Authentication and Authorisation for Research and Collaboration

AARC Blueprint Architecture for interoperable AAIs

Christos Kanellopoulos (GRNET)

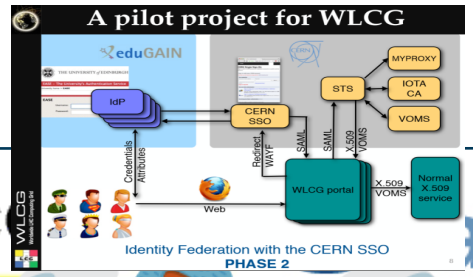
Digital Infrastructures for Research 2016

28 September, 2016

Krakow

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 UK Access Management Federation
FOR EDUCATION AND RESEARCH

AUSTRALIAN ACCESS FEDERATION

confia

SWITCHaai

grnet

ID cz

SIFULAN

CILogon Service

Belnet
R&E Federation

WAYF
Where are you from

eduGAIN
Gaining Access to Education

SURF CONEXT

RCTSaai
REDE CIÊNCIA, TECNOLOGIA E SOCIEDADE

Carsi

RENATER
CONNECTEUR DE SAVOIRS

Colfire
Colombian Federation of Identity for Research and Education renata

GakuNin

TAAT

InCommon

Tuakiri
NEW ZEALAND ACCESS FEDERATION

@EduHr

arnes

eduID

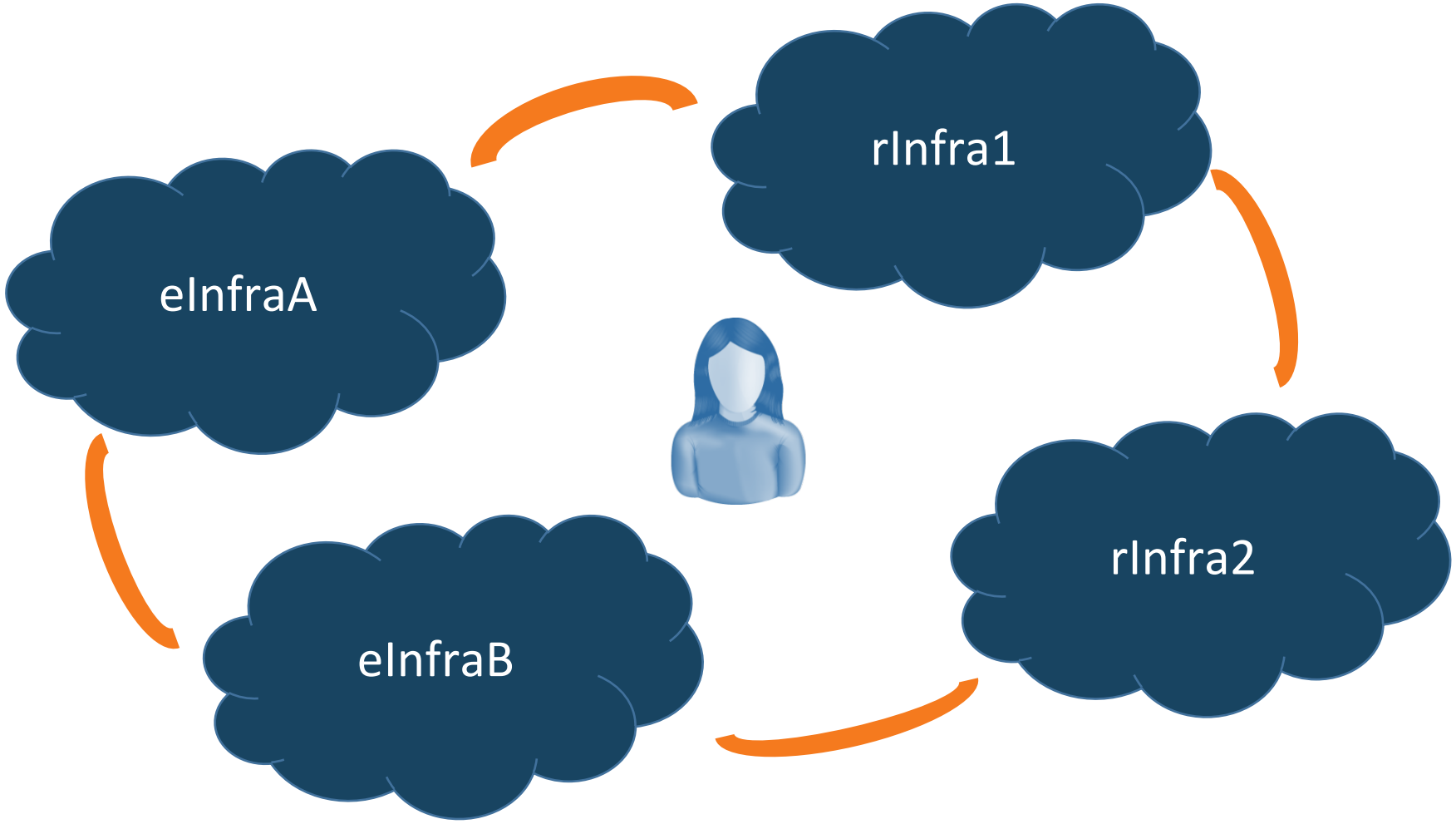
SWAMID

AARC Facts

Authentication and Authorisation for Research and Collaboration

- Two-year EC-funded project
- 20 partners
  - NRENs, e-Infrastructure providers and Libraries as equal partners
- About 3M euro budget
- Starting date 1st May, 2015
- https://aarc-project.eu/

AARC's Role - Connecting the islands



AARC Vision and Outputs

Avoid a future in which new research collaborations develop independent AAIs

Impact

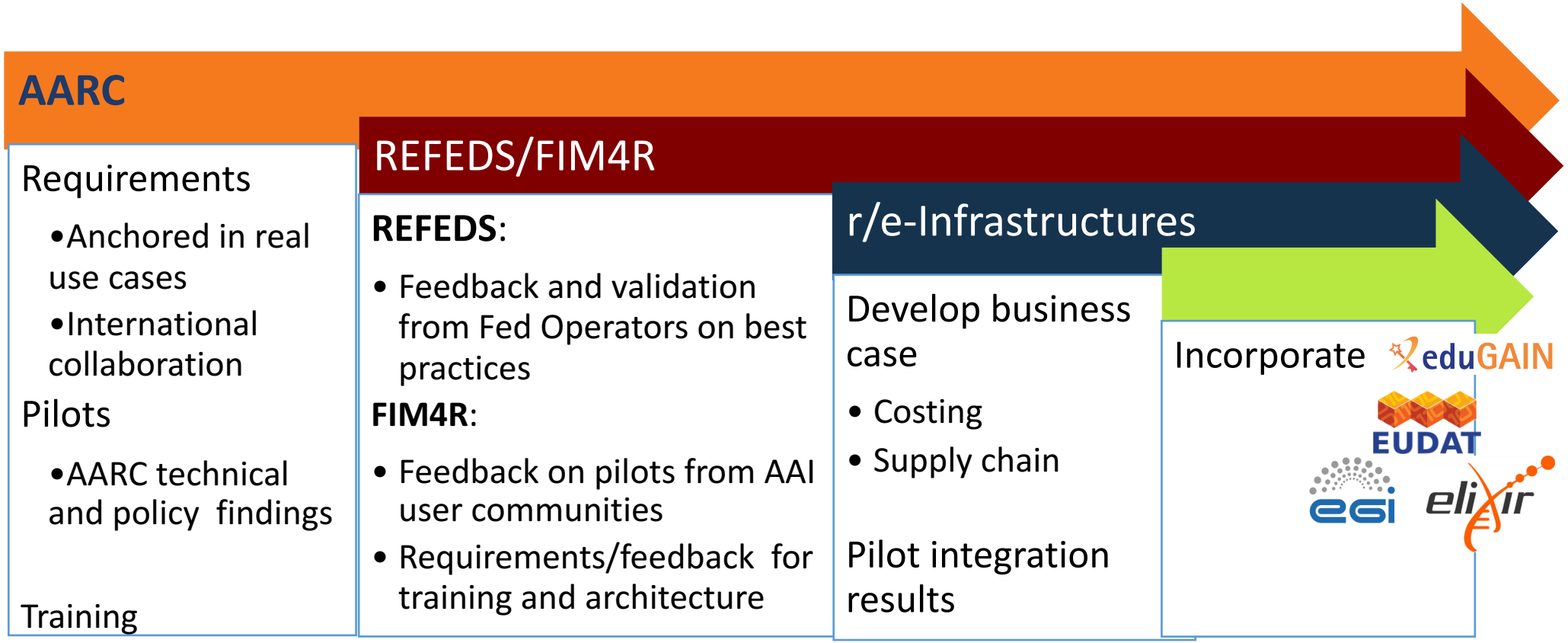
- Bring federated access and eScience close to each other
- Create a cross-e-infrastructure ‘network’ for identities
- Reduce duplication of efforts in the service delivery

Outputs

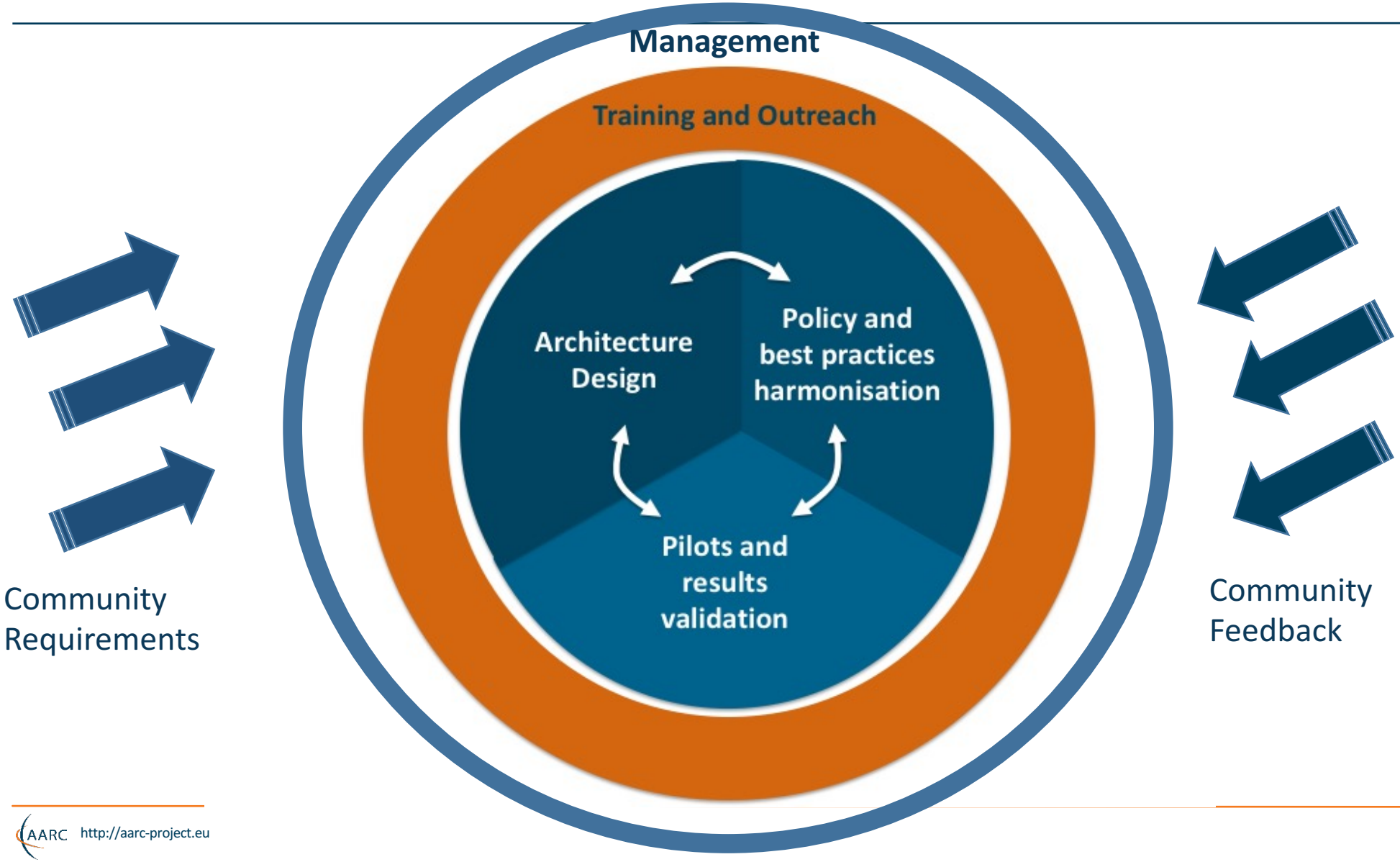
- Design of integrated AAI built on federated access
- Harmonised policies to easy cross-discipline collaboration
- Pilot selected use-cases
- Offer a diversified training package

AARC and T&I ecosystem

- GN4 project, REFEDS, FIM4R, RDA, and various AAI work within other projects
- Liaisons with international collaborations



AARC Methodology



Starting Point

ID FEDs

- Mainly nationally focused
- Provide webSSO (SAML) to access a number of services
- Support fine-grained AuthZ

e-Researcher

- Typical inter-fed use-cases
- Provide SSO (X.509) for e-Research services
- Requirement for stronger AuthN (LoA)

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

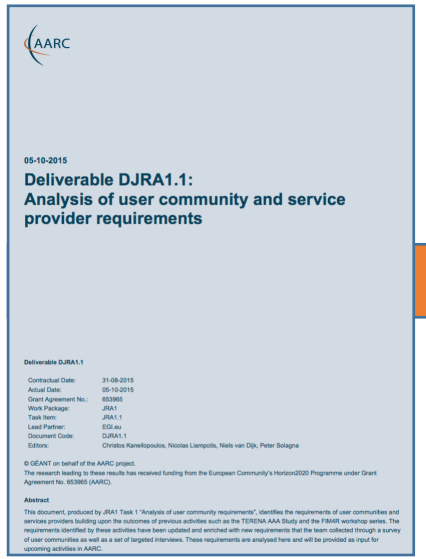
6. Services should not have to deal with the complexity of multiple IdPs/Federations/Attribute Authorities/technologies.

Identified Requirements

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

The Functional Components and available AAI tools

Analysis of
User Communities



And Infrastructure
Providers

IdPs

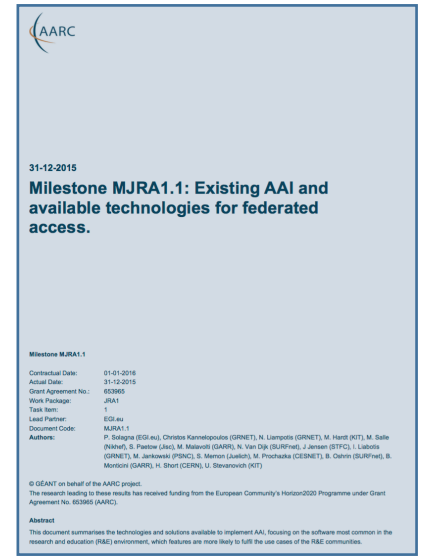
Attribute
Authorities

Proxies

Token Translation

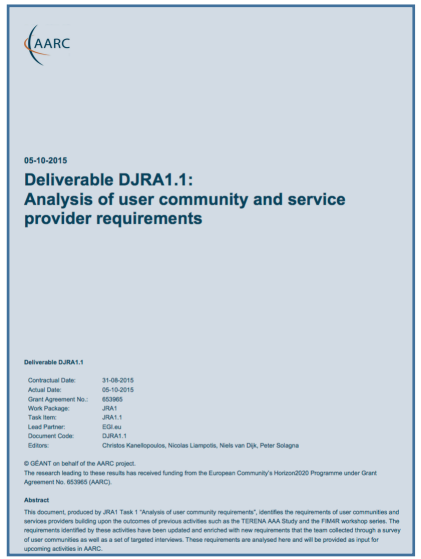
Service Provider

Available
AAI Components



aarc-project.eu

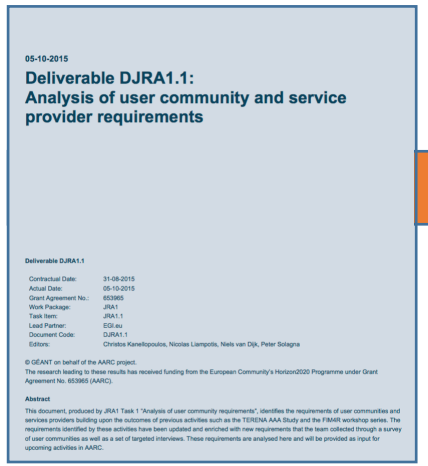
AARC: Analysis of User Communities and e-Infrastructure Providers



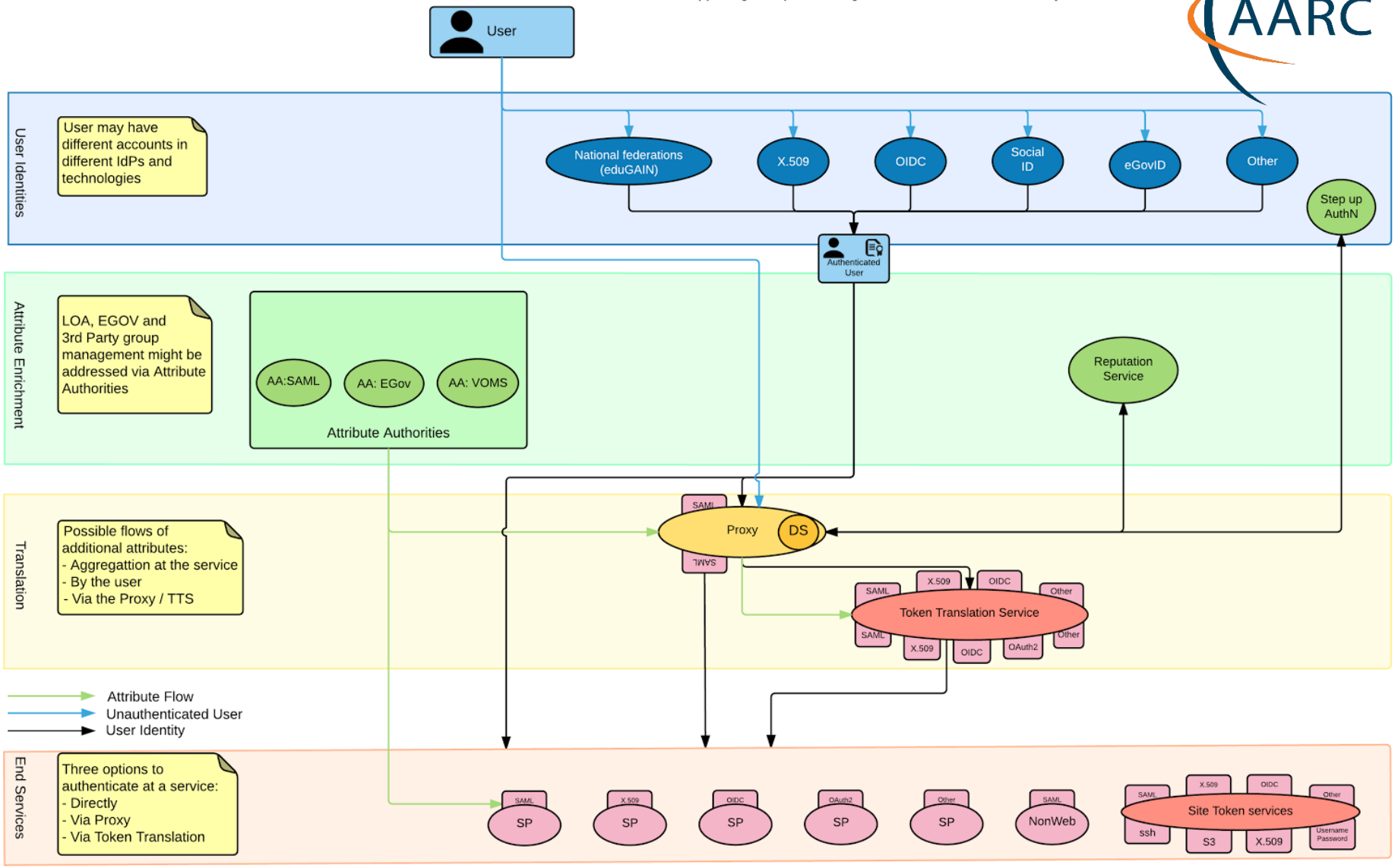
Attribute Release	Attribute Aggregation	User Friendliness	SP Friendliness
Credential translation	Persistent Unique Id	User Managed Information	Credential Delegation
Levels of Assurance	Guest users	Step-up AuthN	Best Practices
Community based AuthZ	Non-web-browser	Social & e-Gov IDs	Incident Response

AARC Blueprint Architecture (1st Draft)

User Community Requirements



https://goo.gl/kSxENp



https://wiki.geant.org/display/AARC/AARC+Architecture

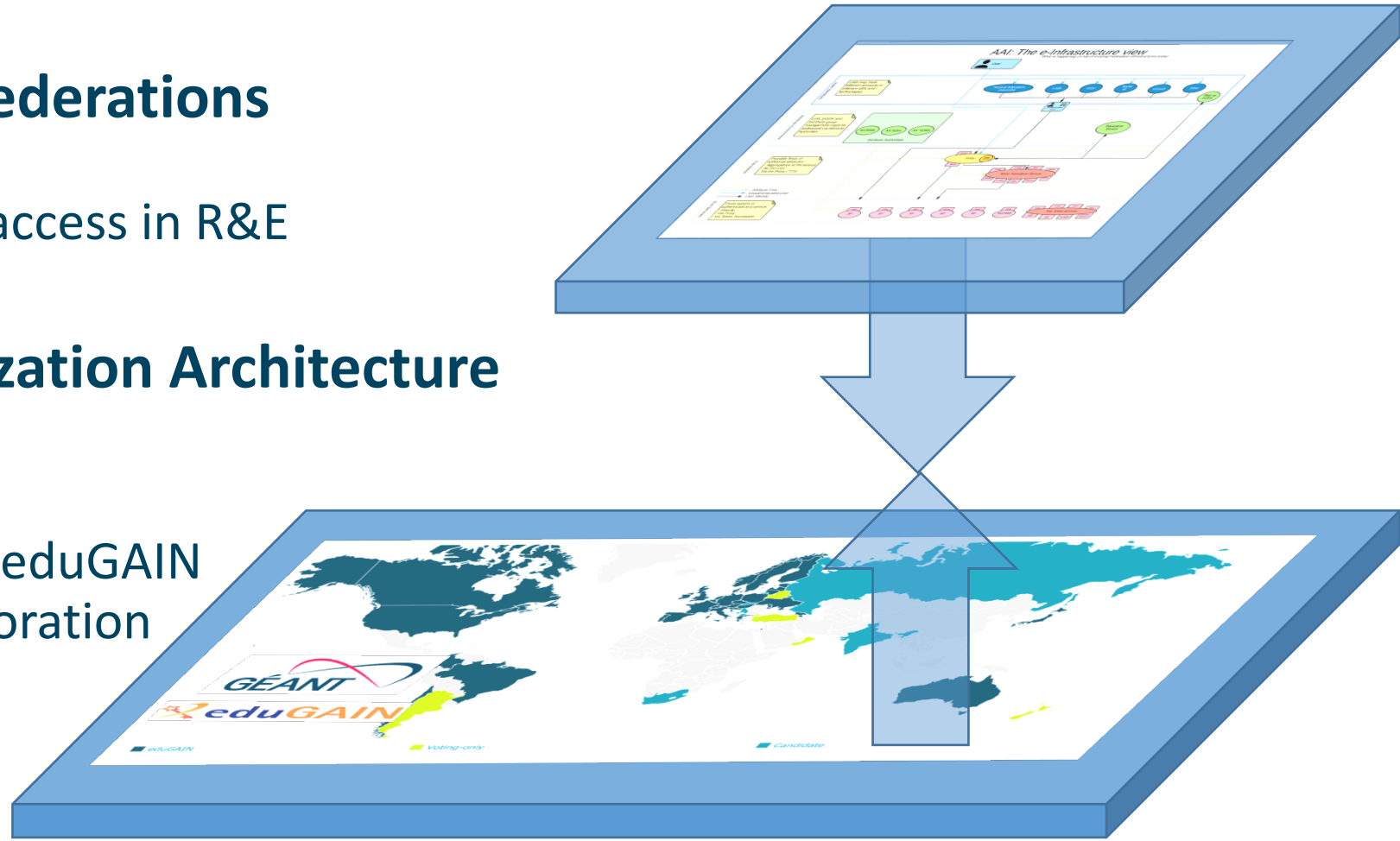
AARC Blueprint Architecture & eduGAIN

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



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
- But it comes with each own **new challenges**

Policies & Sustainability models

- **Security Incident Response Trust Framework for Federated Identity**
  https://refeds.org/sirtfi

- **Minimal Assurance Level for low-risk research use cases**
  https://wiki.geant.org/display/AARC/LoA+-+Level+of+Assurance

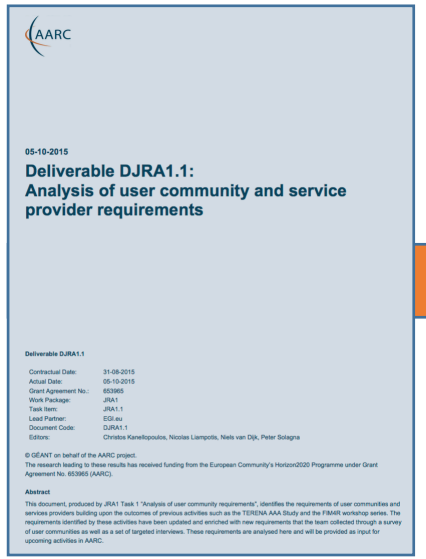
- **Policy and sustainability models for a pan-European Token Translation Service**
  https://www.rcauth.eu/

- **Sustainability models for ”Guest IdPs”**
  https://wiki.geant.org/display/AARC/Sustainability+models+for+Guest+IdPs

- **Requirements for Accounting and Data Protection**
  https://wiki.geant.org/display/AARC/Accounting+and+Data+Protection

Pilots

Requirements User Community



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

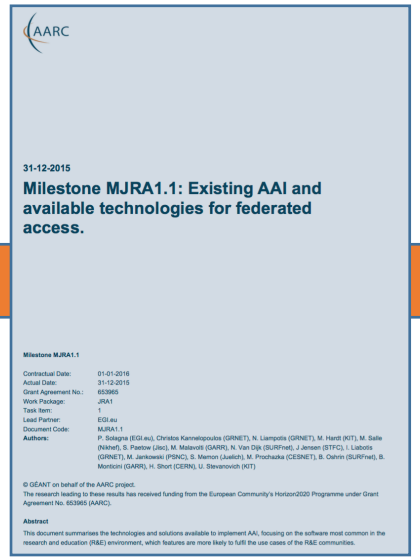
© GÉANT on behalf of the AARC project.
The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 653965 (AARC).

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

Overview 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 Kanellopoulos (GRNET), N. Liampotis (GRNET), M. Hardt (KIT), M. Salle (Nikhef), B. Pawlow (Uiio), M. Malawski (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)

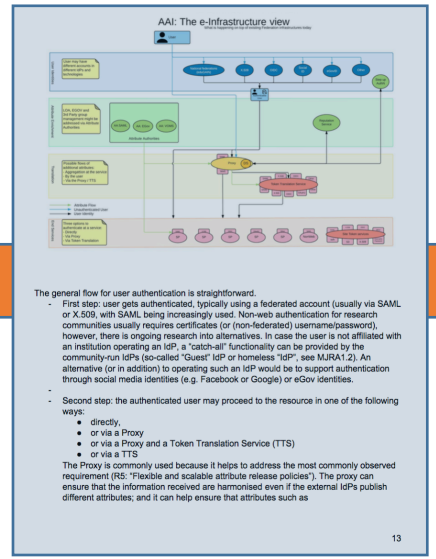
© GÉANT on behalf of the AARC project.
The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 653965 (AARC).

Abstract

This document 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.

https://goo.gl/NzQA2U

Draft Blue-Print Architecture



AAI: The e-Infrastructure view

The general flow for user authentication is straightforward.

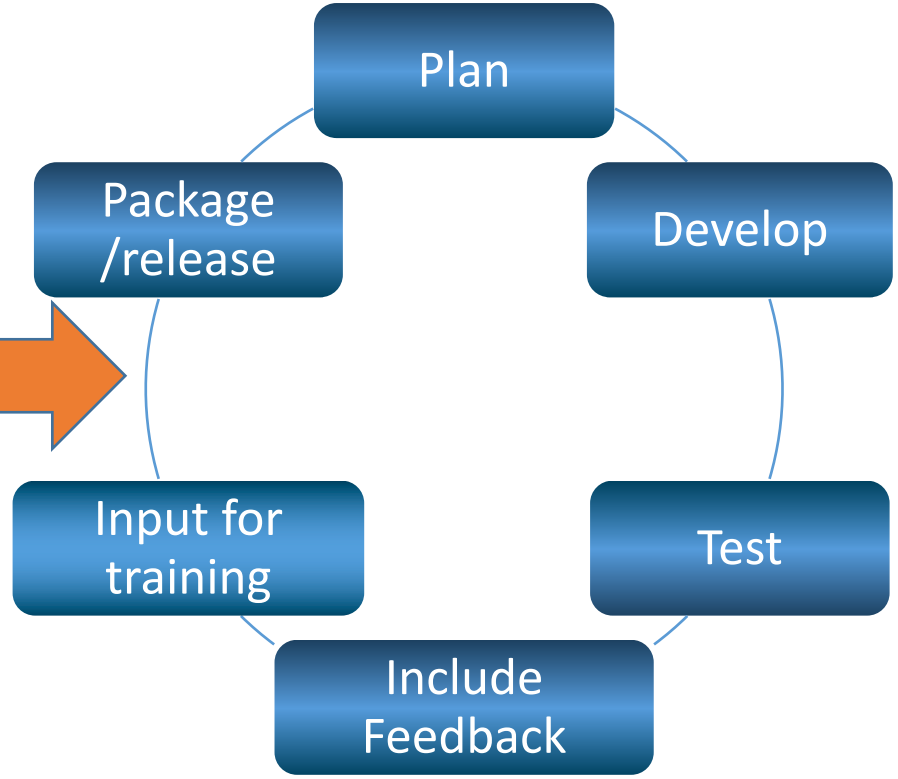
- First step: user gets authenticated, typically using a federated account (usually via SAML or X.509, with SAML being increasingly used. Non-web authentication for research communities usually requires certificates (or (non-federated) username/password), however, there is ongoing research into alternatives. In case the user is not affiliated with an institution operating an IdP, a "catch-all" functionality can be provided by the community-run IdPs (so-called "Guest" IdP or homeless "IdP", see MJRA1.2). An alternative (or in addition) to operating such an IdP would be to support authentication through social media identities (e.g. Facebook or Google) or eGov identities.
-
- Second step: the authenticated user may proceed to the resource in one of the following ways:
  - directly,
  - or via a Proxy
  - or via a Proxy and a Token Translation Service (TTS)
  - or via a TTS

The Proxy is commonly used because it helps to address the most commonly observed requirement (R5: "Flexible and scalable attribute release policies"). The proxy can ensure that the information received are harmonised even if the external IdPs publish different attributes; and it can help ensure that attributes such as

13

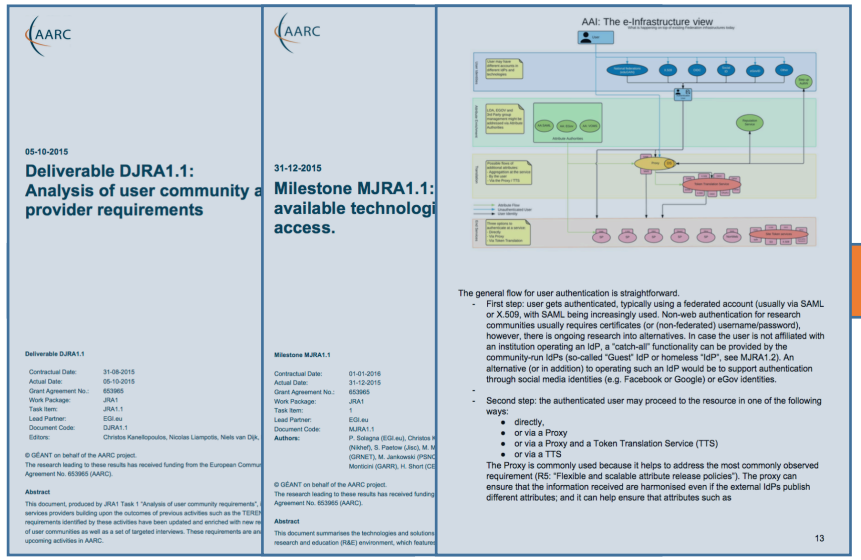
https://goo.gl/7dZZF4

Pilots With Communities



aarc-project.eu

Pilots



https://goo.gl/kSxENp

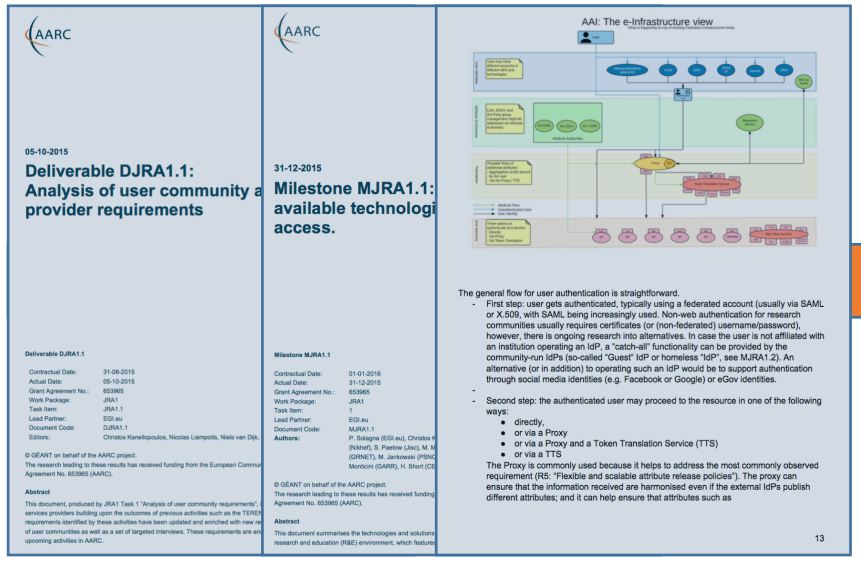
https://goo.gl/NzQA2U

https://goo.gl/7dZZF4

IdPs	Library, hybrid AuthN Library, IdP-SP proxy approach
Attribute Authorities	Perun and COmanage AAs for BBMRI & EGI OpenConext attribute aggregation
Proxy	
Token Translation	TTS with CI-logon and VO portal for Elixir
Service Provider	ORCID SP, LoA Elevation, Reference implementation of the BPA…

https://wiki.geant.org/display/AARC/AARC+Pilots

First e-Infrastructure implementations



https://goo.gl/kSxENp

https://goo.gl/NzQA2U

https://goo.gl/7dZZF4

- EGI CheckIn Service

  https://wiki.egi.eu/wiki/AAI

- ELIXIR AAI

  https://www.elixir-europe.org/services/compute/aai

- EUDAT B2ACCESS

  https://www.eudat.eu/services/b2access

- GÉANT eduTEAMS

  https://www.eduteams.org

Work for the next year

- Policies and best practices for proxy operators
- Framework recommendations for RIs for coherent policy sets
- Guideline documents
  (e.g. group Membership, non-web access, authorizaton)
- Feasibility study for the use eGOV/eIDAS e-IDs
- Pilots, pilots, pilots…
- Focused trainings

Thank you

Any Questions?

skanct@admin.grnet.gr

http://aarc-project.eu/

© GEANT on behalf of the AARC project.
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).