09[45].

Nabil Welcome.

Connected Participants: setup video + Adobe. See list of participants.

Hassan. HARNAN. → see presentation.
Geant link more exp. than general IP. only EU NRENs. through Geant.
Rest (ES, I2) through general telco IP.

Eric. (60[th]). AP Status. →
many countries joined EGI & INSPIRE
MSA → Mongolian Academy of Sciences is instantiating.

TAGPMA. Dave K + Milan + DG? going to ORNL.

IGTF RAT (Jens). comm. test outstanding.
Other issues: support SHA2 in s/w. Talked to GIN in OGF. Discuss in Lyon.
Rest in Soapbox.
DG: discuss Djinder etc. New profiles are better, but useless you have
credit card! there is no certainty. But checking is even the point!!
These attacks were very resourceful. Do we stand a chance.

SA: BG.ACAD: still pending. Edgars + Dana reviewing.
MARGI: awaiting CP/CPS upd.
Baltic redo? expired → ask. Baltic Grid people.
(ACI). INCC: MUST in Yabl. or be kicked out.
should migrate to PCS. esc?!
Ule: new CP/CPS tomorrow,
pkIRIS: no news, Jens to ping Javi.
gridIreland: Nuno waiting for CP/CPS. David OC will send once.
DPA section is complete.
DFN: is OK. / Done.

10[20] [coffee break until 10[50]]

Feyzan. EUMed Update:

* HIAST accreditated end of June.
* Algeria is next. almost done, review done and now on-line.
  last call ends on Sep. 20.
* JUNET: is present.
* TNGrid: CP/CPS, bid awaiting introduction. Present tomorrow.
* Egypt: waiting for online repo before application. (next mo).
* UAE: present, not on line yet.

TN (+EG) will send general info doc for introduction to PMA.

Ahmed. Ankabut: see presentation
very much progress → Ready. RSN! :-).

Anwar JUnet: presentation. Q's:

* naming: c= → dc ? Trade Registration ja ensures unique name.
* CP and on-line does not match! (extensions). will update CP/CPS. Online OK!
* PolicyOID: add classic AP OID? Online OK.

#9 * linkage of request. to vetting? PIN code.
#10 * sysadmin eligibility? → whois DB lookup.
#11 * last issue: doubles?! :-) 8.
#12 * can a CSIRT request presenting evidence of violation? [CP/CPS upd]
#13 * patches to off-line system. How? CD + USB → think about it :-).
#15 * (copies of) ID's: risk in keeping them for ID theft? in Jordan that's OK.
#16 * auditing by PMA members (incl. RP's). is OK as well for RP's.

Next: send update CP/CPS and Milan + DG to check their questions.
beg in two weeks.
after that another 2 wk final email call accreditation on list.

13[30] [Lunch 14[00]]

Kaum MAGrid update.

Fedora 4?! → no. It has been through patched to later Fedora's F14+.

MARWAN vs MaGrid. No reason to have two → MARWAN to supersede MaGrid.
if the policy are almost the same.

Ankabut will also become a generic CA (will drop "grid" everywhere).

15[05] Cosmin SELF-audit

quite rigorous. Peer reviewers: Ursula + Yury.

peer review process as policy expert. Ds major rewrite.

15[50] Jean-C/R BEGrid update.

migration. Homeless users also problem in CESNET.

Acceptable solution by TCS is a special IDP and use existing RA structure to manage the IdP.

But the federation rules may prohibit it, which may block BE federation. outside the federation it may then live.

[tea]

16[30] Milan TACAR update. → doc on agenda.

(PCI). agree on policy this meeting.

Tuesday 13 09[30]

Yury 2 Belarusian CA. S/A.

↳ section numbers in GFD 169 should be checked. Can there be variants as to where to find certain info?

Most major change to AP was in Oct 2008, so by accreditation time in Apr. 2009, the CP/CPS was very old.

2 (of 3) RA's "dead" due to lack of funding :-).

* REVIEWERS: Ursula, DG.

09[35] Onur. TR-Grid.

already new CP/CPS prepared.

Q: videoconf ID: based on .br model with paper trail. TR has global DB and vetting for all eligible applicants in academia & chain of control.

Q: do you ask appl. to read CP/CPS? User cannot really read CP/CPS :-) Should understand obligations.

REV: Jean-Chr. R; David CC.

TN Grid Reviewers: Alexandru, Fayaz.

CERN.CP. * also process for renewals would be useful :-)
describe this one case as well..!
* also for virtual hosts?
* Ursula is also interested in this model. But would it then work for other sites than Karlsruhe.
* how to guarantee that only proper CM Robots are allowed to request.
Share with other PMA.
* DFN: in another phi (1000 access points etc) similar problem. There CSR generated and the request form handeled. The RP's generate. their own request. These are essentially batched classic request.
* SCEP? Use case? There are several protocols to facilitate the SCEP requests. Also CMC.
* as orthogonal to trust and vetting.

Need text proposal, but if secure PMA would approve of this kind of pratice.

[$11^{00} \rightarrow 11^{30}$ Coffee]

11^{30} Marco B. IGI Portal.

[@: separate MICS? How many portals?? Renewal of proxy from MICS sent?
Auditing of portals by the MICS CP vs. PKP guidelines]

Reimer: storage of private key. Consistent?
Store PIC in MyProxy. Why also the portal.
Why not store long-term proxies in MyProxy. for #1.
for #2. Store on MyProxy.

Marco: store in MyProxy server. all PIC's.
Reimer: Upload of PIC? Why not a lt. proxy at user end?
user end cannot do that easily. Portal only transient stuff.
User end has no software whatsoever.

DG+Reiner Fat or Thin Portal? Combine bridge + MyProxy and cert/PK uploader on a single? Does that make sense.

Marco will be separate s/w module. Could be on ded. machine. shared by multiple portal & submitters.

⇒ Will be separate box handling security functions.

MICS / TCS responsibility for cred mngt. CP/CPS ok for Roberto. software may be problem, GARR / IDEM ok. TCS likely ok as well.

* own CA? No, if GARR / IDEM ok then is no need. And MICS is complex + costly. 1 CA per country!

⇒ Separate box ingr! Reiner: CA bridge + MyProxy logical combination.

* Remove MICS CA keypair after MyProxy upload? Considering ok.

Reiner UC#1: payloading of PK must be to security box, NOT to general portal. CA bridge box must handle the upload.

may there be many MyProxy boxes? There is only one (dedicated) one. linked to the portal.

[12:30 Lunch → 14:00]

14:00 Jens PKP Updated Guidelines. PKP WG

= expand also for OPS, but focus on EE's persons incl. Roberto.

#13: ack important if somebody else is generating the keypairs

#15: becomes the proxy also within the realm of the CA. (c.f. long (1yr) proxies!).

Destruction: cf. IGTF Portal case.

Reiner: why can IA (CA) not generate? Trust issue is complex whenever somebody else (! subscr.) generated. The IA/CA is as trusted as others...

Currently status 3rd party/CA unclear. Reiner+DG think 2nd party ≡ LHO. so 3rd party is anybodyelse.

Jens: Key word is "duty of care" to make auditing plausible and "stand up in court"
→ infra needs to ensure that, and the CA is already the trusted entity in the exchange.
a "rogue CA" is an artificial risk. It's auditability + that's important.

Reiner: burden on EE may increase in paperwork needed for the audit trail.
e.g. auto-portal. Should log. making it more difficult.
Jens: Electronic log. of steps.
RHM: How to document uploading of EE key?

- Also advantged in CA generating keys. (cf OpenCA) in key + rnd quality.
and better central knowledge.
- select by OID LOA in keygen.
- users should be allowed to generate their own keypair! ✱ Keep option.
↳ should be a requirement of the AP.

Issue was that CA's had problems in accepting responsibility for generation and destruction.
First get terminology right.
AP already shifted.

* Next: draft new policy text for private keys.
⇒ Should be clear for EE's what is allowed!

(ACT). Jens to come with draft text by end of Nov. Circulate to mailing list.
Conclude by next meeting in Sam.

[15:30 – 16:00 tea]

16:00 Jens CA Roll over./ new policy. c.f. the selfaudit open issues.
* start with the off-line CA 2B.
* 30-day rekey window.
* OpenCA WE hacks mostly no longer relevant.
# 6 "CN" = Cert Wizard app server. PeCR2 ≤ bulk request tool (in PERL w/ REST).
* No current plans to accredit SSO.
Full subscriber name release possibly in Moonshot (not current SWITCHaai).

Jens Rollover.

Jens will send new CP when complete to Willy & Alexey
should be a rewrite, not a new policy, once complete.

Currently still operating under old CP/CPS with 2A+2B as well.

17^00 PGP key signing party.

17^30 Closing.

Wed 14th 09^30

Mischa KIT SIA. See document/slides.

#5 Robot naming: abstract function like "client."
URL's have fzk since it is not yet migrated to "kit.edu."

GFD 16q check? ~~not yet~~ based on 2-yr old review? Not yet. this change driven by name change.
New review/SIA by end of year.

Send to list (Mirosław to comment). and w/ 2wk. default OK.

10^00 Future Meetings May. 7.-9. @ Karlsruhe. 2½ day. Need techy?
ask people to contribute techy/app topics on PKI, federation or see. m/w.
* apps using PKI.
* OCSP & HSM.
* namespace stuff & RPDNC. * glite 3.2.
* release schedule.
* Federation EEF. results.

(RG) - [2-3 new EEF Id Fed NS]

(RG) @ 27th Same Standards. WAE. offer!

16th Sens BB.

CommonName: is there not another requirement to have a CN?!
ought to be there!
EGI RP's actually insisted in questionnaire on the Real Name in CN.
wording is now unclear in RP's. Question of SPOKES is coming back, although
there are 7 things blocking it.

* Moonshot RP/IdPs? ↔ link to STS and generalised SLCS
- since SAML assertions are short-lived anyway.

[→ 10:30]

(AG). (A). present Moonshot in Ljubjana. by Sens. + hands-on.

AOB: Sens: namespaces update? Sept 26th
last Monday of each month.

DG

Participants 23nd EUGridPMA meeting, Marrakesh 2011

Monday

		Name	Affiliation	Membership
✓	1	David Groep	Nikhef	DutchGrid and EGI
✓	2	Dusan Radovanovic	University of Belgrade	AEGIS CA
✓	3	Ahmed Dabbagh	Ankabut	Ankabut-Grid
✓	4	Ursula Epting	Karlsruhe Institute of Technology (KIT)	GridKa-CA
✓	5	Dobrisa Dobrenic	SRCE (University Computing Centre Zagreb)	SRCE CA
✓	6	Oleg Alienin	NTUU KPI	UGRID CA
✓	7	Sergii Stirenko	NTUU KPI	UGRID CA
✓	8	Anwar Al-Yousef	JUNet	JUNet
X tomorrow	9	Khalil AJAMI	HIAST	HIAST
✓	10	Yury Ziamtsou	UIIP NASB	Belarusian Grid CA
✓	11	Onur Temizsoylu	TUBITAK ULAKBIM	TR-Grid CA
✓	12	Hassan Bouhaddou	CNRST	MaGrid CA
✓	13	Nabil Talhaoui	CNRST	MaGrid CA
✓	14	Karim Oustouh	CNRST	MaGrid CA
✓	15	Milan Sova	CESNET	CESNET CA
✓	16	Jean-François Guezou	RENATER	GRID-FR
X	17	Jean-Christophe Real	BELNET	BEgrid
X tomorrow	18	Bouhamidi My El Mehdi	Cadi Ayyad University	MAGRID CA

Video:

Andrei N. §
Cosmin. §
Alexandre Babu §
David OC. (~~no Sirca~~)

Miroslav. §.

Jens. §
Fayza §
Roberto C.
~~Eric Yen~~

Adobe §

Vladimir
~~+ §~~.

Edgars.

410 Remote.