



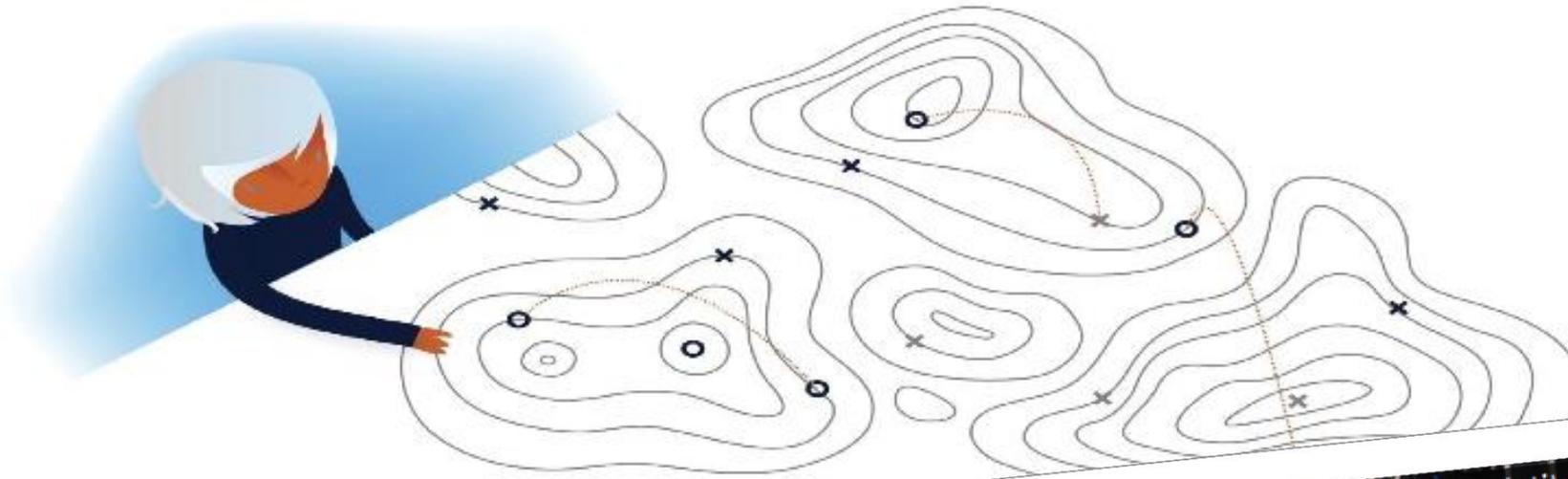
Gestione dell'identità nella comunità della Ricerca e dell'Educazione in Europa

Licia Florio
GÉANT

GARR Workshop, Roma
20 aprile 2016

The Global Nature of Research

No Researcher works in isolation



ESPERIMENTI PROGETTI COMUNICAZIONE OPPORTUNITÀ DI LAVORO

Istituto Nazionale di Fisica Nucleare

🇮🇹 🇬🇧

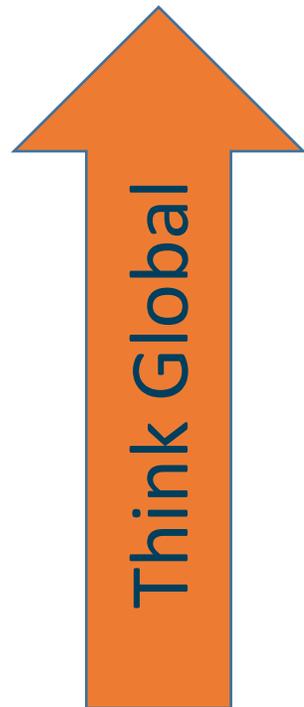
OSSERVATE LE ONDE GRAVITAZIONALI A 100 ANNI DALLA PREVISIONE DI EINSTEIN

LIGO and VIRGO:

- More than 90 universities



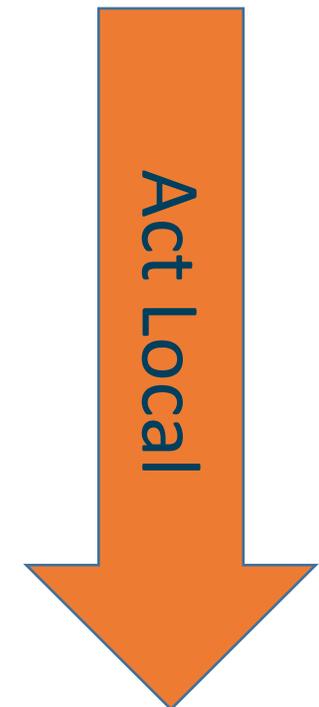
Think Global, Act Local



Reuse, rather than reinvent
Harmonise policies
Agree on community best practices

Support institutions to adopt global solutions

Ease the pain with training and supporting tools



Think Global - GÉANT

Identity is a key aspect of the service delivery for the whole R&E community.

Trust is critical to ensure the uptake of services, particularly in a federated and cloud environment

e-Infrastructures and research infrastructures recognise the need to harmonise existing approaches to enable service delivery across e-Infrastructures.

Enhance collaboration within the global R&E community by meeting users' needs for T&I for networks, services and applications.



Support the needs of other strategic interests for NRENs, e-Infrastructures, ESFRI projects, Cloud, and life-long and government eID.

Enable collaboration between the R&E community and other sectors, on terms favourable to the R&E community to reduce costs.

1. Operate T&I systems for global R&E:

- Integrate national initiatives
- Develop these further in response to user requirements.

2. Harmonise deployed AAls:

- Agree on common strategies and policies
- Development roadmaps and marketing to meet user and operational needs.

3. Facilitate open global cross-sector systems for T&I:

- Use global R&E's scale to incentivise market to provide solutions suitable for our users.
- Facilitate R&E's adoption of these solutions adding additional value where necessary.

From Local to Global - T&I Infrastructures



- To enable federated access to services operated by national R&E identity federations
- In production since 2011



- To enable federated access to the network
- In production since 2004



Built on national infrastructures!

Think Global - AARC

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/>



Avoid a future in which new research collaborations
develop independent AAls

Impacts

- Create a cross-e-infrastructure 'network' for identities
- Reduce duplication of efforts in the service delivery
- Improve the penetration of federated access

Outputs

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

Very Common Scenario

- A **research community internationally distributed;**
- **Increasing number of services** need authentication and authorisation;
- A **solution** is needed:
 - But the **focus of researcher should be on that research area** and not on AAI
- There are some solutions available, but...



It would be nicer if there was also
compatibility & interoperability



Requirements Overview Available Draft Blue-Print
 User Community AAI Components Architecture

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

05-10-2015

Deliverable DJRA1.1

Contractual Date: 31-08-2015
 Actual Date: 05-10-2015
 Grant Agreement No.: 653665
 Work Package: JRA1
 Task Item: JRA1.1
 Lead Partner: EDU.eu
 Document Code: DJRA1.1
 Editors: Christos Kanellopoulos, Nicolas Lamprou, Niels van Dijk, Peter Soldaga

© 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. 853665 (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 PMART workshop series. 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 targeted interviews. These requirements are analysed here and will be provided as input for upcoming activities in AARC.

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.: 653665
 Work Package: JRA1
 Task Item: 1
 Lead Partner: EDU.eu
 Document Code: MJRA1.1
 Authors: P. Solagna (EDU.eu), Christos Kanellopoulos (GRIET), N. Lamprou (GRIET), M. Hand (KIT), M. Sale (RWTH Aachen), S. Fiedler (L3L), M. Katsanos (GARR), N. Van Dijk (SURFnet), J. Jensen (DFKI), L. Labadie (GRIET), M. Jankowski (PDS), S. Neman (Lancaster), M. Prochaska (GRIET), B. Ooms (SURFnet), B. Markovic (GARR), H. Short (CERN), U. Stevanovich (KIT)

© 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. 853665 (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 now key to fulfil the use cases of the R&E communities.

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 (RS: "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



aarc-project.eu

Requirements



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

Trust and Identity Players

GÉANT	AARC	Other R&E Projects/Groups	Policy Groups
<ul style="list-style-type: none">• Operates global T&I infras with the support of NRENs:• eduGAIN• eduroam (EU)• FaaS• Support for VOs	<ul style="list-style-type: none">• Support international collaboration• Integrated architecture• Policy harmonisation• Training• Piloting	<ul style="list-style-type: none">• EC funded projects• ESFRI projects• r-e-Infras• ORCID• Gov IDs	<ul style="list-style-type: none">• REFEDS• Kantara• IGTF• ISOC• IETF• Etc.

Act Locally

Key Role of NRENs

Backbone for all global infrastructures

NRENs exists to support their customers

NRENs exists to support their customers

NRENs services are built on standards, security and privacy

Universities and institutions that contribute to big picture

Summary

Federated Approach is the way to go
(but the technology may change)

Right time for cross infrastructures
collaboration

AARC has shown that a framework in
place facilitate collaboration

Much more awareness about AAls,
but the lack of attributes is an issue
that has to be addressed

