Minutes from the euGridPMA meeting in Brussels (23-24 Sept 2004)

Table of Contents

List of participants

A/a	Name	Email address	CA/RP	Home affiliation	Present day 1	Present day 2
1	Rosette Vanderbroucke	Rosette.vanderbroucke at belnet.be	BEGRID	BELNET	YES	YES
2	Tony Genovese	Tony at ES.net	DOEGrids	ESnet	YES	YES
3	Mike Helm	Mike at ES.net	DOEGrids	ESnet	YES	YES
4	Bob Cowles	Rdc at slac.stanford.edu	OSG-sec	SLAC	YES	YES
5	Dane Skow	Dane at fnal.gov	FNAL	FNAL	YES	NO
6	Yoshio Tanaka	Yoshio.tanaka at aist.go.jp	APGridPMA	AIST	YES	NO
7	Christos Kanellopoulos	Skanct at physics.auth.gr	HellasGrid	AUTH	YES	YES
8	Rolf Gartmann	Gartmann at switch.ch	Switzerland	SWITCH	NO	YES
9	Ian Nielson	Ian.Nielson at cern.ch	CERN	CERN	YES	YES
10	Ara Grigoryan	Aagrigor at mail.cern.ch	ArmSFO	ArmSFO	NO	NO
11	Brian Coghlan	Coglhan at cs.tcd.ie	Ireland	TCD	YES	YES
12	Ursula Epting	Ursula.Epting at iwr.fzk.de	GermanGrid	FZK	YES	YES
13	Jens Jensen	J.Jensen at rl.ac.uk	UkeScience	RAL	YES	YES
14	Borut Kersevan	Borut.kersevan at ijs.si	Slovenia	IJS	YES	YES
15	David O' Calaghan	David.OCallaghan at cs.tcd.ie	Ireland	TCD	YES	YES
16	Milan Sova	Sova at cesnet.cz	CESNET	CESNET	YES	YES
17	Lev Shamardin	Shamardin at theory.sinp.msu.ru	Russian DataGrid CA	MSU	YES	YES
18	Dave Kelsey	D.P.Kelsey at rl.ac.uk	LCG GDB Sec	RAL	YES	YES
19	Lauri Anton	Lauri.anton at eenet.ee	Estonia	EENet	YES	YES
20	David Groep	Davidg at nikhef.nl	DutchGrid	NIKHEF	YES	YES
21	Alexander Kryukov	Kryukov at theory.sinp.msu.ru	Russia	MSU	NO	NO
22	Anders Waananen	Waananen at nbi.dk	NorduGrid	NBI	YES	YES
23	Willy Weisz	Weisz at vcpc.univie.ac.at	Austria	UNI-VIE	YES	NO
24	Nikos Vogiatzis	Nvog at admin.grnet.gr	SEE-GRID	GRNET	NO	YES
25	Sophie Nicoud	Sophie.Nicoud at urec.cnrs.fr	DataGrid-fr	CNRS	YES	YES
26	Alice de Bignicourt	Alicde.de-bignicourt at urec.cnrs.fr	DataGrid-fr	CNRS	YES	YES
27	Edith Knoops	Edith.knoops at urec.cnrs.fr	DataGrid-fr	CNRS	YES	YES
28	Fotis Karagiannis	Fkara at grnet.gr	EIRG	GRNET	YES	NO
29	Jules Wolfrat	Wolfrat at sara.nl	DEISA	SARA	YES	YES
30	Emanouil Atanassov	Emanouil at parallel.bas.bg	BULGARIA	BAS	YES	YES
31	Diego Lopez	Diego.lopez at rediris.es	TF-AACE	RedIRIS	NO	NO
32	Licia Florio	Licia ata terena.nl	TF-AACE	TERENA	YES	NO
33	Usman Ahmad Malik	Usman at ncp.edu.pk	PK-Grid-CA	NCP	YES	YES
34	Darcy Quesnel	Darcy.quensel at canarie.ca	GridCanada	CANARIE	YES	YES
35	Miroslav Dobrucky	Dobrucky.min at sarba.se	Slovakia	II SAS	YES	YES
36	Eugene Ryabinskin	Rea at mbslab.ktar.ru	Russian DataGrid CA	RRC KI	YES	YES
37	Wer-Long Ueng	Wlueng at srnica.edu.tw	TW Grid	ASCC	YES	YES
38	Szabdes Hernath	Hernath at sunserv.kfki.hu	KFKI RMKI	KFKI	YES	YES
39	Rafael Marco	Rmarco at ifca.unican.es	IFCA	IFCA	YES	YES

Status and news from current CAs

TACAR

TACAR was formally presented in the first euGridPMA meeting in Florence, Italy. It will provide a repository for CA certificates. The web server that is hosting the repository will be using a self-signed certificate and will have the hash-key of the certificate on the web site, which has been moved to www.tacar.org due to the growth. After reviewing the site statistics it seems that it is mostly used by site administrators. Anders asked who should use that site. The reply was that initially it was built in order to make the life of the NRENs easier. The target group is system administrators, trust installers, grid deployment teams (like the LCG deployment team) etc.

Another issue that was raised was the case that TACAR stays out of sync with the current CA certificates. Would it be easier if there were only links to the CA certificates rather than the certificates themselves? Even although the certificate change would be transparent, somebody will have to update the hashes. It is up to the CA Manager to update TACAR.

GermanGrid CA

Around 600 certificates have been issued and 22 different institutes are served. The CP/CPs was changed recently as due to a typo the OID mentioned in it was different than the one embedded in the certificates. There is a new national Grid initiative in Germany under the name D-Grid. A connection has been established between the already established PKI structure of DFN and GermanGrid.

NorduGrid CA

Around 700 certificates have been issued. Dave Kelsey mentioned that there is still no CP/CPS describing the policy and the operations of the NorduGrid CA. A dead line until the 1st of December was put for Anders to provide the CP/CPS.

Fermilab

The CA issuing service certificates at Fermilab has ended operations and moved to the DOEGrids CA for service certificates. The root CA and the KCA are still operational.

ACCG CA

The CP/CPS has not been assigned an O.I.D. A revised CP/CPS was sent this morning the euGridPMA list in order to align the minimum length of the passwords with the current minimum requirements.

CNRS CA

Nothing new

CERN CA

There were no changes since the meeting in Florence. The CP/CPS has not been updated yet with the changes that were mentioned during the Florence meeting.

Russian CA

They changed the root certificate 2 months ago as the old one has expired. There are still around 100 certificates signed by the old CA certificate haven't been reissued. They are going to change the CA software to openCA,

SlovakGrid CA

37 certificates have been issued.

GridCanada

There are going to be some changes in the CP/CPS. An RA relationship will be formalized with the west grid. Around 1000 certificates have been issued.

GridIreland

Soon to upgrade to new openCA software

UKScience CA

UKScience CA needs to scale to a large number of certificate. Currently There are 50 Ras and 1500 live certificates. In the following months it is expected that 3000 users from the DIAMOND project will come for

certificates. At this time they are investigating the new openCA software and they are looking at hardware signing modules. UKScience CA has developed a scheme where the CA is generating the keys and delivers them to the users along with the issued certificates. The privates keys will not be kept by the CA. There are projections that user base might scale up to 3 million users. It will not be possible to re authenticate all users every year. There is pressure for SIPS.

Finally UKScience CA was accepted by the TeraGrid project and they were asked to accept the other CP/CPS from TeraGrid CAs. Currently only the DOEGrids CP/CPS has been accepted.

DOEGrids CA

There is a possibillity of a regional American PMA. DOEGrids are investigating the option of changing the software they using for the CA operations. There are European project wanting to cooperate with TeraGrid. We must put effort to harmonize such cooperation perhaps at the PMA leve.

CESNET CA

Planning to move to commercial software and use hardware signing modules.

Spanish CA

The root certificate is about to expire. Within one month a new CA certificate is going to be issued and they are going to move to openCA software.

DutchGrid CA

Need to update the CP/CPS to reflect the current best practices. There are 12 RAs which have issued around 1500 certificates. 99% of the work has been shifted to the end users by introducing more paper work. A new CP/CPS version will be ready by the next euGridPMA meeting.

APGrid PMA

APGrid started on July 2000 in order to create a meeting point for all Grid researchers in Asia Pacific and to establish a communication channel to other international bodies like the GGF. The APGrid testbed is based on GT2. The process for a new site to enter the Testbed is to install GT2, gather and exchange CA information and trust with each other, configure MDS and finally install additional software on project basis.

Most participating organizations are satisfied in using the Globus Simple CA. While that might be acceptable within APGrid, it make it impossible to open cooperation channels with other international projects. In order to cooperation with projects in EU and North America production level CAs must be launched. As a result on June 1st 2004 the APGrid PMA was launched to act as a general umbrella for the Asian-Pacific region.

APGrid PMA will create two levels of CAs. At the first level there are going to be the experimental CA which will be alternatives to the globus Simple Ca. At the second level there are going to be the production CAs, which will have strict management and will trusted by international communities. Currently the KISTI Grid CA and the AIST CA are accepted as production level CAs. ASCG CA is under reviewing and Australia has plans to launch a production level CA.

Some question raised are:

- Does euGridPMA need to review each CA CP/CPS individually?
- How do we keep consistency of CP/CPS?
- Can TeraGrid trust AIST production CA?
- Can APGrid/PRAGMA trust the TeraGrid CAs?
- How can APGrid PMA help?

David Groep noticed that the CAs in APGrid PMA seem to be institutional. Would there be a possibility to turn into national CAs? It seems it is not possible. We should have something that scales to 300-400 identity providers.

- Does euGridPMA need to review each CA CP/CPS individually?

There should be bilateral agreements between PMAs. If two PMAs recognize each other's minimum requirements then it will make them equivalent. Tony raised the issue whether an international federation for accredited CAs should be created. A global coordination organization needs a lot of work and GGF does not want to run such an organization. There was the proposal that a body in Europe take up on this. For the time being limited cross participation is the way to go. The meetings can take place during euGridPMA or APGrid meetings. Each PMA should define it's own minimum requirements and then coordinate this at the global Grid PMA level with the rest of

the PMAs.

- What is the accreditation procedure in the APGRID PMA?

Each ca that wants to be accredited has to sent it's CP/CPS to the APGrid PMA mailing list. The CP/CPS is reviewed by the members of the mailing list and if it covers them it gets the accredited flag.

David Groep asks whether there is a requirement for a face to face meeting before the accreditation. The answer was that there is not enough funding for face to face meetings.

EuGridPMA will wait for the accreditation document that will be produced by the APGridPMA, in order to evaluate it and inform it's relying parties whether there is an equivalence at the minimum requirement level between APGrid PMA and euGridPMA.

Incidents and events

What actions should take place if a User Interface is compromised and there are 100 certificates on it? Bob suggests that we should kill the authorization at the VO level. The minimum time of response is suggested to be 8 working hours.

Software and Tools

David Groep added a cvs repository to the euGridPMA site and create the RPMS for the accredited CAs. Anders raised the issue that currently for the installation of the CA certificates along with the CRL information one needs to have root access.

CAOPS in GGF in the process of producing a document on OCSP.

Accreditations and New CAs

Estonian CA

There is no distinction in the DN between user and server certificates. A suggestion was to introduce an OU field that will distinguish server/service certificates from user certificates. The Estonian CA is accredited.

Hungarian (KFKI-RMKI) CA

The KFKI-RMKI CA will serve only KFKI-RMKI. The focus of euGridPMA is to have national CAs. There has to be a consensus within Hungary on who will be the national CA.

Slovenian CA

Slovenian CA is accredited.

SEE-GRID Regional CA

AUTH was appointed by GRNET and SEE-GRID to run the catch-all CA for the SEE-GRID project. Nikos is the project manager of SEE-GRID.

SEE-GRID is a complementary project to EGEE with the purpose to setup national Grid initiatives in countries that were not yet up to speed for EGEE. It is a SSA for countries that are less resourced so that they can be included later in EGEE. As most of the countries that are part of the SEE-GRID project do not have national PKI infrastructures, a SEE-GRID Regional CA was created. The project is regionally driven and an important infrastructure development. The SEE-GRID project is serving as a role model for other regional efforts.

The name space of the SEE-GRID CA is /DC=ORG/DC=SEE-GRID, so as to keep distinct from the future national CAs. The new RFC was used for the CP/CPS which is going to bump soon to version 1.1. The end users need to re-appear in person to the RA every three years. The usage of signed e-mail to confirm acceptance of the CP/CPS is very nice. The users have to be able to do it.

Jules asked how does the 10 digit challenge help in securing the setup. Christos replied that the RA should be as read-only as possible. This prevents the RA to act on behalf of the user. Jules continued that the RA could spoof the e-mail address and just request a certificate. This could not happen since in order to submit the certificate request he/she should not the full 10 digit number. At this point Mike asked what was the threat that the system tries to eliminate. Christos answered that in a highly distributed environment which spans in different organizational and national domains trust should be kept at the bare minimum that is sufficient for the operations to take in place. Mike commented that the whole process is fine, but it looks more like a SIPS-like thing.

SEE-GRID CA will be accredited if in two weeks there are no comments on the list.

SWITCH CA

There are differences between the SWITCH CP/CPS and those of the other CAs in euGridPMA. Perhaps this is because of the different direction/focus. There are different CA for different usage (e.g. server certificates, user certificates etc).

Switch does not allow users to generate proxies. Are there more liabilities for the CA when users use certs to generate proxies? Perhaps it helps that proxies are now blessed by IETF. We will need to revisit the Switch CA at the next meeting.

Requirement Profiles and Policies

Updates to Minimum Requirements

Regarding the incident response Juls suggested that the CAs must react immediately during working hours. When an incident is reported the reaction process must start within 8 working hours . Within another 8 hours the CA must proceed to revocation and CRL issuance if there is enough information. Mike mentioned that the DOEGrids have a 24/7 hotline for reporting incidents, while Tony raised the question how should the CAs report to each other. The euGridPMA should not take upon the responsibility to mediate in the exchange of information.

Operational audits SHOULD take place. It is a good practice in order to have a valid list of the people that participate in the CA or the Ras as trusted staff. Also there should be checks that the Ras keep the necessary logs etc.

Darcy believes that the CAs have to have the burden of recreating the CA every 5 years. Tony's experience from the time the DOEGrids changed their CA certificate was that the whole procedure was more costly for the community. Milan commented that almost everybody have gone through the procedure of changing CA certificates.

The maximum lifetime of a CA certificate should be changed to 20 years.

Online and key-generation CA discussion

If a CA generates private keys, the CA MUST descrive how it is managed in it's CP/CPS. Either the keys are escrowed or the CA must descrive how it gets rid of it. Verisign does this. Also the latest versions of OpenCA can generate keys on the server side. Switch lets the user to download the PKCS#12.

Windows 2000 Active directory also generates certificates for users. Some of the reasons for a CA generating keys are:

- Smartcards
- Browser support
- password hygiene
- control over certificates and usage

Such a CA can regenerate certificates from CSRs.

A team should come up with the minimum requirements corresponding to this use case. Mike, Tony Jens and Rolf volunteered. Dane volunteers to be a critical observer.

Do we distinguish between CAs generating long-lived and short-lived keys? Different classes: SIPS and other proxy generators, active credential stores, key generating CAs.

Open Issues

Anders reported problems when generating RPMs: Some CAs didn't have signing-policy files. Some CAs didn't specify in CP/CPS which name space they sign. For example, catch-all can sign *any* name space, so if catch-all is compromised, every resource that trusts catch-all is vulnerable. Anders suggests to take out catch-all from the next release. CNRS will set up a new CA with a restricted name space, will still act as catch-all for EGEE, etc. It needs to be approved by CNRS (and by the PMA). For DOEGrids CA, catch-all is just another RA. DOEGrids uses DCs to prevent name space overlap. Timescale for replacing the /* catch-all: 1 year from now...

Questions:

- How many certificates are currently caught-all?

- Can RPs help find the certs and identity which can now be replaced by national CA certs?
- Can we generate a post-hoc signing-policy file for the /* catch-all?

For China, question how many new institutes will be joining? Need to document remote registration procedure. Problem is that these things don't have a common root at the moment (/C=CN and /C=TW - exercise for the reader). /C=CN/O=<institute> is considered ok. ASGCCA suggests also signing for nearby countries. Globally, the three PMAs should also coordinate so that _their_ name spaces don't overlap. Let's see if APGridPMA can sort out the details.

Question about mirroring. Tony suggests mirroring the EU Grid PMA web site.

Anders suggests signing rpms with a pgp key; then projects can distribute them, and the PMA would not be a single point of failure for fetching certs.

*** What is the relation between projects and PMAs, and to VDT in particular. VDT funded by iVDGL which is NSF-funded and may represent lots of RPs; should they be represented in PMAs?

*** Mike mentions a RADIUS infrastructure to support OTP. Leads to problems with collaborative environments like Grids, so a SIPS type solution required. Go to website and have a look at slides. Eduroam is similar Terena-sponsored project. [web site is http://www.doegrids.org/CA/; scroll down to papers & presentations] [Eduroam: http://www.eduroam.nl/en/index.shtml]

*** What is the relation between projects and PMAs, and to VDT in particular. VDT funded by iVDGL which is NSF-funded and may represent lots of RPs; should they be represented in PMAs?

*** Another Terena effort, sponsored by SurfNet, to set up a European server (and service) CA. There will be a presentation at the next meeting. [http://www.surfnet.nl/en/]

Next Meeting

1.5 days is too short. Marseilles is warmer than Tallinn in January. Wed 26 Jan—Fri 28 Jan 2005, starting 14:00. 2.5 days (lots of coffee needed). Expect 3 meetings/year. The next meeting in turn will be tentatively end of May, 26-27 2005, in Tallinn.