EUGridPMA – 19 Meeting

About 25 attendees – 1400 15 Jan 2007

AI: [Most prefixed with "*" below]
Milan Sova about new profile – 15 mins Wed
Minutes accepted last from last mtg
2 weeks last call for BG ACAD CA (see details
MaGrid CA: 3 reviewers: Jens Jensen, Emir Imamagic and David O Callaghan
DG will fix distribution to properly "expire" Russian Datagrid CA
LS will issue long lived CRL (& make adjustment of policy)

Discussion

Dave Kelsey intro

Dave Groep intro and agenda bashing

Minutes ok
Note takers mwh & emir
PGP keys – trying to organize an actual key party, send keys to Milan Sova and he will prepare a downloadable keyring & print

Discussion of status of EUGridPMA & IGTF
Only LU (Lux) & MT (Malta) missing Grid CAs in EU; plus coverage of a few overseas partners and other European CAs.
IGTF has helped slow growth in EUGridPMA.

Round table updates

(missed a few)

Christos – Greece
INFN – 2000 valid certs
Issued new signing cert with validity of 10 years
Old one CRL only
INFN partners of EUChina Grid, EUIndia Grid, EU Med Grid –
Became catch-all Grid CA for India & EUMed
Hope this is a short term solution until these projects produce national CAs.
For India, not yet issued a certificate.

Estonia – Estonian Grid users moved to Baltic Grid CA

DOEGrids
Mentioned that Tony Genovese has departed from ESnet and will not be returning to the group. Disposal of current work to be discussed.

Croatia – 45 valid certs; interested in short term certs due to national infrastructure being available to take advantage of it.

Spain/RedIris – 300 certs – 250 service

Czech / Milan Sova – probably declining in numbers, moving certifications to other services, CESNet will keep grid customers

SWITCH – some dozens of user certs – service certs (not all grid uses) no number given; KPMG certified cert provider so now can issued qualified certs and a trust anchor linked to our CA will get in browsers. Need to create "g2" (2nd generation) key hierarchy to support this – sometime this year. Mod of CP/CPS to support this. SLCS – left for C Wittig.

Portugal / LIPC – tomorrow

DFN – new CP/CPS in Dec: running online w/ HSM
We host 70-80 CAs on common machine (including this grid CA)
320 grid users, 240 service certs, 40 RAs.

Grid Ireland CA - > 500 certs, not sure how many valid; CA software upgrade planned

Hungary – 300 certs; need CP/CPS mod

UK – 1200 user, 2000 service; need robot certs
NGS setting up infrastructure CAs – smaller CAs, like training CAs
Many are very busy issuing certs

Dutch Grid CA – 350 user certs ; relatively constant; intend to integrate w/ SURFNET AAI infrastructure, but lack of time; joint venture CP/CPS may appear this year

Q: Are people seeing static growth, dynamic growth, &c? DOEGrids sees relatively linear personal cert growth, but lots of bursts of host / service certification.
Discussion: Discuss burst/wild card naming issues Wed.

BG-ACAD (Bulgarian Grid CA; presenter Luchesar V Iliev

Waiting for signal to go forward, hope we are close
Describe changes since Karlsruhe (EUG-18)

- Name construction – interpolated father's initial, Cyrillic, period

- Now use Latin letters (transliterated as needed), full name as per ID document
- Will allow hyphens in name
- No email in subject, instead in subjectaltname
- Multiple roles for the same person – add extra digits to the name
- Hostnames – what about internationalized host names? For now, not eligible for certification; devices w/o FQDN, not eligible
- Prefer host to service certs

Cert application process

- Cert will follow min reqs
  - Secure passphrase
  - 2048 bits (at least, but must be interoperable)
- ID: Natural persons: Face to face meeting with RA, showing government ID

Identity validation

- Defining a WoT scheme for PGP keys (sort of a PGP CA affiliation, that will allow X.509 cert approval)

Subscriber signs an agreement

- Usual EULA-type conditions: read policy, accept the BG ACAD cert, assumes responsibility for private keys and notification of BG ACAD CA if key compromise occurs

Submission

- User is assigned a nonce to submit along with CSR (several options and submission methods are available).

EE Cert profile

Generally follows standard profile; will allow other keypurposeIds such as emailProtection, codeSigning

Subject distinguished names

- Uses DC
- Cert re-key
  - Same explicit statement as after 1st
  - CA reserves right to reject or postpone approval

CRL

- V2 only

CA root cert

- Uses host name form in cn= component
- Decided not to distribute passphrase; instead kept in a locked box

Logging

Keep for a minimum of 3 years after CA &c expired (?)

Repository

http://www.ca.acad.bg

Brief virtual tour of CA:

- Admission desk –
- Entrance to Computer Center – heavy door, RFID lock, video surveillance
- Locked cage in which CA operates (quite claustrophobic)

- Disks kept locked in strongbox between uses
- Offline CA
- Free BSD 6.1-RP12; openssl CA

Operational/tech facilities

CERT Team to be developed

Note: PGP Keys are used to authenticate the submitter of host cert requests and are an essential (but not exclusive) part of this PKI.

Discussion (Jensen, Sova); presenter Luchesar V Iliev
PGP keys – who signs them? Need policy or some kind of CA-like policy to control and make equivalent the identity mapping.
BG comment- binding photo id to key id – basic part of the process
Why limit to 2048 bit user certs? 1024 is ok.
Discussion of the character set escalation problem – should names be restricted to printablestring rather than 7bit ASCII?
How to distinguish host from personal certs? No general rule; ea CA does its own regulation (as does this one).
PGP key lifetime? To be continued.

* 2 week "last call" after PGP adjustments and a few minor changes added to new revision.

[Break – group picture]

MaGrid – Moroccan Grid CA; presenter Redouane Merrouch

General description of service and scope – see slides
Based on MARWAN – Moroccan NREN (?)
Partner of Eumed Grid (1st member to integrate)

CA operations – RA – subscribers architecture
Single CA – RA at each partner (research institute or university)
CA cert is available: http://www.magrid.ma/ca/ca_cert
5 year validity
Software-based
EE key management – follows classic min reqs
EE CSR UI and process – follows classic min reqs
Revocation – follows classic min reqs
Revocation done by email (?) or by physical appearance
Repository: Http://www.magrid.ma/ca/crl
Classic requirements on issuance
Physical / logical security controls: Standard
RA security controls – (page 22) –
Logging / Archive – standard

Status:

- CP/CPS in draft and delivered – EUGrid PMA & EumedGrid lists
- Repository available (see earlier)
- Signing machine available

Discussion
JJ: How do you check request was done by user? OpenCA has pin feature, so it ties request from a specific user to a specific content (CSR) and which user can present to RA &c.
JJ: How do you protect the frequently-changed copies of the passphrase?
Why change so often? Makes life harder for operators.

* 3 reviewers: Jens, Emir Imamagic and David O Callaghan

Will be installing openCA (probably) before complete approval.

Russian DataGrid – final report; Lev Shamardin

Superseded (in concept) by RDIG CA in 2005
Basically, this has a broader range of projects

Last issued cert of data grid CA expired on 26 Sep 2006
Removed from latest CA distribution
This presentation constitutes "notification of termination" to relevant security contacts
Logs will be kept until end of 2009.

* DG: Forgot to update the 1.11 distro to show the datagrid CA has been obsoleted, but didn't include it in distro (will be corrected in next distribution).

* Will change CP/CPS to allow a very long term CRL to be issued (so CA need no longer be active).

Discussion of various monitoring and administrative services

Q: Who issues certs in Russia?
RDIG for a while – slow transition.

SlovakGrid – Miroslav Dobrucky

New operator-manager
Running since 17 Dec 2002
Only minor changes in 4 years –
Root cert expires in Dec 2007

Have decided to refresh the key pair, extended another 5 years.
Will rekey on or before 2010.

Valid: 45 user / 39 host / 0 service certs ; Revoked: 14 (9 host / 5 user)

Checks public key for reusage [as part of CSR approval/acceptance?]

[General review of current operations – see slides]

Updated CP/CPS & process to conform to evolving IGTF classic profile policy (hash function, longer passphrase, lifetime extension, &c).

Discussion of various issues –

- How to include OID
- Translation to Slovak
- Sign CP/CPS? By? [EE]
- LDAP repository? [probably not]
- Name collisions? [perhaps add disambiguating string?]

Discussion:
JJ: Same serial number in new CA cert?
Yes – so each Mozilla user will have to remove the old CA cert
JJ: Not just restricted to citizens
JJ: firm personal acquaintance (ie attestation)
(Discussion of attestation vs documented records.)
JJ: recommend that you remove personal acquaintance as acceptable identification criterion for EEs to RAs.
JJ: If you translate CP/CPS, should describe which is the authoritative one.
Perhaps just translate user / RA obligations