Category: meeting minutes
Status: DRAFT
Document: minutes-eugridpma19-20100420-davidg.docx
Editor: davidg
Last updated: Thu, 22 April 2010

Minutes 19th EUGridPMA meeting

Abstract
Minutes of the 19th EUGridPMA meeting, held in Riga, Latvia and gratiously hosted by Edgars Znots, SigmaNet, and the Institute for Mathematics and Computer Science of the University of Riga.

This meeting was impaired by the ash cloud from Eyjafjallajökull and the resulting restrictions on air traffic.

Table of Contents

1 Preamble

The 19th EUGridPMA was affected by a Europe-wide air traffic ban, which resulted in a low in-person attendance and increased reliance on teleconferencing. Although most urgent topics could well be discussed this way, all open discussions were postponed to the next meeting (Zagreb, September).
The agenda at http://agenda.nikhef.nl/conferenceDisplay.py?confId=1027 reflects the topics discussed, although exact timings differ. Also all presentations and the document discussed are available via http://www.eugridpma.org/meetings/2010-04/.

2 Monday, April 19, 2010

2.1 Attendees

In-person: Edgars Znots (SigmaNet), Christos Kanellopoulos (HellasGrid), Alessandro Usai (SWITCH), David Groep (DutchGrid and EGEE, chair and note taker)

Via tele-presence (for at least part of the day): Christos Triantafyllidis, Dave Kelsey, David O'Callaghan, Javier Masa, Miroslav Dobrucky, Yury Ziamtsou, Alice de Bignicourt, Pawel Wolniewicz, Majid Arabgol, Thijs Kinkhorst, Reimer Karlsen-Masur, Nuno Dias, Willy Weisz, Feyza Eryol, Milan Sova, Alexey Tselishchev, Ursula Epting, Daniel Garcia, Adeel-Ur-Rehman, Sergey Stirenlo.

2.2 Welcome

Notetaker: David Groep

2.3 APGridPMA update

Deferred since Jinny Chien is not yet on-line

2.4 TAGPMA (Dave Kelsey)

Present the updates from the TAGPMA. The CI-Logon project is advancing well and is discussing the identity vetting details with InCommon. The InCommon Silver level is inspired by NIST SP800-63 level 2 but has also differences. The process of remote vetting – and whether it is sufficient in case of third-party vetting – needs to be considered.
Changing the wording in the InCommon Silver requirements is possible but not likely.

The Optical Networking Initiative has applied for membership, but since this application is very recent it is unclear whether they apply as an authority or a relying-party member.
Concern is expressed by DG about fixed term projects and initiatives, and how they meet the need for long-term stable operations in the trust fabric.

2.5 Risk Assessment Team report (David Groep)

There have been no new incidents or vulnerabilities reported since the January report. Also, no response challenges have been run.

The use of more secure hash algorithms, in particular SHA2 replacing SHA1, is not critical, but relying parties (and thus also their upstream software providers) should realize **that *after January, 2012* the CAs *may* start issuing certificates based on SHA2 hash algorithms**.

So: post January 2012, certificates based on SHA-2 hashes will be used in production by CAs.

2.6 Self-audit reviews (based on https://www.eugridpma.org/review/selfaudit-review)

AEGIS	Alice: no updates to report
SRCE	Edgars: no updates to report

ArmeSFO	David OC: peer-review has been completed, but still has to be sent to the CA (Arsen)
pkIRISGrid	David OC: the review has not yet started
UKeScience	No updates
LIP CA	A new CP/CPS has been sent by Jorge, Alice and Daniel still need to comment on this latest version
IUCC	There has been no observable activity from Aviyah, but then also there has been no follow up from the reviewers (ChristosK). It should be in progress.

2.7 HellasGrid CP/CPS updates (Christos Kanellopoulos)

The new CP/CPS proposal for HellasGrid was presented. The new version implements two new features:

- Robot certificates, as per the Guidelines for Approved Robots. Here, the COLON (":") character will be used to terminate the string "Robot" in the CN. Any software issues are expected to be resolved at the software layer, not by digressing from the recommendation.

- Authentication can proceed via notarized documents supported by a F2F meeting over a video link. This mimics the already approve processes implemented in Brazil and Turkey.

These proposed changes **are agreed as per consensus in the meeting** (all local plus all active remote participants agreed). The new CP/CPS will be send to the list shortly. Following that, there will be a two-week period in which objections can be raised, following which tacit consent will endorse these changes.

In addition, the following statistics regarding the HellasGrid CA: ~200 valid users, ~180 hosts.

2.8 SWITCH SLCS CA Self-Audit (Alessandro Usai)

The main information is contained in the slide desk that was presented on-line and is available to PMA members on the self-audit status overview.

The SLCS CA has issued 2544 certificates as of April 19th (approx. 20 users). The review is based on GFD.I-169. Commentary related to the slides:

- The agreements with the institutions (IdPs) are going to be re-signed and contain more guidance and best practices, or alternatively auditability requirements . Not having these new agreements in place causes some of the current B marking in the review

- (#13) All RAs have a long-term QuoVadis certificate

- (#13) revocation guidelines will be improved slightly, but already today the advertised client tool will ensure that the private key protections are set to safe defaults and the keys are protected also by operating system mechanisms

- (#15) the check on key length is currently client-side only, but the next software release will also have the same checks on the server end

- (#20) the SLCS Administrators are registered on a list maintained by the CA, and in additional are also personally known to the CA staff

- (#22) in the GFD given template, point 53 refers to TACAR in our case, so this point should be graded "A" as the SWITCH SLCS CA is already in TACAR

It is also clear that the review was done against the *classic* profile, not the SLCS profile. This is triggered by the GFD, which has only the classic profile as an example audit guideline. If the CA

would have been evaluated against SLCS, it is likely that many of the identity-vetting and IdP related points would have scored higher, and many of the B/C ratings would have been A's.

In the new setup, the end IdPs will either have to explicitly abide by the best practices established by the SWITCH SLCS CA, or alternatively be auditable by SWITCH. Likely, if most IdPs can live with the best-practice guidelines, a few of the remaining IdPs could actually get an audit. If the balance shifts the other way, a new procedure should be sought.

It is agreed that a SCLS (and MICS) self-audit template needs to be produced.

No changes to the CP/CPS are needed, but since the SWITCH SLCS CA accreditation was based also on the agreement document with the IdP, the new version of this document will be produced and peer-reviewed by the assignees.

2.9 The TERENA eScience SSL Certificate Service (Milan Sova)

Slides at http://agenda.nikhef.nl/materialDisplay.py?contribId=7&materialId=slides&confId=1027. Comments to the slides:

- (#3) The CA Operator is Comodo, the Members are TERENA members that will perform the RA functionality, and the Subscribers are institutions. This is like in the eScience Personal CA
- (#4) The structre and path of the root of trust is complex, due to the cross-signing with the AddTrust root that Comodo acquired. . . . . this will be changed in the CP/CPS text, where the longer chain will be described. This longer chain is needed also for Grid applications, since services will be visited by end-users with browsers.
- (#6) "Requestor" is the original requestor of the actual certificate
- (#7) All relation
- ns described in the CP/CPS are governed by legal contracts
- (#8) The Admin portal is operated by the NREN. Each site administrator should set up procedures to approve machine administrators as the site admins assume responsibility by approving any certificate request in their domain.

  David OC: currently, the 'plain' SSL TCS CA supports wild-card certificates. Will these also be supported in the eScience SSL? Milan: No, there will not be wild-card support in the eScience SSL CA, and it will use a different issuing CA cert so that reliance will not be mixed.
- (#9) The OU component is not normally used. The CN component causes an overlap with the eScience Personal CA, but in that CA the CN will always contain at least one SPACE character (separating the readable name from the unique identifier, whereas in the SSL case there will NOT be any space. Thus, their namespaces will not clash
- (#11) the URLs listed in the CP/CPS are at times wrong and will be fixed (Reimer)
- (#12) the OID of the Comodo policy resolves to a non-public document. The document does exist, and this referfence was also accepted for the eScience Personal CA

Both Roberto and Reimer have commented on the fact that the scope of the eScience SSL CA may cause overlapping constituencies in some countries. This issue will need to be resolved at the national level. The aim of the clauses in the Charter and APs was to keep the PMA scalable and not have too many (short-lived) CAs. So a super-national CA is actually better in this respect. Since

at least one national CA will withdraw after this one is accredited, the intent of the clause is satisfied. Any further handling is a national matter. If any reconciliation is needed, this will be dealt with in the usual way by the PMA.

A URL pointing to the CA cert should be made available. Since this is currently not there, the format is irrelevant. TACAR could be this reference point.

Representation: for the coming time, Milan will represent the eScience SSL CA on the PMA, on behalf (again) of the TCS PMA.

Time line: (i) by April 25rd, a new CP/CPS will be sent to the list incorporating the response to Reimer's comments, (ii) the certificate chain will be sent to DG for inclusion in the IGTF Common Source. The reviewers agree that the CA is ready for accreditation once the listed comments are taken care of.

Decision: a new CP/CPS will be sent to the list incorporating the comments, and is will be deemed accredited by tacit consent unless objections are raised within two weeks.

2.10 Trust anchors as part of the operating system distribution

Following suggestions from Anders Waananen, it is to be considered if distributing the trust anchors as part of the operating system distributions, as part of the 'contributed packages' schemes that some of the open source OS distributions today support.

Several arguments in favour and against were raised:

- It would facilitate installation of trust where trust exists, but whether the distribution itself can be trusted is then unclear, since the source may not be trusted or have an unclear process. Also the way packages are signed might be too lax. However, if this signing process follows the rest of the OS distribution, the 'WebTrusty' packages suffer from the same lack of trustworthiness.

- The IGTF anyway does not have real control over any form of downstream packaging, so it could be done by unknown third parties even today. At least if the IGTF endorses a packager and this is known, no other packager could replace it – thus improving trust and reliability

- At least for the Debian GNU/Linux OS, maintainers of contributed packages are vetted.

- Latency for updates may be longer that is advisable from a security point of view. Thus, if they get included any updates should be classed as 'security patches' and be pushed through a quick path.

In summary, it is quite doable but not currently time critical.

The meeting concludes that

- The base-line attitude of the EUGridPMA is positive

- More background is needed on the Fedora and Debian processes (since these distributions are the ones currently targeted)

- It will not replace the IGTF Distribution in any way

2.11 GFD125 Compliance Test Suite (David O'Callaghan)

- The number of provisions evaluated is now more complete. However, since some checks require on-line verification or a comparison between several trust anchors, the current version will merely flag such checks to the user
- A Nagios feed is in progress
- By trawling the Grid information system in EGEE (BDII), a set of services was obtained and their certificates retrieved. This gives a good sample of certificates for testing.
- A journal paper is in preparation and a poster presented to the EGEE User Forum 5

Unrelated to this, David Groep strongly encourages CAs to actually look at the Nagios status today and act on any unavailability and CRL expirations in a timely fashion, i.e., before they happen.

3 Tuesday, April 20, 2010

3.1 Attendance

In-person: Christos Kanellopoulos, Alessandro Usai, Edgars Znots, David Groep (Chair, note taker)

Tele-presence at 0700 UTC: Feyza, Usman, Alice, David OC, Miroslav, DaveK, Adeel, Eygene, Cosmin, ChristosT, Milan, Javi, Nuno, Ursula, *and others that joined at a later time*.

3.2 Self-audit of the PK-Grid CA (Usman)

The presentation is attached to the agenda pages.

This is actually the 2nd self-audit, and the evaluation shows that re-reviewing after implementing the changes in CP/CPS version 1.1.3.0 results in a audit sheet with almost exclusively A's.

Peer-reviewers for this one will be Ursula Epting and David Groep.

3.3 Self-audit of the RDIG (Russian) CA (Eygene)

The presentation of the self-audit is attached to the agenda page. The presentation touches on most of the relevant points, but fails to follow the structure of GFD-I.169 and therefore lack most of the critical data.

Slide #4: the kidsn of ID used include institutional IDs. This is not a government ID but does contain a photograph. It is in that respect similar to the practices of, e.g., the UK eScience CA, and is also acceptable by the PMA.

Decision: **in three weeks, by May 14th, Eygene will produce a self-audit in the GFD-I.169 format and use the grading system described against the classic profile check list.** This check list is included in the GFD itself.

Peer reviewers will be Jens Jensen (already agreed) and Christos Kanellopoulos.

3.4 SEE-GRID and the EGI Catch-All CA (Christos Kanellopoulos)

The SEE-GRID CA was originally linked to the project of the same name, providing CA services as a catch-all for all countries in the region. From May 1st onwards GRNET, the operator of the SEE-GRID CA, will provide also catch-all services for the EGI.eu organization (EGI is the European Grid Initiative), for those persons and systems that belong to or are affiliated with EGI.eu but who do not yet have a CA service available to them nationally or through other agreements.

To support the EGI.eu catch-all CA, the SEE-GRID CA will be used and thus its target constituency enlarged. Catch-all subscribers of the current EGEE catch-all CA, which has been run by CNRS since the very inception of Grid in Europe and been in operation since 2001, will be migrated to the new EGI.eu catch-all with the consent and endorsement of Alice. The CP/CPS of the GRID2-FR (CNRS) CA currently acting as the catch-all for EGEE will then also be updated and re-scope its constituency to France only. At the moment, only a few (3-5) subscribers are affected.

The new CP/references CPS for the SEE-GRID CA has been sent to the list on April 20th, 2010 by Christos Kanellopoulos. It will add a new namespace "/DC=eu/DC=egi/…" to the list of namespaces. This namespace is available and the delegation by the egi.eu domain owners OK.

A small (2 months) overlap period will be provided, where users can still renew at the GRID2-FR CA, until ultimately July 1st. Meanwhile, the accreditation process should complete and the new CA distributed.

The changes to the CP/CPS will be reviewers by DavidG and Dave Kelsey. Others should send any issues to the list within a two-week period. Once the reviewers are OK and there are no

outstanding issues, all changes will be approved by tacit consent and the new CP/CPS can become operational.

In a related activity, catch-all services for the Mediterranean (in the context of the new project lead by ULAKBIM) will continue to be provided by INFN. In particular, this affects Algeria, Tunesia, Egypt and Syria. There is no update on any progress from HIAST (Syria) to pursue their own accreditation. Thus, the application from HIATS will remain pending as is.

3.5 New directions in TACAR (Christian Gijtenbeek and Licia Florio)

(slides will be made available later, see also demo at https://repos.tacar.org/)

New functional requirements for TACAR could no longer be incorporated in the existing portal, so the entire software was revised and re-implemented to streamline the process.

Comments to the slides

- The sign-in to the TACAR portal for CAs is actually *not* an authentication step, but just a means to get most rogue people out. The actual authentication of any enrolment or chang is dones by the signed email (PGP) that will be sent to the TACAR Administrators later in the process.
- Some of the URLs are needed for the PRQP support which is now implemented in TACAR
- The TACAR and Group administrators use a webSSO system, which can be linked to any federation. TERENA can provide some catch-all services for those administrators that are not a member of a recognized federation (like the APGridPMA and TAGPMA people)
- The actual security model for TACAR itself (securing changes and enrolment) does not change, since this still depends on the signed email. The sign-in just facilitates the process. Maybe in the future some checks can be automated (Milan).
- Every action on TACAR is extensively logged
- TACAR is open to (obviously) the whole TERENA constituency, as well as to the IGTF members. The new portal does not change that, not does it change the TACAR policy as such.

The ongoing discussion of PGP vs. S/MIME with X.509 is not definitively resolved, but since it is not urgent, the current work will continue to use PGP. The focus of effort is on the new portal.

3.6 Accreditation Process guidelines (David Groep)

The current process is ill-described, dates from 2004 when we were just few people, and generally tends to confuse people and results in delays and mailbox pollution.

The new document describes also the membership gaining process, which is also relevant for relying parties. Thus the title needs to change. Since the EUGridPMA does not have another document that describes the RP membership process, thius doc is the best place to do it now (changes to the Charter are ‘expensive’).

A new document has been posted to the agenda page, drafted by DG, that describes the actual current process and gives guidance on what to do at which stage. It also adds a section on the CP/CPS change review process, codifying the current best practice.

Adding the self-audit process is proposed and accepted. In brief:

- Every 2 years
- Based on the GFD-I.169 template
- Needs to be presented to the PMA meeting
- Two reviewers
- Convergence on the results, like for initial authentication (including reconciliation and interventions).

DavidG will add a section to the document describing the self-audit process and circulate it to the list for final comments (done on April 21th, see http://www.eugridpma.org/temporary/EUGridPMA-accreditation-20100420-2-0-1.pdf for the latest version circulated then). Comments on the list are invited.

Other items:

- Authorities will only become members after inclusion of one trust anchors in the distribution (not on accreditation itself)
- The TAGPMA process may have some interesting text for a subsequent iteration
- For accreditation, the self-audit spreadsheet would provide a good template as well.
- The DC naming is not a matter of this document, but for the IGTF and APs
- For changes to the CP/CPS, only consider *material* changes, not patching typos.

Based on this consensus, the document will be circulated on the list. After resolving all issues raised there, is can be approved by consent after a two-week period.

3.7 Next meetings

The 20th EUGridPMA meeting will be held in **Zagreb, September 20-22nd, 2010.**

See http://agenda.nikhef.nl/materialDisplay.py?contribId=19&materialId=slides&confId=1027 for the presentation of the city and the wonderful sights in the city. You're all invited and expected to be there in person!

On **October 4-6**, Alan Sill and the TAGPMA organize celebrate 5 years of TAGPMA and IGTF in a authentic Texan setting.

Subsequent meeting:

- January 24-26, 2011 in Seville (tbc), gratiously hosted by redIRIS
- For the May 2011 meeting, you're invited to consider hosting it, preferably in a location that is reachable by air (but a emergency way out by land might be nice as well).
- The September 2011 meeting will be held in Ljubljana, Slovenia, hosted by the IJS and the SiGNET CA.