



Authentication and Authorisation for Research and Collaboration

WP SA1: Pilots on the integrated R&E AAI

SA1 Team

AARC EC Review

Brussels



Agenda AARC AHM – SA 1 pilots 9.30-10.30 + 10.45-11.45


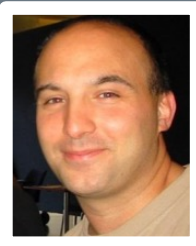


- Overview of SA1 in AARC1 – based on Review slide template, filling in the gaps, highlights of 24 months of AARC – 30m (see slides)
- What do you think is still missing/inaccurate/incorrect?
- What could be highlighted as a success for SA1?
- What has been finalized recently, is in the pipeline for AARC1 and/or will be continued in AARC2 (15m each)
 - Status RCAuth (and role in several pilots), VOMS COmanage integration - Mischa
 - Perun VOMS provisioner – Slavek
 - EGI-EUDAT x-infra pilot - Nicolas/Shiraz
 - PRACE-EUDAT x-infra pilot - Michal J.
 - WATTS extensions – Uros
 - Social ID, LoA enhancement – Mario/Nicolas

Agenda (for the review)

- **Structure and administrative matters**
- **Objectives**
- **Task Achievements**
- **Challenges**
- **Conclusions**
- **Looking ahead**

Structure SA1



<p>Activity Leader</p>  <p>Paul van Dijk SURFnet</p>	<p>T1: Pilots of solutions for guest users</p>  <p>Mario Reale GARR</p>	<p>T2: Pilots of an attribute management framework</p>  <p>Peter Solagna EGI</p>	<p>T3: Pilot to improve access to R&E resources</p>  <p>Maciej Brzezniak PSNC</p>
---	--	---	--

Partners



Resources



Total 2 Year effort	<i>96 PM for 2 years: flat distribution: 48 PM (4 FTE)</i>	<i>XX PM used xx% of resources</i>
Participants	<i>11 partners</i>	
Underspent: SURFnet		
2/2 Milestone completed in the reporting time 4/4 Deliverables in the reporting time		

High-level objectives WP SA1: Pilots on the integrated R&E AAI



Facilitate researchers to collaborate in a secure and trusted virtual research environment **by providing AAI tools** to support collaborative research in a distributed environment



Showcase solutions for guest identities and to ease the deployment of non academic identity providers



Demonstrate through pre-production services the integration of distributed attribute providers with (e-infrastructure) services to implement attribute-based AuthZ capabilities to communities and providers



Demonstrate through pre-production services that existing AAIs can be leveraged to access (non-web) resources that are offered by different e-Infrastructures and enable SSO capabilities for users



Support commercial service providers in the area of pay-per-use and contracted services

Pilots on the integrated R&E AAI



Achievements:

Task 0 | Coordination of the pilots activity

Objectives - Pilots on the integrated R&E AAI

Task 0: Activity leadership to coordinate the overall work



Objectives from Technical Annex

Coordination of activities

Establish pilot approach and test bed infrastructure for the pilots

Plan Demonstrators

Provide feedback to other AARC activities

Results

✓
VCs every 2 weeks
Reporting on the wiki
F2f meetings, wrap ups in infographics
Plugfest for dedicated effort on X-infra
Use cases

✓
Testbed established and heavily used
Good compliance with pilot approach
enrolment forms, pilot cockpits with results

✓
Started with single components, focus gradually shifted to multicomponent, distributed X-infra pilots

✓
Wrapped up results, created blogs, videos and infographics in collaboration with outreach activity. Ongoing interaction with JRA1/NA3. Pilots trigger new challenges and ideas

Approach and status of the pilot activity Pilots guided by AARC JRA1 deliverables



Requirements User Community

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

05-10-2015

Deliverable DJRA1.1

Contractual Date: 31-09-2015
Actual Date: 05-10-2015
Grant Agreement No.: 633665
Work Package: JRA1
Task No.: JRA1.1
Lead Partner: EDS-ae
Document Code: DJRA1.1
Editors: Christos Karamanolakis, Nicolas Lampiris, Nikos van Oik, Peter Stragies

© EC/NT on behalf of the AARC project.
This research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 633665 (AARC).

Abstract
This document, produced by JRA1 Task 1 "Analysis of user community requirements", identifies the requirements of user communities and service providers leading upon the outcomes of previous activities such as the TESSIS AAI Study and the WAIW working group. The requirements identified by 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 digital business. These requirements are presented here and will be provided as input for upcoming activities in AARC.

Overview Available AAI Components

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

31-12-2015

Milestone MJRA1.1

Contractual Date: 31-12-2015
Actual Date: 31-12-2015
Grant Agreement No.: 633665
Work Package: JRA1
Task No.: 1
Lead Partner: EDS-ae
Document Code: MJRA1.1
Authors: P. Sotgiu (EDS-ae), Christos Karamanolakis (GRNET), N. Lampiris (GRNET), M. Haral (NTT), M. Sule (HAWK), S. Panter (LSE), M. Mavrou (GARR), N. Van Oik (EDS-ae), J. Jansen (DFK), I. Laidis (GRNET), M. Janssens (DFK), S. Nounis (Laidis), M. Probst (EDS-ae), S. Sauer (GARR), S. Sauer (GARR), H. Short (EDS-ae), L. Stenavich (NTT)

© EC/NT on behalf of the AARC project.
This research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 633665 (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.

(Draft) Blue-Print Architecture

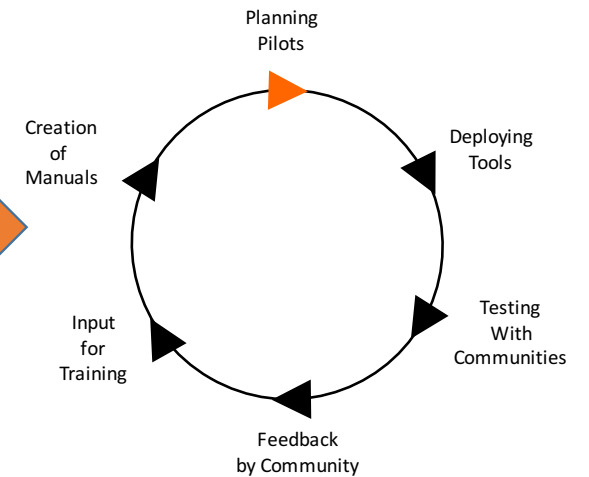
AAI: The e-Infrastructure View

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 "pseudo-idP" 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) could 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 (NS: "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

Running Pilots With Communities



Pilot intake forms to initiate pilots – define aims, commitment....



Contact data of AARC participants involved

Please provide contact details for AARC participants involved in this pilot

	Name(s)
AARC SA1 Pilot name:	
AARC SA1 Pilot subtask:	
Technical contact(s) in AARC:	

Contact data of Parties involved

Please provide contact details for additional organisations involved in this pilot

Organisation Name	Person names	Role in pilot

Pilot description

- Please describe high-level goal of pilot, provide overview of activities and participants. Please describe how commitment from various partners is secured.

Pilot goals

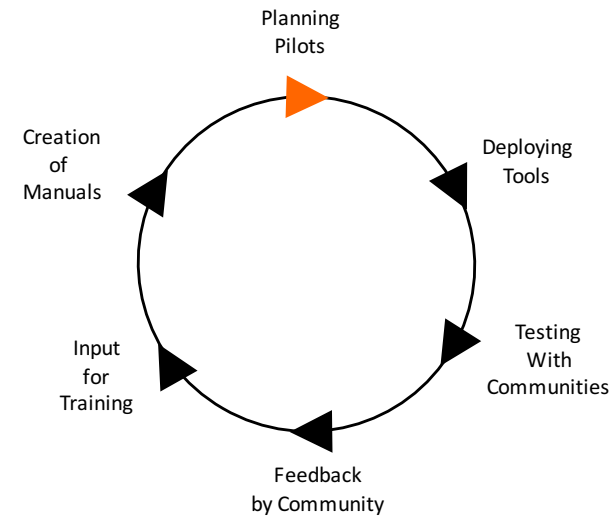
- Please describe goals of pilot, including activities and participants. Describe when the pilot is done and how to measure the success of it, in a SMART way.

Pilot resources

- Please describe required resources for the pilot, including VMs, DNS and certificates. Need for piloting in eduGAIN policy framework?

Contact data

Date	Activity	Owner	Minutes
January 1, 2015	Kickoff meeting		



Achievements – Task 0: Activity leadership to coordinate the overall work Established a pilot platform



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

Pilot coordination, pilot platform, outreach of pilot results



31-08-2016

Deliverable DSA1.2: First report on the Pilots deployed by SA1

Deliverable DSA1.2

Contractual Date: 31-07-2016
Actual Date: 30-09-2016
Grant Agreement No.: 653965
Work Package: SA1
Task Item: SA1.2
Lead Partner: SURFnet.nl
Document Code: DSA1.2
Authors: P. van Dijk SURFnet

© 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 Pilot Workpackage (SA1) provides an overview of the pilots running in AARC after one year of its start. The document provides information on the preliminary pilot results and plans to finalise them.

Task 1, Pilot 1	SAML / IP bridge
Focus	Support access to federated and non-federated library resources – bridging SAML and IP-address based access methods (SAML to SAML + SAML to IP)
Approach/AARC identified solution	Establish a proxy to bridge SAML and IP address access methods, a so called access mode switch
Components piloted	EZ-Proxy for SAML-IP bridge
Gain for end-users/administrators	<ul style="list-style-type: none"> • Same effort required • A better access w • An easy access w authentic
Demo/video	Demo Flow Video
Detailed technical description	wiki
Documentation of components	documentation for
Software source(s)	EZproxy
Lead	GARR
Community partners	IT: GARR, Library NL: UKB library co
Status	Close to finalizati

Table 2 - Ta

Authentication and Authorization in Collaborative Organizations

Attribute management, aggregation and consumption

www.aarc-project.eu

Use cases & aims

In a federated environment Identity Providers and Service Providers establish a trust framework to handle **Authentication** based on institutional accounts. Today this approach (see scenario 1) is common practice and even global IDP - SP scenarios become mainstream using eduGAIN as an inter-education vehicle.

Authentication infrastructures have proven to be useful in collaborative organizations (COs) but in those scenarios there is a strong need for additional attributes (e.g. entitlements) to handle **Authorizations** in a scalable and federated way as well (see scenario 2). In addition, there is a growing need to include users with **guest/social identities** but at the same time establish a sufficient level of trust for such identities.

The pilots presented here provide clues to (1) establish external CO managed Attribute Authorities (AAs), (2) to aggregate attributes from different sources in a central proxy, (3) forward the enriched set of attributes in such a way that they can easily be consumed by Service Providers (SPs) upon which these SPs can make authorization decisions and (4) to provide suitable approaches to include users in the CO who own only a social identity by integrating multiple authentication technologies like OIDC and OAuth2 with SAML.

1 Basic scenario (common practice)

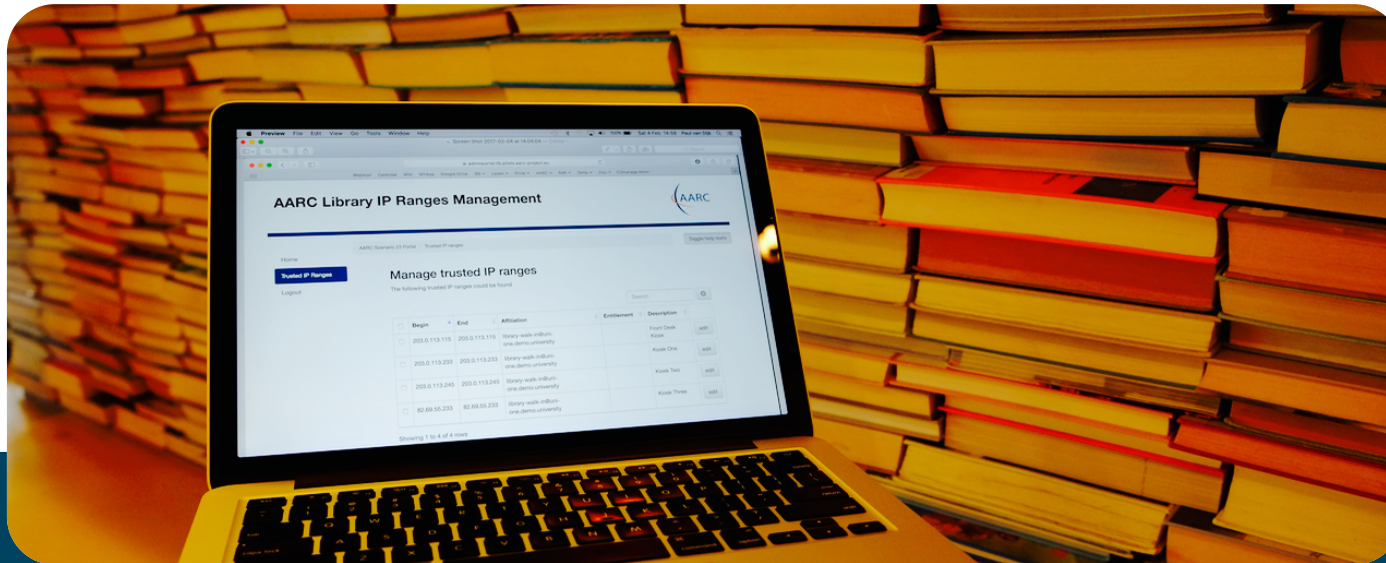
2 Collaboration scenario

3 Collaboration scenario including social identities

In the first pilot we investigated the usability of SAML based AAI components to use externally managed attributes to provide and restrict access to cloud services. We provided a demo where attribute management is based on CO managed and a user is able to access an OpenStack Liberty based cloud service (scenario 2)
demonstrator <https://wiki.geant.org/x/LAHSaW>

In the second pilot pilot we demonstrate possible mechanisms to include Social Identities in the Authentication and Authorization process for providing federated access to resources within a given research collaboration, exploiting mechanisms to enhance the LoA of the users (scenario 3)
demonstrator <https://wiki.geant.org/x/ZIq5Aw>

Pilots on the integrated R&E AAI



Achievements: Task 1 | Pilot solutions for guest users

Objectives Pilots on the integrated R&E AAI

Task 1: Pilot solutions for guest users



Objectives
from
Technical
Annex

Lower thresholds for participation in identity federations

Solutions for guest access

Showcase ways to support scalable LoA for guest users

Showcase AAI approaches for research libraries

Results

✓
Add components to be all inclusive, lower threshold to add services

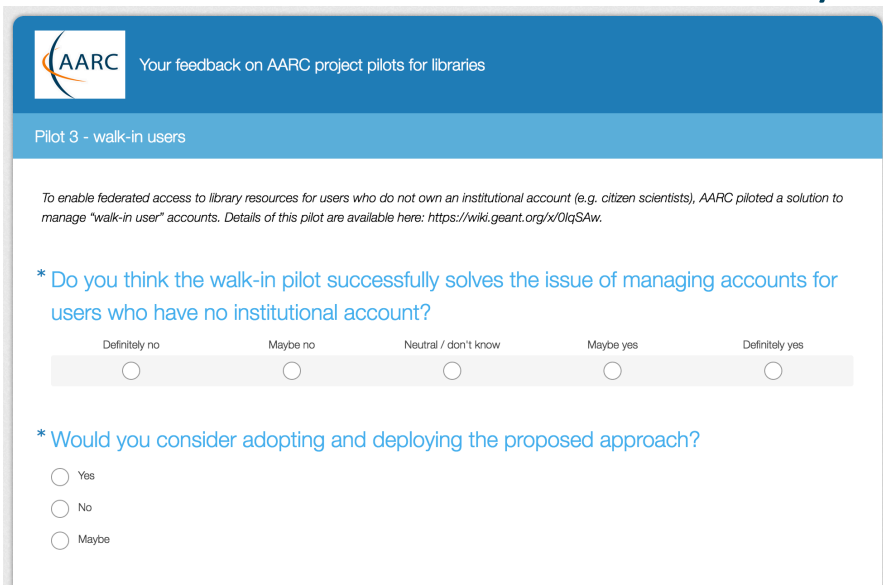
✓
Provide access for visitors of libraries, enable use of external identities link ORCID iD

✓
Detect LoA from AuthN source Increase & forward LoA to SPs link sources

✓
Several clues to increase adoption of AAI solutions @libraries/consortia

Library pilots

- Reported results/provided demo
- Produced a leaflet
- Created questionnaire
- Received feedback from community



AARC Your feedback on AARC project pilots for libraries

Pilot 3 - walk-in users

To enable federated access to library resources for users who do not own an institutional account (e.g. citizen scientists), AARC piloted a solution to manage "walk-in user" accounts. Details of this pilot are available here: <https://wiki.geant.org/x/0lqSAw>.

* Do you think the walk-in pilot successfully solves the issue of managing accounts for users who have no institutional account?

Definitely no Maybe no Neutral / don't know Maybe yes Definitely yes

* Would you consider adopting and deploying the proposed approach?

Yes
 No
 Maybe



Federated Access To LIBRARY RESOURCES for EVERYONE

Do you grant access to your library's resources based on IP-addresses? Do you maintain the correct IP-address ranges yourself — a labour intensive and inaccurate process? Can you manage multiple identity provider - service provider connections? Are your users confronted with confusing interfaces? Can walk-in guest users access e-resources easily?

AARC is developing solutions!

Centrally Managed Access for Consortia

- Manage publisher contracts centrally, as a consortium.
- Save time implementing and managing; no need to establish many trust relationships with IdPs and SPs.
- Retain control of branding and all policies.
- Produce accurate statistics quickly and easily.

Guest Access for Walk-in Users

- Allow all users, even those without institutional accounts (eg. 'walk in' guest users), to access federated e-resources.
- Configure or change any setting via an intuitive web-based interface.

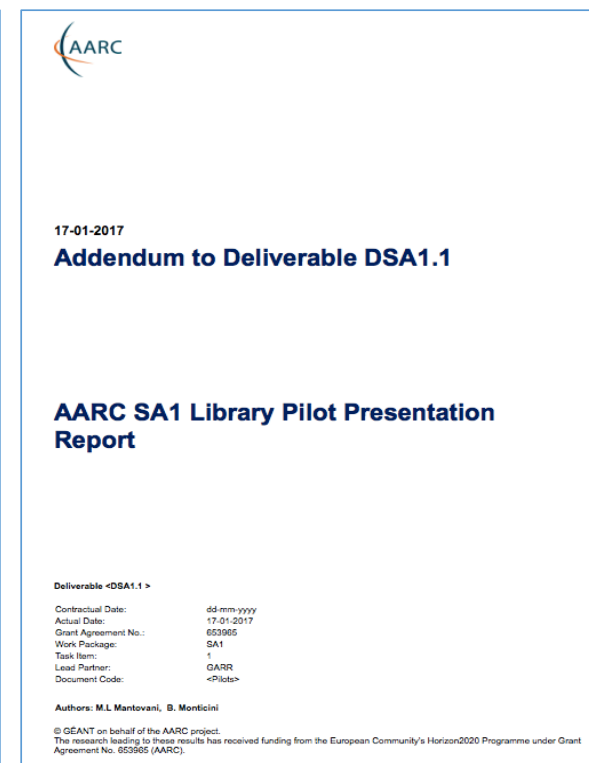
Federated Access to all Resources

- Give quick federated access to all to e-resources, even those which currently only support IP-based authentication, using AARC's suggested set-up of the EZProxy software.
- Ensure back-up access to federated e-resources, in case of problems with the e-resource service provider.

“ We have been running EZproxy for many years now and we also have walk-in users. By adopting these solutions, we could change our configuration and it could solve our problems. ”

-Tullio Nicolussi, University of Trento

www.aarc-project.eu/libraries



AARC

17-01-2017
Addendum to Deliverable DSA1.1

AARC SA1 Library Pilot Presentation Report

Deliverable <DSA1.1 >

Contractual Date:	dd-mm-yyyy
Actual Date:	17-01-2017
Grant Agreement No.:	653905
Work Package:	SA1
Task Item:	1
Lead Partner:	GARR
Document Code:	<Pilots>

Authors: M.L. Mantovani, B. Monticini

© 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. 653905 (AARC).

Social ID pilot

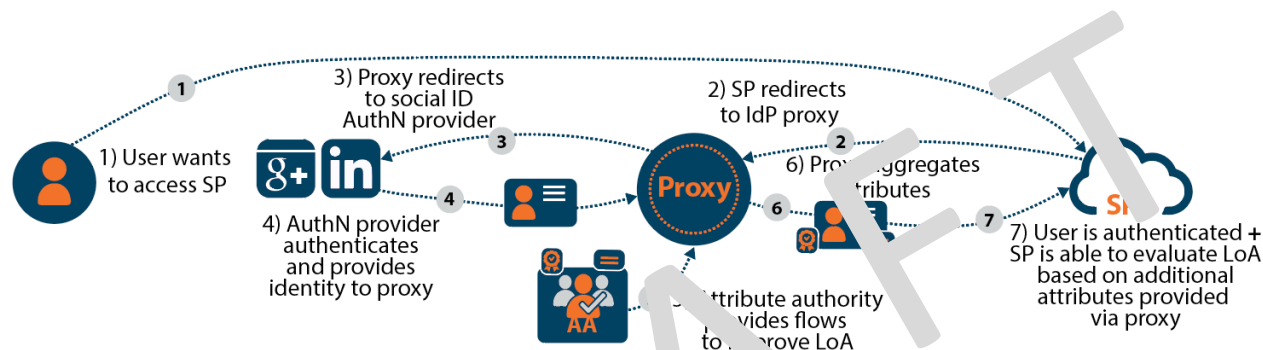
Purpose

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

Services/Components used

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

wiki.geant.org/x/ZlqSAw



BPA building blocks

IdentityProvider

AttributeAuthority
CManage

Proxy
simpleSAMLphp

TokenTranslation

ServiceProvider
OpenStack Horizon

Administrative domains



E-infrastructure/Collab. Organizations



eduGAIN SPs



Pilots on the integrated R&E AAI



Achievements:

Task 2 | Pilot solutions for attribute management

Objectives Pilots on the integrated R&E AAI

Task 2: Pilot solutions for attribute management



Objectives
from
Technical
Annex

Tools to support
registration and
management of
attributes

Solutions for
attribute aggregation

Attribute based
authorisation
including scalable LoA

Results



Pilots with Perun, COnanage,
VOMS, ORCID



EGI pilot....simpleSAMLphp
BBMRI pilot....



EGI pilot....OpenStack Horizon
BBMRI pilot....lifescience services (?)

SAML – ORCID account linking pilot

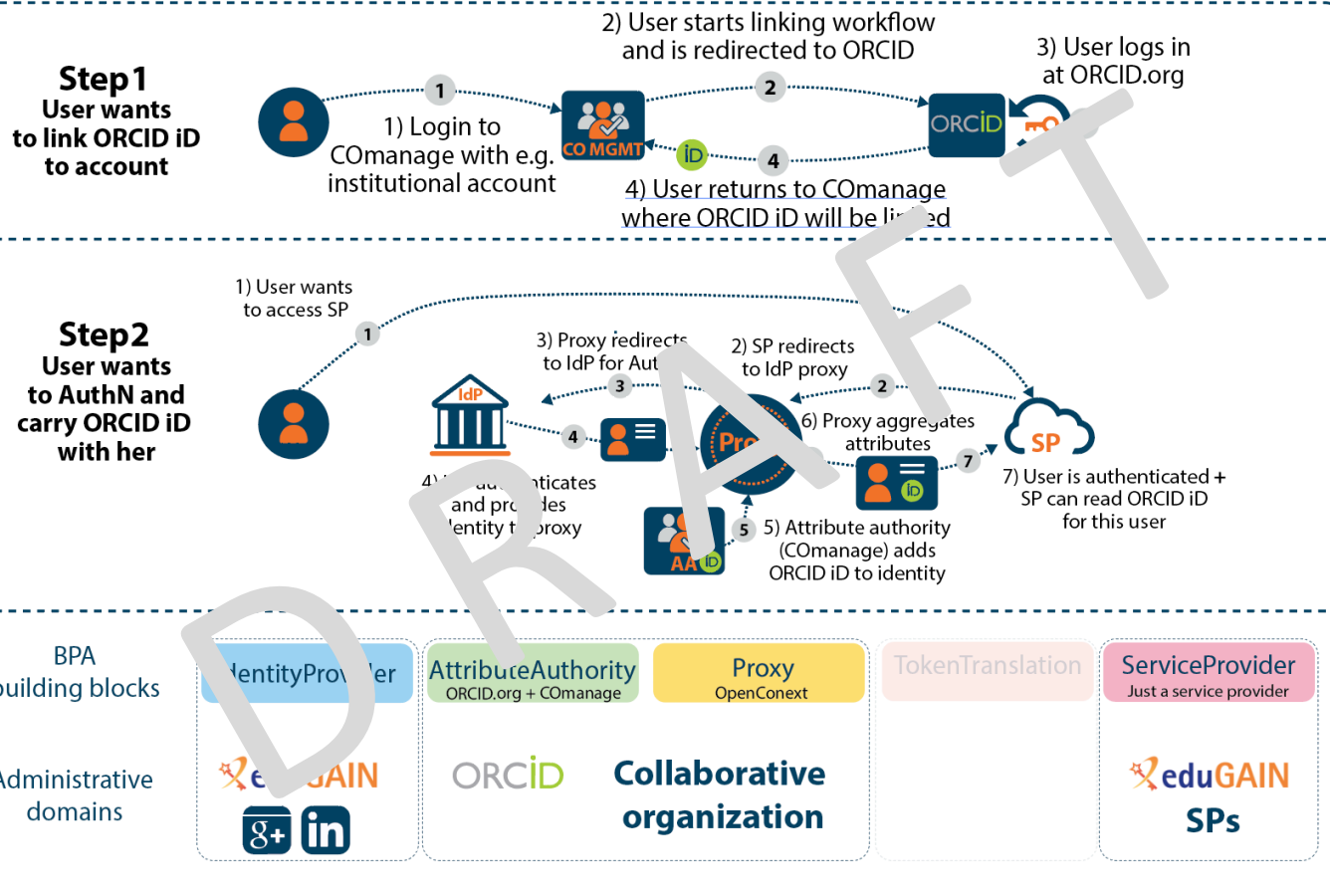
Purpose

- ORCID provides persistent IDs which are researcher centric and useful for use in collaboration services, therefore we implemented a workflow to link ORCID to user account

Services/Components used

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

wiki.geant.org/x/WAH5Aw



Attribute management & aggregation pilot – EGI + similar approach @BBMRI)



Purpose

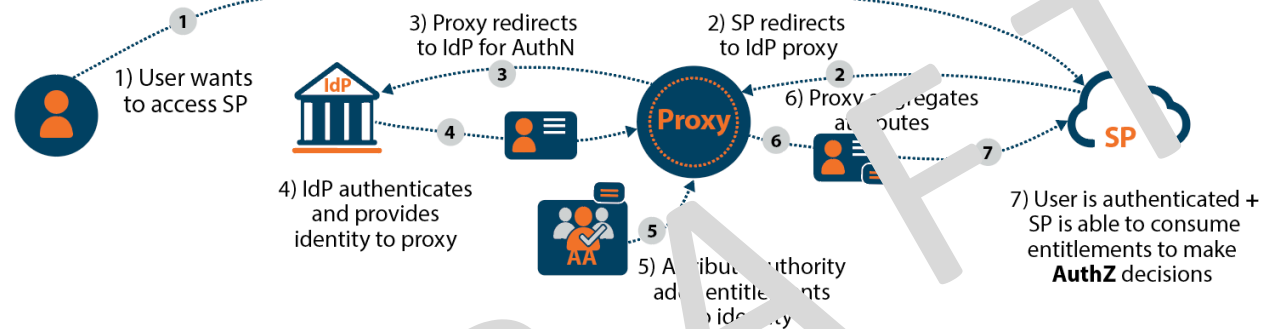
- Show how attributes from multiple AAs can be used for AuthZ in a fed. environment
- Delegate AuthZ decisions
- Minimize impact for SPs

Services/Components used

- COmanage/PERUN AAs
- SimpleSAMLphp proxy
- OpenStack Horizon SP/BBMRI SPs
- Tested with AARC, EGI & BBMRI community

EGI: wiki.geant.org/x/LAH5Aw

BBMRI: wiki.geant.org/x/HgD5Aw



Pilots on the integrated R&E AAI



Achievements:

Task 3 | Pilots to improve access to R&E resources

Objectives Pilots on the integrated R&E AAI

Task 3: Pilots to improve access to R&E relevant resources and services



Objectives
from
Technical
Annex

AAI mechanisms to
access non-web
resources

Integration of
research
infrastructure
services

SSO access to
(commercial cloud)
research services

Results

✓
CILogon-like pilot
Comanage SSH, OTP and ASP pilots
Watts OIDC to ssh & X509
LDAPfacade

✓
EUDAT – EGI pilot
EUDAT– PRACE pilot

✓
Federated access to ORCID
LibreOffice/Owncloud pilot
Everything that happened
in collab with HN initiative & GN3+

TTS: CILogon Pre-pilot, RCauth

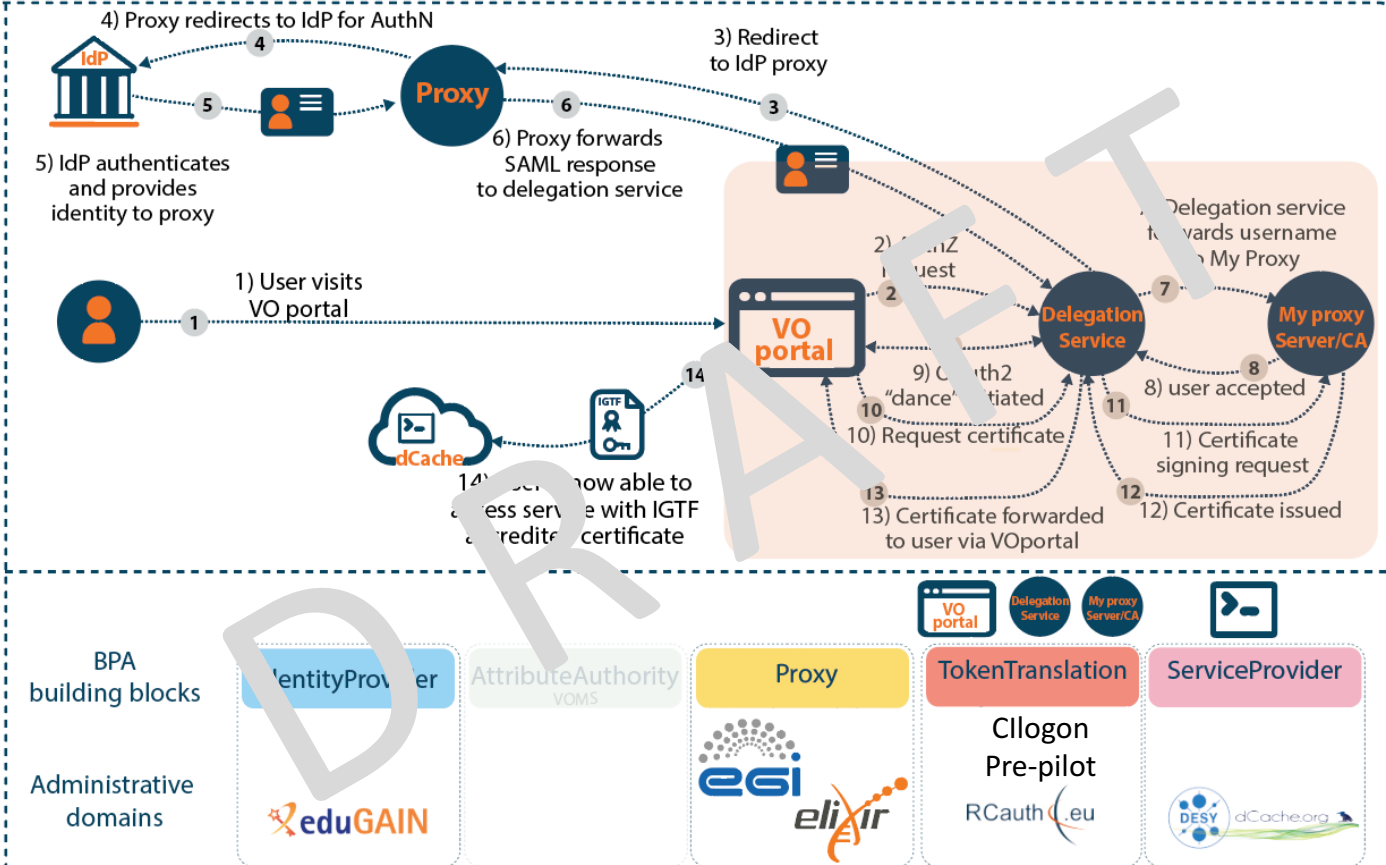
Purpose

- Enable access to certificate based services for users with an institutional account by generating certs on the fly
- Bridging eduGAIN & IGTF
- No need to understand PKI!

Services/Components used

- Cilogon, labeled as RCauth
- Several master portals
- Several science gateways
- SimpleSAMLphp
- Tested in context of EGI & Elixir...

wiki.geant.org/x/yADaAw



TTS: RCauth

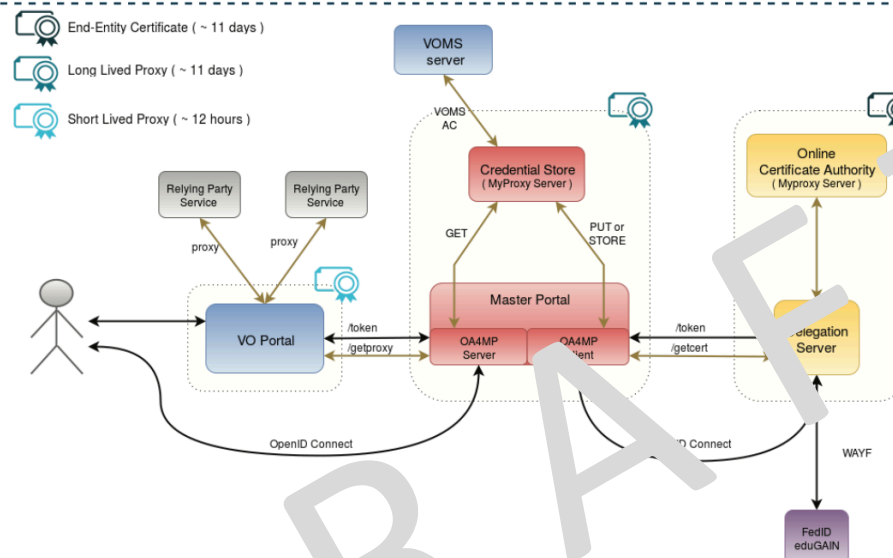
Purpose

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

Services/Components used


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

wiki.geant.org/x/yADaAw



BPA building blocks

IdentityProvider



AttributeAuthority VOMS



Proxy simpleSAML.php



TokenTranslation CILogon + extra services



ServiceProvider gsiftp-enabled storage



Administrative domains

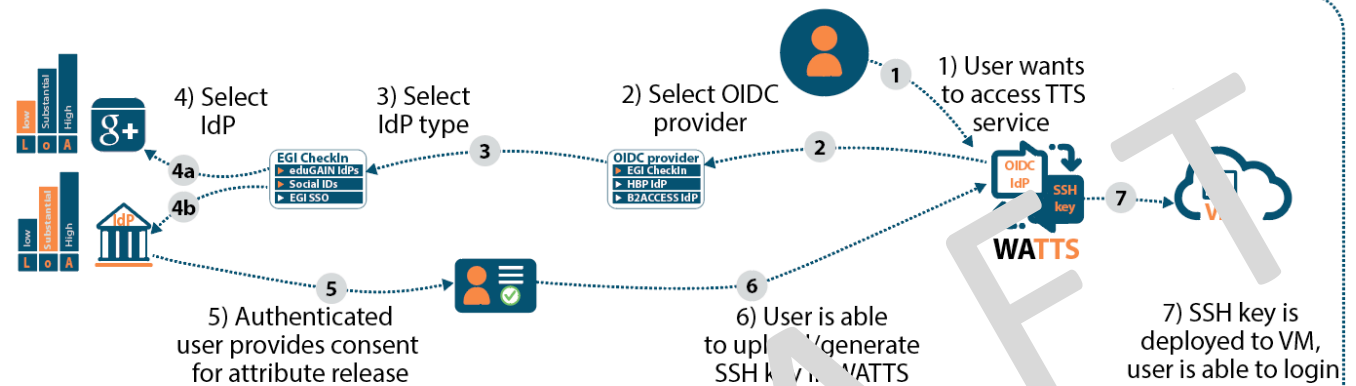
WaTTS token translation pilot translating from any OIDC provider to SSH/X.509 (still being extended)

Purpose

- For cases where users can (only) be authenticated via OIDC but require different credentials like SSH or X.509 to access services.

Services/Components used

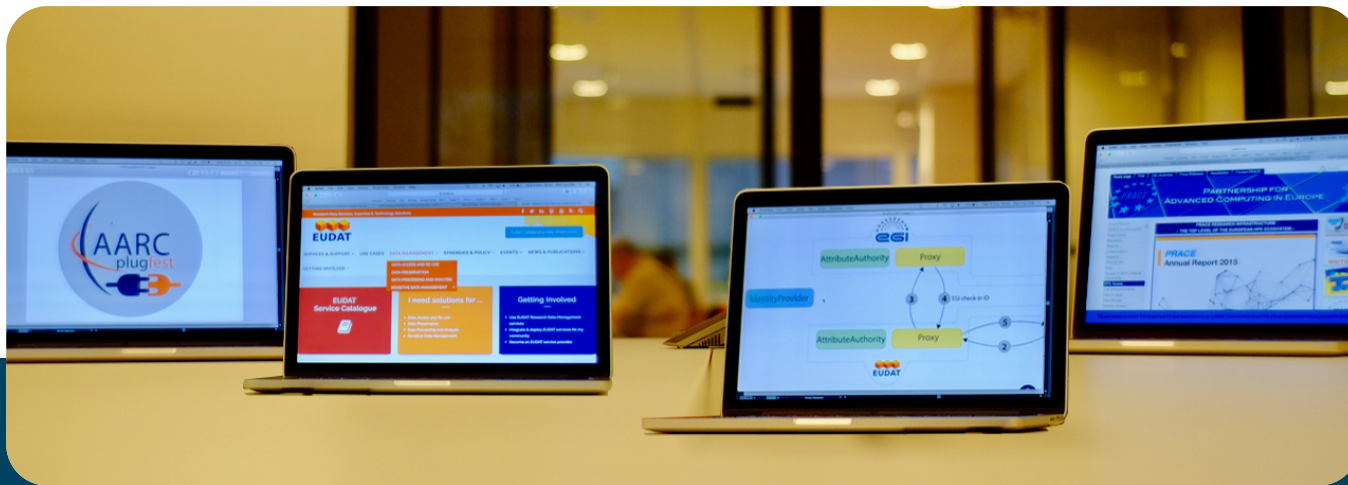
- EGI check-in
- WaTTS
- RCAuth
- Tested with AARC community, Indigo (?)...
wiki.geant.org/x/c4I0B



Report – pending....

Testing with template...in progress

Pilots on the integrated R&E AAI

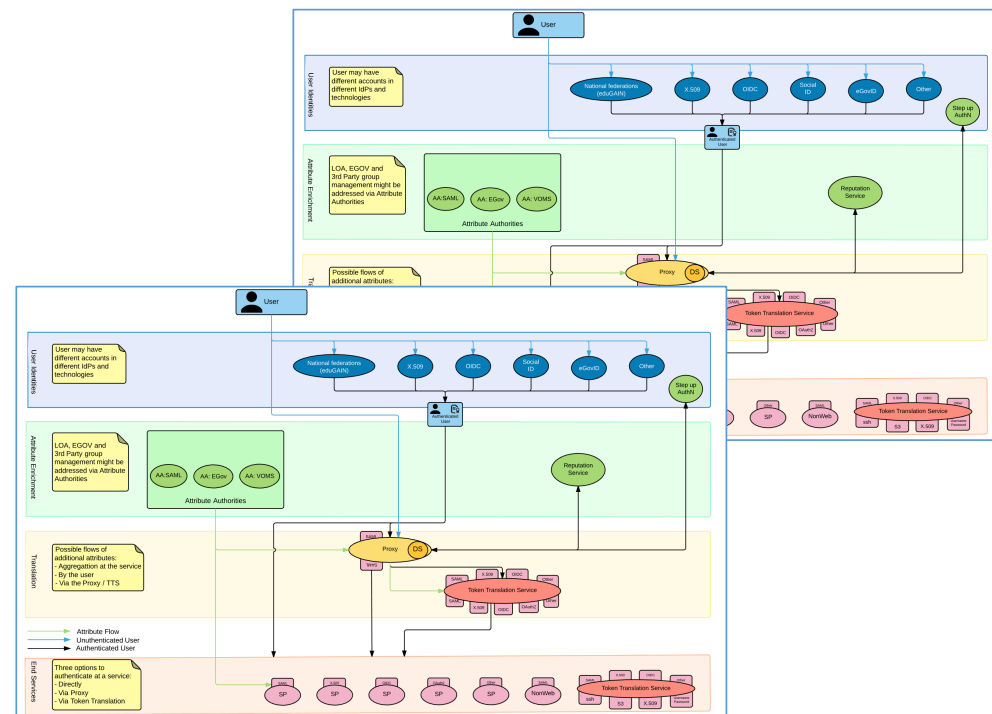


AARC1 and beyond...

Two X-infra pilots in the pipeline



AARC
blueprint
architecture



X-infra pilots, EUDAT - EGI, web based scenario

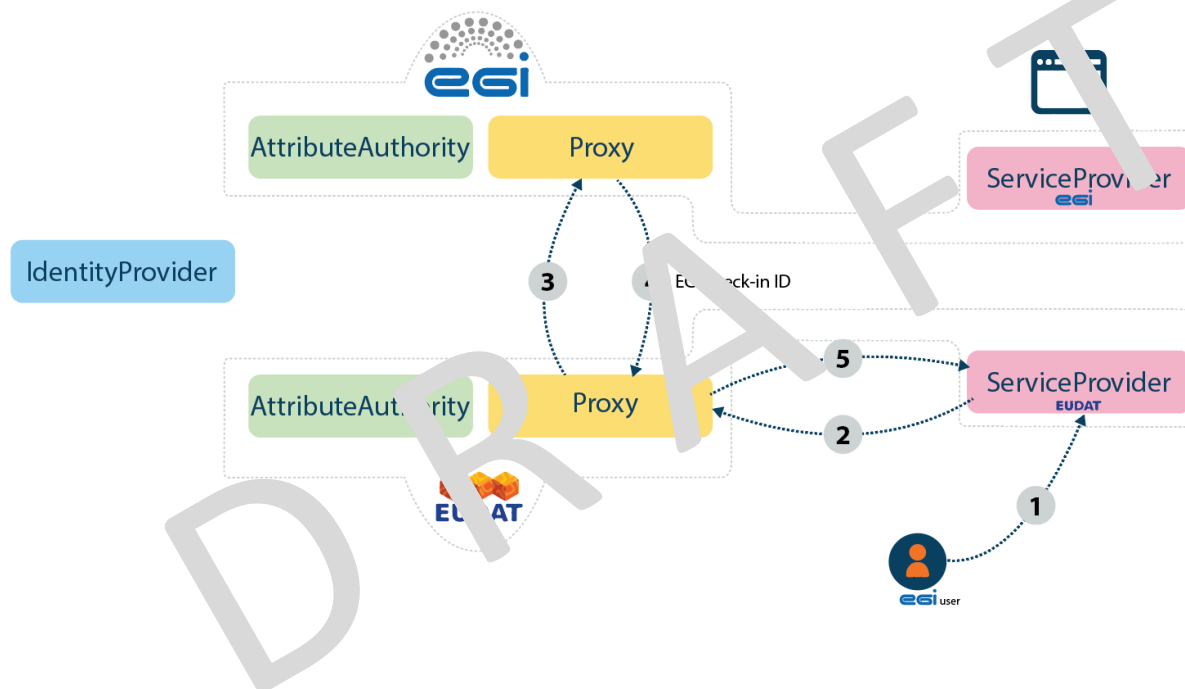
Purpose

- Enable access to web based EUDAT and EGI services for users registered @EGI or EUDAT

Services

- EGI check-in service
- EUDAT B2ACCESS

wiki.geant.org/x/hwf5Aw



X-infra pilots, EUDAT - EGI, non web based scenario

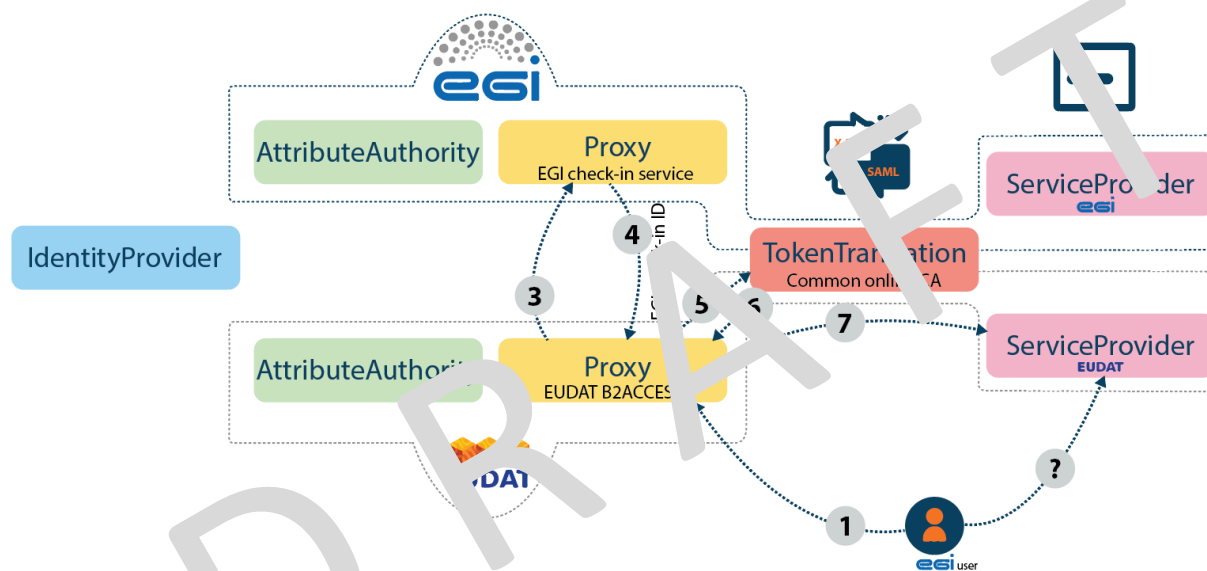
Purpose

- Enable access to certificate based EUDAT services for users registered @EGI
- Bridging EUDAT – EGI infra

Services

- EGI check-in service
- EUDAT B2ACCESS
- RCAuth

wiki.geant.org/x/Mwj5Aw



X-infra pilots, EUDAT - PRACE, non web based scenario

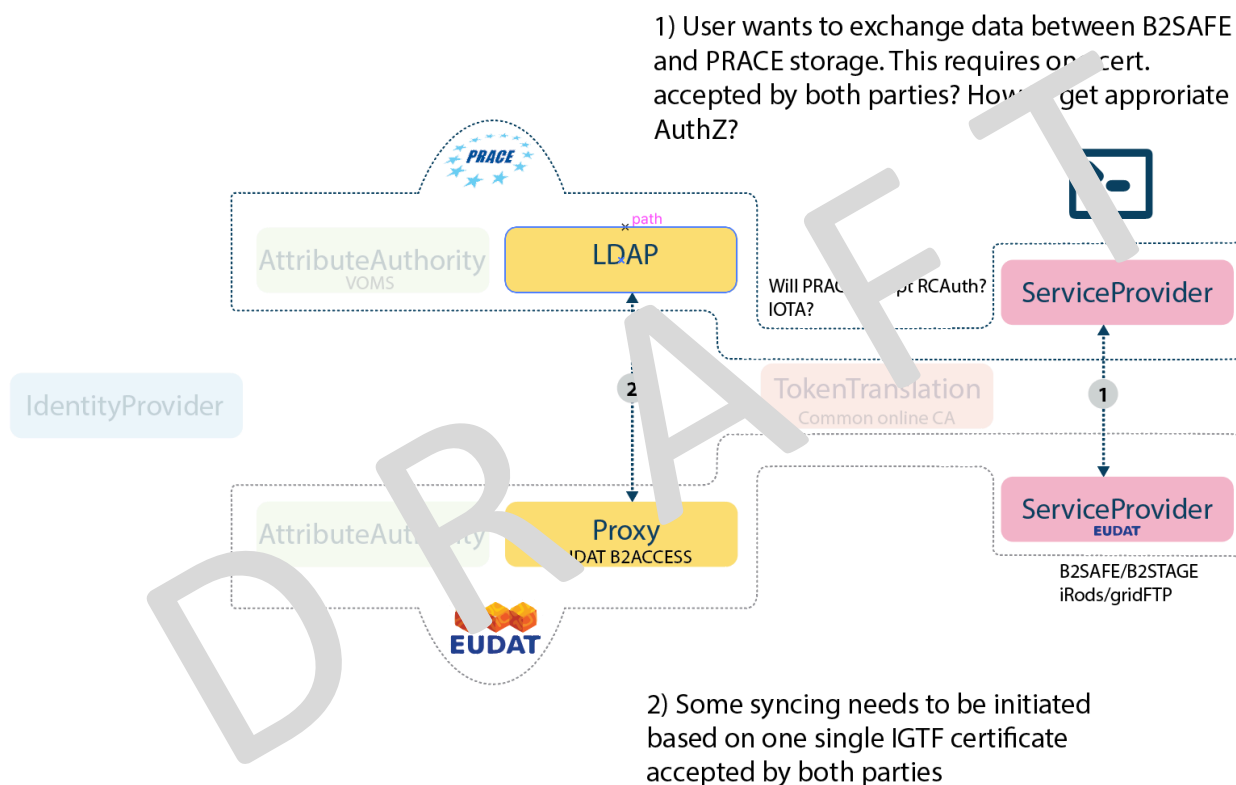
Purpose

- Enable access to each other's resource to exchange data
- Both e-infras accept the same cert. authorities
- Enable proper syncing of Authz

Services

- B2ACCESS
- PRACE tier 1 node LDAP

wiki.geant.org/x/oADaAw



AAI platform comparisons --> map & harmonize where possible

- Compare technical architectures
- Identifiers and attributes used
- Identity's cardinality and lifecycle
- Protocols and external account linking
- eduGAIN presence – principles and policies
- eduGAIN presence – technical aspects
- LoA approach – AuthN, AuthZ (?)



- Document is work in progress (see doc)
- Learning on the fly (see x-infra pilots)
- Flow into AARC2 (discussion)



Ongoing challenges

- Sustainability of components
- Business models for deployment and hosting
- Lower thresholds for all stakeholders
 - User friendliness (e.g. fix multiple redirect problems?)
 - Create manuals
 - Create deployment scripts of single and multiple component setups
- Harmonisation of attributes in X-infrastructures use cases
-

Conclusions¹

Successfully

- Deployed many different AAI components: XX in total
- Reused and glued together existing components
- Assessed maturity of components
- Tested/discussed with communities
- Documented flow, architecture, software sources
- Created summaries, reported results in leaflets
- Handed over lessons learned and best practices to the AARC outreach and training activity

Conclusions²



Successfully **bridged** eduGAIN NREN (SAML) world to IGTF GRID (ssh, X.509) world



Pilots – Reporting, finalized pilots

✓ Public wiki presence (updates?), @git...presented@?

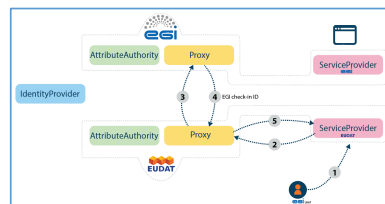
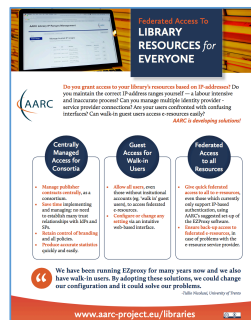
✓ Mapping to requirements & BPA

✓ Produced leaflet

✓ Video

✓ Feedback from community

✓ Sustainability plans



AARC / ... / Pilot results and demos
LibrariesCockpitPanelEZproxy
 Created by Mario Reale, last modified by Paul van Dijk on Nov 25, 2016

- Introduction
- Detailed description
- Demonstration Portal
 - Workflow
 - For federated users
 - For non-federated users
 - Components
- Benefits
- Demo Video

AARC Authentication and Authorisation for Research and Collaboration

WP SA1: Pilots on the integrated R&E AAI

SA1 Team

AARC EC Review
 Brussels



“ We have been running EZproxy for many years now and we also have walk-in users. By adopting these solutions, we could change our configuration and it could solve our problems.

-Tullio Nicolussi, University of Trento

Project background	Research
What is the pilot about?	The "walk in EZproxy" pilot is consisting of a proxy (EZproxy) which will allow walk-in users to have non-federated access to AARC services, without authentication enabled on their user per national library consortium deployment.
What problem does it solve?	The pilot serves a specific purpose and consists of two main components: - Walk-in users which provides their functionality via the user interface with the system.
Why is it important for the project?	Enable EZproxy to register and walk-in EZproxy authentication
How many elements compose the service?	Configure a Shibboleth Identity Provider which authenticates users against users, based on the campus LDAP system, as well as allowing authentication to the proxy, which is configured to proxy requests.
Specific objectives (if possible, use numbered)	This solution has been chosen because the university already has a Shibboleth-based identity provider, and the national library consortium is already providing walk-in access.
Deliverables (if possible, use numbered)	Established walk-in authentication service for library consortia
Policy considerations	The solution proposed here may be included in a suite of solutions e.g. combined with EZproxy, a consortium proxy, to improve transparency and to ease integration by the national consortium for national library consortia.
Are there specific security requirements?	The pilot serves a specific purpose and consists of two main components: - Walk-in users which provides their functionality via the user interface with the system.
Estimated user base	10,000
Expected duration (days, weeks, months, years)	10 Wk.
Availability requirements	99%
Expected financial impact	no impact
Estimated overall costs in other units	10k
Estimated overall costs monthly	10k / 10 = 1k
Resource model	10k / 10 = 1k

Overview of pilots carried out

	description	flow	video	live demo	pros/cons	(git)sources	leaflet	Feedback community
<u>Libraries</u>								
	LibrariesConsortiumProxy							
	LibrariesEZproxy							
	LibrariesWalkInUsersPortal							
Using external identities to provide access								
	SocialIDpilot							
	IGTF to eduGAIN proxy							
	eduTeams							
<u>Attribute management</u>								
	EGIAtributeManagementPilot							
	BBMRIAAIPilot							
	ComanageORCIDPilot							
	PerunVOMSCILogonPilot							
	ComanageVOMSprovisioner							
<u>Access to non-web resources and TTS pilots</u>								
	CILogon-like pilot							
	ComanageSSHPilot/OTP/ASP							
	Watts							
	LDAPfacade							
Access to services								
	ORCIDpilot							
	Libreoffice OwnCloud pilot							

DRAFT

Thank you Any Questions?

paul.vandijk@surfnet.nl



<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).