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: <https://documents.egi.eu/document/2049>

# Executive Summary

This document describes the EGI vision for a pan-European Authentication Infrastructure 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 really fill the gap between the different e-Infrastructures and the institutional Identity Providers supporting the user communities.

The document has been prepared as input for the relevant sessions scheduled during the ‘EGI Towards Horizon 2020 Workshop’ held in Amsterdam during December 2013, and it is supposed to be expanded with the inputs gathered during the workshop.

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.

# Introduction

Identity and access management are a critical issue in 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.

# Overview of the current EGI AAI solution

The main authentication framework for EGI services is 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.

# Use cases and objectives for an integrated authentication infrastructure

## Single Sign On (SSO) for across the e-infrastructures

Enable SSO across services provided by the European e-infrastructures. 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 institutional or national electronic identities to access institutional or community attribute servers 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.

The inputs from both user communities and service providers are critical to

## Attribute providers federation

IdP by policy or because of local laws restrictions often cannot release all the user attributes required by the service providers. User communities often collect the attributes of their members and should be able to integrate the attributes available from the IdP in order to fulfil the service providers policies. A federation of attribute providers should enforce a minimum set of requirements, e.g. the availability of the user information over time and the acceptance of a set of operational procedures.

The service providers, part of the different e-infrastructures, should define a core set of attributes that must be available to access the services.

A user should be given full visibility and control over the attributes that are needed/going to be delivered to a service. In the event that the user refuses to release some attributes, some services (based on the profiles above) may not be accessible.

## Differentiated level of assurance

The current AAI solutions are rather monolithic, the policies enforce the same minimum Level Of Assurance (LoA) for all the credentials accessing the e-infrastructures. The AAI must be flexible, enabling different LoA for different use cases, allowing service providers to choose the minimum LoA required for the IdP of the users who want to access the services and resources. The outcome of this objective should be a small set of simple profiles to classify the IdP by their LoA. This should fit with the requirements of service providers and user communities.

Several user communities need to handle a variety of credentials, for example where open access to data is a requirement, users should be able to use their social credentials to retrieve data, for usage accounting only.

## 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, examples are:

* Which are the main sources of user community ID provisioning?
* Which are the IdP policies on releasing attributes and private data?
* Do gradual release policies exist, i.e. specific circumstances mapped to specific attribute sets?
* What are IdP federation policies and requirements on operational services, operational security, e.g. incident response?
* This targets emerging and existing identity federations. Chances are that there will not be a single ID federation to integrate with.

User Community (UC) requirements in ID federations, examples are:

* What are UC policies on their role as Attribute Authority in releasing attributes, and which?
* What are UC requirements and policies on operational services, operational security, e.g. incident response?
* UCs must be considered a first class citizen as they play a key role in attribute management!

Service providers requirements, examples are:

* How do these map/fit with national/local requirements?
* Which stakeholders does EGI accept as attribute authorities? (IdPs, VOs, etc.)
* Which trust model? Hierarchical (IdP ← VO ← EGI) or threeway ( IdP ← VO ← EGI → IdP)? Or other?
* Are gradual resource access policies feasible? Which are the possible models?
* Which is the absolute, consistent minimum amount of information necessary across EGI to allow an individual access to resources?

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.

## Best practices

The previous solutions and use cases must ultimately be enabled in the users’ tools, for example scientific gateways and portals. The project or the activity delivering the previous objectives should also provide best practices and implementation advises for the developers of the user interfaces, in order to have an uniform use of the authentication framework. The contribution of the technology providers, e.g. providing solutions for the credential translation, is an added value.

# Questions and topics for the panel discussion

* Create an inclusive European identity federation that enables SSO in the different e-infrastructures
	+ Can this federation build upon the existing institutional IdP, is there the need for a catch-all service?
	+ Is it possible to have a scalable policy framework that makes possible such a huge federation?
	+ Identity migration, is the integration of a solution like ORCID advisable?
	+ What are the security risks to be taken into account?
* Implement a differentiated level of assurance
	+ Define a basic classification that can fit to most of the service
	providers
	+ What are the requirements for a differentiated level of assurance?
	+ Who should certify the IdP to 'label' them into one of the categories?
* Federation of attributes providers
	+ Can a minimum set of required attributes be defined in order to
	focus on this core set?
	+ How can user communities collaborate integrating the attribute provided by the IdPs?
	+ What kind of services are needed? Who can operate them fulfilling
	the policies?
	+ Is it possible to provide a catch all Attribute Authority service ? Or an
	attribute translation service?
* Best practices for the implementation of the SSO in the existing services
	+ How can the credentials from different IdP be integrated in a uniform way by the different resource providers
	+ What are the technical gaps?
	+ Are there open source solutions already available to address most of the use cases?

# 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 |  |