PMA Updates

13/10/2008 9:16 AM

APGridPMA (Jiny Chien)

NCH CA was accredited
PRAGMA UCSD CA changed base DN and started operations
NGO/Netrust was accredited and was included in 1.23 release. It was removed from IGTF 1.24 and added back in 1.25
Started review of the Indian Grid CA
Meeting in OGF 24 Singapore:

- Approved SLSCS profile
- New Charter: Refer to IGTF Min requirements
- Vice Chair Jiny Chien
- Indian CA still under review
- Issue of heavy CRL traffic and frequency in CRL issuing
- AIST will host a replica of the Netrust CRLs for the IGTF communities
- Discussion about CRLs will take place in EUGridPMA meeting
- Next meeting to be denied (between end of March – May)

JENS: There were already 2 problems with accreditation. We need to see a few operational isuues. DavidG: Automated way to check the operation status of the CA. Jim: This should be done before the accreditation

TAGPMA (Jim Basney on behalf of Vinod)

Peru and Colombia expected to join soon
Re-elaction in July 2008
Infrastructure moved from CANARIE to ESnet
None of the CAs were affected by the Debian Openssl incident.

- But that incident clearly showed that the intercommunication of the PMA members was patchy

Updated the TAGPMA Charter
PMA membership will last for 2 years
Ties the representative to the soliciting institution

Currently working on more updates to the charter.

- Inactive membership

Two year term of office for elected posts

Last TAGPMA f2f: 7th TAGPMA in Oakland
Next TAGPMA f2f: 8th TAGPMA in La Plata City, Argentina
Video Conferences every other Tuesday

IGTF RAT (Jim Basney) 13/10/2008 9:16 AM

Operate by consensus. Use the apache voting process.
For communicating with the CAs they will use the email addresses found in the distributed .info files.
Expected to answer within 1 business day

IGTF RAT responsiveness test:

- Majority responded within one day.

The use of a descriptor in the subject could be useful in order to filter out these emails
DavidK: For a real case scenario, you do not want to use the igtf-general
Jens: There are the closed (members) mailing lists.
DavidG: Not sure if they are properly maintained. TAGPMA and EUGridPMA have one.
Rheimer: Its better not to use acronyms in the message subjects because the tend to be characterized as spam
Jim: run the test twice per year
Jim: What next?
Perhaps collect further contact information
CK: focus on risk analysis and risk assessment. Handle the results back to the PMAs for actions
DavidG: how do we collect contact information.
DavidK: TAGPMA is doing it.
Rheimer: The contact information should be enough for renounce in 1 business day.
DavidG: There is no central repository for CP/CPS. And if there were one it might be down. You need you have alternatively means of contact.
Jens: the contact information in the CP/CPS is about the people responsible for the document.
DavidG: We should collect the info our selves. The goal should be to have an escalatation process. Private email addresses will be used first and if no reply then try calling on the specified phone number.
The collection of this information will become part of the accreditation process.
RAT will create a web page with the RAT contact information
Jim: to host a pgp encrypted mailing list for RAT members.
The PMA chairs will collect necessary information from their members. Each must reply within a month.

CA Reviews

13/10/2008 9:16 AM

Latvia

- They released a new CP/CPS recently, but Jens did not have time to review it. Probably it can be done via e-mail. Also operational review is still pending

Moldova

- The website is inaccessible. Actually http://www.ca.grid.md does not work. http://ca.grid.md does work but there is no information on the website.

Request to join the PMA from South Africa and Senegal

INFN CA Internal Audit

13/10/2008 9:16 AM

The auditing is an ongoing process. Not everything has finished
They have already issued robot certificates!
More than 100 registration authorities (103). The large number of RAs was one of the major problems for the audit
For the audit:

- 3 CA staff
- 2 external reviewers for the CP/CPS. Worked in Universities with operational CAs

Disagree with the the following items:

- Item 5 Conformance to RFC3647
- Item 15 & 16: Already they have changed the key two times. Although the process is not properly documented in the CP/CPS. Is it the CP/CPS the right place to document such things?

Failing compliance with RFC3280. Currently issuing only v1 CRLs. Considering to move to CRLv2, but will not revocation reason. It is not compulsory by the RFC either.
The CP/CPS says that the must be a FQDN registered in the DNS. It is not mentioned that it has linked to a single entity.

Item 43: 8 certificates not rekeyed but renewed. They were not used for Grid. They are now revoked. All request were from CISCO boxes.

Item 50: Operational audits of the CA staff at least one per year. Roberto asked what an operational audit of the CA staff means

Disaster recovery:

- NIST 800 -53 for the contingency planning
- NIST 800-34
- Daily backups of the online system
    - Encrypted and signed by PGP
    - Weekly backup of offline system

The PMA of the INFN needs to be revised. Only Roberto is left from the original PMA group that was created back in 1999

Move from FreeBSD to Debian
Integrity check & log monitoring

- OSSEC

QuoVadis Accreditation for SWITCH (Alessandro Usai)

13/10/2008 9:16 AM

QuoVandis is based in Vermuda and has offices all around the world

Qualified yearly by several bodies
3 Root CAs

- 1 CP/CPS for CA1 and CA3 and a separate for CA2
- HSM FIPS Level 3 and EAL 4

The Grid CA will be linked to the Root CA 1

- Root CA 1, → QuoVadis Grid ICA

SLCS CA is not affected by the transition
The RA Management will stay the same

The new CA will be issued by the end of this year
The final CP/CPS version needs to be approved by the QuoVadis PMS (this should be fairly quick)
Finally it will come to the PMA for approval

Rheimer and Jens to review the CP/CPS. The updates to the current CP/CPS will be minor
Would like to have accreditation by May 2009
A representative of QuoVadis might attend the meeting in Cyprus, if this is deemed useful

- Rheimer: It would be useful because e.g. the hardware architecture is not normally mentioned in the CP/CPS.

NetTrust made available the results of the Auditors. Yoshio looked the audit report in person.

What about robot certificates and more OIDs ? How easy is it for them to add certificate profiles pm demand. They are running Unicert (seems to be highly extensible software) so technically the platform can support this.

Good option for server certificates. Actually this is the main deal with switch. Grid certificates go along.

CRL Discussion

13/10/2008 9:16 AM

SLCS profile

CRL validity between 3 and ∞ days.

If you have a certificate which lives less than 5 days, then you should not have to issue a CRL. The point is that next business day might result to less time. Imagine if there is an issue the end of one day. Is it feasible to have a response by next business day?

Jim: 5 days is far too long for a certificate no to have a CRL. The maximum should be 1 day. If the certificate lifetime is 1 day or less and if you have to react within one day, then you do not have to issue a CRL.

Rheimer: Why 3 days?
Jim: 3 days is less restrictive than the 7 days

NetTrust is issuing CRLs every 24h with lifetime of 25h. This behaviour has been problematic. If you check every 6 hours then there is a window of 5 hours where the last one that has been downloaded will have its nextUpdate field in the past.

According to the Classic Profile:
Validity between 7 and 30 days. 7 days implies continuous issuance

Proposal:

- Automatically generated CRL for onlines CAs, we change the minimum lifetime to 3 days
- For manually generated CRLs and CRLs of Offline CAs stays at 7 days
- Max life time stays at 30days

Rheimer: if there is a problem on a long weekend (e.g. holiday plus weekend), then having 3days will certainly interrupt service.

DavidG: In general there is more downtime for manually generated CRLs than with those that are automatically issued by online CAs

OSG: downloads the CRLs every 24 hours. They should change it to 6 hours. Of course this will affect the CAs who have a bandwidth limit to the download of the CRLs

OSG: 3 days minimum validity period is acceptable.
Jim: There is a problem also with CERN CA, which is issuing CRLs every 2 days.

New version of the minimum requirements → 4.2

GEANT 3 PKI (Milan Sova)

13/10/2008 9:16 AM

Part of SA3: End User Services in a Federated Environment
SA3 Task 1: European PKI Co-ordination

Plan:

- Establish a PMA for European NREN PKI
- Gather information on the status of NRENs existing PKIs
- Gather information on the status of GEANT services requirements
- Definine minimum requirements for participating PKIs
- Define accreditation process
- Define new TACAT functions and procedures to support the PMA requirements
- Establish and operate a CA for users whose NRENs do not operate a PKI. This CA the PMA and TACAR will operate throughout the lifetime of the project.

The host and service certificates are going to be used within the project. Personal certificates are not expected within the project. A policy is needed for this and it is going to be managed by the PMA.

DavidK: who are going to use these services that need these certificates? There are not going to be any relying parties in the terms of users. The users are not expected to meet those certificates. The relying parties are going to be the administrators of another nodes within the network.

Milan is going to be the leader of SA3 Task 1.

Use cases:
Eduroam is going to abandon the static hierarchy of radius servers that has been using up to now and will move to a dynamic infrastructure where radius servers can find each other

DavidG: In the GEANT proposal it is mentioned that the goal of the PKI is to make it accessible to the end users !
Milan: There are no plans for user certificates!

The differences from the server profile we use in the IGTF:

- Component identifiers
  - URN (hierarchical, structured, registered)
- subjectAltName.URI

All the other stuff is more or less the same

The SA3 leader is JISC. The participants of this tasks are CESNET and DFN. DFN is going to run the catch all. The managers of the NREN CAs will participate in the PMA.

Project about to start in 2nd half next year.

Federated SLCS CA for Northern Europe

13/10/2008 9:16 AM

Norway, Netherlands, Denmark. Sweden, Finland

Leveraging the national federations, all fronted by a single SLCS service

There is already a working prototype at UNINET

Within a year or so it will go to production

All the existing home organizations will have to join the federation. Right now the members of the Federations are the Librarians.

Milan: Can the new SLCS CA replace the classic CA? SLCS CA for users and SCS service for hosts/services. What about robots ?

The other option might be to go for a MICS like CA based on the Federation.

The CA needs that all the IdP in the federation must provide permanent and unique identifiers.