Minutes 21st EUGridPMA meeting, 2011, Utrecht

Monday, January 24, sessions

Agenda (see http://agenda.nikhef.nl/conferenceDisplay.py?confId=1172 for supporting material)

09:30	Welcome & introductions (10') (Slides)	
	Introductions; agenda bashing; note takers; minutes of previous meeting;	
09:40	Round table updates (05')	
09:45	The Asia Pacific Grid PMA (30') (Slides)	Eric Yen
10:15	IGTF Risk Assessment Team report (30')	Jens Jensen
10:45	Report-out from the self-audit review teams (15')	
	please refer to https://www.eugridpma.org/review/selfaudit-review	
11:00	Coffee (30')	
11:30	EUMedGrid II Support Programme: Around the Med (30') (Slides)	Onur Temizsoylu
12:00	Self-audit I: DFN-PKI Grid CA (45') (Slides)	Reimer Karlsen-Masur
12:45	Lunch (1h15')	
14:00	Discussion: role for PMA with introduction of STS services in e-Infrastructures? (05') (Slides)	David Groep
14:05	A security Token Service at SURFnet (25') (Slides)	Remco Poortinga-van Wijnen
14:30	Authorization Operations Working Group 1/2 (1h00') (DEISA review ; document)	David Kelsey
15:30	Tea (30')	
16:30	Authorization Operations Working Group 2/2 (1h00')	David Kelsey

Welcome & Introductions – David Groep

Round Table

The Asia Pacific Grid PMA - Eric Yen

- 14 accredited CAs
- New CAs in the pipeline
- Number of certificates growing for region (due to WLCG)
- Self audit report procedure is established
- Next f2f meeting together with IGTF all hands (21-22 March, Taiwan), also OGF31 and other meetings in the same week.

- **Q**: Why is there a large numbers of revocations? **A**: Old, expired certificates, are revoked too. Discussion: it is not mandatory to revoke, status expired should be enough.

IGTF Risk Assessment Team report – Jens Jensen

- There was a problem with renegotiation in openSSL: man in the middle attack (CVE 2009 3555). Disabling the functionality or applying patches (RFC5746) did break some browsers if these were not patched.

- Communication tests, which are held from time to time (last one in August), are satisfactory – most CAs respond within 24 hours.

Report-out from the self-audit review teams

Refer to https://www.eugridpma.org/review/selfaudit-review

PolishGrid CA:
It is agreed to change status to completed.

IUCC CA:
There is no update on self audit results. Warning will be issued that status must be updated before or at Prague meeting. It is mentioned that they would consider to move to the TCS, but there has not been much activity (as known from the TCS side).

UK eScience CA:
Jens reports. They plan to migrate to a new service. New set-up (software) is prepared and new policy is written. By September new service should become operational (current root cert will expire by October 2012).

pkIRISGrid:
Still some updates need to be done (to be finished by Prague meeting).

AEGIS:
Will be present in Prague.

RDIG:
Status will be presented on Wednesday, so status will be updated then.

EUMedGrid II Support Programme: Around the Med - Onur Temizsoylu

- Follow-up project of EUMEDGrid project – a support action project – no infrastructure maintained.

- WP4: Support the consolidation of the existing EUMedGrid infrastructure. One of the tasks is to "Promote the completion of the process of creation of CAs in the MPCs": Task 4.2: Consolidation of Certification Authorities in the Mediterranean (TUBITAK-ULAKBIM, INFN, CCK, CERIST, CNRST, EUN, HIAST, JUNET, UoM)

- Request is done if September 2011 meeting of EUGridPMA can be held in Marrakech, so still in EUMedGrid II project priod. This will give (new) CAs from the Mediterranean area the possibility to attend. This must be discussed with Slovenian partner, already planned as the host for the September meeting. To be decided later in the meeting.

Self-audit I: DFN-PKI Grid CA - Reimer Karlsen-Masur

- The self-audit is based on "Guidelines for auditing Grid CAs" (v1.1) and reference material:
  IGTF-AP-Classic v4.3, Grid Certificate Profile (GFD.125) 31.3.2008, Guideline on Approved Robots (9.2.2010), and Private Key Protection Guideline (v1.1)

- Results, out of 67 auditing items:
  - 55 A's (good)
  - 9 B's (recommendation of minor change)
  - 3 C's (recommendation of major change)
  - 0 Ds (advice of must change)

- The full audit report is available for the audit reviewers

- Volunteers for review of audit report: Nuno Dias and David Groep

Discussion: role for PMA with introduction of STS services in e-Infrastructures – David Groep

- Based on EGI + M/W project develop middleware roadmap:
  On EMI roadmap is a study on 'native integration' of multiple security mechanisms, based around the Security Token Service (STS).

- Basically a STS (Security Token Service) is a source of security tokens, which are based on other tokens (so acting as a translator)
  Policies for such a service are needed too, e.g. is a new profile needed? This is the reason to discuss this within the EUGridPMA.

- Jens Jensen reports on his experience with a STS based service.
  Experience with a genomics project, led by Constellation Technologies, where different companies did want to work together: www.pistoiaalliance.org. They were looking for a trusted environment and investigated a service based on STS in the MS environment.

Lunch

A security Token Service at SURFnet - Remco Poortinga-van Wijnen

- Based on two use cases.

- Addressed with SOAP technology.
- What next? Small test environment will be set up with two interacting web services.
- Jens: his work was based on WS-Passive, so a different approach.
- Jens is interested in interoperability tests between different STS facilities., however currently there is no SURFnet environment available.

Authorization Operations Working Group – David Kelsey

Discussion of AA profile

Feedback given by DEISA is presented, a comparison between the AA profile and the DEISA user administration policies (covering attributes used for authorization like in VOMS).

- One important difference is how attributes are used; in DEISA assertions are not signed (it is a directory lookup) and lifetime is not explicitly limited.

Discussion of updates made by David Groep and David Kelsey some days before the meeting (from revision 22 to 23***):*** https://grid.ie/eugridpma/wiki/AA_Profile?action=diff

- What requirement is there for the lifetime of an attribute assertion? Should not be longer than the assertion about the identity to which it is tied?
- Is an attribute assertion always tied directly to the identity to which it relates?

- Must the namespace in which the AA operates be defined? So, restrict it to the IGTF namespace (authentication scheme)?

- A long discussion on the definition for “attribute assertion” (section 2 of document) follows:
  “ An attribute assertion is a statement that a subject is the holder of a specific attribute”
  “attribute assertion” also should cover a database lookup, e.g. if information from an attribute DB is replicated to another repository. What should be understood by “attribute assertion” is expanded, so to cover all use cases of attributes.

- Definition of AASP is refined (section 2).

- Relying Party obligations section is updated (section 11)

- AASP naming section (13) is discussed
  What name scheme to use? What is the role of the name? For discovery service?
  Persistent names needed? No.
  This section needs more thinking.

- New updated revision of AA is uploaded to the wiki.