Present: Remote: Edgars, Dave, Miroslav.
Local: Ursula, DG, Usman, Emir, Reimar, Irwin, Jean-François, Eygnan, Milan, Dóra, Hardi, David K, Nuno, Keith, Christos T, Christos K, Fergus, Willy, Oleg, Sergii, Roberto, David OC, Derek, Scott, Alexandre, Cosmin, Eric.

09.45 Agenda: IPv6, RPS → Scott.
Notes: David OC, Cosmin. (Monday).

10[00] RT <see above>

10[13] Eric AP Grid PMA status.

10[30] Derek. TAG PMA Updates. → Panama meeting will be during the week 35 (end Aug).
IGTF Brazil CA in next 1.6q distribution by end of May.
Classic 4.4 approved → [Global accept now].

10[48] RAT/Dos. RAT needs to be more proactive (prodding members etc) needs a co-chair.
↳ Co-chair. to run: - challenge to RAT on encrypted mail list. (1x per quarter).
- 2x per year response of CA's.

(ACT) . Willy volunteers as co-chair for RAT.

11[00] - 11[30] Coffee.

Christos K. Kellogg grid CP self audit.
See presentation for issues. → fixed in CP/CPS repo and this week CP/CPS.
issuance issues are going to be fixed this week, archival issue: later.

Christos T SEE Grid audit all CA.
There will be a new CA cert for SEEGrid in 2012 (early '13) due to Africa demand on catch-a

(ACT) . Reviews: Edgars, David for both.

11[55] Eric. RA migrations.
separate RPS idea from org membership discussion
RA "accreditation" may explode CA2, turn PMA into moderating body, or with RA's that don't belong to a CA?! RA scope is smaller.
RP's ultimately decide anyway.
RA's with an RPS can migrate easily, but PMA will be strong CA's.
(ACT) : members in new business that will affect the charter, the CPS.

(2)

there may be other policy formats than 3647.
but if the RA does have 3647 you can move amongst CP's.

(AGD). (not in ~~text~~ morning). Time after lunch → Eric issue for NZ.

13^15 lunch → 14^30. accelerating curve of danger → tool available.
- CRL DoS attack avoiding revocation.
-

OCSP response in TLS session. Milan.

attacks include: impersonation, but also changing validity status
blackmail against CA.

- PRACE → no s/w concerns (Globus Unicore).
tested? only OSG list, for Unicore since it's java.
what to test? CRLs, server + client certs with SHA-2 (for all services).
and all variants? 256 or 512.
NIST does not ~~stay~~ say which SHA-2 version..
we? should at least 256 and 512. m/w needs to parse all.
we should maintain the panic level. In USFed, ban was placed on using SHA-1.
(ACT). UMD-2 certification: use SHA-2 for testing. 256+512

rekey is required? (NIST reason): issuing CA that signed SHA-1 and re-use it,
so that the attacker can sign SHA-2 objects using SHA-1 set of keys?!
but that is again breaking RSA.
revoke old certs should also help - since we use CRL's unlike the rest :-)

(ACT). CA's should test if their s/w can change to SHA-2 now?! themselves.... ...

v0.3

09:00 Call on mailing list for those who would definitely go to either the Dublin or to Florence.
Dates: 10-12 Sept 2012 (Lyon); 14-16 Jan 2013 (TBD); 13-15 May 2013 (Uppsala); 9-11 Sept 2013 (Bucharest).

09:05 Dave K. <Live editing>

11:00 Eric RA migration / multi-CA ops. [Monday's slides]
RA's should keep document to be able to migrate.
namespaces will be clipped.
how to associate new request to existing vetting data.

Best scenario: CA1 will terminate but allows for natural death, and they arrange to move to CA2 and re-use all staff including the RA's. CA1 will only do CRL's.
- then why not re-root the hierarchy and transfer keys of CA1?
- encrypted data is also an issue - same for escrowed.
or re-issue based on existing card, authenticating with card of CA1.
↳
Revocation stays also be CA2.

* RA has to keep auditing data
* CA2 has to audit doc. evidence of RA for compliance.
* CA2 will issue in new namespace.
* CA1 will stay in basic operation, to allow its users to authenticate to CA 2.
* Authentication of users @ CA2 RA's new requests to existing documentary evidence of RA.

Rest of 13:00 (OU) EUN: OU op review next 3 weeks by Usman Tayyab. Acc. by email thereafter, → distr. by end of June 9

Roberto. revocation of the certs will be needed. Roberto is writing the CP/CPS.
but implementation is not ready yet anyway.
to prevent renewal by end-users, the service should not be require authN through IdP.

- How will knows that the HRxy holds the keys, and it will be a new CA.
- Can this 'central mgt' CP instance be shared across countries as a nice central service.
- Pen testing invited by Roberto (controlled please :-).

↓ 'TOS' like business model.

David CC 13[55] Grid-Ireland Update.
robots as presented are OK. DavidCC to send new CP/CPS in the next few weeks. The content will be accepted.

Scott 14[15] Revoc. enh. PKI.

15[45] Sens PKCNP. / Soapbox.
(AT) draft Word on new wiki to be written by Sens (BEFORE OGF33, where it will be discussed.
16[30] Sens Soapbox

Wed. ag[30] Scott <see presentation>Δ

IPv6: CDP v6: host on v6 + AAAA record.
(AT)- preferably before 1 oct 2012, warnings months before, weekly after until v6 endpoint is deployed.

⟹ ALL CA's to provide IPv6 endpoint for CRL + AAAA record by 1 oct 2012. ⟸

Lunch 11[30]-13[00]

OCSP 13[00]. - use lightweight "GET".
- is HW ready? It might already be implicit on simple configuration.
- publish end-point in AIA.
- ocsp daemon is there → OpenCA would if now multi-threaded. with HSMs. Non HSM is OK. HT
- does server-side support stapling? → anyway EGI RT ticket.
- http+ lightweight should be doable. (for all except Mozilla NSS) → works for CDN's.
- CABForum will write two whitepapers: one on server, one on client.
- for heavyweight ocsp need to issue signing cert → update CP/CPS.
  lightweight ocsp → can be signed by issuing CA or Root.

OCSP (cntd). if ocsp response is signed by issuing CA the response can be a lot shorter.

preference: - practice documentation and refer to CABForum doc.
- start implementation for all existing IGTF CAs → deploy OCSP
(ACA). - include AIA by 1 Jan 2013.
- from then on, AIA in client certs can be used, will still take 400 days.
- there should be controls around the responder server and it should be very controlled. OCSP 'heavyweight' signing and should be 'short lived'. Then the key preferred on HSM, or well secured.
- precomputed is a lot better. → 0-day validity? → precompute future responses in case of off-line CA.
- You may need to update your CP/CPS for the OCSP cert for OCSP.

What kind of issues? Unknown = = bad is a client-side decision. See CABForum.

SHA1 Exc → Jules gets input from PRACE-RI & Unicore. → RP involvement.

- IGTF needs capability now anyway. → report by Oct 1st (certs + CRL)
- live in the sand on Jan 1st 2013. (once m/w fails in due → see RAT doc)
- other doc → explanation to users.
- post Jan 1st 2013 users should be able to get SHA-2 from all by default to allow 'good' users to migrate in orderly fashion.

- for SHA-1 after 2013-01-01 → shorter cert life time? :-)
→ final date will then remain mid-2014.
some CA's may do this, but not all.

test CA: OpenID from NCSA. for testing, is in IGTF exp. distro.

EUGridPMA 25 (6)

DAOB NP Dwell. <finalize document>.
The discussion on sec 6 converged.

GFD125 new version on agenda page.