32nd EUGridPMA Meeting - Poznan - Day 1 - Monday 8 Sep 2014

Present in room: David Groep, Bob Cowles, Dave Kelsey, Willy Weisz, Scott Rea, Vladimir Dimitrov, Emanouil Atanassov, Marc Turpin, Paweł Wolniewicz

Remote on Vidyo: Addel-ur-Rehman, Anders Waananen, Heidar Saadatmand Javan, Kaspars Krampis, Lidija Miolsavljevic, Miroslav Dobrucky, Roberto Cecchini, Ronald Osure

Meeting started at 09:30.

1. DavidG welcomed all, thanked Pawel our local host, and showed the agenda. No changes required.

2. Roundtable. Full introductions (local and remote) were made.

DavidG - also now represents TCS.

ScottR - here as vice-chair of TAGPMA but also DigiCert.

Anders has some news - consumers of NorduGrid CA gradually moving to TCS, but it has not been working in Denmark since start of the year - an acknowledged bug in MS Server 2012 patch level 2 - awaiting fix from MicroSoft. This is running ADFS as the backend IdP. DavidG says NL does have these issues.

3. TAGPMA update - Scott Rea - see slides

Next meeting is Oct 20-22 2014 in Chile, collocated with CARLA conference.

Experiment of Latin America chapter is working well.
ESnet has retired. SENAMHI in Peru is suspended.
CIDETYS/UTP Panama have not yet participated - suspended.

Current work includes RPS and two LoAs (ASPEN and BIRCH) - more on this later in this meeting.

4. Kaspars - Self Audit status

See https://wiki.eugridpma.org/Members/SelfAuditStatus

Things have not progressed much since the Tartu meeting, probably because of the holiday season and H2020 proposal preparation.

Kaspars takes us all through the current status and points out where peer reviews are still needed.

Armenia - ask them to start again - last audit was two years ago.

5. CA Update - AustrianGrid - Willy Weisz - see slides.

Aim of new developments is to improve the turn-around for subscriber requests, using an online CA with an HSM.

Wants to go operational soon, so asking for a fast review.

Discussion about use-cases or problems encountered with multiple email-addresses in alternativeSubjectNames - nothing to report here.

Note - code-signing with IGTF CAs has been made very difficult by Oracle/Java. Microsoft likely to make some changes whereby the code-signing CA has to be a separate CA. Code signing under the new TCS will work for Microsoft as well (pilot starts in a couple of months).

Subscribers from the old CA can request to keep their old DN but they will be recommended to change to the new naming scheme.

The new CA has a new name of course.

DavidG reports an ongoing campaign to get RP VOMS servers to only check subject DN and not the issuer - a configuration choice which is not always adhered to.

Discussed the processes whereby institute nominated people who can requests server/service certs are handled - a database on front-end online service. Noted that it would be good to log all changes to this database. RA usually knows these people too so could notice requests from new people.

Discussion about the security of the front-end system - if this is compromised rogue CSRs could be inserted for signature. There were suggestions of signing and storing all requests in a remote logging

system which should then be checked before signing. But as ever the weak link is always the RA's machine.

Reviewers for Austria: ScottR and DavidG.

Aiming for new CA during November for the end of November release.

Recommendation from Scott and others to generate the keys outside of the HSM and do an import. This avoids vendor lock-in.

—— coffee break at 11:35 ——

6. Start again at 12 noon - CA Update - Self Audit Bulgarian Academic CA
See slides. Vladimir Dimitriov.

Self-audit done last week. One D score - CP/CPS will be changed. Also to fix C scores. CA cert expires in Feb 2017 - they plan to re-key at east 13 months before that. Looking for input and advice from others who have already done this.

The CA has a choice - either re-key with 4096 bits or issue new certificate with extended life with the existing 2048 bits key.

Reviewers for Bulgaria: Pawel and DaveK.

—— break for lunch and tour around PSNC at 12:30 ——

Meeting restarts at 14:30

7. Topic - naming of robots - DavidG introduces - see slides

Based on recent email questions from Scott Rea. DavidG shows the current requirements. Then shows pros and cons of also allowing FQDN. Scott also goes through today's input from Jens J by email.

Text expressing a new allowed form of commonName subject DN based on FQDN. See new Robot Guidelines (V1.2) for the exact text.

8. Planning for AAI in future - AARC - David Groep - see slides
A Consortium and a project proposal to H2020 - submitted on 29 August 2014.
DavidG presents the aims and plans of the project.

This links in well to separation out of the IGTF LoA requirements and plans for IGTF in 10 years.

——————— coffee break

9. Guidelines for Online CAs

DavidG shows the current wiki page - see document linked to the agenda.
He also reminds us of the Hungarian interesting Raspberry Pi design (shown at Abingdon F2F in Jan 2014). We looked at the document in detail.

We made changes to the document, including recommendation that Root CAs should not be online. Reminder that we have to have the intermediate CAs in the trust anchor distribution, because of the behaviour of OpenSSL. Lots of detailed discussion resulted in a new version of the document.

One issue remains - “where to store the activation data”. Apart from that all are happy that the document is finished.

Meeting ends at 17:35 for the day.