* Dawson, Mike. taking minutes
* Eric Yen presenting for AP
* Jim Basney presenting for TAG with Vinod's slides.
  - IGTF charter change for namespace mngt approved.
  - Interoperability section 3.3 remained unclear to TAG, should be discussed by EUGridPMA as well.
  - Four Bridge CA group formed in USA, the Bridge WG to look at interoperation. (Some activities ongoing in SURA and MS Windows)
  - Joint Meeting: Canadian Thanksgiving might be in this weekend.

Jim: RAT summary.

#2: - Polish Grid already switched to SHA-1
- globus: proxy will use the hash function of the EEC.
- CERN CA had the DSA keys (for host certs). NO EC DSA.
- Sara will default to DSA.

#6: - RAT survey: still missing new Polish Grid (fixed now) and IUCC. Follow up with IUCC

#8: Survey system: Dans might be able to get a 'private' service from RAL / Janet.

public results publication of response time (not info).

NO	YES
inhomogeneity in fabric	peer pressure to improve.
operators are not authorized to respond to surveys, but only to actions, if it's made public.	

acknowledgements may be enough. needing email for response to revocation. (e.g. for revocation).

There is a difference between a revocation and a survey. But RAT also needs statements in order to release public announcements. Issue is with response in the infrastructure as a whole. Like firedrills.

* Firedrills and tests will be done (agreed).
* For publication only high level statistics, not naming CAs, like in slide #7.

RAT

Mike: SHA-2 support in laptops will remain a problem for very long.
- ask IDTrust, cryptographers were not overly concerned
- vulnerabilities in SHA-1 may also apply to the SHA-2 suite.

Jens: - uptake of MD5 was slow (years) after algo was broken
- new algo contest might be implemented before SHA-2 gets there!

Urban - Serious break of SHA will be a myth/rumor anyway.

Willy: - if we don't change to SHA-2+, middle zone will never change. We should sound the alarm.

Milan: - should only at those that will listen ...

Mike: - CA certs are the most vulnerable? Jim: not for their trust anchor, since they are manually installed. (self-signed).

Jens: - what about 1024 RSA.
at least we know we can migrate to 2048/4096 immediately. We can't do it with SHA-2 yet.

Mike: - there is a lot more than OpenSSL.

David L: announce we ~~will~~ may stand with SHA-2 by end 2010.

David CC: - who should be surveying it? NIST?

Willy: - write a roadmap and let the shouting start!
↳ give advise and example CA/certs.

Milan: - we should also be careful, since a false alarm will derail future IGTF warnings.

David L: * "We need the ability to move to SHA-2 if the old ones break".
* "So, you must ~~[illegible]~~ support SHA-2"

Milan: requirements without reason sound weird, c.f. IETF response to NIST.

RPs don't track new distributions. After a month, still 25% using old CRLs for DoEGrids.
* List should not be public, since this is the list of ill-managed machines.
* We can't do too much about it., as we agreed last time.
→ distribute list internally so CA's in a country can follow up.

Peer Review: Jens: it's a lot like an operational review.
peering reviewers is the way to go.
Christos: started NIF review, but only public items, private items cannot be checked.

(Act) Review status monitoring:

- keep A/B/C/D status on Wiki sub-area.
- Wiki area closed (r/w) to members only
- Reviewers poster CA for updates and status changes
- Chair will poster reviewers.
- PMA web site has global status, based on reviewers + link to Wiki

* changes as fast as reasonably possible, but anyway within 6 mo.**
* reviewers to keep track as often as reasonable,
* agree with reviewers on exact time line.

Nilly: Austrian Grid CA.

(INFO) Java applet: access permission bits to c400 perkey, Requires Java 1.6+

Jens Ø. at: CRL of root can be long, eg. 1 yr. (in classic profile, 30 day slg is on issuing CAs).

(Act) Root profile: discussed but not ready yet

DG: EGEE & WLCG doesn't accept it yet! → SSPG!

Jens: prefer separate CP/CPS's for Root and Issuing.

Nilly: what to insert in TACAR? both Roots and subordinates are in today, but only roots are really needed.

Christos T: Yoalang: store on Wiki, Nilly: will do.

Tewi: the production CA is on a VM. Nilly: but the physical, second machine does the whole process of CSR to CERT, the VM is only a web thing.

Alessandro: the checks are all on the server side? Nilly: yes.

Milan: CRL's? DG: old CA should issue CRL's as usual until last cert has expired. Then, stop or revoke the issuing CA itself :-).

Milan: fingerprint reader is weak, since there are plenty of fingerprints right next to the reader ;-).

Reimer: which model? Nilly: model B.

David OC:

DG: RDN element sequence for Users, Hosts or Robots? If you want to use them in namespacing, put these earlier, just after dc=grid; may relabel to DC=Users; or DC=Robots, ...

(REMD) Q: Robots in "virtual smart cards"? Discuss tomorrow.

Jan M

Issuing CA: → TERENA TCS from COMODO? Being looked at, no timeline yet

* continuity: good 8 yrs w/ COMODO so far: we can swap out the backend and setup our own in 6-8 mo. to guarantee it after 2014.
* traceability to physical person: follow incident response model for getting personal information.
* IdP will release a displayName for use in sDN.

→ consensus on agreement structure through federations and IdP ↔ SP contracts.

Timely revocation should be in the IdP agreement (but easy to explain) [Alessandro?]
Tenn: deprovisioning is usually the most difficult.

Dave K: How valuable is the federated account? Are you going to require that the fed. account is the primary HP account?
Jan: today with can deal only with "good" federations.

"Active" accounts only? (i.e. the accounts are used regularly, e.g. for protecting valuable stuff). Jan: could be put in the service agreement with the IdP's.

No blockers! :-)

Pawel

Technical profile → push for implementation.
(Pct) new CA combat cookie: request it for 1.30 release.

Jens: → in similar RA situation where there were no copies, said RA was required to collect these within 1-3 mo.
DG: other option for traceability (and RA turnover:) collect hand-written signatures to get compliance with Data Protection Laws (since Poland has no reasonable exceptions)
Pawel: Polish CA 2.0 project has work package to address this. but this is a long-ish project...
Reviewers: Dave K., David OC.

Eric: Dramatic Incidents.

Milan: SIERENA TCS

server certs first. Recv. of pers. certs by September?

Pick reviewers when CP/CPS req. Mike +

format is not exactly RFC3. Milly objects to the format, but the IGTF PP has a "standard" and although others sympathise with Milly, its not blocking. Just a change for the reviewers, and Dave points out that content is most important and format does not necessarily help. This is a pre existing CP and is acceptable.

- no issues with this for majority.

Jan: Nagios.

CRL Rollover: add to cdl.url file (comma separated in .info?)

Alexey. CERN CA.

- Yoshio's auditing doc has question & Ans.
- Reviewers: Mike, Feyza

Mike Await Review result presentation.

review was satisfactory → all OK! & DONE → (Act) reset timer.

MICS / David Groep

In 4.4: .... The IdM ... has already changed.

Suggestion to Tag pma.

Review of all changes, based on Mary's presentation:

- lots of activities, but more blocking
- suggestion for future version.

(DEC) EUGridPMA accepts v1.1 as of May 2nd. → approved version attached to agenda

---

LUNCH

Roman Brunner / QuoVadis.

Jens:

Docs

create an HG. to actually make progress on docs., like for the AD profile.
* start with concrete use case; or req.

Approved ideas, HG would contain: - Sens (has astore)
- ChristosT (idem) + K.
- Mike
- Jim B
- Dawidl.

Phases ① look at requirements } split work in to sections and
② use cases. } assign work.

StHTokens: - addition in 6.1.1. is useful for operational purposes } → new "non-export" ISCP
- add: hyg gen quality.

→ lots of new ISCPs, only "hosts" pending → others on agenda page.

~~WEDNESDAY~~

* - Next Meeting: Berlin : Hotel before Aug 3
* - Majid: - RFC 2527 → 3647 migration took several weeks full time over a couple of month
- easier than, e.g. DoEGrids, since the doc was reviewed and accredited recently and many reviewer comments still applicable.
* Mike: Res: - distribution is ok, H/P is really good.
- one cert for all: good idea, no concrete action yet. → see how it works w/ DoEGrids first
* Christos K: stores.
issues with stores to be discussed in the HG.
include discussion on liability, and availability.
- if you use certs for high-value resources, availability is involved.
- difference between repo's that generate or merely store keys?
HG to follow up and report back.
RP's should check back, based on list of options.

DG: Data centre move → no concerns.

LUNCH

Eric:

Eric: OA Federation Ideas in the AP.

Mike: Slide #11. Looks a lot like what would be needed in the USA.

David: discuss at an IGTF all-hands?

Milan: Use in AP Region (except .au) should be in REFEDS.

RPDNC: only Sens & DG going to OGF Chapel Hill. :-(

Wiki: David: request a part of the Wiki to be public
↳ David OC to reply
- use an SCS cert for the site.

For OGF: - define what we mean by "traceability".
- working party on private key protection.

Monday 11th

Participants 16th EUGridPMA meeting

Meeting Information	Registration

		Name	Affiliation	Membership
✓	1	David Groep	Nikhef	DutchGrid CA
✓	2	Willy Weisz	University of Vienna	AustrianGrid CA
✓	3	Reimer Karlsen-Masur	DFN-CERT Services GmbH	DFN-PKI GridGermany
✓	4	Majid Arabgol	IPM	IRAN-GRID CA
✓	5	Shahin Rouhani	IPM	IRAN-GRID CA
✓	6	Jan Meijer	UNINETT	TERENA Grid CA Services pilot project
✓	7	Teun Nijssen	Tilburg University	TERENA Grid CA Services pilot project
✓	8	Alessandro Usai	SWITCH	SWITCH
✓	9	David O'Callaghan	Trinity College Dublin	Grid-Ireland CA
✓	10	Jim Basney	NCSA	OSG
✓	11	Michael Helm	ESnet/LBNL	DOEGrids
✓	12	Dusan Radovanovic	University of Belgrade	AEGIS
✓	13	Kaspar Brand	SWITCH	SWITCH CA
	14	Christoph Witzig	SWITCH	SWITCH CA
✓	15	Alexey Tselishchev	CERN	CERN CA
✓	16	David Kelsey	STFC-RAL	WLCG RP
✓	17	Feyza Eryol	TUBITAK-ULAKBIM	TR-Grid CA
✓	18	Nuno Dias	LIP	LIPCA
✓	19	Jan Jona Javorsek	JSI, Slovenia	SiGNET CA
	~~20~~	Borut Kersevan	JSI, Slovenia	SiGNET CA
✓	21	Jens Jensen	STFC RAL	UK e-Science CA
✓	22	Cosmin Nistor	Romanian Space Agency (ROSA)	RomanianGRID CA
✓	23	Alexandru Bobe	Romanian Space Agency (ROSA)	RomanianGRID CA
✓	24	Alice de Bignicourt	UREC / CNRS	GRID-FR
✓	25	Pawel Wolniewicz	PSNC	Polish Grid CA
	26	Valentin Pocotilenco	RENAM	MD-Grid CA
✓	27	Milan Sova	CESNET	CESNET CA
✓	28	Daniel Garcia	RedIRIS - Red.es	pkIRISGrid CA
✓	29	Christos Triantafyllidis	AUTH / GRNET	HellasGrid CA / SEE-GRID CA
	~~30~~	Christos Kanellopoulos	AUTH / GRNET	HellasGrid CA / SEE-GRID CA
✓	31	Eric Yen	ASGC	ASGCCA
✓	32	Anders Waananen	NBI	NorduGrid

This is a test