What has the AARC project added?

Christos Kanellopoulos - GÉANT

Internet2 2017 Global Summit
April 25th, 2017
International Research Collaborations

1. Users should be able to access the all services using the credentials from their Home Organizations when available.

2. Secure integration of guest identity solutions and support for stronger authentication mechanisms when needed.

3. Access to the various services should be granted based on the role(s) the users have within the collaboration.

4. Users should have one persistent identity across all community services when needed.

5. Ease of use for users and service providers. The complexity of multiple IdPs/Federations/Attribute Authorities/technologies should be hidden.
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/
Identity & Access Management for International Research Collaborations

A Blueprint Architecture for authentication and authorization

A set of architectural building blocks on top of eduGAIN

eduGAIN and the Identity Federations

A solid foundation for federated access in Research & Education

https://aarc-project.eu/blueprint-architecture/
AARC Blueprint Architecture

https://aarc-project.eu/blueprint-architecture/

Guidelines and support documents

- Best practices for managing authorisation
- Expressing group membership and role information
- Scalable attribute aggregation
- Implementation of token TTS
- Credential delegation
- Non-web access
- Social media IdPs
- Use cases for account linking
- Use cases for LoA elevation via step-up authentication
AARC Blueprint Architecture

https://aarc-project.eu/workpackages/policy-harmonisation/

Policy recommendations & frameworks

- Security Incident Response Trust Framework for Federated Identity – Sirtfi
- Scalable Negotiator for a Community Trust Framework in Federated Infrastructures – Snctfi
- Recommendations on Minimal Assurance Level Relevant for Low-risk Research Use Cases
- Differentiated LoA recommendations for policy and practices of identity and attribute providers
- Recommendations and template policies for the processing of personal data by participants in the pan-European AAI
Three types of pilots

To expand the reach of federated access (i.e. libraries)

To test technical and policy components in production infrastructures

To test cross infrastructure scenarios

https://wiki.geant.org/x/RIOjAw
Moving to production - Architecture

Adopted by e-Infrastructures providers (GÉANT, EGI, EUDAT, INDIGO, EOSC-Hub) and research infrastructures

• Examples:
  • EGI (https://wiki.egi.eu/wiki/AAI)
  • ELIXIR (https://www.elixir-europe.org/services/compute/aai)
  • EUDAT (https://www.eudat.eu/services/b2access)
  • GÉANT eduTEAMS (https://www.eduteams.org)
  • INDIGO (https://www.indigo-datacloud.eu/identity-and-access-management)

• Working on a cross e-Infrastructure platform alignment recommendations document
Moving to production - Policies

• Security Incident Response Trust Framework for Federated Identity – Sirtfi
  • Already supported by 160 IdPs/SPs

• Scalable Negotiator for a Community Trust Framework in Federated Infrastructures – Snctfi (coming out soon)

• Cross e-Infrastructure LoA profile based on the REFEDS LoA Framework
Moving to production – Pilot services

• Social ID integrations
  • Guidelines document available and open for comments
  • Already available on most EIs/RIs

• SAML - ORCID account linking
  • Nascent implementations
  • Guidelines document under preparation

• RCAuth Token Translation Service
  • Existing RCAuth CA/TTS in production with limited capacity
  • 1/2018 phased rollout of the new RCAuth CA/TTS by EGI, EUDAT and GÉANT

• Bridging IGTF to eduGAIN proxy
  • In production since 3/2017
  • More global instances coming up
AARC 2\textsuperscript{nd} edition – A wide range of research communities committed
Thank you

Any Questions?