Authentication and Authorisation for Research and Collaboration

AARC Blueprint Architecture

Christos Kanellopoulos

February 21st, 2017

The starting point

- The scenario:
  - There is a **technical architect of a research community**
  - Her community is **distributed internationally**
  - **Increasing number of services** need authentication and authorization
  - Her job is to **find a solution**
  - She wants to **focus on research** and not reinvent the wheel

The goals

1. Users should be able to access the all services using the **credentials from their Home Organization**

2. Users should have one **persistent non-reassignable non-targeted unique identifier**.

3. Attempt to **retrieve user attributes** from the user's Home Organization. If this is not possible, then an alternate process should exist.

4. Distinguish **(LOA)** between self-asserted attributes and the attributes provided by the Home Organization/VO

5. **Access** to the various services should be granted **based on** the **role(s)** the users have within the collaboration

6. Users and services should not have to deal with the complexity of multiple IdPs/Federations/Attribute Authorities/technologies.

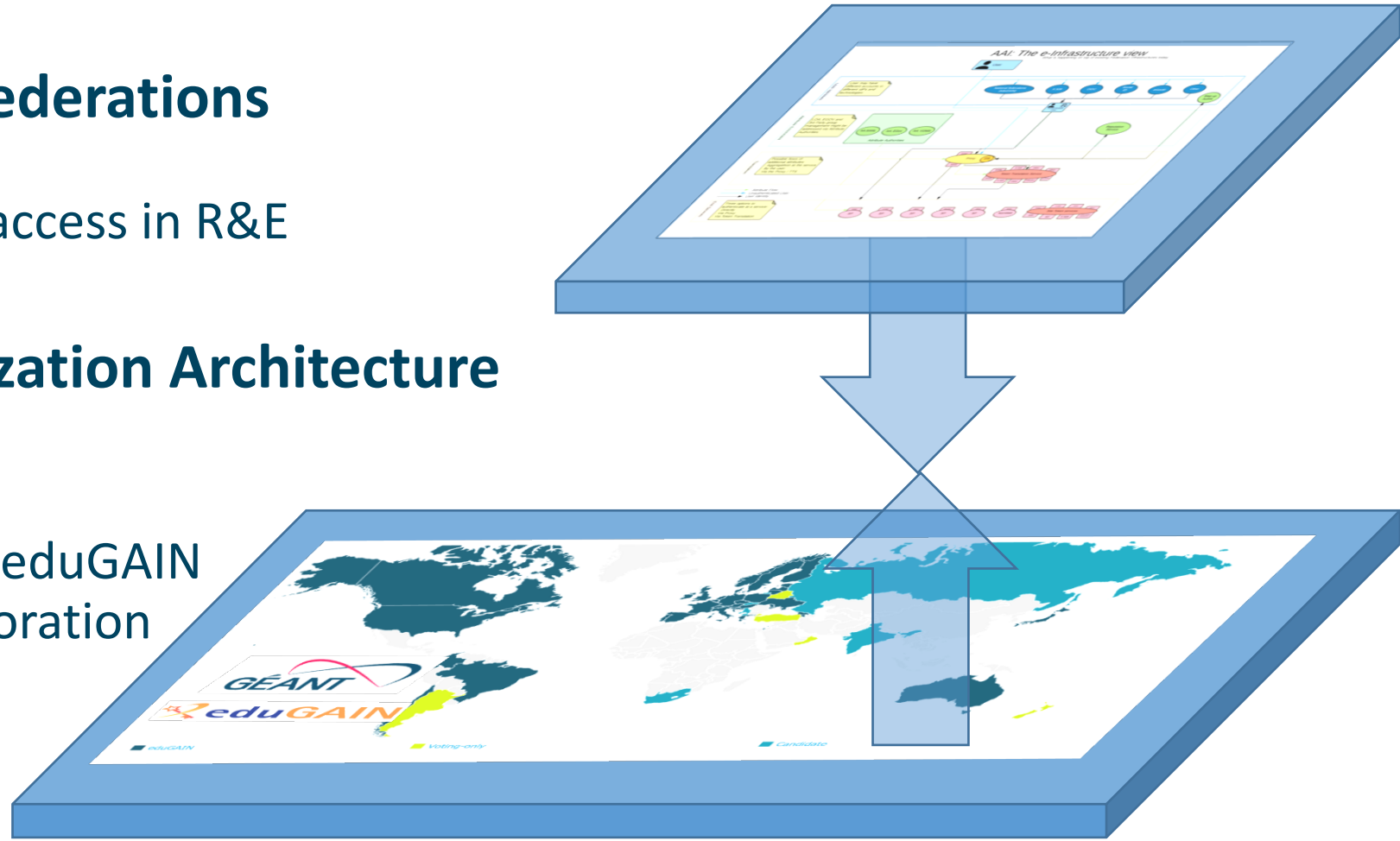
AARC Blueprint Architecture & eduGAIN

eduGAIN and the Identity Federations

A solid foundation for federated access in R&E

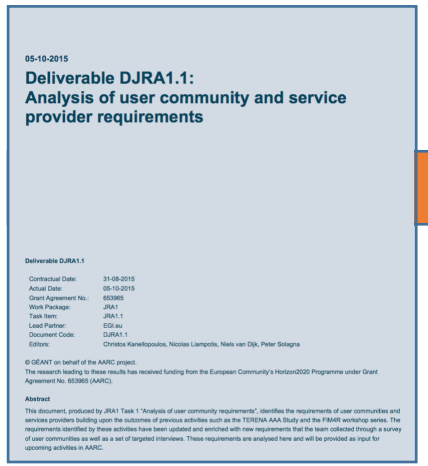
Authentication and Authorization Architecture for Research Collaboration

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

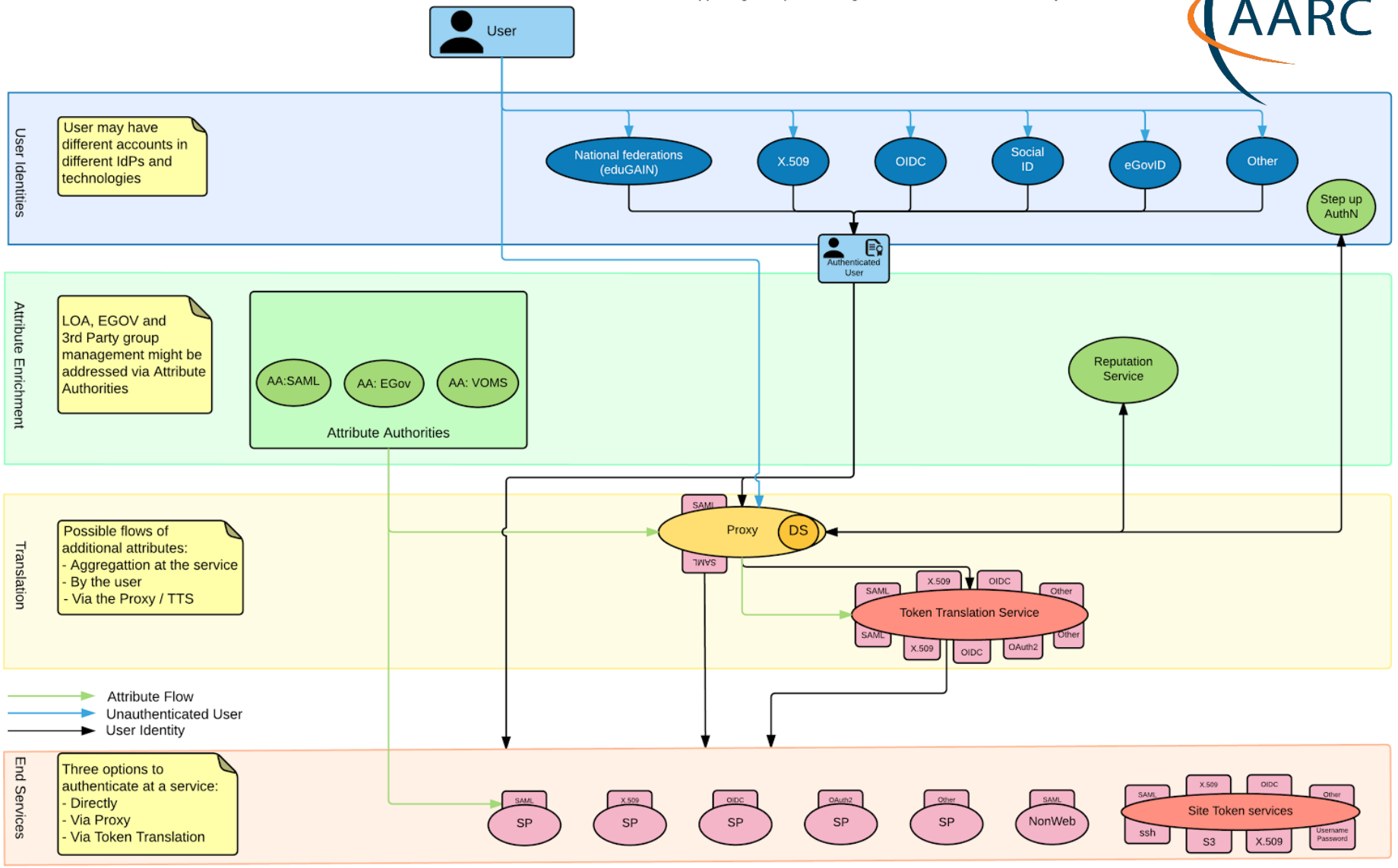


AARC Blueprint Architecture (1st Draft)

User Community Requirements

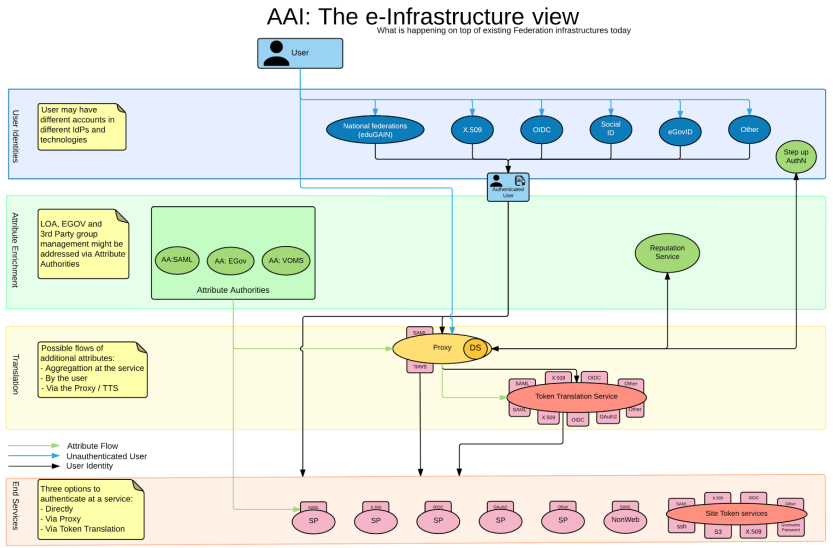


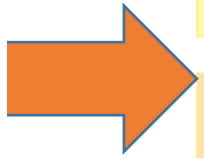
https://goo.gl/kSxENp

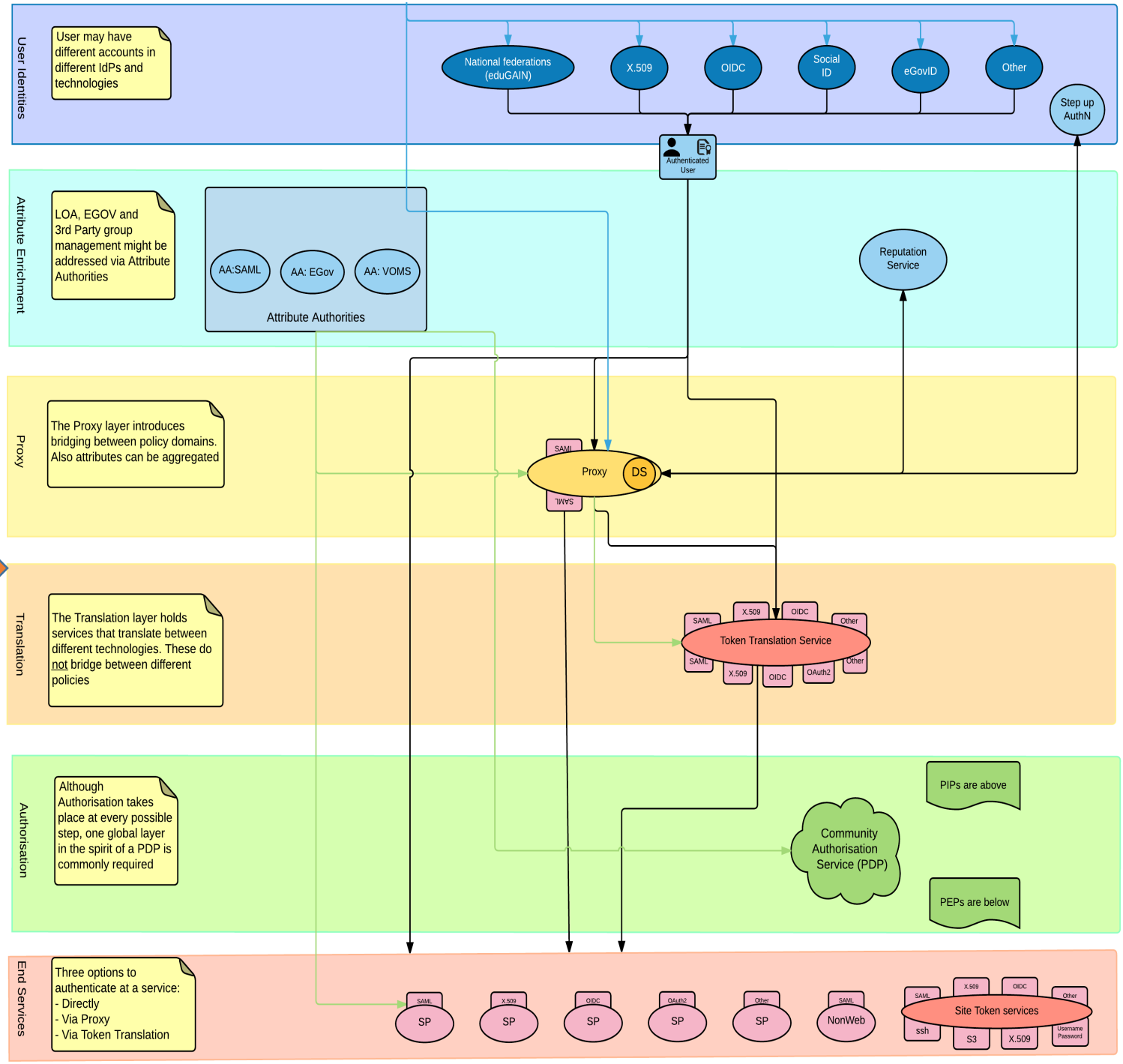


https://aarc-project.eu/aarc-draft-blueprint-architecture-available-for-comments/

AARC Blueprint Architecture (2nd Draft)







Highlights of the next version of AARC Blueprint Architecture

- Non-web access
- Token Translation Services
- Best practices for managing authorization
- Expressing group membership
- Attribute aggregation

Recommendations for AAI implementations in the context of international research collaborations

Highlights of the next version of AARC Blueprint Architecture

- Non-web access
- Token Translation Services
- Best practices for managing authorization
- Expressing group membership
- Attribute aggregation

Recommendations for AAI implementations in the context of international research collaborations

NOT meant to be documents for general AAI deployments in the academic environment (e.g. for campuses etc)

Highlights of the next version of AARC Blueprint Architecture

- Non-web access
- Token Translation Services
- Best practices for managing authorization
- Expressing group membership
- Attribute aggregation

Recommendations for AAI implementations in the context of international research collaborations

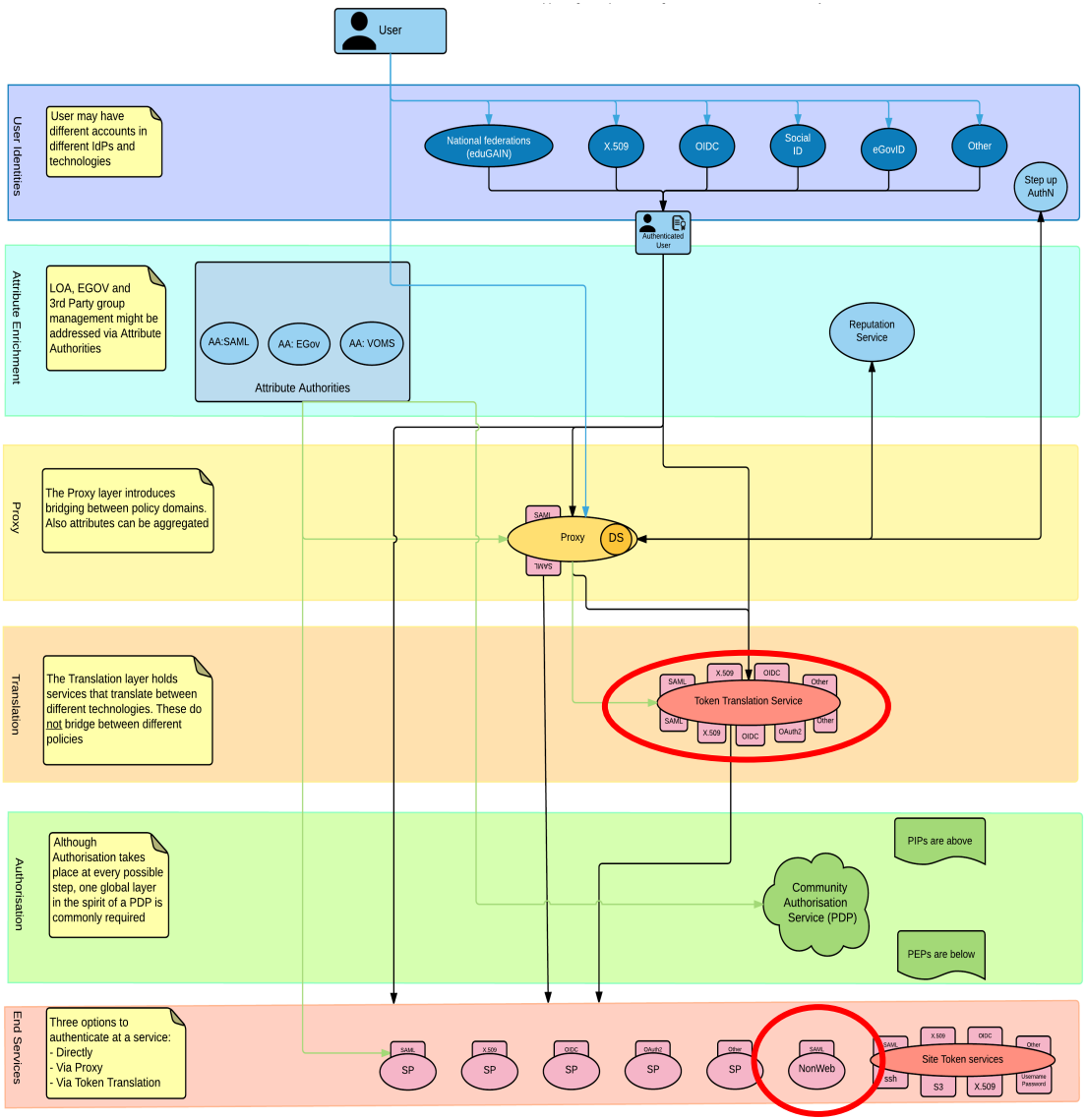
NOT meant to be documents for general AAI deployments in the academic environment (e.g. for campuses etc)

Open for comments until the end of February

Non-web access

https://goo.gl/JzatTx

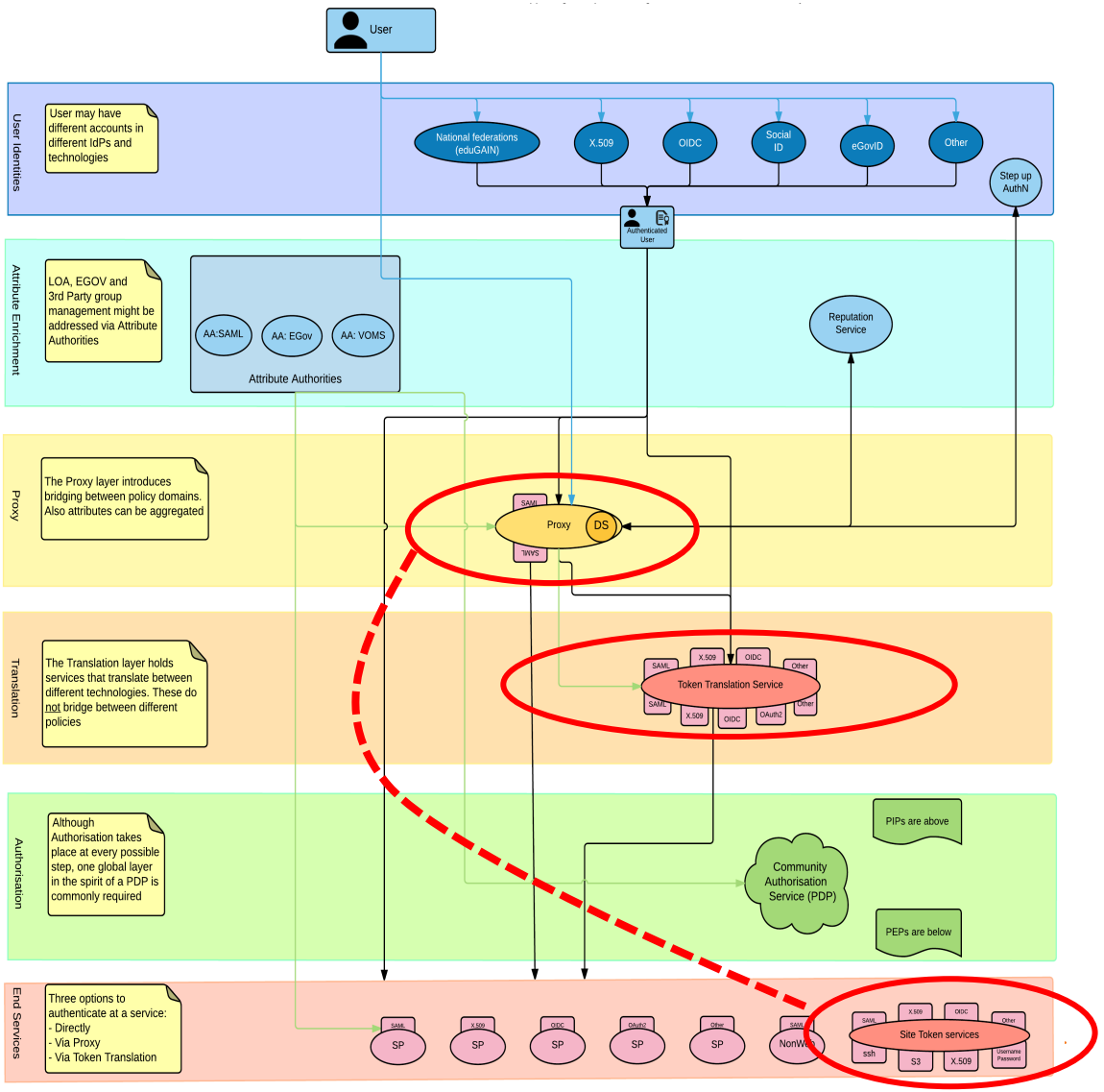
- Services that are NOT accessible with the use of a browser. Typically, command line access
- SSH / SFTP
  - SSH Key provisioning via access web portal
  - GSI Enabled SSH (x509v3 (proxy) certificates)
- HTTP APIs
  - OIDC/OAuth2
  - X509v3 (proxy) certificates
- Batch Job Submission and Data Management Systems in eScience environments
  - X509v3 (proxy) certificates
- **All require some kind of Token Translation system**



Token Translation Services

https://goo.gl/RNCsm3

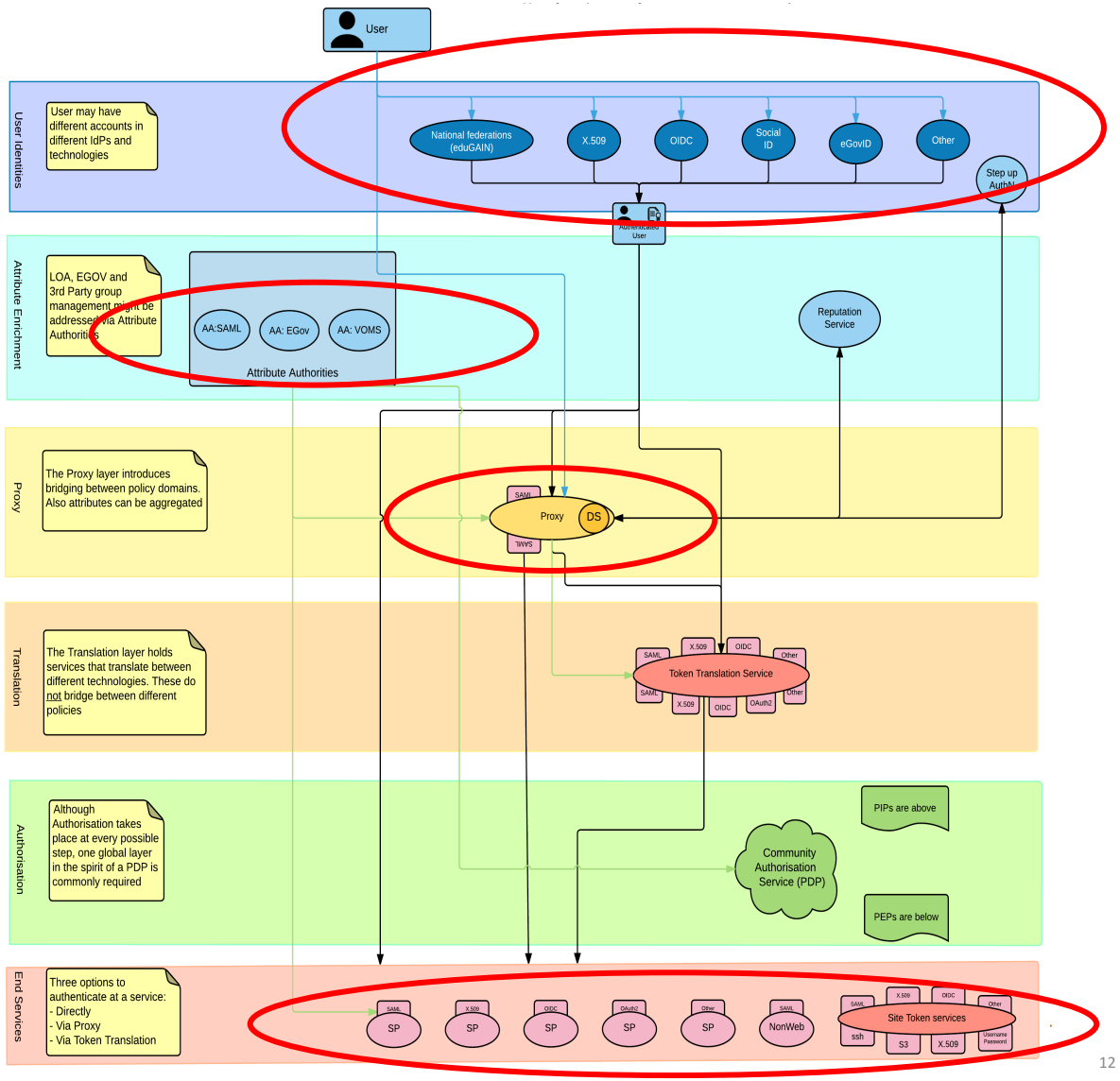
- Mechanisms that enable access to services that support different token formats
- Typical scenarios
  - SAML Assertions <-> X509v3 (proxy) certificates
  - SAML Assertions <-> OIDC Tokens
  - OIDC Tokens <-> X509v3 certificates
- Deployment use cases
  - Standalone vs Embedded
- Token Translation Type
  - Direct vs Indirect (provisioned)



Best practices for managing authorization

https://goo.gl/aFFPS1

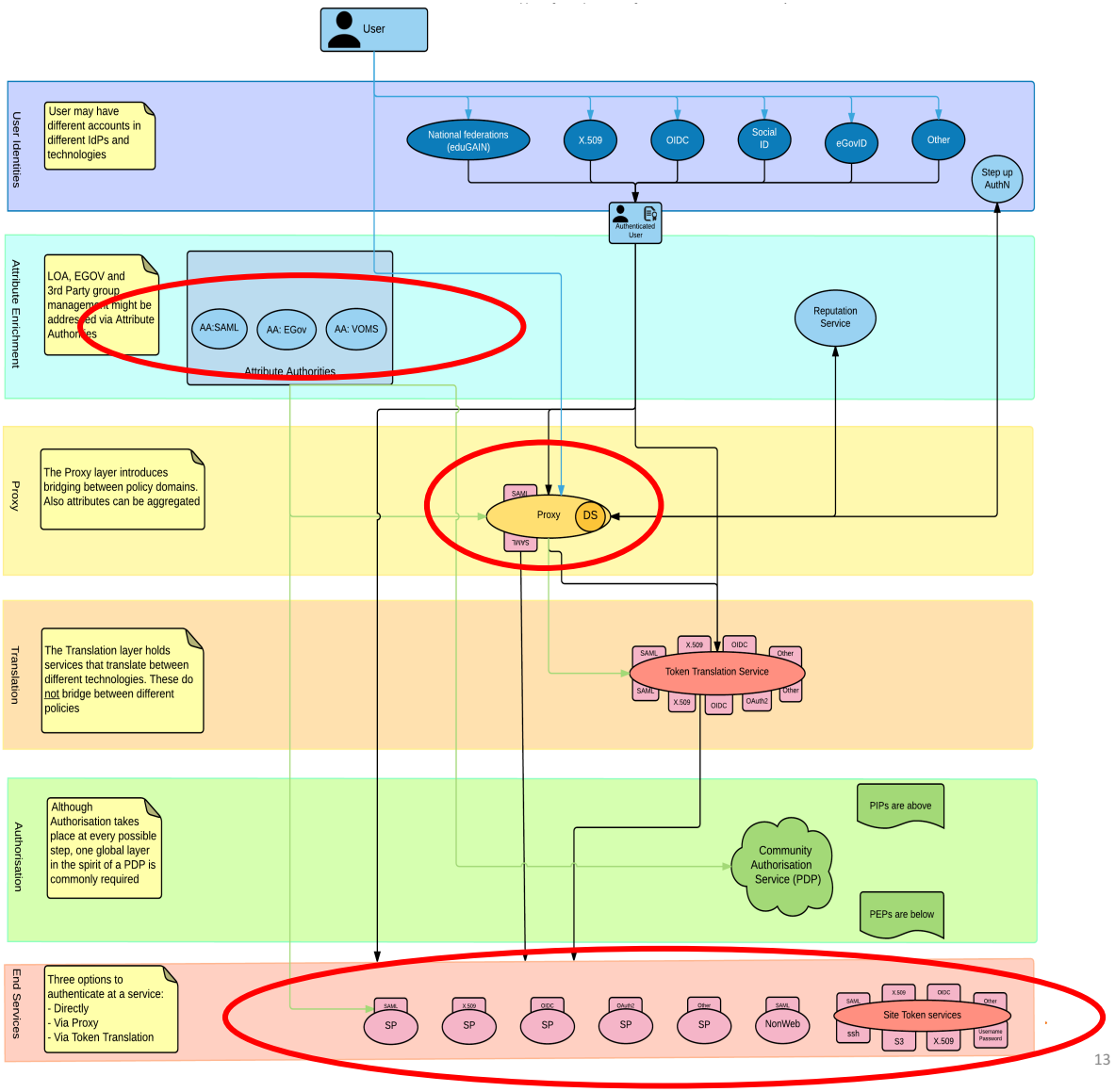
- In Research Collaborations access to services is authorized based on the role/group membership of each user in the collaboration
- Other possible parameters:
  - Affiliation of the user
  - Strength of the authentication / Level of Assurance
- Centralized vs delegated authorization management



Expressing group membership

https://goo.gl/Maz4R2

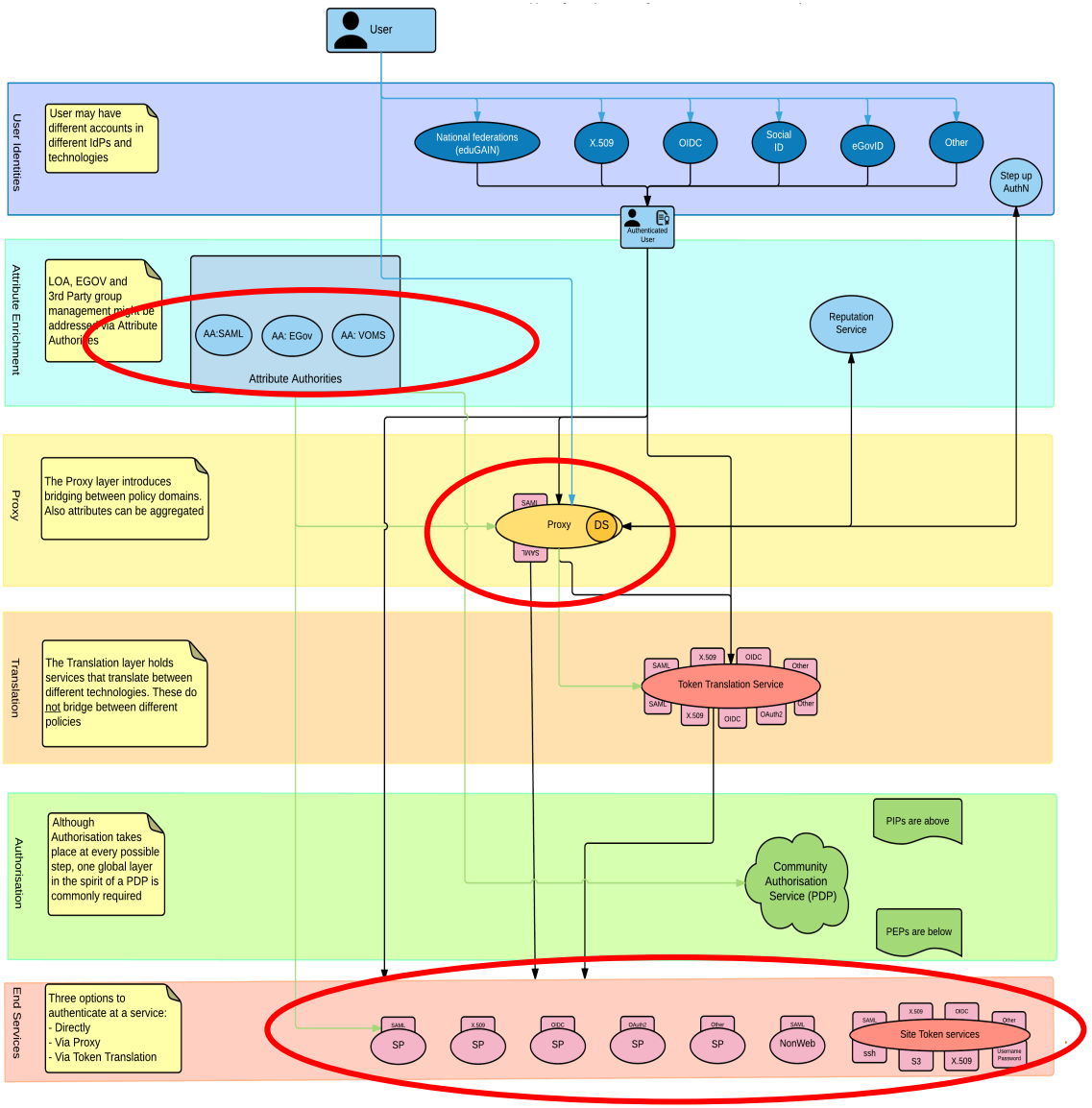
- Syntactic and semantic harmonization of group membership information
- Scoping of group membership information:
  - Specify the scopes where the identified group membership information is valid.
- Group membership and role information
  - Use the eduPersonEntitlement attribute
  - Group hierarchies



Attribute Aggregation

https://goo.gl/lQd3Rt

- Necessary when gathering attributes from more than one source
- Push vs Pull model
- Persistent unique identifiers and record/account linking
- Where attribute aggregation should take place?
- Attribute filtering and harmonization



Next steps

- Documents open for comments until the end of Feb
  - Accepting comments in the Google docs and the AARC Connect ML (https://lists.geant.org/sympa/subscribe/aarc-connect)
- Next version of the BPA due end of March

Thank you

Any Questions?

skanct@gmail.com

http://aarc-project.eu/

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 653965 (AARC).