22nd EUGridPMA meeting, Prague, 11-13 May 2011

Minutes of Thursday morning sessions, 12 May
(See agenda page for presentations: http://agenda.nikhef.nl/conferenceDisplay.py?confId=1481)

Security Token Services: EMI implementation and plans - Christoph Witzig
Use cases discussed:

1) Obtain X.509 certificate (short and long lived) based on another token;
2) AAI enabled portals, portal obtains X.509 from a) MyProxy or b) a "CA";
3) AAI enabled portals for displaying and accessing Grid information (low priority);
4) STS (Example: Incoming token: SAML, Kerberos, Outgoing : X.509);
5) Use of AAI attributes in Grid services (e.g. attributes from VOMS);
6) VO registration.

Architecture of STS is presented.

Issues/questions presented for:

- Handling trust between trust domains
- Issuance of certificates – proxies

Discussion:
Jules: PRACE would be interested to interface to LDAP as Attribute Authority.

The GEMbus STS - Diego R. Lopez

Questions/comments made (for both STS sessions):

GEMbus accepts the EMI STS profile.
Christoph: timeline for next version of profile is next couple of months

Documentation available? Some information is available on the website? Also some documents are available. And GEMSTS demonstrator is available.

Teun: X.509 and SAML exists and accepted. Does DNSsec play a role? Diego: We should consider this. Christoph: we have to look at this.

How about collaboration between GEMbus and EMI? In principal the projects are collaborating, but they are addressing different use cases.

How many STSes do you want to have, e.g. one per country or one per federation that is accredited?

Use cases: authorization for GEANT services, e.g. by PRACE staff, commercial clients etc.

Is it a SLCS profile always? Diego: GEMbus yes. Christoph: in principal yes, but others should be possible too. Renewal is also part of the functionalities considered.

Data use case?

Is there interest in a profile for STS? SLCS profile has similarities. Different outputs produced. Which role can Moonshot play here?

AuthZ operations WG – David Kelsey
This is a continuation of the discussion on day one of the AA profile:
https://grid.ie/eugridpma/wiki/AA_Profile
The document is updated during the sessions. Some comments:

Assertions should not be valid for more than 24 hours. This means that the AASP is not responsible for what is done with the information after this period. For LDAP the log file provides the time a service has queried the information.

Separation of responsibilities between AASP and AA provider is not always easy to make.