



Authentication and Authorisation for Research and Collaboration

## **AARC Pilots**

Paul van Dijk - SURFnet



## Pilots on the integrated R&E AAI



## The pilot approach in AARC

## Why we run pilots?

We tested existing AAI components to assess to what extent they meet:

- Functional requirements
- Technical (AAI integration) requirements
- Required “readiness” levels

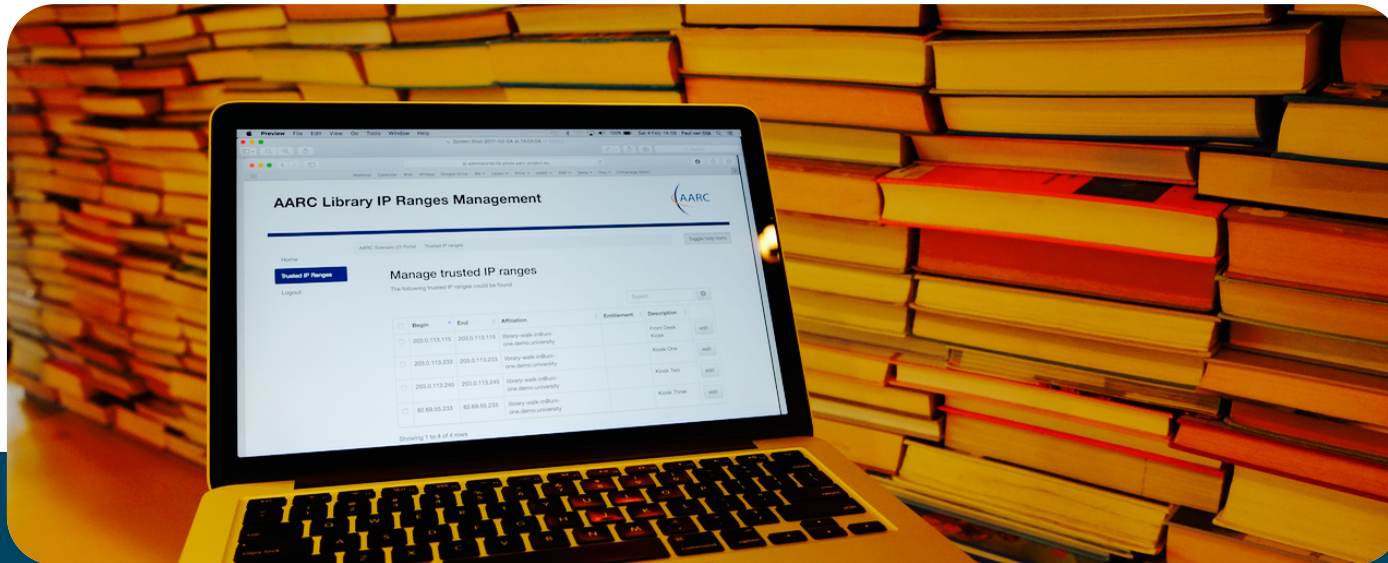


- Running pilots is inevitable to get a good sense of these aspects
- While running pilots, new clues and ideas arise
- Where possible improve components and ease deployability
- Improve visibility of useful AAI components for R&E

## Establish a common test-bed infrastructure

- A staging area for piloted services
- Technical platform delivered by keanos
- >20 VMs instantiated
- Using Ansible scripts for deployment
- SimpleSAMLphp DIY IdP available
- Online support by SURF NET staff





**Expand the reach of federated access (Libraries, external IdPs)**

## Library proxy pilot(s)

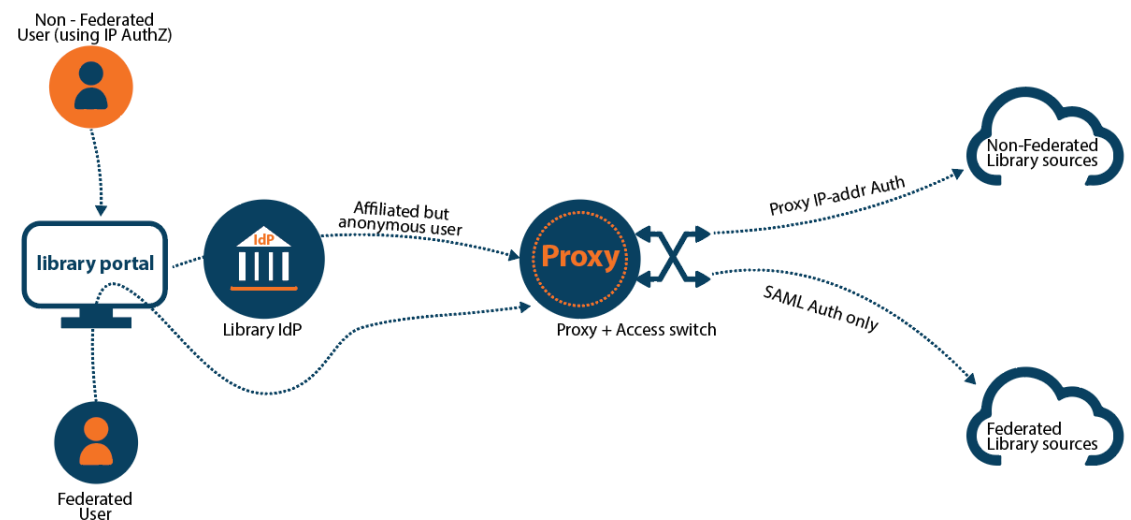
### Purpose

- Dealing with “walk by users” → Setting attributes based on IP-address
- Dealing with providers supporting IP-address access only → SP Proxy translating SAML to IP if needed

### Services/Components used

- Shibb add-on to filter on IP-address
- EZproxy with access switch mode
- Several library resources

[wiki.geant.org/x/a4qSAw](http://wiki.geant.org/x/a4qSAw)



# Social ID pilot

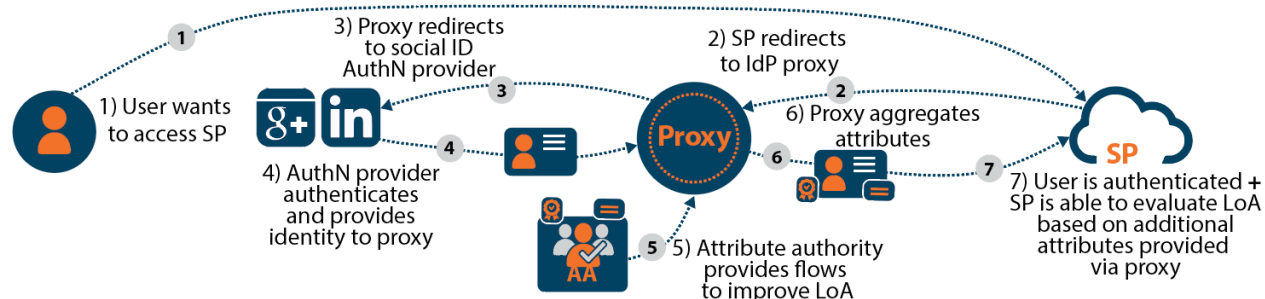
## Purpose

- Demonstrate possible mechanisms to include users with Social Identities
- Explore clues to enhance LoA of users

## Services/Components used

- Social ID providers (Google, ORCID, LI)
- COmanage AA
- SimpleSAMLphp proxy
- OpenStack Keystone SP
- Tested with EGI and AARC pilot community

[wiki.geant.org/x/ZlqSAw](http://wiki.geant.org/x/ZlqSAw)



BPA building blocks

Administrative domains





## Testing technical and policy components



# SAML – ORCID account linking pilot

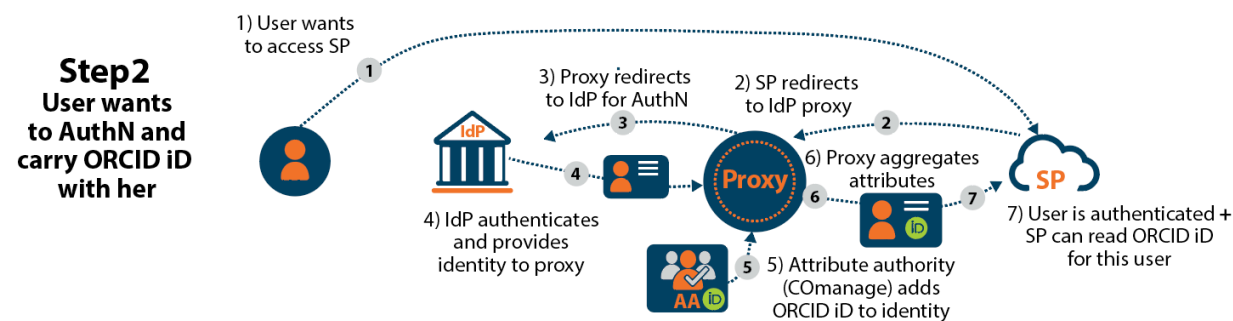
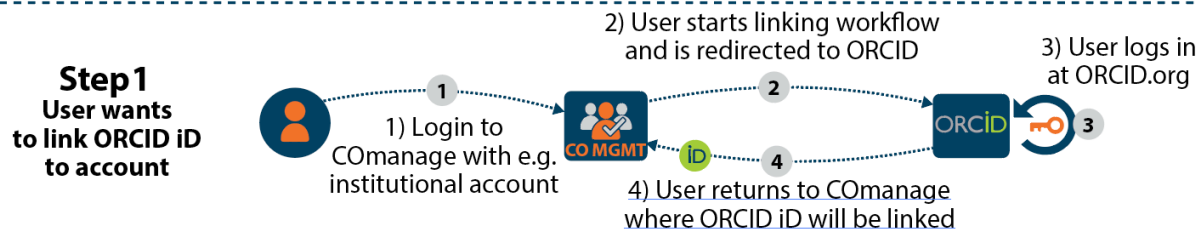
## Purpose

- ORCID provides persistent researcher centric IDs which are useful for use in collaboration services → include this ID in the assertion

## Services/Components used

- ORCID API - persistentID source
- COmanage – link ID to account
- Proxy – attribute aggregation
- Tested with the AARC community

[wiki.geant.org/x/WAH5Aw](http://wiki.geant.org/x/WAH5Aw)



BPA building blocks



Administrative domains

# Attribute management & aggregation pilots



## Purpose

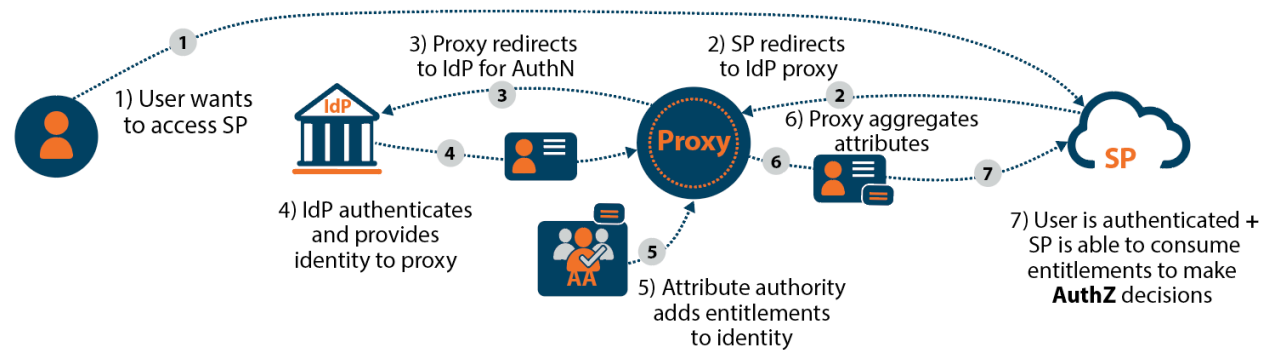
- Show how attributes from multiple AAs can be used for AuthZ in a fed. environment
- Delegate AuthZ decisions
- Minimize impact for SPs

## Services/Components used

- COmanage/PERUN AAs
- SimpleSAMLphp proxy
- OpenStack Horizon SP/BBMRI SPs

**EGI:** [wiki.geant.org/x/LAH5Aw](http://wiki.geant.org/x/LAH5Aw)

**BBMRI:** [wiki.geant.org/x/HgD5Aw](http://wiki.geant.org/x/HgD5Aw)



BPA building blocks

IdentityProvider

AttributeAuthority  
COmanage

Proxy  
simpleSAMLphp

TokenTranslation

ServiceProvider  
Just a service provider

Administrative domains

eduGAIN IdPs

E-infrastructure/Collab. Organizations  
ESI

eduGAIN SPs

# TTS: RCauth



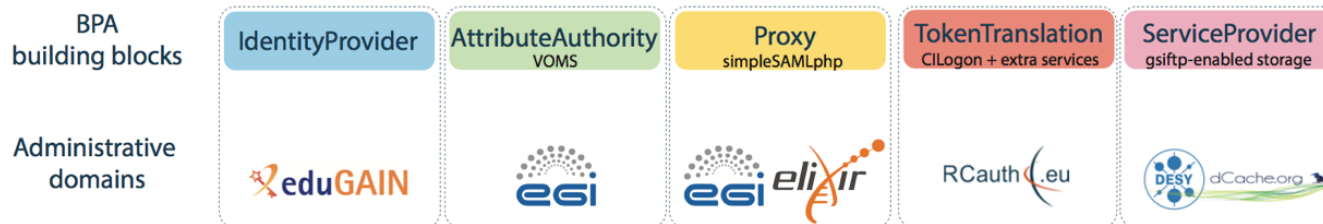
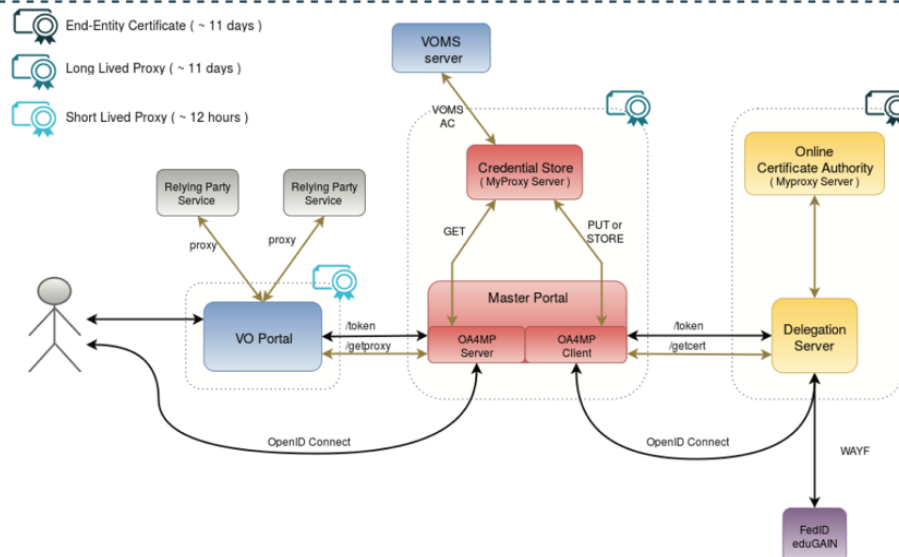
## Purpose

- Enable access to certificate based services for users with an institute account, generating certs on the fly
- Bridging eduGAIN & IGTF

## Services/Components used

- CILogon, adapted as RCAuth
- Several master portals
- Several science gateways
- SimpleSAMLphp
- VOMS Attribute Authority
- Tested with AARC community +...

[wiki.geant.org/x/yADaAw](http://wiki.geant.org/x/yADaAw)



# Bridging IGTF to eduGAIN



## Purpose

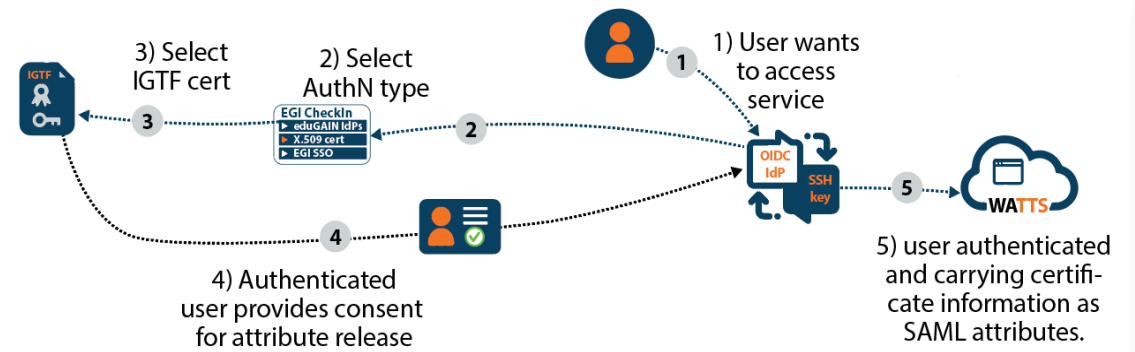
- Demonstrating how researchers can use X.509 certs to access eduGAIN services with substantial or higher LoA
- Not forcing them to use organization accounts



## Services/Components used

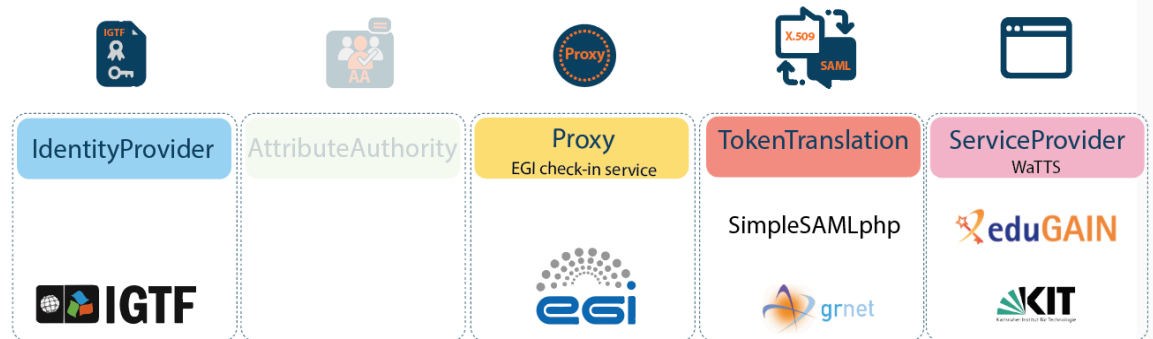
- SimpleSAMLphp add-on
- WaTTS one-stop-TTS-shop
- ~Okeanos infrastructure

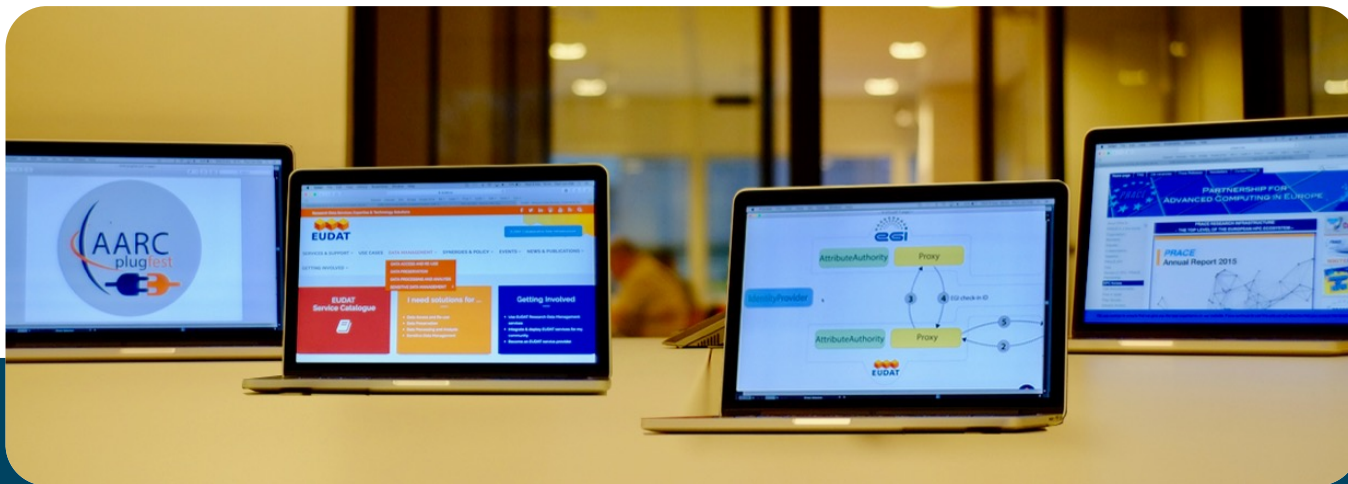
[wiki.geant.org/x/JoEKB](http://wiki.geant.org/x/JoEKB)



BPA building blocks

Administrative domains



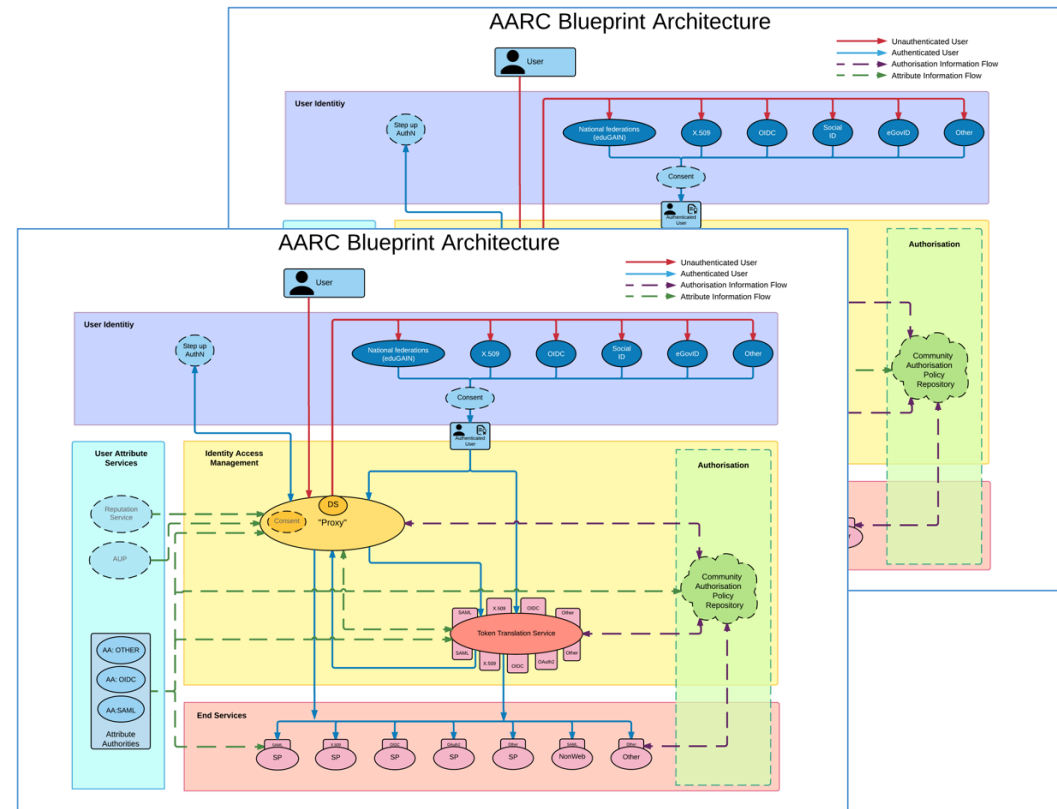


## Cross infrastructure pilots

# Cross-infrastructure pilots



AARC  
blueprint  
architecture



# Cross-infrastructure pilots, EUDAT - EGI

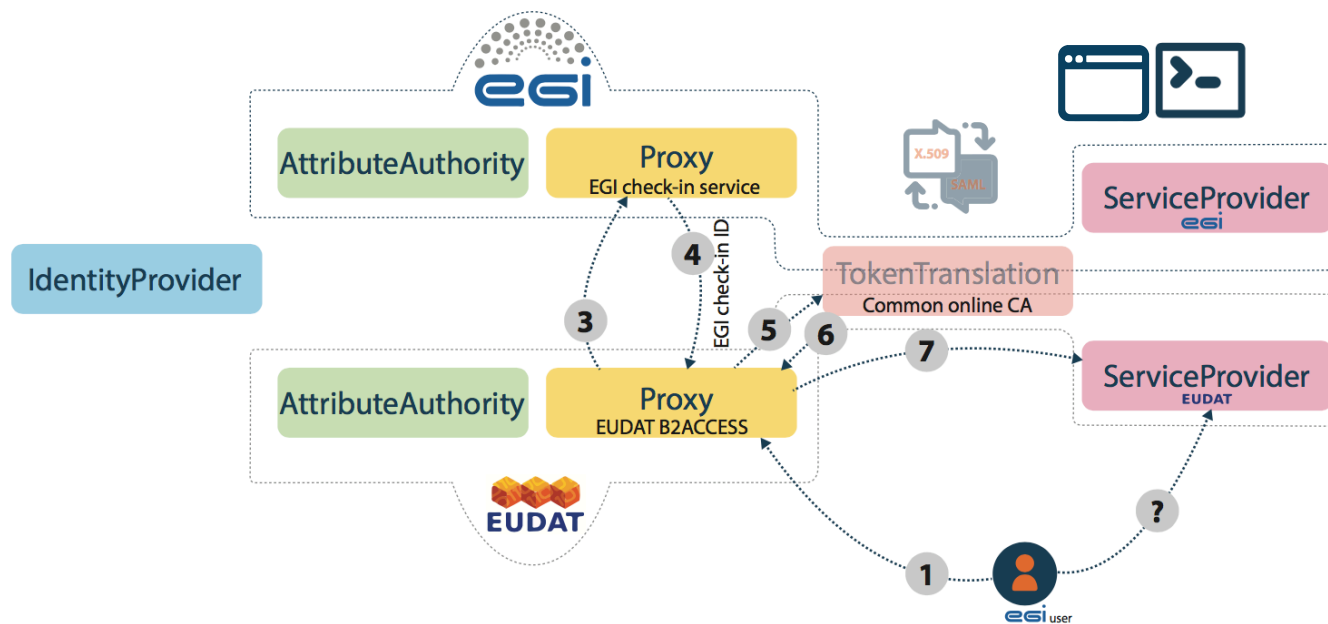
## Purpose

- Enable access to EUDAT services for users registered @EGI
- Bridging EUDAT and EGI infra

## Services

- EGI check-in service
- EUDAT B2ACCESS
- RCAuth (for non-web services)

[wiki.geant.org/soon](http://wiki.geant.org/soon) available





Authentication and Authorisation for Research and Collaboration

## **Conclusions, Lessons Learned and looking ahead**





## Conclusions<sup>1</sup>

---

### Successfully...

- ✓ Deployed many different AAI solutions approx. 20
- ✓ Reused and glued together existing components
- ✓ Tested/discussed pilot results with communities
- ✓ Provided architecture and guidelines
- ✓ Provided software sources and deployment scripts

**Many results are being rolled out in production already in R&E infrastructures**

We've shown that

# Proxy = a key element (!)

in research collaboration use cases

E.g.:

- Library pilots → bridging SAML to IP-access
- E-infra pilots → collect, aggregate and forward AuthZ attributes, easy to digest by SPs
- TTS Pilots → bridging SAML to ssh/x.509 and v.v. while hiding complexity



## Conclusions<sup>3</sup>



Successfully **bridged** eduGAIN NREN (SAML) world to e-infrastructure (ssh, X.509) world



## Lessons Learned

---

- We needed this project to show the full **potential of AAI components for Research and Collaboration**
- Scoping and executing the **pilots** was a challenge
- Bring the communities together, speak the same language and increase mutual understanding. E.g. the **Blueprint Architecture** allowed to establish common understanding
- Engage with communities from the very beginning and have demos available to increase adoption
- Thanks to these results, AAI for research is on the radar, many e-infrastructures and research communities recognize the added value of AAI and are engaged now → **2<sup>nd</sup> edition of AARC**



# AARC 2<sup>nd</sup> edition – A wide range of research communities committed



More information: [aarc-project.eu](http://aarc-project.eu),  
Full list of pilots: [wiki.geant.org/x/RIOjAw](http://wiki.geant.org/x/RIOjAw)

A screenshot of a web browser displaying the AARC website. The browser's address bar shows 'GÉANT Association'. The website header includes the AARC logo and the full name 'Authentication and Authorisation for Research and Collaboration'. A navigation menu contains links for 'Welcome to AARC', 'Roadmap', 'Work Packages', 'Blog', 'AARC Infoshare', 'Documents', 'Meetings', 'Wiki', 'About', and 'Admin'. The main content area is divided into four columns, each with an icon and a title: 'Architecture' (orange cube icon), 'Training and Outreach' (green circle icon), 'Policy Harmonisation' (brown paper plane icon), and 'Pilots' (black smartphone icon). Each column contains a short paragraph of text and a button with a link to further information.

**Architecture**  
AARC has designed an architecture to help e-infrastructures and research communities to enable secure, scalable and interoperable federated access to their resources.  
[Discover AARC blueprint architecture](#)

**Training and Outreach**  
AARC is producing different training modules and information packages on federated access and AARC results.  
[Learn how AARC can help you](#)

**Policy Harmonisation**  
AARC is working with research communities, e-infrastructures and identity federations to deliver a common policy framework for integrated AAI.  
[Discover AARC best practices](#)

**Pilots**  
AARC has built a testing environment to test technical and policy results based to address research communities requirements.  
[View AARC results in the real world](#)

Thank you  
Any Questions?



<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).