EGI position for a pan European identity federation for researchers

**Position paper for H2020**

Authors: Sergio Andreozzi (EGI.eu), Peter Solagna (EGI.eu)

Date: 3 December 2013

Document status: draft

Document link: …

1. Copyright notice

Copyright © Members of the EGI-InSPIRE Collaboration, 2010. See www.egi.eu for details of the EGI-InSPIRE project and the collaboration. EGI-InSPIRE (“European Grid Initiative: Integrated Sustainable Pan-European Infrastructure for Researchers in Europe”) is a project co-funded by the European Commission as an Integrated Infrastructure Initiative within the 7th Framework Programme. EGI-InSPIRE began in May 2010 and will run for 4 years. This work is licensed under the Creative Commons Attribution-Noncommercial 3.0 License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc/3.0/ or send a letter to Creative Commons, 171 Second Street, Suite 300, San Francisco, California, 94105, and USA. The work must be attributed by attaching the following reference to the copied elements: “Copyright © Members of the EGI-InSPIRE Collaboration, 2010. See www.egi.eu for details of the EGI-InSPIRE project and the collaboration”. Using this document in a way and/or for purposes not foreseen in the license, requires the prior written permission of the copyright holders. The information contained in this document represents the views of the copyright holders as of the date such views are published.

# Executive Summary

This document describes the EGI vision for a pan-European Authentication Infrastructure (AAI) that enables Single Sign On capabilities for the researchers accessing the e-Infrastructures in Europe.

The document contains the initial analysis of the objectives of an integrated European Authentication and Authorization infrastructure that can fill the gap between the different e-Infrastructures and the institutional Identity Providers supporting the user communities. The objectives are the outcome that EGI expects from a project that aims to enable a uniform AAI across Europe.

# Introduction

The European Commission has emphasized that, “as most knowledge creation and transfer uses digital means, all barriers preventing seamless online access to digital research services for collaboration, computing and accessing scientific information and to e-infrastructures must be removed by promoting a digital ERA (European Research Area)[[1]](#footnote-1).” The lack of an identity and access management strategy is the single biggest impediment to that vision as well as to a shared distributed infrastructure.

Defining digital credentials, evaluating the degree of confidence that this is associated to the related entity (also known as level of assurance) and making credentials portable across heterogeneous systems are key aspects for many entities such as data, dataset, users, groups or organisations. Various initiatives have tackled this issue in Europe but still research communities need to use different AAI systems for different infrastructures.

 An integrated pan-European AAI must allow researchers in Europe to authenticate and to be authorised to services from the major e-Infrastructures (EGI, EUDAT, GEANT/NRENs, PRACE), and it should be easy to manage and be compliant with the relevant legal aspects.

In several cases users, in their workflows, need to access services provided by resource providers in different e-infrastructures, in some case they currently have to use different credentials to access different services. This is not optimal, the user should be able to leverage existing personal, institutional, or national electronic identities to access institutional or community attribute servers as well as to gain access to distributed data and services.

Transparent Single Sign-On across services provided by the European e-Infrastructures should be available.

The authentication process should be user friendly, simple and intuitive. The user should be able to handle the authentication process with a user experience comparable to the most common Web applications.

# Overview of the current EGI AAI solution

The historical authentication framework for EGI services has been based on X.509 certificates and the related proxy certificates. Authorisation relies on attributes stored in a service called VOMS that can be retrieved by interested parties. NGIs have been integrating federated authentication systems (e.g., Moonshot, OpenID) and have a different degree of maturity. EGI is committed to the integration of other sources of authentication and to offer a simple single sign-on mechanism that may rely on the institutional identify provider or to other sources selected by the research, if matching the needed level of assurance for the service being accessed.

The main approach relies on translation of credentials from one system to another e.g., translate the credentials provided by the users’ institution into an X.509 certificate needed to access the Grid infrastructure. The most common solutions to achieve integration are: Online CAs, SLCS/MICS, myproxy servers or robot certificates. Each of them has pros and cons.

The ongoing activities for meeting the need for integrating the Grid AAI framework with the federated framework are different among the various NGIs, thus being valid only at the national level due to the lack of harmonisation across Europe.

# EGI expectations for a European AAI project

## Policy framework to enable easy use of federated identity by federations of Service Providers

In the current scenario, Identity Providers (IdP) release user credentials and attributes only to trusted service providers. A service providers who wants to serve users who are members of a particular IdP or federation of IdP, must explicitly agree with the IdP policies. While in most cases to endorse a policy or a code of conduct is a simple process that does not require too many steps or effort, in a pan-european scenario this point-to-point endorsement cannot scale. There are too many service providers and too many identity providers, this process to enable service providers would require a huge mesh of P2P interactions.

IdPs and SPs federations must agree on a policy framework, including code of conduct for service providers, that is satisfactory for both of them. A service provider, joining a SP federation (aka resource infrastructure) must acknowledge and endorse the code of conduct, as he endorse the other federation policies. In this way IdPs can release user credentials to all the SP part of the federation, without the need for additional bureaucracy. On the other side the policy framework should establish a minimum set of released attributes and operational procedures that are satisfactory for the SP federations.

Within this simplified policy framework a defined set of procedures can allow the turninig over to users the responsibility for their own attribute management as the IdPs cannot make all decisions on their behalf. In doing this then researchers have a broader set of resources at their disposal as a broader set of resources can then be integrated.

### Legal constrains

Policies should be compliant with the European and local legislations, in order to enable information sharing across countries. The project should assess the compatibility of the policy framework with the applicable lows, at least from a significant subset of countries.

### Requirements gathering

To build an uniform policy framework for the identity federations in Europe that fulfils the use cases of user communities and service providers there is the need to collect and analyse the requirements from the different actors: identity providers, user communities and service providers.

* Elicit Identity Provider (IdP) requirements and capabilities for IDM integration.
* User Community (UC) requirements in ID federations, examples are:
* Service providers requirements
	+ Resource providers requirements are the main input for this activity

The policy should be shared by the main European e-infrastructures with the objective to allow European researchers to use the same credentials to access the resources part of the different infrastructures.

## Distributed Attribute Authority services mesh (design and pilot testing)

The user identity is only one of the information needed to authorize access to services. Users are allowed to perform their work on the infrastructure based on the attributes that are associated to their identity. The AAI also has to make possible for user communities to manage the attributes of their members to group them and authorize their access to the services, and also to integrate the attributes released by the IdP to fulfil SP requirements. Users should be empowered to choose which attributes can be released to SP.

A mesh of Attribute Authority (AA) services should be provided as a service to users and SP, and be compliant with the IdP and SPs policies in order to be able to access user credentials and be considered a reliable source of information for the SP.

A uniform attribute management infrastructure will enable a higher interoperability between e-infrastructures, if not a uniform authorization system.

The project should design the structure of such mesh of services (using existing software solutions), how they are going to technically interact with the SP and with the IdP. And what are the service operations policies required for such services. There should be pilot deployment of the services with successful examples of use cases.

## Distributed Credential translation services (design and pilot testing)

As per the AA services, the credential translation services can be provided as a service by infrastructure providers and IdP to user communities. The translation services should allow users to use the same credentials with different services that use different technologies for user authentication.

As an outcome of an AAI project, the existing solutions should be evaluated and tested in pilot deployments, the pilots should also produce best practice guidelines for developers of services that use such translation services.

# References and related documents

|  |  |
| --- | --- |
| R 1 | [Advancing Technologies and Federation Communities](https://confluence.terena.org/download/attachments/30474266/2012-AAA-Study-report-final.pdf) (From EC):https://confluence.terena.org/download/attachments/30474266/2012-AAA-Study-report-final.pdf |
| R 2 | e-IRG Blue paper on data management:[*http://www.e-irg.eu/images/stories/dissemination/e-irg-blue\_paper\_on\_data\_management\_v\_final.pdf*](http://www.e-irg.eu/images/stories/dissemination/e-irg-blue_paper_on_data_management_v_final.pdf) |
| R 3 | FIM4R report on federated identity management: https://cdsweb.cern.ch/record/1442597 |
| R 4 | REFEDS answer to FIM4R paper: https://refeds.terena.org/images/4/4d/AnalysisFIM4RDocument1-0.pdf |
| R 5 |  |

1. Brussels, 17.7.2012, COM(2012) 392 final, “A Reinforced European Research Area Partnership for Excellence and Growth” [↑](#footnote-ref-1)