EuGridPMA Meeting
Tallinn 25 May 2005

Wednesday Afternoon session

Round table

1. Christos Updates

2. DOEGrids updates
Revision ongoing. Significant changes: there is a new security officer and a secretary role to better handle things
Update of CP/CPS is ongoing. Major changes

- DN ownership will be allowed
- Change of OCSP

3. Germany
CP/CPS has been updated, no comments received. The CP/CPS would be in place at the end of May

4. David O Callaghan
Nothing really interesting to report

5. IUCC
Issued certificates (personal) = 34
Institute certificates = 2 or 3

The Israeli CA has embedded in subject the email address of the CA. Sophie said that they used the same construction, but since one week they have moved the email address to the extensions.

6. Austria
They have changed the CA accordingly to the requests. They went operational in March. Issued certificates so far: 120.

7. CRS
They issue a lot of server certificates.

8. Slovenia
Rather new CA. They are trying to open some RA.

9 Portugal
Since June 2004 new CA online.

10 Russia

No changes since February, about 1200 certificates

11 Darcy
No changes. Their root CA will expire in March 2007 and they would like to get a transaction period.

12 Denmark
?? sorry I've missed this

13 Hungary
Nothing to report.

14 Estonian grid CA
100 certs issued, about 15 of them are expired. Plans to start a Baltic CA, there is already a RA in place for Estonia, Latvia and Lithuania. Agreements are already in place.
The Baltic CA will replace eventually the Estonian CA.

Auditing
The talk was based on the NAREGI wg criteria and the auditing of AIST GRID CA.

IGTF
David presented the draft document that describes the

- federation description
- site security
- general architecture
- membership

There could be in the future the possibilities of other PMAs and this should be taken into account.
It was proposed IGTF to be the publishing authority for minimum requirements profiles.
The chairs of the 3 PMAs would coordinate the work.
A discussion about the charter followed and it was agreed that
1. if a CA leaves the PMA, all the other CAs should be informed
2. some wording changes were implemented by David during the discussion
3. Tony to write something on section 10 and 11

ACTION: Tony to write something on section 10 and 11 of the IGTF document.

Authentication Profile
David showed the latest version of the Authentication profile.
ACTION: Christos to write about the use of users' private key.

Section 9 requires some text. Someone who has idea is invited to send them to the list.
David asked whether this document replaces the min req and it was agreed to replace the min req.

Thursday

Bob Cowles

Bob presented the requirements coming from the relaying parties open science grid. One of the requirements was that the three PMAs should coordinate their work and liaise with standardisation body (GGF).
A discussion followed:

Q: How do we accept new relying parties?
A: There could be cases when the relying parties are not happy with the minimum requirements defined by this group and therefore the CA is not able to represent them. In this case the relying parties should be able to express their concerns not only their CA, but directly to the EuGridPMA.

ACTION: It was agreed to have a list called info@eugridpma.org Each pma will have an info list.
ACTION: The CA should advertise that they are member of the Eugridpma .

Repository structure

The repository hosted by the EuGridPMA should allow relying parties to easily pick up the CAs that are complaint with some authN profile.
For this purpose the relying parties can use the RPM installation, which is only used for for Eugridpma and doesn't allow for a differentiation of the authN profiles.

Several issues were discussed such as:

1. Can a CA get accredited by different PMAs that are all part of IGTF?
   Didn't get the answer
2. Can a CA belong to another PMA that is not part of IGTF?
   In principle yes, but this not in the scope of this group to discuss.
3. If a CA makes a change in their distribution list, where do they need to announce it?
   It was agreed that the CA should communicate to the PMA where they belong to that being part of IGTF will communicate the change to the other members PMAs.
4. A common repository of all the PMAs under IGTF is needed

Still open issues about the distribution.

Bejing CA

There was a presentation about the Chinese CA which has requested to be accreditated by the EuGridPMA.
Q: Why do you allow people to authenticate themselves by phone? People should do this personally with the RA with an ID (according to the min req)

A: Because they know all the people and the phone is only used to prove that the person belongs to the organisation

Q: Why is the passphrase on the USB stick?
A: We use the flash driver as on off line media.

Q: what is the web site of the CA?
A: didn't get the answer

Christos and Yoshio went to China to verify to Chinese CA and they recommend the approval.

DFN Grid CA

Reimer presented DFN CA.
Q: There are some friction in the minimum requirements for instance about the hierarchy. Could be possible to leave out some level? Is there need to have a CP for each intermediate level?
A: One possibility would be to move GridKA-CA under the root of DFN CA.

There were some issues about the merging of the two German CAs, which will happen in the next future. The D-grid project should start in September and therefore the merging of these two CA would take place immediately afterwards, but there might be delays.

There should be a new version of the policy that includes the comments received mainly from Ursula and Jules, then the CP/CPS should be sent to the list.
The discussion should take place on the list, 2 weeks will be allowed for comments after the final version is sent to the list. After that DFN will be approved.

Baltic CA presentations
Sorry missed this ☹

Russian CA
It is a huge amount of work for the VO changing the name of the CA.

Q: is the key length a problem for java?
A: EGEE uses java software so that could be a problem

Q: how do you ménage the email address of the users in the certificates?
A: Russia would like to have this in the certificates, but there are also other possibilities

Q: Lifetime is 20 years. Is it ok for Russia? The exception was made for DoE because they use security software.
A: no proper answer, so I would assume people are not unhappy

Q: is this a country CA or a project CA?

A: It satisfies mainly the EGEE context, but David reminded that it was agreed to operate the CA also outside the EGEE area also. Due to some instability it is hard to predict, but it is envisaged that this CA will operate as Russian CA for the next 3-5 years.

UK escience
Jens provided an update of the UKescience CA. The root Key is valid for 5 years. UKescience doesn't allow for encryption for liability issues.

Polish CA
Pawel presented the polish CA.

If the minimum requirements change, should the CA change to satisfy the new changes? David said that the CA should consider these changes and normally some time is required to implement the changes (typically 18-20 months). Not clear what the solution was

Pawel brought up the issue how the changes of the min req are announced to the ca admins. This should be done in a better way.

There was a long discussion about the use of the name within the CA. The CA must assure that a DN is assigned to the same person for authorisation problems.

Group certificate? How do we deal with them? Change in the min req needed?
It was said that this is out of the scope of the grid authN. The signing policy allows to use different sets.

Anonymous users: how do we deal with them? In same cases users might not want their name in the certificates, but a nick name.
It was agreed that this is ok as long as, the CAs maintain a table to resolve the nick names in univocal way.
Dave K said that he is not sure this would be acceptable by LCD.

ACTION: Dave K to verify whether LCG users would accept nickname in the certs.

Cesnet CA
So far they gather users' information from the registration request. The change will foresee key generation after registration. They are moving to a new software Entrust and Milan gave a demo how it works.

Friday

The day opened with a review of the agenda.

Next meetings
The location of next meetings was decided as follows:
- 28-30 of September in Poznan.
- January 25-27 in Vienna.

Status of OCSP

David asked how many people tested OCSP support and only a couple of the presented made some tests.
Milan asked if anybody tested about the traffic performances with OCSP. No answers.
Milan asked David G to send to the list his experience using openCA-OCSP. Ian said that he likes the idea of having someone else running the critical services (like OCSP) on the CA behalf.
Where should the OCSP service advertise? The answer was in the certificate.
If the OCSP is in the cert should that be a production service? It depends on the implementation. Milan proposed to define this in the policy, so relying parties know.

The conclusions were that:

1. the group wants OCSP
2. some CA (like Cern) doesn't want to run a production service
3. security issues about OCSP were also discussing. Certs for the OCSP have a short life time (terms of day), which is due to the fact that OCSP can't verify whether its own certificates are revoked or not. The OCSP pk is stored in an usb.

Robot Certificates
Milan said that they are using Simba mailing list to encrypt mailing list. The process is completely transparent which means that there is no way for the user to verify how the mails are encrypted.
The security levels of the private key was discussed.
At the moment there are only two classes: either the private key is encrypted or not.
There could be something in the certificate to provide more information, for instance an attribute.
It was agreed to have a wg to look into these issues.

ACTION: Ursula, Jensen and Milan to set up the WG.

Group users certificates
The security of tokens was discussed. The token should be given to the users who would be responsible for it. This solution would work v well for RSA administrators and generic PKI users. In the special case of grid most of the users connect from their computer to a remote computer from which they submit the grid jobs. The users' pr key is stored on these remote computers, so in this case it gets almost impossible to use the token.

ACTION: Milan to send to the list any result about rainbow etoken.

Host key generation

Host key generation: the current situation is that the sys adm must generate the key on the machine.
Sophie reported that a user can request a server certificate only if he has got a personal certificate. The request can be done on line, so the server generates the key that are sent back to the user via encrypted email (the email address is taken from the certificate).
No copy is kept on the server.
This solution works well, but there must some assurance about the security level of the machine that generates the key.
The host key needs a better level of protection. If it is generated by the CA this creates security issues. So the decision was not to have any more CA generated host key.

There is no page or documents for best practice. This would be better discussed on the CPOPS wg group.
It was agreed to have a wiki to share documentation. Milan proposed to have certificates to access to it. The proposal was agreed. There should also a document describing the reasons behind the min require.
The IGTF charter should be finalised before the next GGF.

ACTION: Tony to produce a new version of the IGTF charter doc.
ACTION: David oC to set up the wiki.

Summary of the actions

ACTION: Christos to write about the use of users' private key in the authN profile.
ACTION: Tony to write something on section 10 and 11 of the IGTF document.
ACTION: It was agreed to have a list called info@eugridpma.org Each pma will have an info list.
ACTION: The CA should advertise that they are member of the Eugridpma .
ACTION: Dave K to verify whether LCG users would accept nickname in the certs.
ACTION: Ursula, Jensen and Milan to set up the WG whose proposed name was "Security level of private key"
ACTION: Milan to send to the list any result about rainbow etoken.
ACTION: Tony to produce a new version of the IGTF charter doc.
ACTION: David oC to set up the wiki.