Agenda. [20070919]

- Requesters per country.

27-29 Feb 2008
7th TAGPMA
Berkeley, CA (LBL)
(All IGTF?)

→ closed list needed for compromise.

→ OpenID pilot (Fri).

→ country 'ownership' (also: CyGrid issue)

↳ INFN

DG: email to Roberto what happened.

ACT

RTU

- CESNET: new CAs backed by the ID Federation.
- UKeSc: 50-60 RA's; 1200 people; 2000 hosts
  Root CA 'suspected compromise'.
- LIP: looking for new S/N; 398 issued
- Grid-FR: planning/looking into ID Federation.
- pkIRIS: 10000 issued; 25 RA's.
- DoE: between 2 PMA's; gateway CA between ID Federations.
  rewrite Root CP/CPS. → where? → ElCoTAG?
- DFN: 150 hosted CA's; 4 hierarchies (Grid is one) other subordinate of Telekom in DE, Mozilla by 2008).
  grid: 61 RA's
  Rollover: July '09 rollover for EE issuing CA (end May 2008)
- SWITCH: SLCS ~200 issued; classic → no changes.
- ASGCC: AP-catch-all; rollover. in Oct.
- CyGrid: 145 certs. Tamis left; Kyriakos back for training.
- DE: physical updated; no change in EE profile yet → 2 mo
- HellasGrid: rolled over.; RA schema changed. (LHO active).
  SEEGRID catch-all phasing out. (18-24 months)
  OpenID from PKI

Vinod

11:10 Sergey → 30 char was too long to type or remember (comment by Milan
→ new version w/ issue from slide #4 fixed tomorrow (1.2).
→ reiterate w/ reviewers; in parallel start op. tests; email accred is an option. otherwise in APS.

Willy → in-depth update.
→ verification of SAN email address: by RA is too error prone.

→ check YT's doc
Jan '08: DoEGrids
Belnet
IUCC
HellasGrid.
SlovakGrid TBC
CyGrid.

ACT

11:30 Anders → 'renewals' use new keypair, signed by old cert
Milan and Mike will be reviewers of the NDGF new CA

Cosmin → v1.3

Belnet → Usage wrong., critical issues open
→ rp's nervous.
→ procedures. Are they followed?
⇒ IN-depth ± self-audit in person. MUST

ACT

IUCC → critical errors. in EE cert.
→ server-side key gen. on web.

Sens. Christos K TAGPMA op rev. patch by APS meeting

Jens. HLCA

3647 → "no stipulation" sections may be left out. (also for 18CP's)

or a ~~PPS~~ PDS (PKI Disclosure Statement). [were there IPR issues from Entrust?!]

→ common namespace recommended. [contentious]

Target → Santiago v0.4

---

eduGAIN. * "Component identifier" in x.509 cert? ?

→ multiple PKI's supported. → trust anchor distr. still needed therefore!

THU. 20/9

Distr. Doc v 22 aug '07

→ TACAR fills gap in ~~establishing~~ bona fides of our membership.

* Split document? user / builder/committer (KEEP ONE for the time being)

issues

* "worthless" naming.

(ACT) sec. 4.5 elaborate s/w formats and the ./configure && make

* SKS password is the empty string.

* backup process description.

→ * replication of CVS repository.

Fixes needed?

→ Replication! (CVS, repository, signing).

Update by mid-Oct

* add TACAR URL to .info ? perm link is going to be there!

* TACAR reg integral part of accred. presentation meeting

(ACT) Forms handy at each meeting.

(a picture of relationships.) flowchart.

(ACT) Find out who is not yet in TACAR, prig them, and fix by next meeting.

(ACT) upgrade to Java 1.6

Jens: signing-policy format doc.

CRL → central redistr. points
multiple URL's in .crlurl file.

→ Recommend web caches to sites. ✓ → Milan to doc what CA's should do to enable caching ("200" / "402" /...)

UK. Cyprus ~~rest~~ NREN cluster went to INFN catch-all. Probably Roberto did not know.

---

* Repository of 'good' and 'bad' things regarding CA software.
ability to "removing features you don't need".

* measure many CA's already have self-developed s/w. (for the last ~10%).

→ requirements gathering via the PMA. (wiki)
matrix, indicating who wants/needs the requirement, to gauge interest in a feature.
- ChristosT
- Jens (OpenCA requests).
- Ajay (for colleagues :-))

DigitalSignature keyUsage.
everyone to comment today on GridForge.

OCSP: → no Proxies, as no consensus (Tokyo)
→ profile for Trusted Responders is still useful!
? make fairly short profile for Trusted Responders.

Christos: general revocation requirements as well.
what do we not have today
on the OSG side requirements gathering does not really work.

Change title to "An approach for using Trusted Introducers for OCSP in Grid Environments"

What to measure in the experiment (with OpenSSL? mod-gridsite? GT4?)
- stability of the service?
load measurement is harder (Mike)

→ How to demonstrate that OCSP gives benefit over a web caching of CRLs.
(Bob, Milan): web caching is indeed very simple and can be done today.
OCSP requires client changes, and we will be a first.
"no untested solutions of undescribed problems"

Christos: new sketch for Seattle OGF multiple docs.
↓
Mike: Trusted Responder, otherwise people go off into the CRL-style direct-download nightmare

Vista → OCSP first from AIA.
discussions ongoing.

Mike will make simple doc for Seattle. ←

RP namespace constraints → Jens to do a full cleanup.
doc really needed.

Audit → Yoshio. Christos: adding experience is needed.
Matt Viljen would incorporate experience from auditing UKeS CA IRP's.
Yoshio to provide more guidelines.

IASProfile → finalize before Seattle?

Jens' Soapbox

Storage of private key → can't distinguish soft token with or without encryption
↳ assertion based on a user promise.
↳ OID's are needed now!

ACT OID parsing in gLite. → TCG priority?

is LoA private info?
certain US people escaped PKI since it would release their LoA and clearance level!

Meaningful OIDs: RECOMM. to put oid of AP and under which you're accredited, but not the version. ACT

18CP: arc → privkey prot → on H/W token
↳ identity vetting.
Robots should assert H/W privkey protection in addition to anything else.

LoA: for DEISA it's not an issue → all partners trust eachother.
→ trusting PMA has settled.

Davelt → simplicity!
only issues 'private key on disk'
'F2F' → hotcarts.

BobC → solve via portal and proxy via (single) cert ~ Mike? ~ Davelt: in EGEE all ranges. anon ↔ certificate.

TAGPMA spread → Mike: they are not that pushy anymore for a lower level.

Dave: we've already simplified their life already, they don't have to register everywhere

Jules: was similar in DEISA in the beginning, since they all trusted eachother. now that's cleared.
"Teragrid knows users better"

"F2F only to ensure reregistration consistency."

In TAGPMA: Brazil and US same size, but Brazil is very rigorous.
US / DoEGrids is very lax and unclear.
OSG RA process has not moved since 2002.
but tracing generally does work.
Auditing works but DOE Agents are doing "reasonable" but not F2F.
HEP labs have no F2F tradition for their own accounts.

Mike

Vinod In Brazil notarized copies are part of (non-grid) common life in general
also in other parts of life.
Socially acceptable., all through LA.
Mike → It's only a US problem that notarization is so uncommon.

[LoA in the US (when Mike talked) did not 'stick' in the community]

Mike → see Sens' presentation! a few directions and checkboxes, not the opaque NIST-style stuff.

non-revokable SLCS certs for 1 Ms
↓ Milan, BobC, MikeH

BobC: private key protection more important than F2F!
Vinod: Sens' framework. → different axes
Willy

Host cert
admin or domain owner should be aware of issuing host/service cert.

ACT try impersonate a DP cert req. (via SARA?)

Davelt Auth2

comments: Sens → (how many) other people should we take on? → Mike: not too many...
Jules: who are the responsible persons?
Milan: who against who? to weigh decisions.
Jules: VOMS hosting provider is omnipotent.

two different profiles → VO admin
→ techn/sysh.

VO and CA different: ~~not accept all VO's~~ (
-Size: we cannot audit all

} analogy: IGTF ↔ ISO
egee, --- ↔ KEMA/i
VO/server ↔ device.

"RA" (not VOMS)

Accepted

MaGrid (Nabil)

presentation →
current 1.2.0 (3 July 9)
#6 →

JS + DoC ok with changes.

Accredited → key exch. start

✓-RFC 3647 framework.
-SLCS draft.
✓-Nabil.
✓-Bob C.
✓-AMS.
✓-Auth2-working party

Auth2 NP → DoC, Willy, DK, Mike, Jens, BobC, DG, Christos K. + Milan. (+Oscar)
↳ discuss in Ams. meeting

ISO (15408) ↔ SP800-53 (http://www.17799central.com)
17799 ↙

risk assessment to drive prioritization of criteria.
("top20")
↓
octave (cert-CC)
as a classification guide.
↓
DK (RP views) ↔ DSPG views
Reiner (list of risks, translate)
Kyriakos. (Cy).

Amsterdam meeting

For ROSA:
must start < Oct 15
so release end of Sep.

RFC 3647 mapping to the Classic AP 4.1
(Vincal used this as a template for BrGRID/LAC) → original work.
↳ best one out there.

→ Feedback requested →
→ useful for new CA's.
→ Seattle.

SLCS update.
needs language will explicitly allow federations not only sites/enterprises.
↓ ↳ TLCS as inspiration.
SWITCH to review?
Santiago deadline.
↳ next revision before Seattle

---

incident list? → specific membership list.
update list. → new host? → ACT → Mike
closed.
- CA mngr personal
- alternate
- all RP reps personal.
- closed list
- other PMA's can join
→ "igtf-members @gridpma.org"

add link to ACT PGP keyserver for each email address in the members-full table

Each pma to do this?
Seattle