EUROPEAN MIDDLEWARE INITIATIVE

MJRA1.9 - AAI REQUIREMENTS OF DCIS

EC MILESTONE: MS34

Document identifier:	**EMI_MS34_v1.0.doc**
Date:	**30/11/2010**
Activity:	**JRA1**
Lead Partner:	**UH**
Document status:	**Final**
Document link:	**http://cdsweb.cern.ch/record/1277567?ln=en**

Delivery Slip

	Name	Partner / Activity	Date	Signature
From	John White	UH/JRA1	15/12/2010	
Approved by	PEB		15/12/2010	

Document Log

Issue	Date	Comment	Author / Partner
1			
2			
3			

Document Change Record

Issue	Item	Reason for Change
1		
2		
3		

MILESTONE REPORT

1. Background

The "AAI for DCIs Workshop" was held on September 14th 2010 during the EGI Technical Forum in Amsterdam. The agenda is available at:

https://www.egi.eu/indico/sessionDisplay.py?sessionId=11&confId=48#20100914

In order to access this event a Google search with "AAI EGI Technical Forum" will give the above page. All talks have been uploaded to the agenda page.

This workshop was timely and appropriately scheduled during the EGI Technical Forum as the event hosted a significant number of National Grid Infrastructures (NGI), research communities and ESFRI projects. The main drive for this workshop was early collaboration with the above-mentioned groups and communities and was held very early in the project schedule, in agreement with the EU, in order to provide some early responses and directions in the security area. These are needed in order to produce a first year security middleware plan for harmonization between the three stacks and also a direction for the mid-term evolution of the EMI security components.

There were approximately 40 participants in the workshop with half from EMI.

The aim of the workshop was for the EMI project to understand AAI (Authentication and Authorization Infrastructure) needs of current and future clients. This was achieved with the presentation of current AAI status and future AAI needs of a number of ESFRI projects, Grid communities and NGIs.

2. Questions

In order to prepare for this workshop the following set of questions was sent to each participating project or community.

For projects crossing national boundaries:

1. How are users currently authenticated?
    (a) Which credential(s) is/are used?
    (b) How is the user vetting done?
2. Is there a link to national identities? If so, how are different national identities leveraged?
3. Which types of resources are in use and how are users authorized?
    (a) Resources accessed through Grid technology: computing resources, storage, etc.
    (b) Resources accessed without Grid technology: computing resources, storage, etc.
    (c) Web-based resources.
4. Where does the project want to be in 5 years with regards to authentication and authorization?
5. Are your users and resource owners happy with the current AAI scheme that you use?

For NGIs:

1. How are users currently authenticated?

(a) Is there a national AAI infrastructure in place or in the process of being set up?

(b) Which credential(s) is/are used?

(c) Which policies do you have with respect to credentials? Do you support long-lived and/or short-lived credentials? Are there any preferences?

(d) How is the user vetting done?

2. Is anonymous and/or pseudonymous access to resources supported?

3. Does the NGI support virtual organizations - if so, how?

4. Where does the NGI want to be in 5 years with regards to authentication and authorization?

3. Results

The questionnaire was partially answered in most talks and the complete set of talks is available at:

https://www.egi.eu/indico/sessionDisplay.py?sessionId=11&confId=48#20100914

The outcome of the workshop is that the EMI Security area gained a better understanding of the following points. That, overall, projects use the current authentication method (mostly X.509 certificates) as it is the default method but would prefer to migrate to federated identities. Grid users do not like to manage X.509 credentials. The use of X.509 credentials within the Grid infrastructures is acknowledged for the foreseeable future.

In response to these findings, the EMI Security area has started discussions on which AAI tokens will need to be accepted and handled by the Authentication software and services such as the future Security Token Service. A more detailed summary of these points can be found at the “Current AAI report” at:

https://twiki.cern.ch/twiki/bin/view/EMI/EmiJra1T4AAI