minutes: Ursula on monday.

Intro: Ursula: 12000 issued, 2000 valid of which 50% users 50% hosts
Sven: 25000 issued, ~3500 valid. 33% user.
DavidG: moving to TCS! (~6000 issued, ~1000 valid).
Reimer: 1200 valid certs and 105 RA's. SLCS is not a lot yet!
Alice: 800 valid users + 800 server = 1600 valid.
catch-all stopped.
Emir + Dolori: 438 issued, 117 active (50/50%).
self-audit issues fixed.
ChristosT: 2500 issued / 700 valid. SEE-GRID is new catch-all for EGI
Milan: going to switch off the current CP and migrate to the new one.
Nuno: new CP/CPS send last week.
Roberto: 2400 valid certs. & 85 RA's of which 15 are international.
moving users to TCS. (with a QRRA hat).
Mine:
Eric: ASGC
Daniel: pkIRIS
DavidCC: TCS has run into local ie policy issues and is on hold.
Thys: still <100 active.
DaveK:
Miroslav: 150 valid (of ~700 issued). 8 RA's
Cosmin: >400 issued, 150 valid.
AlexanderB:
Valentin: Tamas: Jan Jona Javorsek:

Remote: Pawel, Jules.

10:00 Eric: APGridPMA
- NGO request withdrawn - and now looking for new CP in Singapore.
- New Zealand will setup a new CA, but for now supported by ARCS.
- 1404 users, 2672 hosts in total for APGridPMA.
- JP, TW: considering federated CAs.

10:12 TAG (Mine/DaveK):
- remote proofing is most contentious issue in TAGPMA. NIST 800-63 allows remote proofing, based on e.g. utility bills and postal address.
- TAGPMA in Texas in 2 weeks, then Colombia.
- PKP guidelines for SLCS/NICS working.

10:22 RAT (Jens).

- no real incidents.
- SHA1-2.
- what about 1024 → 2048 for EEC's?
- CRL expiration.
- communication tests: 8 of 10 responded within 18 hrs, 4 within 60 min!

Current system works reasonably well.

M/N communication: need to demonstrate things that are broken.

where is the responsibility? CA → } cannot know where to test but need it to work.
RP → communications needed.
Subs. → are clueless.

Action: use a test CA.

- RP's need a test certificate from the CA's
- OSG / EGI can then do the software validation.
- through GIN? not very active anymore. → raise at OGF30.

→ set up page with test CA & certs on the PMA page.
- DFN has a "CA in half-a-day" package.

Taskforce: SHA-2
Jens, Mine, DG, Milan?

- after 2012: not all CA's should migrate at the same time.
- date "Jan 2012" was an educated guess based on SHA1 attacks and RP agility

- IGE training CA can be used to test generate test certs - as long as OpenSSL supports it.

Test Cases: → SHA2 (EEC; CSR; intermediate CAs; CRLs) + mixed chains.

→ 2048 performance should now be less of an issue

- 1024 NIST recommendation → why deviate?

2048 is already commonly in use already by many CA's.

- 768 now routinely breakable with enough desktops or EC2's.
- 2048 is default for Firefox already.

NCSA did some tests. → Jens talks to Sim B. (next test are on public key and is thus faster with a 'simple' public key with a few bits set)

already 2048 bits used frequently. - no test needed

switch is not yet requirement, but it's not forbidden. Recommendation to change.

news already there.

CRL download

still download issues in OSG sites.

three complain about expired CRLs and download issues. Many of these are network issues, esp. with firewalls.

~~~

Chair: re-elected DavidG.

Self/An ? ILCC: no news from Aygul. Jens & Christoph.
(since Berlin)
ChristosT to poke Ole.

§ LIP: complete.

~ UKeSc: new CP/CPS upcoming.

? pkIRBs: no updates yet.

§ ArmeSFo: live audit completed July 2009. detailed review done.
update from Ara sent to list and was thorough.
only minor nits left.

§ SRCE: done and completed with v1.2.

X AEGIS: nothing heard from Dusan

§ SWITCH: OK.

§ NHIF BalticGrid: OK.

BalticGrid: still awaiting replies.

X RDIG: self-audit was sent and Jens reviewed and commented.
~~Jens not~~ there are some lacking items not listed, and not get fully answered.
Technically it should not be terribly wrong. Response is good, CRL OK.
not appeared for 3½. worrisome that there is nobody but Eygene.

Steps: - wait for tomorrow.
- Jan 2011 Utrecht is DEAD
- otherwise suspend automatically.
- David - follow-up via WLCG.
(ACT) - management should know about this last chance

12:35 Milan Sova TCS & TACAR.

- TCS SSL in next distribution.
- TACAR: new website and process → live demo.
with CESNET-CA-3.
the SHA-1 FP of the CA cert is of the DER one, so use openssl --fingerprint.
→ this should be fixed/documented by Chris
→ Request: Java keystore as a format.
~~~

downtimes (DC).

- the website has a notification area
- mailing list? different from announce list, as most RP's won't notice brief downtimes.
- integrating with projects?
- differentiate between DOWN or AT_RISK?

what do we communicate? CRL unavailability, no new service, or? All of them! Messages should be differentiated for users, security teams, sites. Sites only care about CRL & CA web.

(A) Announcements of downtime at least a week before!
on a stable (web) page. Wiki table! on PMA with RSS feed.
Recommendation: 1 wk ↳ as it allows subscription to the page!
RSS feed is only useful if you have a cleaned-up or new page
anyone editing the wiki → design should be RSS friendly + email.
→ other options include RT &c.

Requirements:
- CA's enter their own notifications, authenticated.
- email. (+ RSS as very nice) subscription.
- web-based list output.
- one category at least.
- expiring of old messages. (archiving)

Tech investigations by:
- Christos T
- Milan.
- David CC.

(REC) B Downtime announcement: preferably 2 days in advance. (and not too much earlier!)

NLCR profile. & distribution.
structure is not usually re-packaged locally.
build combination packages with proper dependencies.
> then provide checksum files for big data in the distribution?
downloads of tarballs requires admins to think.
IGTF packages are also intended to be repackaged downstream.
! who uses the 'profiles' separately!? now, everyone takes all RP's.
when real LOA comes in, we will face the issue now dean with the worthless training CA's like in the EUGridPMA case.

HLCA / Jens:

- last discussed OGF 28/29. but since dead.
- * aim is to complete this today, and then have it approved by all PMA's, so that we can then build a test distribution.

§3.3 #3: single provider key for "CA" or "Trust Anchor"? definition is == from definition. confusion on semantics in document text (e.g. on publishing by piece of data) both CA and HLCA or object CA. Terminology is not 100% consistent yet.

① The organisational body should be defined in the glossary.
it is still unclear who is supposed to be responsible. Require "persistent and long term commitment" - like language?
[In the QVad's case, QV also operated the issuing CA, so had to show up.]

② - name space must be provided, but actual writing is usually by IGTF
CA MUST ensure that there is enough information to write the RP NNC and signing policy files.

③ - is support for dynamic hierarchies ("implicit") really needed?
but this is not supported in middleware anyway!
↳ so clean up. and take it out.

New version by OGF 30 with all changes, to be made by Jens.
- other PMA's should comment before that, send 1 week before OGF
- then EUGridPMA shall own the profile.
- maybe document consistent.

~

David K. Birthd NG.

putting requirements on the operation of other authority types. Live editing of the Wiki.
- This document does not actually defines accreditation, but use it for self-assessment (and maybe later to have NGI's do the accreditation)
- The thing accredited would be an IPASP, hosting one or more IP's.
- extend scope to deal with any kind of assertion, but still limit to VOMS?
- try to do without the VOMS word, and see how far we get... incl. common name authorities
<live editing ensues>

09:30

- Eygene - Self-audit of RDIG. [Refer also to Jens' discussion yesterday]
  Eygene presents all "hard" issues from the audit.
  → Slide 5: "designated personnel"?
  Slide 13: not deleting any logs...
  Report is consistent with assessment by Jens, except that the self-audit was too hard on the CA itself.
  How many operators: 2 persons.
  all Revocations come in by phone, which is one of the reasons why CRL issuing works with so few people. Also, the personal union with security incident response means that revocations are known early.
  The PMA commends the fact that this can be done with so few people ...
  Roll-over plan circulate to PMA to resolve the "D".
  Otherwise audit looks OK

  It is seen as essential that RDIG shows up in January 2011. In-person appearance is essential. The ~~best~~ best-effort level historically has not been enough. Non-appearance would affect the accreditation status.
  PMA sees this as important. It has now been much longer.
  Consequences for the Russian Federation and WLCG is severe.
  If help from PMA or WLCG is needed, we can give that!

  PMA thanks Eygene for presenting and the thorough self-audit.

[Dave K to take notes]

David CC - GridIreland Self-audit - see presentation on-line.
  practices are at times better than document.
  changes held off as a new CA was planned, but this has failed to materialise.
- Reviewers: Nano and Jens. - additional doc is available.

NIST 800-63 and Remote Validation (Mine)
  the proofing requirement of L2 require the RP to have read access to the agency/issuer databases!
  Actually: all students in a dorm will share IDs, since they share address and mailbox! Email address is also enough.

[NIST] at L2 security is based on email, the assurance level of passwd/email is highly variable in countries.

In existing IGTF remote has notary publics, e.g. for classic.

new, a level NIST L2/L3 new profile? No (IGTF) do not need to match NIST, exc & but InCommon is using NIST.
CA's with NIST L2/L3 can go into ~~level~~ new bucket.
↳ would RPs pick only MICS, or always pick all anyway?
SLCS already fits for a NIST L2!
~~CILogon~~ CILogon + InCommon may use Comodo as a back-end.
historically InCommon was slightly different from NIST L2/L3.

The InCommon Id vetting adds the student ID as valid, which may result in a circular proofing possibility as per 4.2.2.3.3!
so maybe NIST is not really the issuer. InCommon is moving to NIST, though.
InCommon: also email is enough.

~~Address~~ InCommon: what about the audit trail? Is left to RHO, CA only records issuing RHO.
TCS retained F2F!
Is remote vetting really critical, does it add much to the business case.
Limit it to only F2F? TCS can do that, so why not in US?

WLCG: probably not interested in remote students, as mainly rely on staff and PhD students, and these would show up in-person anyway.
would RP's accept a new profile as they do MICS today? do they think there would not be an effective difference.
ask CILogon for the use cases where remote vetting is critical. for RP's.

We want CILogon in, but based on F2F. So IdP's should differentiate like the TCS does., or CERN

Need to understand RP use case!

SLCS would match Remote. now
also: TCS level has effective high level that needs to be conserved.

- use the subject namespace to differentiate between remote and F2F, and only accept it the F2F namespace under MICS. 2 CA's would be better. (policy OIDs cannot be processed).
  anyway, the audit records of Remote should already indicate in the IdP records whether it was in-person or Remote.

Reliance on national infra like postal system is incomparable and complex between countries. The notarized document of Brazil is at least accessible.

↳ Logbook.
- ask CI Logon for RP use cases for Remote.
- split in 2 CA's (not via namespace)
- new profile is also good solution, but differentiation is better, or RP's with MICS will loose out on F2F vetted people.

TAGPMA may view it as equivalent, ~~given~~ given the national background.

and why is in Common Lower then NIST.?!

Conclusion: EUGridPMA NOT happy to include InCommon Remote as-is.

~~ coffee ~~

License and OS distribution.

Debian (Mattias) is requesting import.
Jenkins redistributes certs under Mozilla Public License 1.1
↳ has lots of us blah in it, do not ebrows.

Meta-data CC-BY = OK.
trust anchors of these present: OK.
CV: OK.

- what about use of IGTF IP in derived works, is misuse then illegal or immoral. Sth last sentence should prevent it
- we license only the trust anchors and metadata, NOT our document and the RP's!
- CC BY should be OK, no trouble from Canada accepted.
- we trust "our" CPs to be happy, and we don't need explicit statements.

Encourage downstream maintainers to make timely (security) updates.
Recommend: updates within ~~an~~ hours.
: naming of RP's on proper name, NOT IGTF ~~~
: meta packages on groups may have IGTF on name.
install in separate (e.g. /etc/grid-security) and not in browser or default server default locations?
- how impact on trust for web shops, and everything else.
- do you trust the grid CA's for on-line banking?

may we restrict use of certs to application domain? Does that conflict with Debian Free Software Guidelines. - and we do limit use of our certs, e.g. no financial transactions. So for Debian we may end up in non-free.
but: requirements are on the subscribers and RPs, so limitation is not on the data itself.
is a bit of hair-splitting, but the package you can use any way you want, so it should be OK.
Many, also commercial CPs, will restrict use, e.g. no life-support equipment or nuclear energy.
(DC) ↳ ask Matthias for ok/statement.

PMA is quite happy with this process!

- also they may be put in the OS default locations, so that some (text-based) browsers etc + servers.
- OS distributors should figure out technical details.
- and ensure that the grid software will work!
(Do link or install in /etc/grid-sec--).

§ Sens: update to PKP - related to XRI/PMA SLCS/MICS update
Changes in line 60 and 80 of Wiki are OK.
OID: ... 1.1.5.2
✓ Approved these changes!

new reviewer.

§ 2.2 - 3g. discusses activated private keys, whereas rest is about de-activated keys

RFC1 close. The intent of 2.2.3g was to allow SLCS certs to be used exactly like user proxies today.
This doc is only about renewal process. The intent of the doc is thus OK, even though it may be unclear. The feedback explains it.
Jens will come up with a new draft that is clearer, and the PMA can see if it actually helps.

~~~ LUNCH ~~~ until 15:00 ~~~

SLCS/MICS updates

version 2.2 SLCS: changes agreed by EGP.
MICS? V1.2 last edited July 14th.
- Suggest remove "In particular ... TTS" in sec. 3. since it's in the PKIPolicy.
- reference to GFD.125 differs between MICS & SLCS.
- In 4.4: revocation requirement seems lost. Is that intentional?
  It is correct, but "second part" about revocation in case ID is compromised is missing.
  Request update.
- in sec 9. de-capitalise "Business Recovery"
  for the RCS, having Comodo have a BCDR plan is enough.
  not needed for access/portal services.
  CPS 5.1 is enough.
  it is not needed for the IdM & IdPs.
  with this endorsement approved.

Fetch-CRL promo

support for 2.8: just in OSG. EOL: early 2012 Q2 for 2.7: eol in 2011 Q2.
OSG: tested new distro 1.35th and it works!! Yeah!
EGI: new format for test oct release!

HAST part of EUMedGrid II. Roberto gives review update.
Roberto sent review, no feedback yet.
new reviews do use excel sheet. would be handy, but is not there for Classic. Would be nice to have that.
Outstanding critical issues: in current issue of CP/CPS.
- request coupling vs identification is unclear.
- CP does not have separate RP's
- no working web site, no DC naming, but PC=SY. Unexplained.
~~~

HIPSTI Review by Roberto.
- missing info should be discussed in PMA.
Reaccreditation still seems quite a long way away; but it's part of EUMedGrid workplan.
They would have liked to come. Trag next in UT, NL.

~~ site visit to SRCE Data Centre ~~~

Dens: Soapbox on trust and science.

~~~ WEDNESDAY ~~~ Not

UKeSc. CA new CP/CPS & Software (Jens)
went through a self audit last year. new CP/CPS not yet finished, but direction is new and it will be a complete re-write
new practices will change, just not changing and s/w.
rewrite is to make it read better and possibly shorter. And split CP & CPS.
No re-accreditation needed,
[look at presentation]
rollover expected in 2011 of the ~~signing~~ certificate.
UKeSc → TAG as advisory body.
Replaced software (one longer Open CP), but database is compatible.
CertWizard Sven GUI tool.
Testing possible? Eg for Reimer to test, but the server is not yet outside firewall.
https://svn.esc.rl.ac.uk/trac/ca/wiki/AuthenTication for protected info. via VPN.
not yet open-request info by mail :-)
Jens will send link.

DavidCC - Check Certs
Alan Sill has some attachments to look at/sit, no action yet.

Tech List is useful. - even if it is quiet.
~~~

Robot certs and PKP:

DdC: can the entire robot key pair itself be in a dedicated MyProxy?
(so not a community one, but a dedicated one).

With the PKP guidelines, a MyProxy as a 'virtual HSM' is compliant and OK,
DFN is already using this

SRCE already done S/A → update table.

Next: 2.5 days in Utrecht.