The EMI AAI Strategy.

John White (for the EMI Security Area)

EMI INFSO-RI-261611
EMI All-Hands meeting, Nov 23rd 2010, Prague

Introduction

- **Background**
- **User Requirements.**
- **EMI current services.**
- **Required services.**
- **Rough timetable.**

Background

AAI workshop held at EGI TF, September 14th 2010.

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

Google "egi technical forum aai"

- 3 User communities:
  - Biomed, Earth Sciences, HEP
- 5 ESFRI projects
  - CLARIN, Lifewatch, ELIXIR, EuroFEL, ILL
- 2 NGIs.
  - Italy, UK.

Background

For projects crossing national boundaries:

1. How are users currently authenticated?
   1.1 Which credential(s) is/are used?
   1.2 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?
   3.1 Resources accessed through Grid technology: computing resources, storage, etc.
   3.2 Resources accessed without Grid technology: computing resources, storage, etc.
   3.3 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?

Background

For NGIs:

1. How are users currently authenticated?
   1.1 Is there a national AAI infrastructure in place or in the process of being set up?
   1.2 Which credential(s) is/are used?
   1.3 Which policies do you have with respect to credentials? Do you support long-lived and/or short-lived credentials? Are there any preferences?
   1.4 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?

General User Results

- Grid users do not want to handle credentials themselves.
- Grid users would like to obtain X.509 credentials and VOMS attributes from other credentials and vice-versa.
- Projects would like to use federated identities.
- Projects recognize that both national and international identity federations will become more important.
- User identities and actions on a Grid should be protected, anonymized.
- Projects realize that access to the majority of Grid infrastructures requires and will require in the future, X.509 credentials.

More complete report available at:
https://twiki.cern.ch/twiki/pub/EMI/EmiJra1T4Security/

“Reactions”

- **Grid users do not want to handle credentials themselves.**
- **Projects would like to use federated identities.**
- **Projects recognize that both national and international identity federations will become more important.**
  - Projects are encouraged to use whatever federated/national identity systems.
  - EMI will interface to or provide a means to obtain credentials transparently.
  - Already SLCS, TCS, (EMI STS in the future) can provide X.509

“Reactions”

- **Grid users would like to obtain X.509 credentials and VOMS attribute from other credentials and vice-versa.**
  - Security Token Service (STS), pluggable credential service.
  - Web Service interface. SAML → X.509.
  - Others later.

“Reactions”

- **Projects realize that access to the majority of Grid infrastructures requires and will require in the future, X.509 credentials.**
  - X.509 + VOMS ACs for the future.
  - Need to get federated (SAML?) attributes for use on infrastructures.
  - VOMS Attributes from Shibboleth (VASH).
  - Service between the IDP and VOMS.
  - Integration to VOMS?.

General User Results

- **User identities and actions on a Grid should be protected, anonymized.**
  - Service exists. Pseudonymity.
  - One-time identities in conjunction with VOMS-Admin.
  - Needs integration.

Timetable Estimate

- **Short-lived Credential Service**
  - In production. Integration to EMI-1 if needed.
- **Security Token Service**
  - Under design. Later than EMI-1.
- **VASH**
  - Integration into release. EMI-1.
  - Integration into VOMS. Under study. Later than EMI-1.
- **Pseudonymity**
  - Integration into release. EMI-1.