

* Danson, Mike. taking minutes

* Eric Yen presenting for IAP

* Jim Brasney presenting for TAG with Vinod's slides.

- IETF charter change for namespace might approved.

- ~~Accessibility~~ section 3.3 remained unclear to TAG, should be discussed by EU/IAP as well.

- Four Bridge CA group formed in USA, the Bridge WG to look at inter-operation. (Some activities ongoing in SURP and MS Windows)

- Joint Meeting: Connection theme's giving might be in this week-end.

Jim: RAT summary.

#2: - Polish Grid already switched to STP-1

- Global: proxy will use the hash function of the EEC.

- CERN CA had the DSP keys (for host certs). No EC DSP.

- Sown will default to DSP.

#6: - RAT survey: still missing new Polish Grid (fixed now) and

LUCC. Follow up with LUCC

#8: Survey system: Dons might be able to get a 'private' service from PIA / Sernet.

public results publication of response time (not info).

NO

YES

inhomogeneity in fabric

peer pressure to improve

producers are not authorized to respond to surveys, but only to actions, if its made public.

acknowledge merits may be enough.
sending email for response to revocation.

(e.g. for revocation).

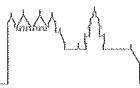
There is a difference between a revocation and a survey. But

RAT also needs statements in order to release public announcements.

Issue is with response in the infrastructure as a whole. Like fire drills.

* Fire drills and tests will be done (agreed).

* For publication only high level statistics, not naming CAs, like in slide #7.



SHA

Mike: SHA-2 support in laptops will remain a problem for very long.

- at IDTrust, cryptographers were not overly concerned
- vulnerabilities in SHA-1 may also apply to the SHA-2 suite.

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

Milan: - trivial break of SHA will be a nightmare anyway.

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

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

Mike: - CA certs are the most vulnerable? Jim: not for true trust anchors, since they are manually installed. (self-signer).

Tenn: - 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: announce we ^{may} stand with SHA-2 by end 2010.

David CC: - who should be managing it? IANIG?

Willy: - write a roadmap and let the shouting start!

↳ give advice and example CA/certs.

Milan: - we should also be careful, since a false alarm will derail the future IETF workings.

David: * "we need the ability to move to SHA-2 if ~~the~~ old ones break"

* "so, you must ~~strongly~~ support SHA-2"

Milan: requirements without reason would work, c.f. IETF response to NIST.

RPB don't track new distributions. After a month, still 25% using old CRLEW for DoE Qrds.

* List should not be public, since this is the list of ill-managed machines.

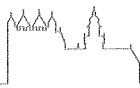
* We can't do too much about it., as we agreed last time.

→ distribute list internally so CA's in a country can follow up.

Dean Review: Sim: it's a bit like an operational review.

proving reviews is the way to go.

Christa: started NIST 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 (open) to members only
- Reviewers paste CR for updates and status changes
- Chair will paste reviewers
- PTH 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 CR.

(INFO)

Anna applied: access permission box to 0400 forkey, Requires dnwa 1.6+

Jens & al: CRL of root can be long, eg. 1 yr. (in classic profile, 30 day sig is on issuing CRs).

(Act)

Root profile: discussed but not ready yet

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

Jens: prefer separate CR/CRS's for Root and Issuing.

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

Christof: Yooling: show on Wiki, Nilly: will do.

Tenn: the production CR 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. 8

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

Milan: CRL's? DG: old CR should issue CRL's as usual until last cert has expired. Then, stop or revoke the issuing CR 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 naming, put those earlier, just after @=grid; or may relate to DC=www; or DC=Robots, ...

(PEND)

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



Jan M

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

* continuity: prod 3 yrs if COMODO fails: we can swap out the lockend and setup our own in 6-8 wks. to guarantee it after 2018.

* 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.

David: how valuable is the federated account? Are you going to require that the fed. account is the primary H/P account?

Jan: today rather 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! :-)

Panel

technical profile → push for implementation.

(Act) new CA control address: request it for 1.30 release.

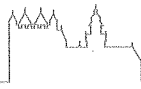
Jens: → in similar RA situation where there were no copies, since RA was required to collect those within 1-3 mo.

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)

Panel: Polish CA 2.0 project has work package to address this. but this is a longish project...

Reviewers: David K., David OC.

Eric: Dramatic Incidents.



Milan: GERENA TCS

server costs first. Recs. of pers. costs by September?

Pick reviewers when editors req. Mike +

format is not exactly 30/7. Willy objects to the format, but the IRTF PAP has a "should" and although others sympathise with Willy, its not blocking. Just a change for the reviewers, and Jens 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.

CRT failover: add to cal. out file (comma separated in .info?)

Alexey: CERN CP.

- Yoshio's auditing doc has question to take.

- Reviewers: Mike, Feyza

Mike Audit Review result presentation.

review was satisfactory → all ok! & DONE

→ (Act) reset timer.

MICS / David Croop

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

suggestion to tag pma.

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

- lots of activities, but none blocking.

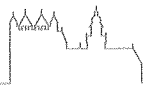
- suggestion for future version.

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

LUNCH

Roman Brunner / Quo Vadis.

Jens:



Docs

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

- Approved roles, req would contain:
- Jens (has a store)
 - Christos T (idum) + K.
 - Mike
 - Jim B
 - Dawidly

- Phases ① look at requirements
② use cases.

} split work in to sections and
} assign work.



JHTokens: - addition in 6.1.1. is useful for operational purposes }
 - add: by gen quality. } → new "non-export" 1SCP

→ lots of new 1SCPs, only "hosts" pending, → others on agenda page.

~~WEDNESDAY~~ ~~XXXXXXXXXXXXXXXXXXXX~~

* - 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. DoE grids, since the doc was reviewed and accredited recently and many reviewer comments still applicable.

* Mike: Req: - distribution is ok, H/A is really good.

- agreed for all: good idea, no concrete action yet. → see how it works w/ DoE grids first

* Christos K: stores

issues with stores to be discussed in the req.

include discussion on triability, and availability.

- if you use cuts for high-value resources, only LT is involved.

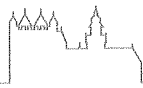
- differentiate between req's that generate or merely store keys?

req to follow up and report back.

RP's should check back, based on list of options.

DG: Data centre move → no concerns.

UNCH
Erm:



Eric: OPA Federation Ideas in the AP.

Mike: Schlechter: looks a lot like what would be needed in the USA.

David: discuss not an IGF all-hands?

Mike: who in AP Region (except .au) should be in REFED3.

RPDNC: only Jens & DG going to OGF Chapel Hill. 2-C

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