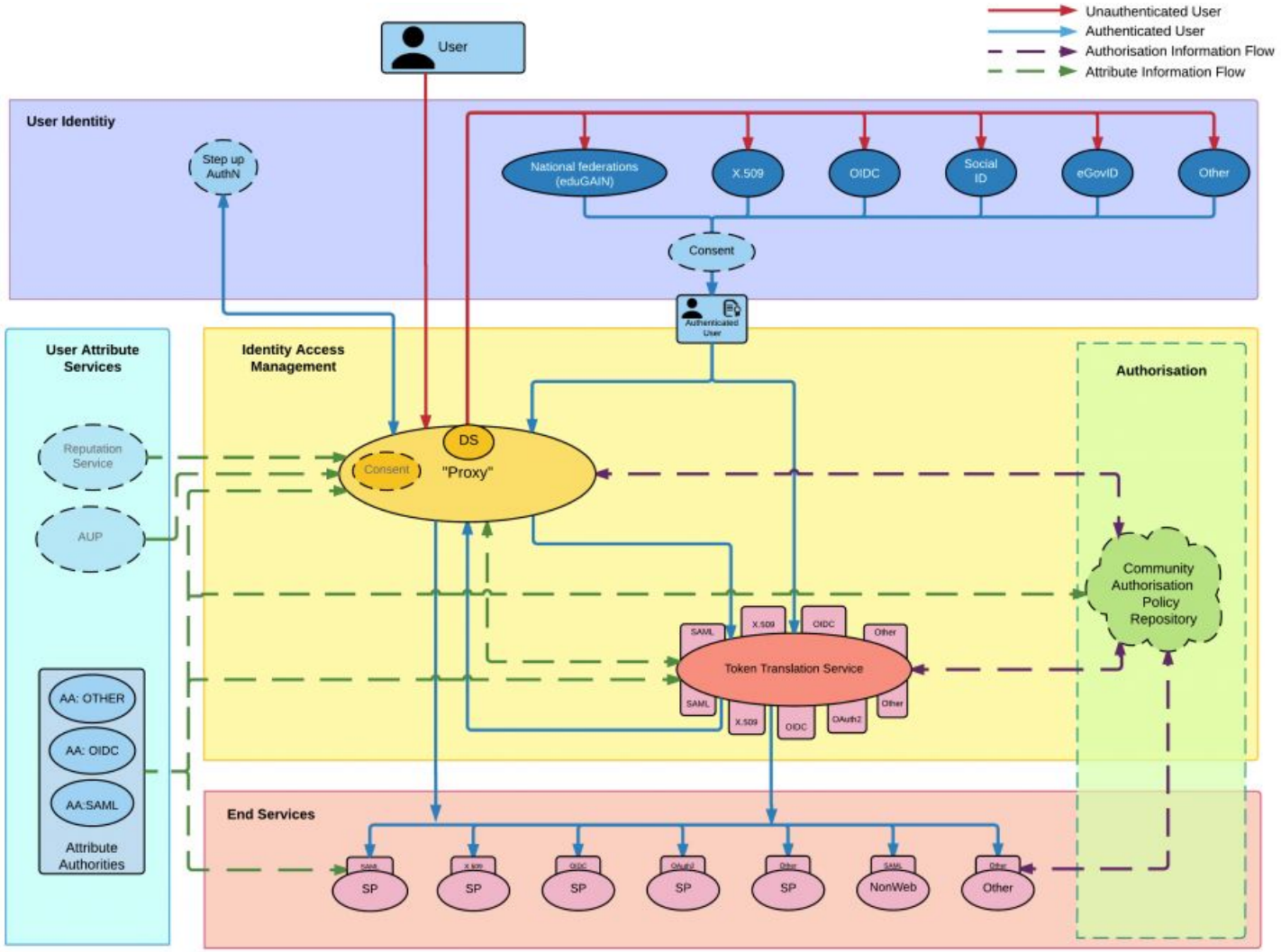
Introduction to the BPA
A Proxy as the central component



The BPA introduces the concept of a "**Proxy**": a community or infrastructure runs an "Infrastructure Proxy" and all of the Infrastructure services connect *only* to that Proxy

https://aarc-project.eu/blueprint-architecture/

Introduction to the BPA
Advantages of the Proxy



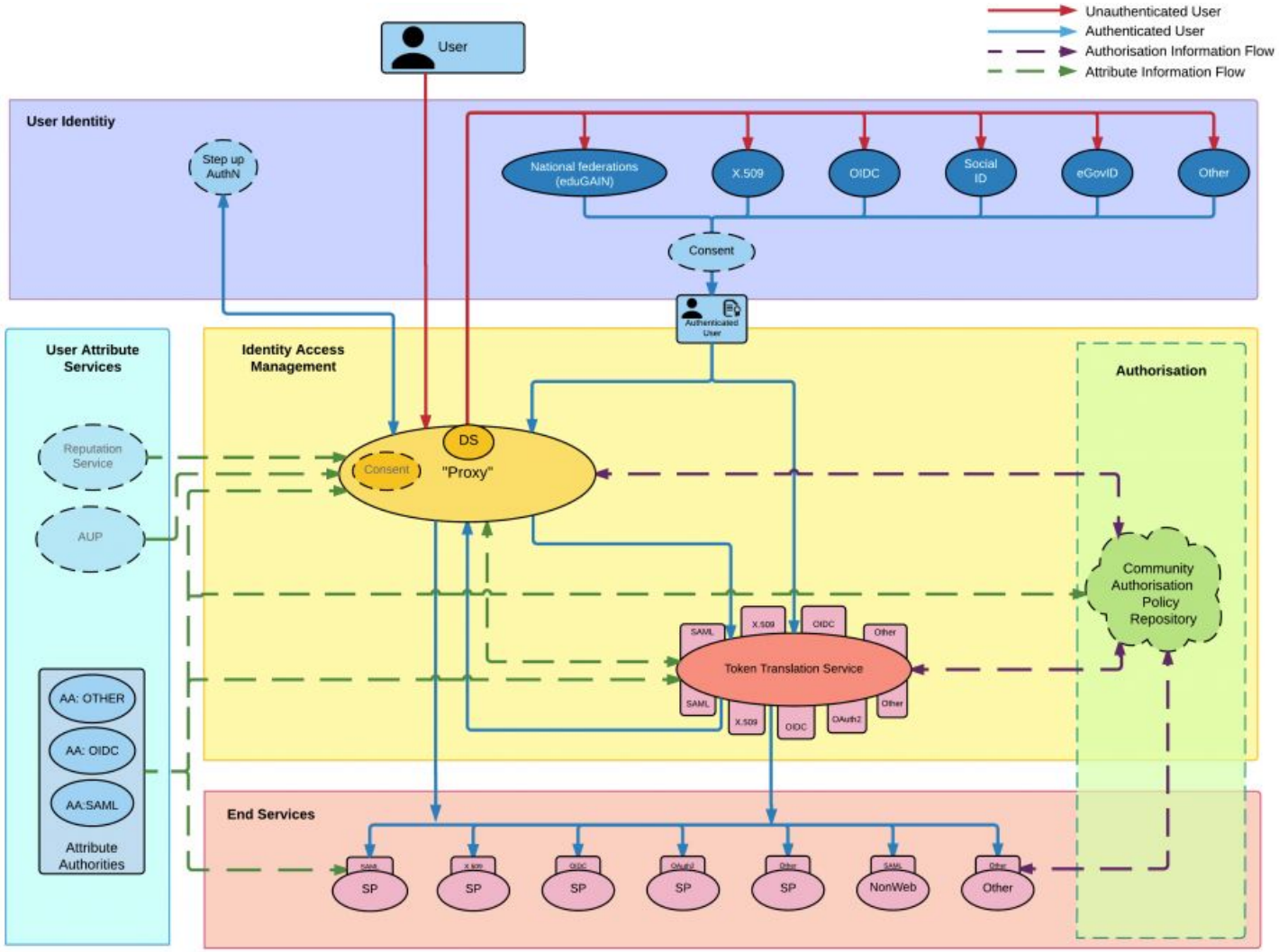
This makes sense because services within an infrastructures usually have common **requirements** that can be deployed and enforced at a **central point**

Also services do not need to **join federations** themselves

https://aarc-project.eu/blueprint-architecture/

Introduction to the BPA

Authentication can happen at the user's home organisation

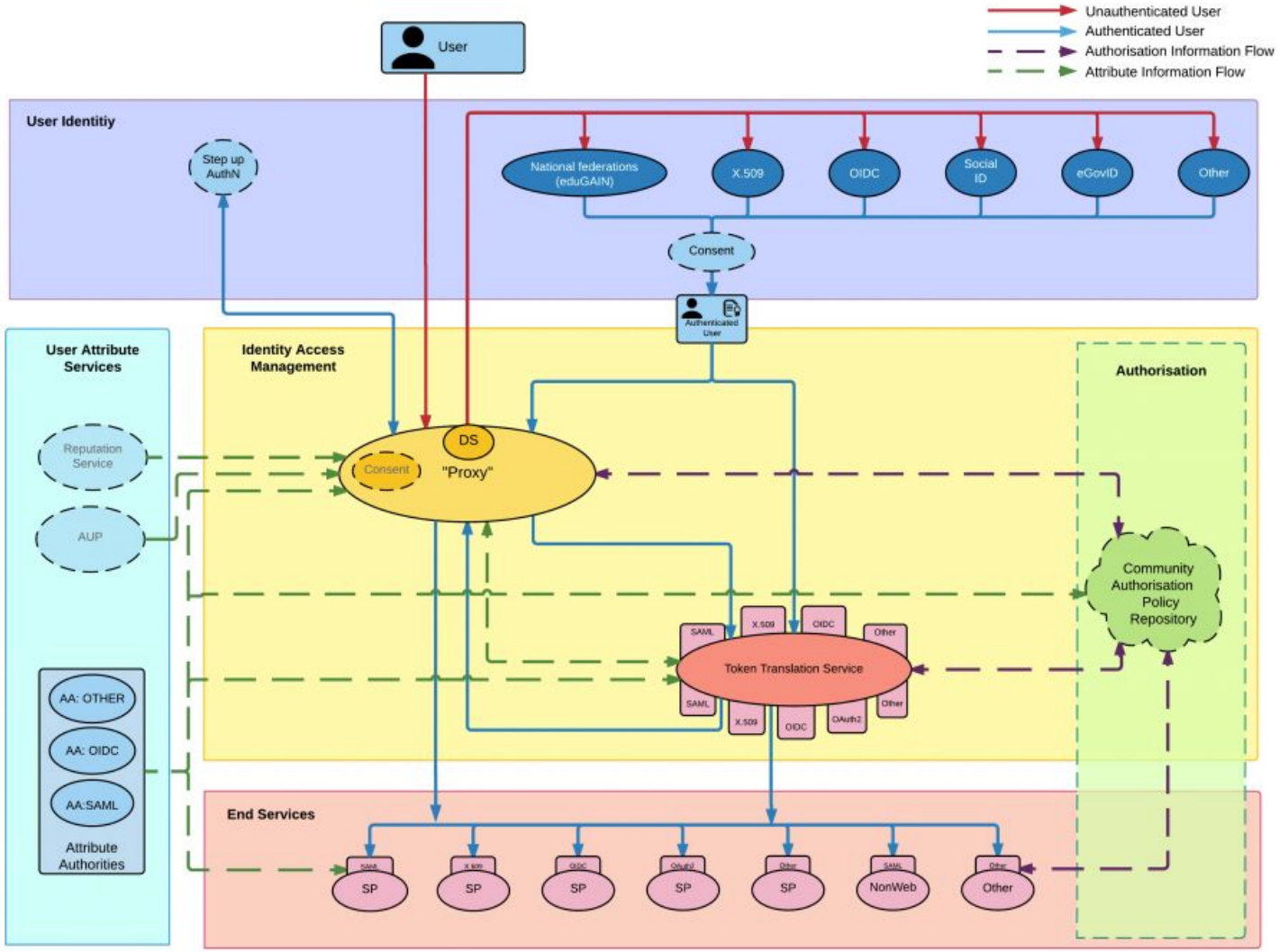


For **authentication** we can still use the IdPs from **home organizations** (they probably know their users best can provide higher assurance of the identities)

https://aarc-project.eu/blueprint-architecture/

Introduction to the BPA

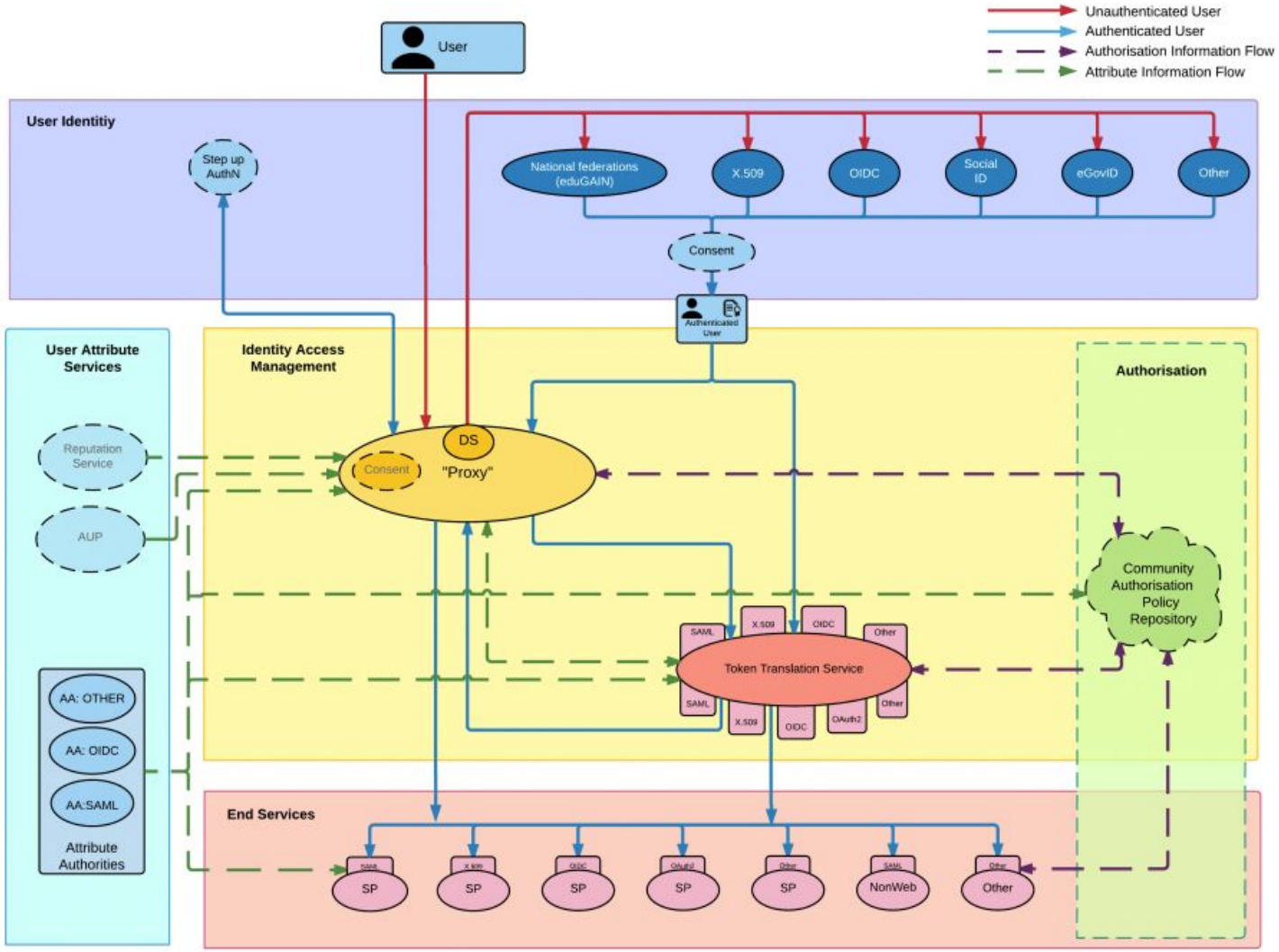
BPA consists of building blocks and guidelines



The BPA also describes **various building blocks** in AAI and gives guidelines and recommendations for them

https://aarc-project.eu/blueprint-architecture/

Introduction to the BPA
Technology agnostic design



The AARC Blueprint Architecture is meant to be **technology agnostic** by design and has been verified against production implementations that use SAML2, OpenID Connect, OAuth2, or combinations of these.

https://aarc-project.eu/blueprint-architecture/

The different layers of the BPA
User Identity Layer

- The User Identity Layer includes services which provide electronic identities that can be used by users participating in International Research Collaborations.
- Typically, identity services in this layer are outside of the administrative boundaries of the International Research Collaborations.
- Services in the layer are expected to use secure authentication mechanisms, in order to bind physical persons to their electronic identities, which are then made available to services in the other layers via secure protocols.
- Examples of this layer include the user's **home organisation IdP**, **homeless IdPs** from communities or **social IdPs**

The different layers of the BPA
Identity Access Management Layer

- The Identity Access Management Layer, defines an **administrative, policy and technical boundary** between the internal services and resources of the RI/EI and any other external services and resources.
- The components in this layer allow the RIs/EIs to
  - take full advantage of eduGAIN and the national identity federations,
  - reduce the administrative overhead of introducing new services and
  - have the flexibility to choose the appropriate security protocols and mechanisms.
- This layer enables the implementation of a **single point** where to provide a discovery service, a group management systems and consistent and where to manage user consent.
- This layer enables the infrastructure to provide guarantees that may not be met by the external IdPs alone, such as unique, persistent identifiers, multi-LoA management, infrastructure-specific attributes, account linking, etc.
- The main component of this layer is the **Proxy**

The different layers of the BPA
User Attribute Services Layer

- The User Attribute Services Layer groups components related to **managing and providing information (attributes) about users**, such as group memberships and community roles, on top of the information that might be provided directly by the IdPs.
- In this layer, apart from Attribute Authorities, we have two other components:
  - the **AUP (Acceptable Use Policy)**: a service which specifically records whether the user has accepted the AUP of the infrastructure;
  - the **reputation attribute services**: a service which records the user's "reputation" (reputation is a value assigned to the user's account by the infrastructure, this value can increase or decrease according to specific user events with the infrastructure and permits to assign higher authorisations and privileges to accounts with a higher reputation).

The different layers of the BPA
Authorisation Layer

- The Authorisation Layer responsible to provide **authorisation of access to services**.
- Typically, in RI/EIs, authorisation can be based
  - on the group membership of the users,
  - on the roles a user might have been granted within the collaboration,
  - on the entitlements users might have been granted,
  - on the affiliations of the users,
  - on the strength of the authentication method used or the quality of the user information or
  - on combinations of these.
- Although authorisation enforcement always happens on the service side, the AARC-BPA allows the implementers to **delegate much of the complex decisions to central components**, which can significantly reduce the complexity of managing authorisation policies, and their evaluation on each service individually.
- Work on this layer was **not concluded** in AARC1 and is expected to be revisited during AARC2.

The different layers of the BPA
End Services Layer

- The End Services Layer contains the **services** users actually want to use.
- Access to these services is **AAI protected**.
- Credential translation or token translation can happen centrally and/or within a service, although the latter is outside of the scope of the AARC Blueprint Architecture.
- Examples of this layer are the **actual services (SPs)** within the infrastructure

AARC Blueprint Architecture & eduGAIN

eduGAIN and the Identity Federations

A solid foundation for federated access in R&E

Authentication and Authorization Architecture for Research Collaboration

A set of building blocks on top of eduGAIN for International Research Collaboration

Supporting documents

Together with the architecture schema a set of documents has been created to describe main architectural aspects:

- [AARC-G002] Guidelines on expressing group membership and role information
- [AARC-G003] Guidelines on attribute aggregation
- [AARC-G004] Guidelines on token translation services
- [AARC-G005] Guidelines on credential delegation
- [AARC-G006] Best practices for managing authorisation
- [AARC-G007] Guidelines on non-browser access
- [AARC-G008] Guidelines for implementing SAML authentication proxies for social media identity providers
- [AARC-G009] Account linking and LoA elevation use cases and common practices for international research collaboration
- [AARC-G010] Best practices and recommendations for attribute translation from federated authentication to X.509 credentials
- [AARC-G021] Guideline on the exchange of specific assurance information between Infrastructures

BPA in AARC2

The work on the BPA **continues** in AARC2

Most of the **missing requirements** will be addressed by guidelines developed in AARC2

In the end there will be a revised version of the BPA, which will focus on topics such as **authorization** and **step-up authentication** in more detail

The AARC Engagement Group for InfrastructureS (AEGIS) was established to create a **channel between AARC and the infrastructures** and push AARC results into production

What we have learnt

- ★ What is the BPA defined in AARC
- ★ How is the BPA composed
- ★ Which are the main layers of the BPA
- ★ Which areas of the BPA are being work on in AARC2

Thank you

Any Questions?

https://aarc-project.eu

The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 730941 (AARC2).