



Authentication and Authorisation for Research and Collaboration

The AARC Blueprint Architecture

Christos Kanellopoulos - GÉANT

International Research Collaborations

1. Users should be able to access the all services using the **credentials from their Home Organizations** when available.
2. Secure integration of **guest identity solutions** and **support for stronger authentication mechanisms** when needed.
3. **Access** to the various services should be granted **based on the role(s)** the users have **within the collaboration**.
4. Users should have one **persistent identity** across all **community services** when needed.
5. **Ease of use for users and service providers.** The complexity of multiple IdPs/Federations/Attribute Authorities/technologies should be hidden.



Attribute Release	Attribute Aggregation	User Friendliness	SP Friendliness
Persistent Unique Id	Credential translation	Credential Delegation	User Managed Information
Levels of Assurance	Guest users	Step-up AuthN	Best Practices
Community-based AuthZ	Non-web-browser	Social & e-Gov IDs	Incident Response

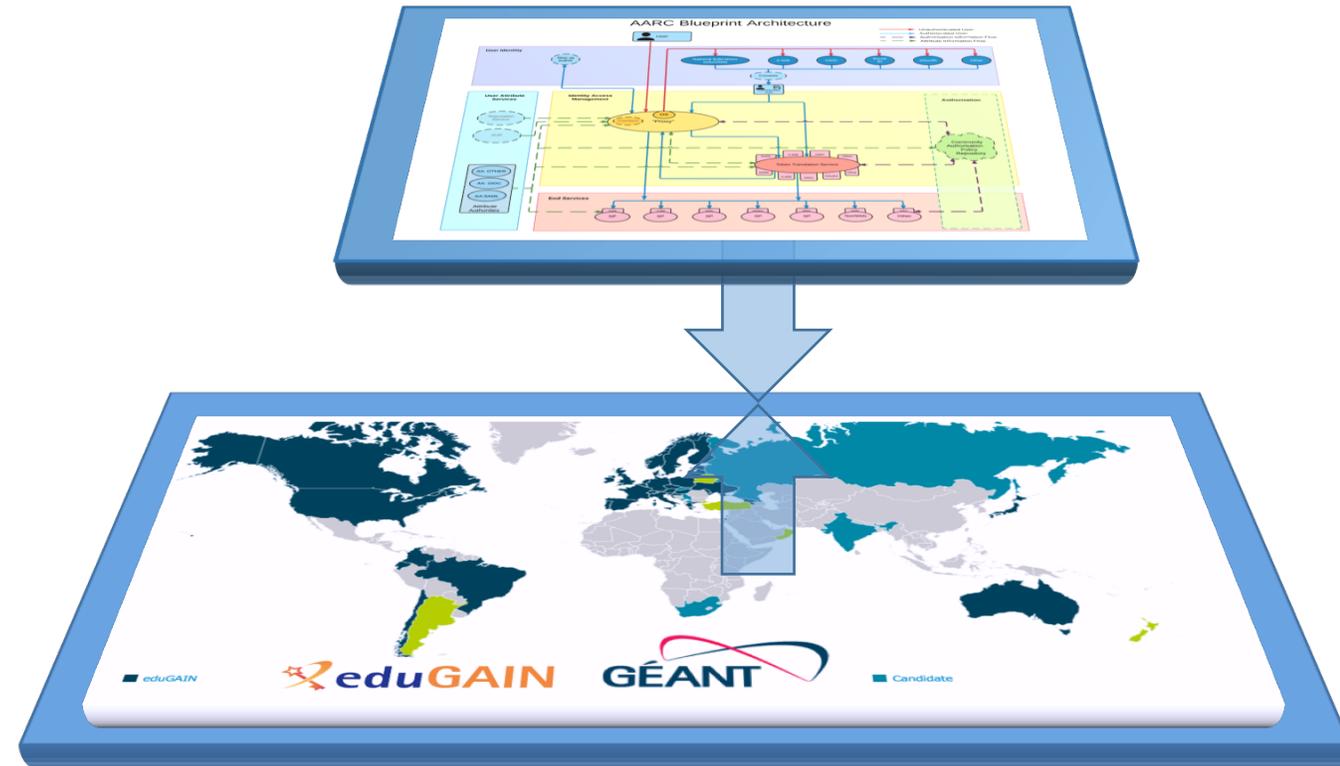
Identity & Access Management for International Research Collaborations

A Blueprint Architecture for authentication and authorization

A set of architectural building blocks on top of eduGAIN

eduGAIN and the Identity Federations

A solid foundation for federated access in Research & Education



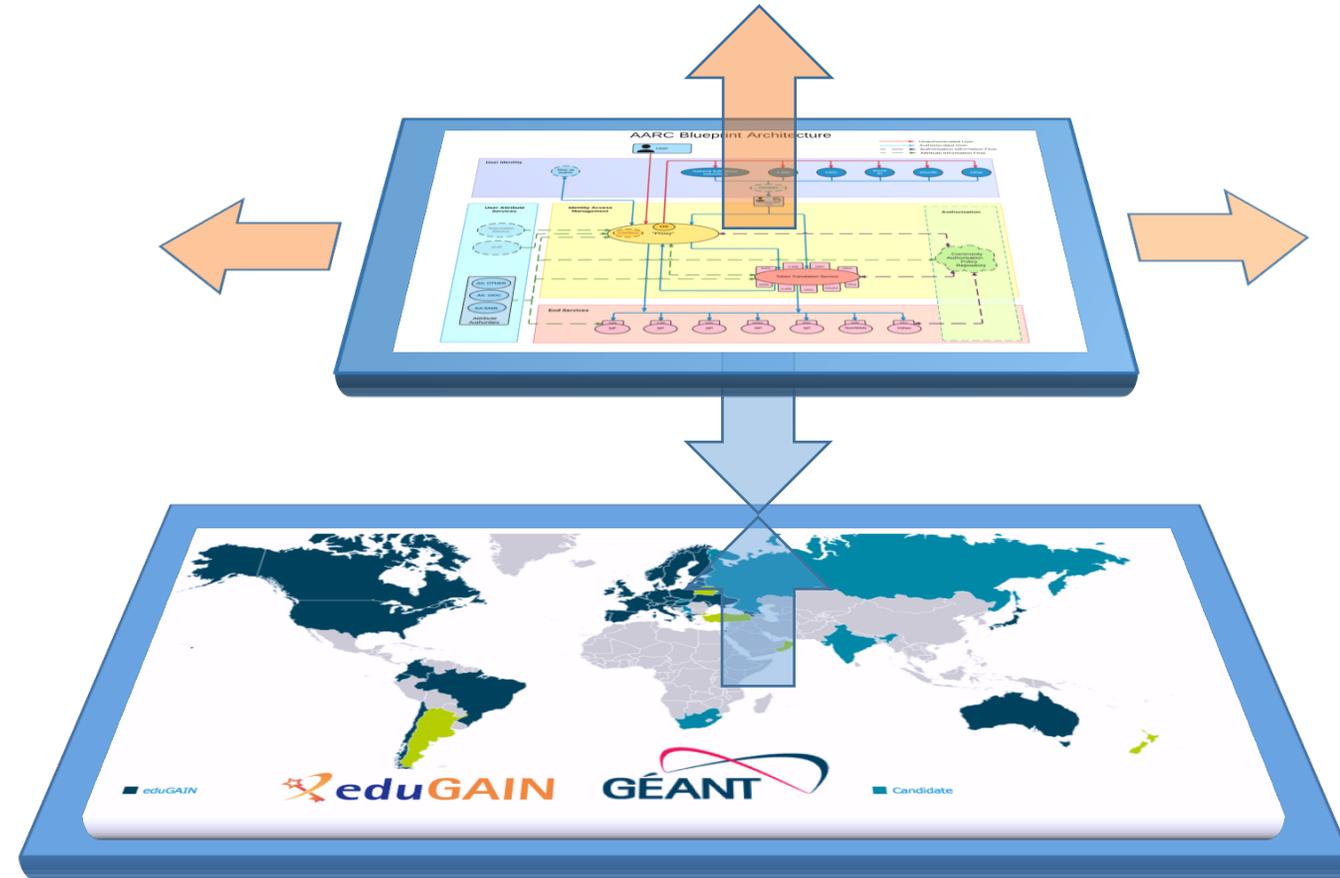
Identity & Access Management for International Research Collaborations

A Blueprint Architecture for authentication and authorization

A set of architectural building blocks on top of eduGAIN

eduGAIN and the Identity Federations

A solid foundation for federated access in Research & Education



AARC Blueprint Architecture

AARC Blueprint Architecture



- Unauthenticated User
- Authenticated User
- Authorisation Information Flow
- Attribute Information Flow

User Community Requirements

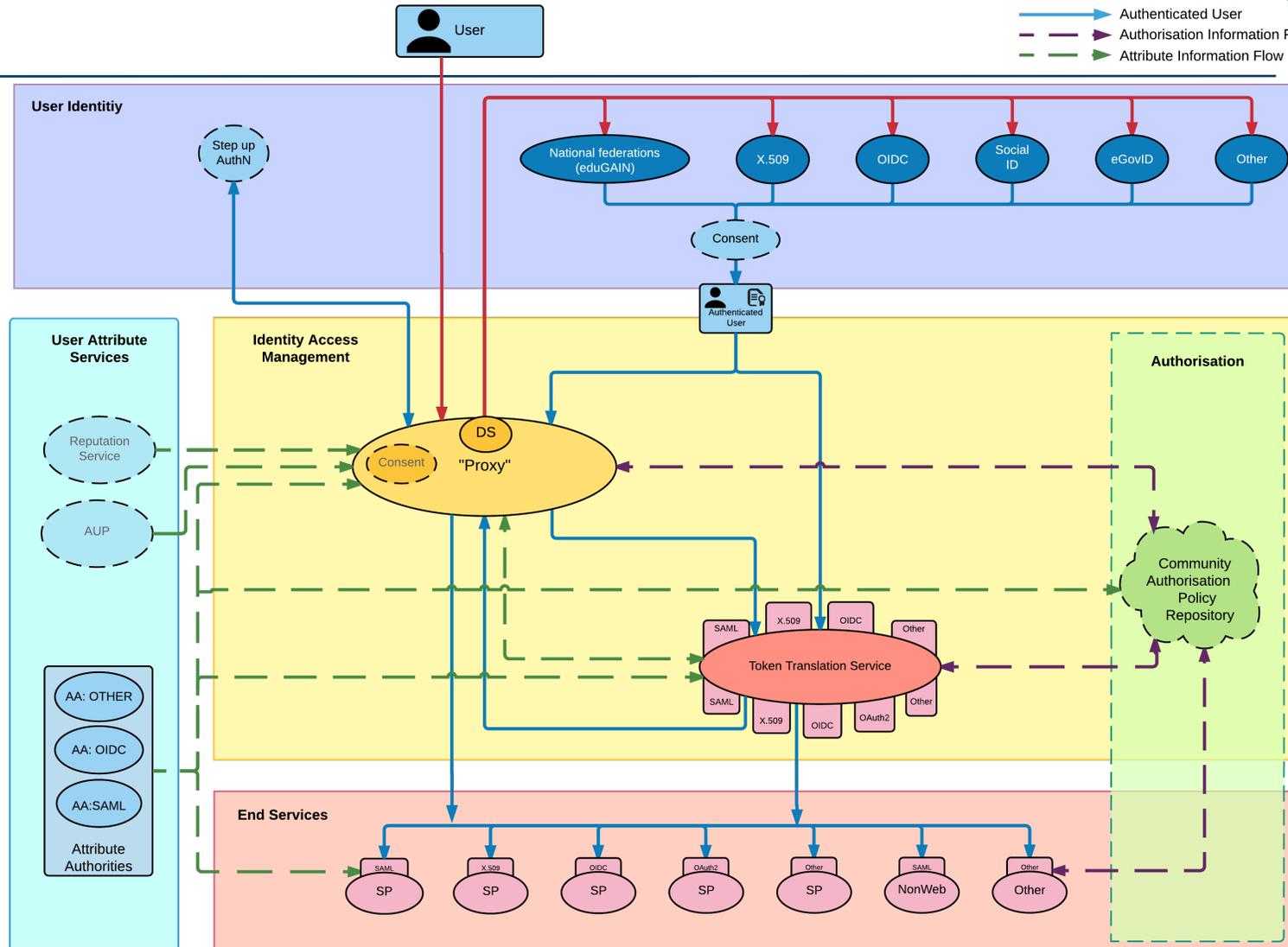


05-10-2015
Deliverable DJRA1.1:
Analysis of user community and service provider requirements

Deliverable DJRA1.1
 Contractual Date: 31-08-2015
 Actual Date: 05-10-2015
 Grant Agreement No.: 653965
 Work Package: JRA1
 Task Item: JRA1.1
 Lead Partner: ESU.eu
 Document Code: DJRA1.1
 Editors: Christos Kanellopoulos, Nicolas Liampotis, Nels van Dijk, Peter Solagna

© GEANT on behalf of the AARC project.
 The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 653965 (AARC).
Abstract
 This document, produced by JRA1 Task 1 "Analysis of user community requirements", identifies the requirements of user communities and service providers building upon the outcomes of previous activities such as the TERENA AAA Study and the FRIB workshop series. The requirements identified for these activities have been updated and enriched with new requirements that have been collected through a survey of user communities as well as a set of targeted interviews. These requirements are analysed here and will be provided as input for upcoming activities in AARC.

<https://goo.gl/kSxENp>

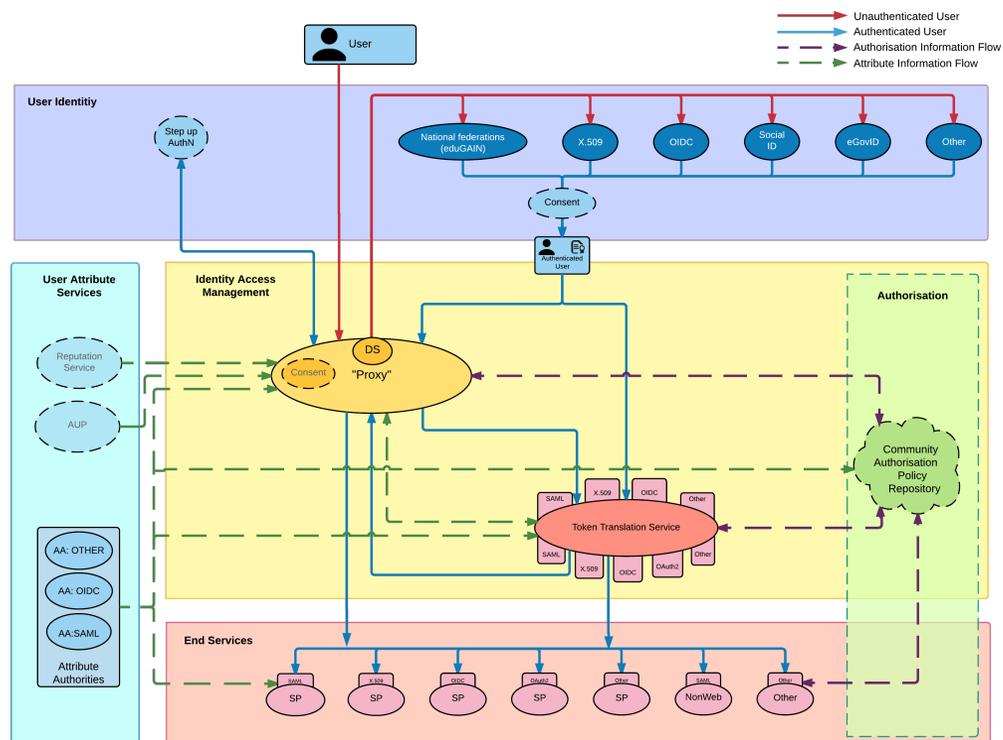


<https://aarc-project.eu/roadmap/blueprint-architecture/>

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

Guidelines and support documents

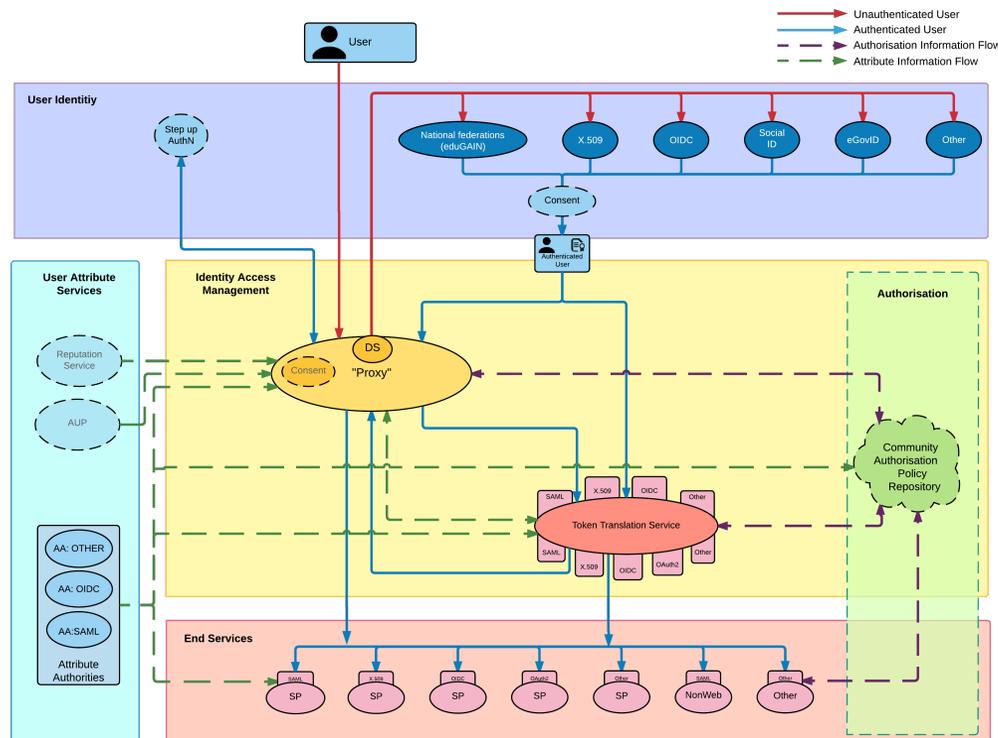
- Best practices for managing authorisation
- Expressing group membership and role information
- Scalable attribute aggregation
- Implementation of token TTS
- Credential delegation
- Non-web access
- Social media IdPs
- Use cases for account linking
- Use cases for LoA elevation via step-up authentication



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

Policy recommendations & frameworks

- Security Incident Response Trust Framework for Federated Identity – Sirtfi
- Scalable Negotiator for a Community Trust Framework in Federated Infrastructures – Snctfi
- Recommendations on Minimal Assurance Level Relevant for Low-risk Research Use Cases
- Differentiated LoA recommendations for policy and practices of identity and attribute providers
- Recommendations and template policies for the processing of personal data by participants in the pan-European AAI



AARC Blueprint Architecture & Requirements



Attribute Release

Attribute Aggregation

User Friendliness

SP Friendliness

Persistent Unique Id

Credential translation

Credential Delegation

User Managed Information

Levels of Assurance

Guest users

Step-up AuthN

Best Practices

Community based AuthZ

Non-web-browser

Social & e-Gov IDs

Incident Response

 05-10-2015
Deliverable DJRA1.1:
Analysis of user community and service provider requirements

Deliverable DJRA1.1
Contractual Date: 31-09-2015
Actual Date: 05-10-2015
Grant Agreement No.: 603660
Work Package: JRA1
Task Item: DJRA1.1
Lead Partner: EGI.eu
Document Code: DJRA1.1
Editors: Christos Kanellopoulos, Nicolas Liampotis, Niels van Dijk, Peter Solagna

© GEANT on behalf of the AARC project.
The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 603660 (AARC).

Abstract
This document, produced by JRA1 Task 1 "Analysis of user community requirements", identifies the requirements of user communities and service providers building upon the outcomes of previous activities such as the TERENA AAA Study and the FRM2 workshop series. The requirements identified by these activities have been updated and enriched with new requirements that the team collected through a survey of user communities as well as a set of targeted interviews. These requirements are analysed here and will be provided as input for upcoming activities in AARC.

Thank you
Any Questions?



<http://aarc-project.eu/>

