Authentication and Authorisation for Research and Collaboration

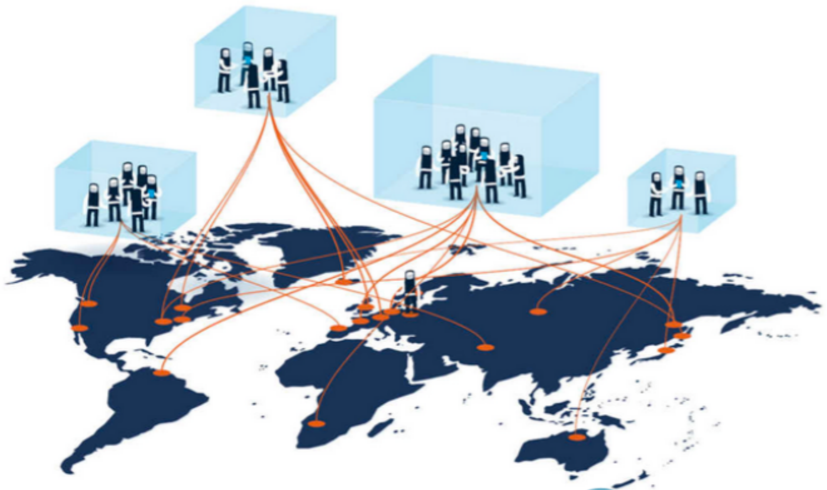
AARC Draft Blueprint Architecture

Christos Kanellopoulos
Architecture (JRA1) WP Leader, GRNET

Internet2 2016 Global Summit
May 15 – 18, Chicago

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
  - She starts googling
- So, there are some solutions available, but…



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**.

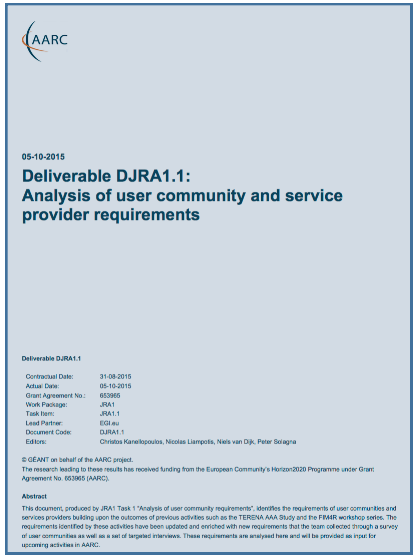
3. Attempt to **retrieve user attributes** from the user's Home Organization. If this is not possible, then an alternate process should exist.

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. Services should not have to deal with the complexity of multiple IdPs/Federations/Attribute Authorities/technologies.

AARC: Analysis of User Communities and e-Infrastructure Providers


AARC

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:	EGI.eu
Document Code:	DJRA1.1
Editors:	Christos Kanellopoulos, Nicolas Liampotis, Niels van Dijk, Peter Solagna

The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 653965 (AARC).

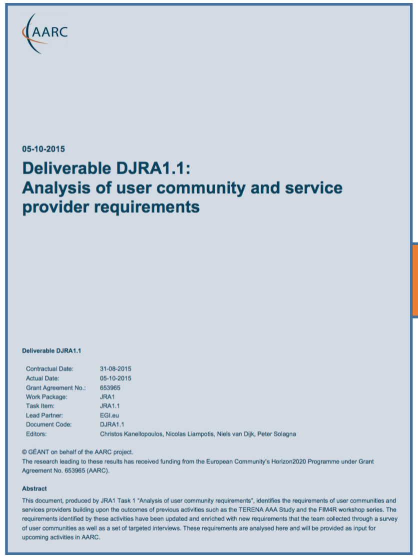
Abstract

This document, produced by JRA1 Task 1 "Analysis of user community requirements", identifies the requirements of user communities and services providers building upon the outcomes of previous activities such as the TERENA AAA Study and the FIM4R 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.

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

The functional Components

User Community Requirements



AARC

05-10-2015

Deliverable DJRA1.1:
Analysis of user community and service provider requirements

Deliverable DJRA1.1

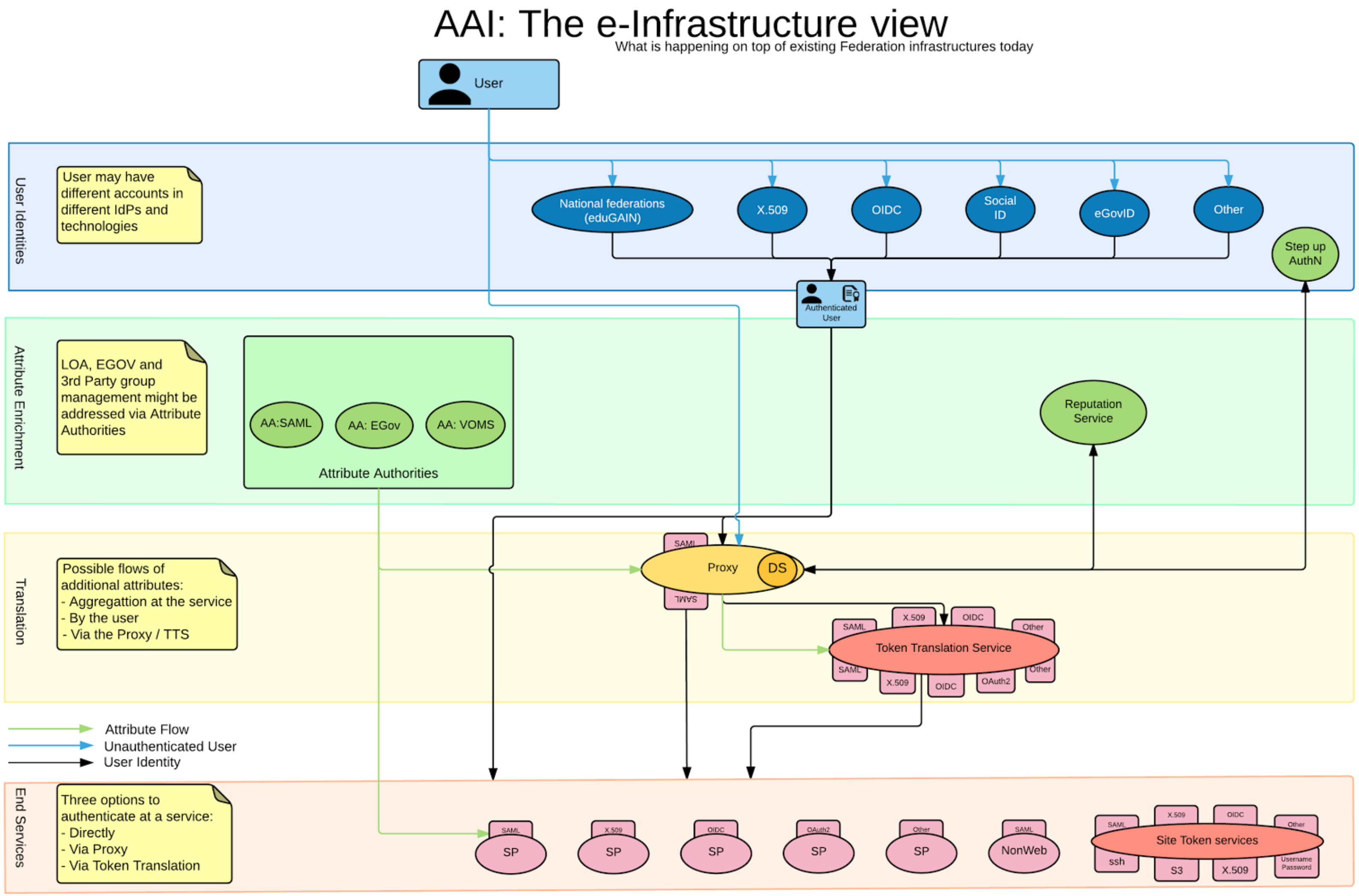
Contractual Date:	31-08-2015
Actual Date:	05-10-2015
Grant Agreement No.:	653965
Work Package:	JRA1
Task Item:	JRA1.1
Lead Partner:	EGI.eu
Document Code:	DJRA1.1
Editors:	Christos Kanellopoulos, Nicolas Liampotis, Niels van Dijk, Peter Solagna

© GÉANT 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 services providers building upon the outcomes of previous activities such as the TERENA AAA Study and the FIM4R 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.

https://goo.gl/kSxENp



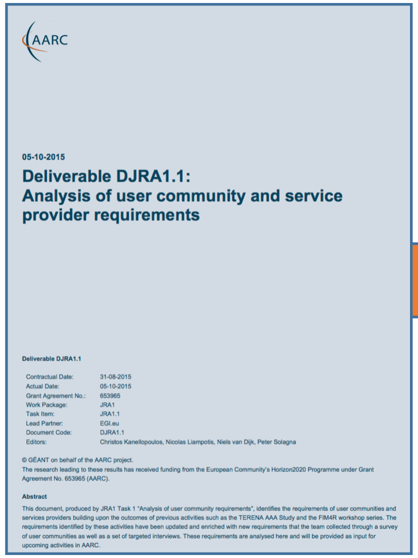
aarc-project.eu

Why the proxy model?

- All internal Services can have **one statically configured IdP**
- **No need to run an IdP Discovery Service** on each Service
- Connected SPs get **consistent/harmonised user identifiers and accompanying attribute sets** from one or more AAs that can be interpreted in a uniform way for authZ purposes
- External IdPs only deal with a **single SP** proxy

The Functional Components and available AAI tools

Analysis of
User Communities



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:	EGI.eu
Document Code:	DJRA1.1
Editors:	Christos Kanellopoulos, Nicolas Liampotis, Niels van Dijk, Peter Solagna

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 services providers building upon the outcomes of previous activities such as the TERENA AAA Study and the FIM4R 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.

And Infrastructure
Providers

- IdPs
- Attribute Authorities
- Proxies
- Token Translation
- Service Provider

Available
AAI Components

31-12-2015

Milestone MJRA1.1: Existing AAI and available technologies for federated access.

Milestone MJRA1.1

Contractual Date:	01-01-2016
Actual Date:	31-12-2015
Grant Agreement No.:	653965
Work Package:	JRA1
Task Item:	1
Lead Partner:	EGI.eu
Document Code:	MJRA1.1
Authors:	P. Solagna (EGI.eu), Christos Kannelopoulos (GRNET), N. Liampotis (GRNET), M. Hardt (KIT), M. Salle (Nikhef), S. Paetow (Jisc), M. Malavolti (GARR), N. Van Dijk (SURFnet), J Jensen (STFC), I. Liabotis (GRNET), M. Jankowski (PSNC), S. Memon (Juelich), M. Prochazka (CESNET), B. Oshrin (SURFnet), B. Monticini (GARR), H. Short (CERN), U. Stevanovich (KIT)

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 summarises the technologies and solutions available to implement AAI, focusing on the software most common in the research and education (R&E) environment, which features are more likely to fulfil the use cases of the R&E communities.

aarc-project.eu

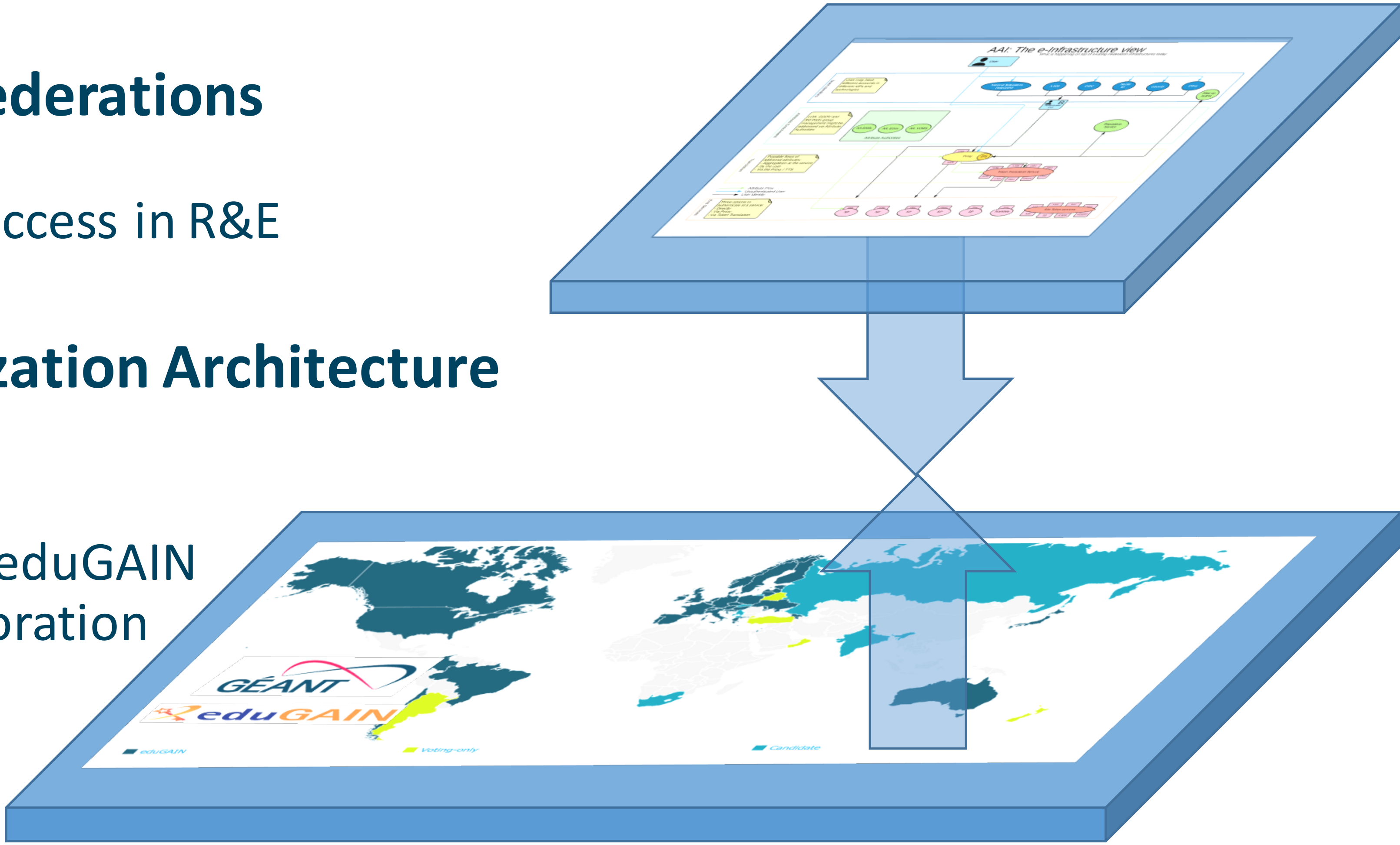
eduGAIN & AARC

eduGAIN and the Identity Federations

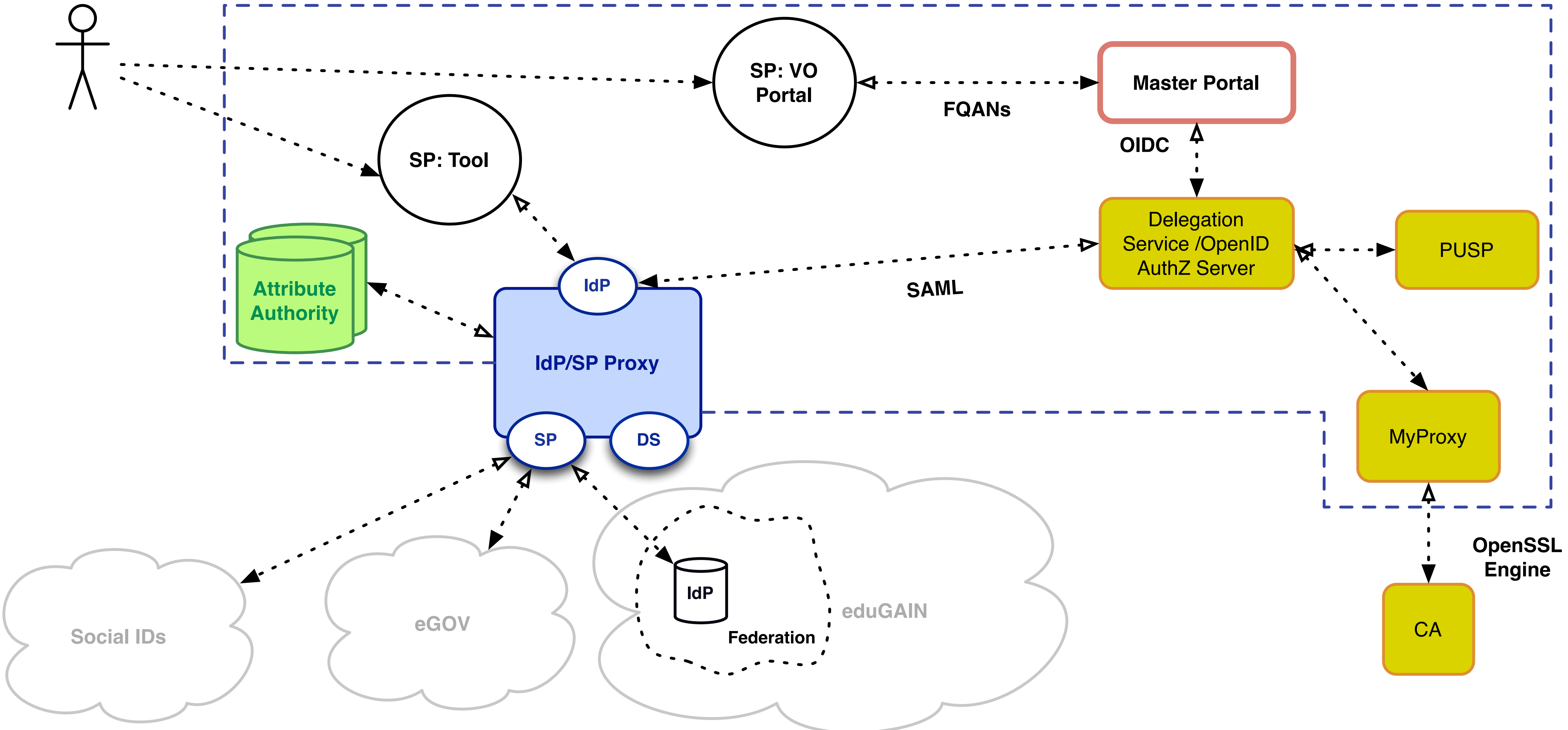
A solid foundation for federated access in R&E

Authentication and Authorization Architecture for Research Collaboration

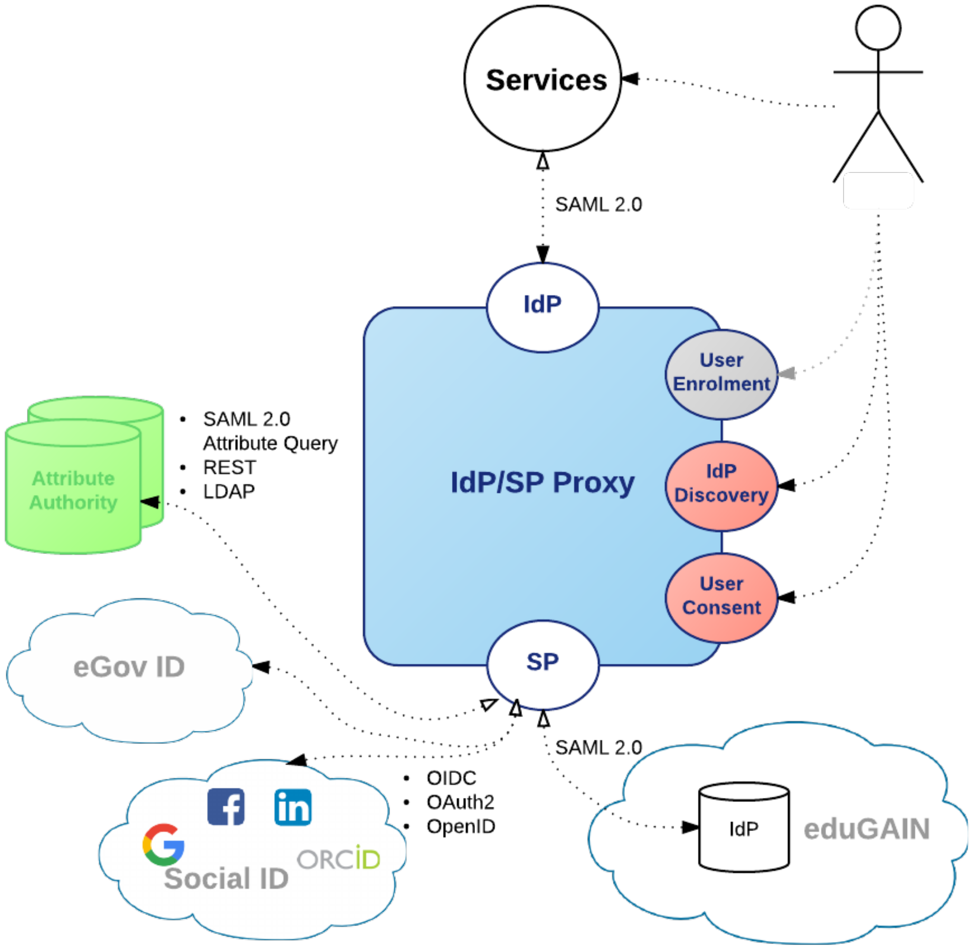
A set of building blocks on top of eduGAIN for International Research Collaboration



A real life implementation...



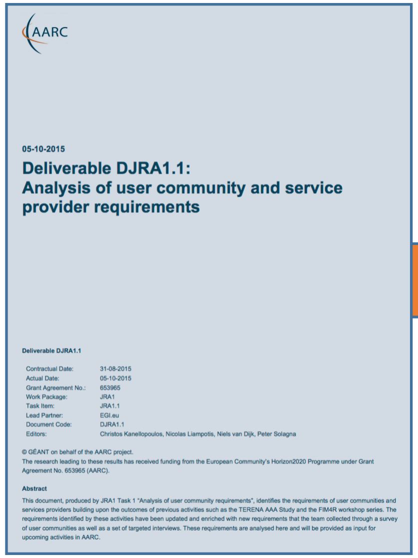
A real life implementation…



- IdP Discovery
- User Enrolment
- User Consent
- Support for LoA
- Attribute Aggregation
  - SAML2.0 Attribute Query, REST, LDAP
- Attribute mapping
- Support for OIDC/OAuth2
  - Google, Facebook, LinkedIn, ORCID
- Support for eGov IDs

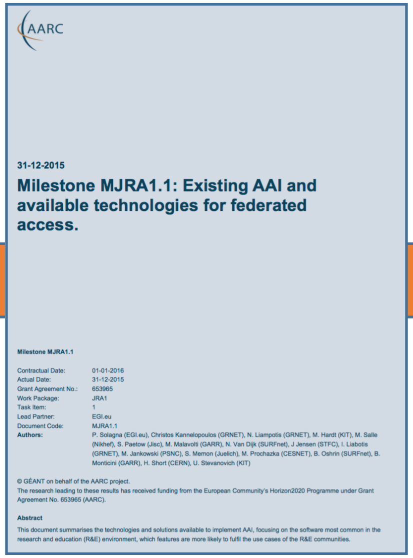
Pilots

Requirements
User Community



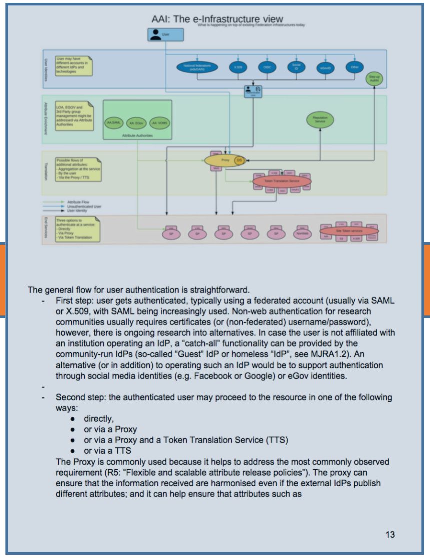
https://goo.gl/kSxENp

Overview Available
AAI Components



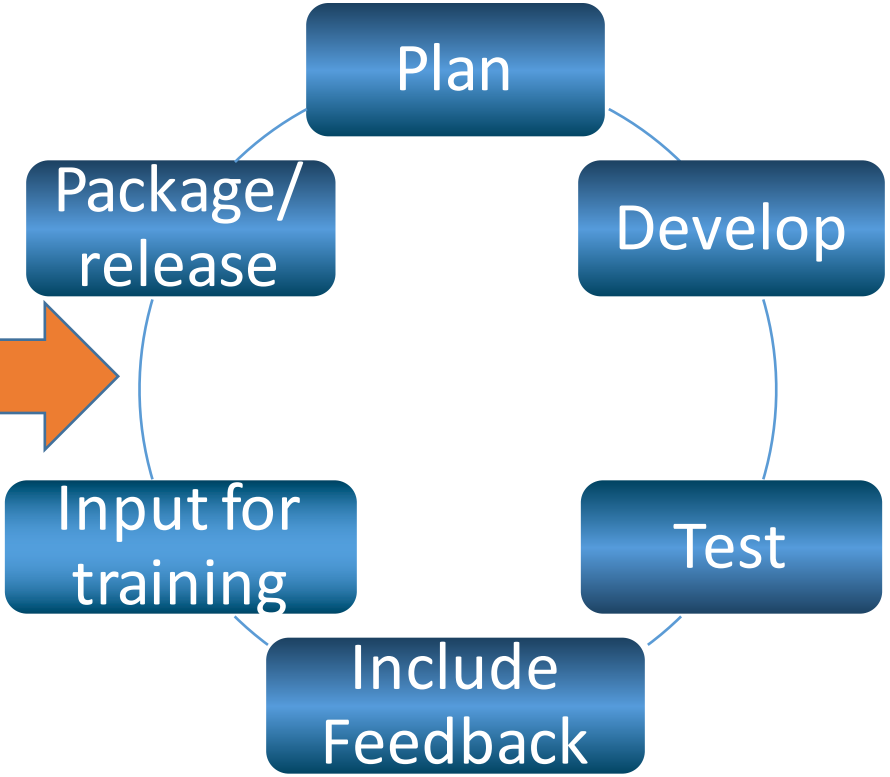
https://goo.gl/NzQA2U

Draft Blue-Print
Architecture



https://goo.gl/7dZZF4

Pilots
With Communities



aarc-project.eu

Thank you

Any Questions?

Christos Kanellopoulos
skanct@admin.grnet.gr

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. 653965 (AARC).