WP SA1: Pilots on the integrated R&E AAI

SA1 Team

AARC EC Review

Brussels
• 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 COnmanage 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

Activity Leader

Paul van Dijk
SURFnet

T1: Pilots of solutions for guest users

Mario Reale
GARR

T2: Pilots of an attribute management framework

Peter Solagna
EGI

T3: Pilot to improve access to R&E resources

Maciej Brzeziak
PSNC

Partners
## Resources

<table>
<thead>
<tr>
<th>Total 2 Year effort</th>
<th>96 PM for 2 years: flat distribution: 48 PM (4 FTE)</th>
<th>XX PM used xx% of resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Participants</td>
<td>11 partners</td>
<td></td>
</tr>
</tbody>
</table>

**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

- Coordination of activities: VCs every 2 weeks, Reporting on the wiki, F2f meetings, wrap ups in infographics, Plugfest for dedicated effort on X-infra Use cases
- Establish pilot approach and test bed infrastructure for the pilots: Testbed established and heavily used, Good compliance with pilot approach, enrolment forms, pilot cockpits with results
- Plan Demonstrators: Started with single components, focus gradually shifted to multicomponent, distributed X-infra pilots
- Provide feedback to other AARC activities: Wrapped up results, created blogs, videos and infographics in collaboration with outreach activity, Ongoing interaction with JRA1/NA3. Pilots trigger new challenges and ideas

http://aarc-project.eu
Approach and status of the pilot activity
Pilots guided by AARC JRA1 deliverables

Requirements
User Community

Overview Available
AAI Components

(Draft) Blue-Print
Architecture

Running Pilots
With Communities

Planning Pilots

Deploying Tools

Testing With Communities

Creation of Manuals

Input for Training

Feedback by Community

http://aarc-project.eu
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

<table>
<thead>
<tr>
<th>Name(s)</th>
<th>AARC SA1 Pilot name:</th>
<th>AARC SA1 Pilot subtask:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Technical contact(s) in AARC:

Contact data of Parties involved
Please provide contact details for additional organisations involved in this pilot

<table>
<thead>
<tr>
<th>Organisation Name</th>
<th>Person names</th>
<th>Role in pilot</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

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

<table>
<thead>
<tr>
<th>Date</th>
<th>Activity</th>
<th>Owner</th>
<th>Minutes</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 1, 2015</td>
<td>Kickoff meeting</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Achievements – Task 0: Activity leadership to coordinate the overall work
Established a pilot platform

• A staging area for piloted services
• Technical platform delivered by okeanos
• >20 VMs instantiated
• Using Ansible scripts for deployment
• SimpleSAMLphp DIY IdP available
• Online support by SURFNET staff
Pilot coordination, pilot platform, outreach of pilot results

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 SAAM + 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 | • Same end-users access required
• A better learning experience
• An easy use of access with minimal authentication

Demo/video | Demo Flow Video
Detailed technical description | wiki
Documentation of components | documentation for EZproxy
Software source(s) | EZproxy
Lead | GARR
Community partners | IT: GARR, Library NLS: UKB library
Status | Close to finalisation

Authentication and Authorization in Collaborative Organizations

Attribute management, aggregation and consumption

1. Basic scenario (omitted in 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 generated scenarios where attribute management is based on OAuth or and a set is able to access an OpenID-based cloud printer domain:  

[Link to demonstration]

In the second pilot we demonstrated the possibility to include social identities in the Authentication and Authorization process for providing federated access for library members. The AARC platform was used to establish trust and collaboration, exploiting mechanisms to enhance the trust of the users. Domain:  

[Link to demonstration]

In the third pilot we demonstrated the possibility to establish a pilot to use AAI components to use externally managed attributes to provide and restrict access to cloud services. We generated scenarios where attribute management is based on OAuth or and a set is able to access an OpenID-based cloud printer domain:  

[Link to demonstration]
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 Project Pilots for Libraries](http://aarc-project.eu)

**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/uStG58w

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

<table>
<thead>
<tr>
<th>Definitely no</th>
<th>Maybe no</th>
<th>Neutral / don’t know</th>
<th>Maybe yes</th>
<th>Definitely yes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Would you consider adopting and deploying the proposed approach?

- Yes
- No
- Maybe

---

![Addendum to Deliverable DSA1.1](http://aarc-project.eu)

**17-01-2017**

**AARC SA1 Library Pilot Presentation Report**
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)
- COmanage AA
- SimpleSAMLphp proxy
- OpenStack Horizon SP
- Tested with EGI and AARC pilot community

wiki.geant.org/x/ZlqSAw
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, COmanage, 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
• COmanage – 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

EDUCAUSE: wiki.geant.org/x/LAH5Aw
BBMRI: wiki.geant.org/x/HgD5Aw
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**
  - CILogon-like pilot
  - Comanage SSH, OTP and ASP pilots
  - Watts OIDC to ssh & X509 LDAP facade

- **Integration of research infrastructure services**
  - EUDAT – EGI pilot
  - EUDAT– PRACE pilot

- **SSO access to (commercial cloud) research services**
  - 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](http://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 RCAuth
- Several master portals
- Several science gateways
- SimpleSAMLphp
- VOMS Attribute Authority
- Tested with AARC community +...

[Link to wiki.geant.org/x/yADaAw]
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/c410B](http://wiki.geant.org/x/c410B)
LibreOffice OwnCloud pilot

Report – pending....
Testing with template...in progress
Pilots on the integrated R&E AAI

AARC1 and beyond...
Two X-infra pilots in the pipeline
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](http://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

1) User wants to exchange data between B2SAFE and PRACE storage. This requires one cert. accepted by both parties? How to get appropriate AuthZ?

2) Some syncing needs to be initiated based on one single IGTF certificate accepted by both parties
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

• .....
Conclusions\textsuperscript{1}

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

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.

—Zahir No kısm, University of Trento
### Overview of pilots carried out

<table>
<thead>
<tr>
<th>Libraries</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>LibrariesConsortiumProxy</td>
<td>description</td>
<td>flow</td>
<td>video</td>
<td>live demo</td>
<td>pros/cons</td>
<td>(git)sources</td>
<td>leaflet</td>
</tr>
<tr>
<td>LibrariesEZproxy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LibrariesWalkInUsersPortal</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Using external identities to provide access

| SocialIdentDpilot |  |  |  |  |  |  |  |
| IGTF to eduGAIN proxy |  |  |  |  |  |  |  |
| eduTeams |  |  |  |  |  |  |  |

Attribute management

| EGIAttributeManagementPilot |  |  |  |  |  |  |  |
| BBMRIAAlPilot |  |  |  |  |  |  |  |
| COrangeORCIDPilot |  |  |  |  |  |  |  |
| PerunVOMSCILogonPilot |  |  |  |  |  |  |  |
| COrangeVOMSProvisioner |  |  |  |  |  |  |  |

Access to non-web resources and TTS pilots

| CILogon-like pilot |  |  |  |  |  |  |  |
| COrangeSHPilot/OTP/ASP |  |  |  |  |  |  |  |
| Watts |  |  |  |  |  |  |  |
| LDAPFacade |  |  |  |  |  |  |  |

Access to services

| ORCIDpilot |  |  |  |  |  |  |  |
| Libreoffice OwnCloud pilot |  |  |  |  |  |  |  |
Thank you
Any Questions?

paul.vandijk@surfnet.nl