18th EUGridPMA minutes

Location: Dublin, IE

Note-taker: Christos Triantafyllidis

Most of the presentations are available at the agenda site

Table of Contents

Updates from the APGridPMA (Eric Yen)

APGridPMA consists of 14 Accredited CAs and 2 planning ones. It has coverage over 9 countries by CAs and over 7 countries via RAs (one new member country since last report).

APGridPMA has done some statistics on the number of issued certificates where since last report there was a 45.5% growth in the user certificates and 36.3% growth in the host ones. This growth is also result of the IHEP CA, which didn't respond with statistics the first time.

The last F2F meeting was held on 16th of December 2009 and the next one on the 8th of March in Taipei. The group is welcome to join the meeting.

Updates from the TAGPMA (Roger Impey)

TAGPMA consists of 15 accredited CAs, 2 pending, 2 proposed and 5 relying parties. The last F2F meeting was held in Banff, which actually became the first IGTF "All Hands".

The next 2 planned meetings are in Peru (end of May) and at Texas (beginning of October).

Roger proposed to have a new IGTF "All hands" in plans.

TAGPMA also has a Video Conference Call every 2 weeks that is open for everyone to join. The next one is at Jan 27th.

RAT report (Jens Jensen)

Jens first defined the role of the RAT where an new action has been added to "report to the PMAs". Jens has taken over the RAT chair on October.

The last 6 months report followed covering a number of issues:

apache mod_ssl (YATMCP)

This is an issue first appeared in June 2009 with the number of the CAs in the IGTF bundle. This is probably not an IGTF issue. RAT considered issuing s statement on this but it didn't.

EC(DSA) and MD5 audit

The audit was done on August 2009 via a survey and revealed problems in the communication.

NUL char
This is a middleware problem.

Communication test (1)
RAT has done a test on the communication channels in August in order to find out if it is possible to have one day response. 74 CAs replied within 24 hours. From the 20 that didn't report, six responded after a quick prod. In the end all responded.

Communication test (2)
RAT has done another test on the communication channels in November. The situation was clearly better as all but two CAs responded immediately.

TLS renegotiation
In November another middleware problem appeared with the TLS renegotiation. Globus had some good announcements that this wasn't seen by all and that this wasn't specifically a Globus issue.

This issue was not in RATs context. Jens is going to return on this in a later presentation.

Questions
A question that was raised was if there any opinions on how to improve the situation. Jens's response was that this depends on the case.

What is the supposed response time?

1 business day but some response needs some additional time (i.e. to check for MD5 signatures)

Self-Audits

BaltiGrid
Hardi mentioned that there is an issue with the CRL v2 extensions. In specific there are no PMA/IGTF suggestions for the CRLs. The group concluded that including just the serial number is sufficient.

NIIF
ChristosT has started the audit. In the beginning asked for the self-audit documents but at that time the CA manager was unavailable (not received yet). Next started the auditing based on the latest CP/CPS documents available at the CA's website. A number of issues were found most of them about things that are stated in other sections within the documents or not stated at all. The items about the CP/CPS structure (it is RFC 2527) and the HSM certification (it is FIPS 140-1 level 3) were rated as B, as they are not OK but no actions are required by the CA at the moment. The detailed audit will be contacted to the CA (either directly or via the PMA list) as the CA representative was not attending the meeting.

PK-Grid CA
There is an update on the CP/CPS not reviewed it yet.

PolishGrid CA
There is an update on the CP/CPS not reviewed it yet.

CERN CA
Both Feyza and Mike reported everything is ok. This is the first CA that has completed the audit procedure!

IUCC CA
There is no new version from CA's side. Peer auditors are requested to ping the CA.

LIP CA
The CA is still writing the CP/CPS. Additional time will be required for the actual implementation.

UK e-Science CA
This is in the implementation phase.

Possible new CAs
There was a discussion regarding the new CAs that have expressed interest in the past.

Bosnia and Herzegovina
There are no news from the CA's contacts. The SEE-GRID CA currently covers this country.

EUMedGrid
Italy still issues certificates for the project. David asked if INFN's CA could keep issuing them till they setup their CA. Roberto replied that this is not an issue.

Terena e-Science Personal CA (Jan Meijer)
Jan first presented tha MICS CA model and how the TCS fits to this profile as a "shared" MICS CA. Shared means that there is no a single federation/portal that accesses the CA but each NREN can access the CA via its federation/portal or any collaboration between them. The current service provider is Comodo.

The TCS is using a "delegated responsibility" model based on agreements. Each NREN is responsible for its Subscribers and each Subscriber is responsible for its users.

The Subscriber does identity Vetting. If a face-to-face meeting with a photo-id has took place during the vetting process a special eduPersonEntitlement attribute value is added to the Subscriber's IdP.

The DNs will be persistently unique and including an Identifier that uniquely and persistently represents the user in the IdP of the subscriber will ensure this.

NREN, Subscriber or the user can ask revocation of any of their certificates.

Regarding IdP data quality, TCS CA has a list of requirements for the IdPs this list will be enforced by the signature and the acceptance of the Subscriber Agreement.

There will be no self-audits but the CA backend (Comodo) will be audited as a part of WebTrust audit. TERENA has asked Comodo to do audits on the issuing process similar to WebTrust but there is no response yet.

Finaly David Groep presented a demo from the NIKHEF side where he requested for a certificate, he received it and revoked it (revocation doesn't work in the test instance)

Questions

Why TERENA is using an external company if they are going to do all the hard bit (identity vetting and IdPs). The profit from using an external company is the existence in the root repositories (WebTrust)

Will a portal be provided to inexperienced NRENs? The confusa portal is open source and available. Both training and a working portal will be provided by experienced NRENs.

Is there any plan for non-EU countries? No. This is out of the scope of TERENA.

Is there a reason to have a PMA in Europe after the accreditation of this CA? The TCS is a candidate for accreditation under the MICS profile not as a replacement PMA.

Is there any transition plan for NRENs who will join the e-Science CAs? Not all NRENs that asked/paid for the personal CA are going to use it for e-Science. The transition is not an TCS issue, NRENs should work with the grid communities within the country.

This will lead to have 2 CAs (the former national and the TCS) covering the same communities. Won't this confuse the users? The common practice will be to keep the former CAs for the communities that are not covered by the federated CA (TCS) and as the federated on will cover more users push them to the federated one.

Is it required to have to have the same portal for e-Science and the standard ones? No. Each CA can have its own portal.

Where is the CA (backend) located? It is in USA.

Is this in the contract? Yes it is.

Personal data are kept in USA? No they are kept in Comodo UK.

Who is responsible to release information in case of an incident? This is the NREN CSIRTs but they are not going to release such information. Classic CAs does not require this too.

Does the PMA has a way to react on possible issues (i.e. remove a NREN)? This can be done via the policy files. TCS is also able to remove/suspend NRENs.

Is there an agreement between users and subscribers? Yes there's going to be one.

Can anyone receive a TCS certificate as far as he/she is listed to the IdP and vetted via F2F? (i.e. the person which is sweeping the floor)? In principal yes. NREN or subscribers can limit who has access according to their policies. IdPs are responsible to keep their record quality.

Will the limited (or no) knowledge of the audit procedure be an issue for the privacy laws for each member? This is a national issue. A country with "crazy" privacy laws my not be able to join the e-Science CA.

There are no details on how the IdM is secured because the effort to do so is high for both IdPs and the CA. This is only required in there are suspects that something is not working well with this IdP.

Is it necessary to have a federation? No. The word federation is not mentioned in any document.

A possible issue with the uniqueness of the DNs: What about re-cycling the DNs if the IdP record is lost (removed due to inactivity)? This should be fixed.

The MICS profile doesn't require the OID of the CA policy in the end entity certificates (as does it is at the Classic Profile)?

DavidG: Probably a "bug" at the MICS profile.

Milan: We should probably remove it from classic profile too.

In a later session the group concluded to remove it from classic too.

Can the portal run on non-NREN institution? This is a national issue

Is there a test CA service up for API testing? No this is the reason we are putting the "TEST" part in the DNs. All tests are done on the production CA. The API to talk to the Comodo CA is only available to the clients of the TCS CA.

The CA was accredited but with 3 changes to be implemented before the begging of its operations:

- In 3.1.5 add the line about non-issuance from the MICS profile

- Add to IdP security requirement for "best current practice"

- Address textual subscriber vs. requestor changes

TERENA TCS SSL CA for host certificates (Milan Sova)

The presentation is the same as last meeting with an update to the "current state" thus there no need for re-presentation. The missing part was the reviewers of the CA. Roberto, Reimer and Jens volunteered for it.

The issue with the OID of the CA's policy in the end-entity certificates re-appeared. The group concluded that the OID of the profile under which the CA is accredited is the only one required.

Questions

Does the OID in the end entity certificates point to the profile or a specific version of it? It points to the profile

Doesn't that mean that the CA should implement all profile changes immediately? We could have specific version, after all the profile versions are not changing that frequent.

CA Self-audit: pkIRISGrid (Javi Masa)

In depth presentation is available at the agenda.

Javi asked how does a CA audit all the RAs?

This is no requirement to audit all of them every time. It can audit a subset of them. It can audit all the certificates that were signed a specific date (as WebTrust does).

A discussion was raised on the re-key period without F2F meeting. Why is it 5 years?

It needed to be something between "on every re-key" and "never". Audit-able identification (which is what the profile requires) doesn't necessarily mean to go through the identity vetting procedure.

Jens and DavidOC have been assigned as the peer-auditors.

Questions

Have you implemented the checks that RAT proposes for new requests at your software? No, we haven't done that yet.

CA Update: ArmeSFo (Arsen Hayrapetyan)

Arsen presented the self-audit via the videoconference. The details are available at the presentation.

There were no questions regarding the audit.

Jens had already volunteered for the peer audit and has done an on-site audit.

Private Key Protection: incorporation the Classic Authentication Profile (David Groep)

DavidG proposes the changes marked at:

http://agenda.nikhef.nl/getFile.py/access?contribId=10&resId=2&materialId=0&confId=914

in order to incorporate the Guidelines on Private Key Protection to the profile. Jens agreed but asked to mention clearly that the document refer to the latest version of the Guidelines document. The OID of the document has been moved to references for clarity.

The CA's CP/CPS OID requirement in the policy identifiers was discussed once more. Is it required? Relying parties doesn't seem to need it. The group decided to make it optional. The required OID is the one that points to the accreditation profile and not the one that points the CP/CPS.

In the Classic Profile document the identification section was missing and added (similar sections already exist in both MICS and SLCS profiles).

This resulted the 4.3 version of the document and APGridPMA and TAGPMA are invited to endorse this new version of the profile.

Self-audit: RDIG CA (none!)

First item in the agenda is the self-audit of RDIG CA. No representative from RDIG CA is at the meeting or the videoconference. This CA has failed both on presenting a self-audit and on appearing for too long. There are concerns on how to continue. Milan proposes to send an email and see what will happen. The conclusion was that the CA MUST present a self-audit during the next meeting (Riga) and send the written self-audit report to the chair for assigning reviewers before the end of February.

Self-audit: SRCE (Emir Imamagic)

Emir presented the self-audit report (details at the presentation at the agenda page). Once more in practice the CA is operating fine but not everything is documented in the CP/CPS document. During the presentation Emir mentioned that the CA is not mentioned explicitly in the list of the entities who can request the revocation of a certificate but rated this as A because the CP/CPS states that "CA manages the functions of its RA". Willy proposed that this should be listed explicitly and the item was re-rated as B.

ChristosT and Edgars volunteered to peer-audit the CA.

Finally Emir mentioned that the CA's certificate is expired soon and as its lifetime is 5 years he would like to re-new it instead of re-keying. The group nodded ok for the renewal.

A Comprehensive Guideline on Robots (David Groep)

During the IGTF all-hands meeting at Banff it was agreed that the EUGridPMA would prepare a guideline on what is an acceptable robot for IGTF.

Naming

The first thing that was discussed was the naming of the Robots. Till now the common practice was the use of the same CN as the personal certificate of the user who is requesting the certificate with the addition of the string “Robot:” in the beginning. This was not applicable when the Robot is not owned by a single person but by a group. The use of the group name or scope (i.e. CN=Project Monitoring Service) drops our warm and fuzzy feeling on trust given human-readable names. The proposition was, in case of a group Robot, to have an email address of the group included in the CN field and require them to respond with CA’s response time (1 working day).

We don’t have the same requirement for personal certificates. What is the way to contact the entity in case of a personal certificate?

There is no actually. For personal certificates you have the fuzzy feeling of identifying the user by his/her CN field.

Who will need to contact the owner of the Robot Certificate?

This depends on the case.

Shouldn't the VO answer the question "who is responsible"?

Yes, but the problem here is that VOs are usually too slow to re-act.

Why not sticking to the Host certificate RFC and adding an email to the Subject alternative name?

The Subject alternative name is not recorded to the log files.

How difficult is to include the AlternativeNames at the log files?

Impossible. This something that requires rewrite of the whole software including parts outside of grid world (mod_ssl).

Having the name of the group responsible for the robot isn’t sufficient as you can go to the CA and ask for more information?

Yes, but CAs are not obligated to respond with contact information of the entities.

Milan asked to not put email addresses at the subject DN.

But this was required for retain the fuzzy feeling.

Jens concerned about the traceability of the responsible person. In the document it was added that the issuing CA should keep traceability information.

For the Naming we concluded to the following statement:

“The commonName subject DN component(s) of the robot MUST include a humanly recognizable and meaningful description of the Robot as well as either:

- an electronic mail address of a persistent group of people responsible for the robot operations; or
- the name of a single natural person responsible for the automated client.”

Milan noted that we have a requirement for groups to respond within one day but not for natural persons.

This comes from RP (OSG - Jim) requirement who asked, in a previous meeting, to either be able to block both the robot certificate and the robot owner's certificate OR to have an instant response from the group behind a robot certificate.

Key material

The discussion on the Key Material followed where the topic was on whether we should drop the hardware token requirement. There are many issues with the hardware token use for Robots including the following:

- The hardware token is always activated or the activation data is stored on the filesytem
- They are not applicable on cases where a portal needs access to hundreds of certificates (as this requires hundreds of tokens on a simple node)

On the other hand dropping this requirement would result:

- Many (group) robot private keys being leaked to network filesystems and there would be no way to traces whether the private key is leaked or not.
- Large communities (i.e. a whole VO) could use a simple certificate for all their users.

RPs noted that there are already large communities behind pilot jobs and the current practice is that if the community cannot protect itself (trace/ban the single user that was misusing the services) then the whole community is banned.

We concluded that we could drop the hardware token requirement and the private key protection guidelines will apply to this case.

The resulted statement was:

“The private key pertaining to a robot certificate MUST be stored either on a secure hardware token OR on a local file system, on an appropriate computer system, to which only those people responsible for the robots operation have access and to which no other people have any access, either privileged or unprivileged. This computer system where the private key is stored MUST be appropriately secured, be actively monitored for security events, and MUST be located in a secured room where access is controlled and limited to only authorized personnel.”

Responsibilities for the subscriber

As a result of the above discussion the following responsibilities where added for the subscribers of Robot certificates:

"In case a persistent group of persons is named, this persistent group of responsible people must react appropriately within the certificate revocation grace period to any request for information, and the issuing authority MUST keep the traceability to a single responsible natural person that assumes responsibility for actions undertaken by the robot and for the actions of the all persons in the group of people responsible for the robots operation. Subscribers are responsible for complying with the private key storage protection criteria and for maintaining appropriate access controls and traceability.

Certificate Policies

It was added that for Robot certificates the 1SCP that defines the way that the certificate was generated should be included.

What's next?

EUGridPMA invites the other PMAs to read and endorse this text but there was a brief agreement by both PMA representatives. CAs can proceed to CP/CPS changes and reviewers will be assigned by their accrediting PMA.