EUGridPMA – 19 Meeting Day 2 (16 Jan 2007)

About 25 attendees – 1000 16 Jan 2007

AI: [Most prefixed with "*" below]
* mwh – to write a strawman classic – lite profile
* SWITCH to post version with minor changes for final ; then 2 weeks comment period – last call
* SWITCH to post certs & CA data to DG
* Need text to describe serial number usage in authority key id – JJ will do this.
* mwh will write alternative nameconstraint text, send to DG for consideration

Discussion

LCG Requirements – D Kelsey

[Same slides as Austin TAGPMA – see slide deck]
LCG project depends on 2 major Grid infrastructures: EGEE (EU) & OSG (US) plus of course others
EGEE – phase 2 now – 91 partners / 32 countries

- Own flavor of Grid middleware – GLITE
- 165 VOs
- Large number of disciplines
- Manchester OGF (May 2007) – simultaneous EGEE User Forum
- 192 sites/40 countries/25k CPU/3 PB disk

Requirements for Grid PMAs (IGTF)

- Endorse OSG requirements

… and …

- Naming: Actual name must be in subject DN
  I consulted LCG board about this – many people responded and insisted they needed full name in CN attribute
- Identity vetting
- RA should be contacted face to face, with govt id presented
- If face to face not possible, CP/CPS must describe:
  - How CA provides accountability: how can get back to physical person anytime during lifetime of certificate
  - What we are actually asking for, is if there is a law enforcement or court issue, the CA records can be accessed and law enforcement can reconstruct a path to the user
  - Doesn't this mean we need to get back to them anytime in the future?

- LCG will have one view on LoA appropriate for this, biomed different ….

Doesn't this apply to face to face too (the requirement for long term contact).
I need to be protected , I know the CA can find this person.
Aren't we requiring ID number/photocopy recording?
Poll: about half or More keep this info.
Another reason for keeping this info is to preserve the identity binding and prevent someone from assuming the identity
One PKI does not renew, but requires people get a new certificate – discussion of whether this preserves integrity of subject name.

DG: About 40-50% cases the face to face info is just lost, not recorded &c.

Discussion … can't note

[Conclusion – part: Need govt id or number, both for law enforcement requirement, and renewal requirement]

Why don't people record this info – A: Might fall into legal areas where need to record / handle this information in special ways.

Holding data – CA vs RA: UK the RA holds it (this is the preferred DOEGrids arrangement). Others don't like this - CA is responsible – burden of management of data – very hard on RAs, extra requirements. Some of this info is considered personal data and falls under the law governing personal information.

Proposed statement: Whether face to face or not, CA must have explicit statement about how to meet these accountability requirements.

Is "institute-based" ID the best ID to use? Somebody who pays you.

Do we need to make this requirement explicit?

Do we need to have 2 levels, one like this LCG above, and one somewhat less, above the experimental level, but without this high govt documentation requirement.

How do you perform as a catch-all CA, and satisfy this requirement?

We don't describe how RAs are appointed, although perhaps this expression of requirements goes around this.

DG: Trivial way of doing LoA. Make LoA correspond to different profiles, RP can install only those profiles he likes; CA can only issue one policy/LoA however.
RC: Realistically, would have to have 2 (N) bags of certificates.
DG: MetaRPM per profile

Who is going to set up these "Rudimentary" CAs? Who would use/accept them?
We have not really tested the market… there is clearly some level of demand but …
Some sites accept for general usage various test/training CAs.

Some AI?
Can we (OSG) strip out the items in the classic profile and provide a lower level?
Discussion about number of CAs per country.

Propose that every profile have a defined assurance level.
Classic lite grouping – a profile – CAs would exist under it.
JJ: We all map to "medium" assurance in the old standard for expressing this.
We need some kind of scale or arrangement of assurance levels.
* AI: for mwh – propose a lite wt profile

Lunch

SWITCH / Witzig

Skipped Shibboleth intro, will describe service in more detail this time

CP/CPS reviewed once, new version posted last week available in review area
11 day certs; no revocation (SLCS profile)

AAI – All Swiss universities hooked up to this; about 150k accounts
AAI began in 2002.

We have been coming from Shibboleth side, rather than Grid; would like to leverage campus infrastructure for grids.

SLCS software design (Slide "design goals")
Shows data flows and auth flows in an authentication – cert issuance process

CA sets on high security / dedicated network; a front end martials/unmartials requests to the back end – 2 CA components, an SLCS server/CA client and the CA server.
Q: What are the protocols between these servers?
Apache front end talks thru modjk? to tomcat server; plus (CCNC?) to the CA?
Q: HSM run in non-interactive mode? Yes

IdP service, run by site, has its own administrator, policy, &c.
A registration step is possible can take place at the SLCS "SP" [service provider] (essentially a Shibboleth authorization step)

Who gets an account on Shibboleth service?
Some commonalities, but some variance between different registrars, and different classes of users.
Federal database is used to guarantee that user is not registered in 2 universities.

Q: How is this guaranteed
Everyone reports, and it is cross-checked

Can also provide service for institutions w/o AAI-compatible identity provider, or for external parties: Virtual Home Organization can take their registration -> another type of account.

How good is AAI
Registration procedures coupled with funding, and tied to unique number;
Used for financial transactions including computer sales to students and sale of court papers to law school students.

Definition of DN
Unique id (tag in cn= component) is generated from Shibboleth unique id.

RA decides whether prospective cert holder can meet 1 of 3 conditions (see slide CP/CPS(4))
1 – issuance of id card linked to financial transacionts
2 – AAI account has 1-to-1 relationship with HR data (salary)
3 – Face to face registration with RA, including proof of ownership of ID card

Currently running in testbed since Nov 2006
http://www.switch.ch/pki/grid/test
(test ca, to demonstrate software service)

Production in progress – to be finished end Jan 2007.

Q: Why isn't it a MICS – has an RA step?
Uncertainty about MICS – need to get on air – don't want to do revocation?

Q: In that case, don't you need a revocation function, because the SP registration is semi-permanent?
AAI account can be revoked, preventing recertification; RA could withdraw enrollment. It's true cert could be valid for some length of time (as with any SLCS).

Q: What about status change of AAI holder? (eg paid to unpaid)
Attributes are moved to SP whenever needed and tested. Provided institution releases data, and it is up to date.

Q: I don't care about account creation, just that the right attribute (paid salary) is set. That is the authorization attributes are up to date.

By just looking at cert, can't see difference in cert. Developing a VOMS interface so the attributes from Shibboleth can show up in certificate.

Q (JJ) What is the VHO –

We do it – it's our own org, that provides the IdP for this organization

Discussion … participant didn't note

* Document to be updated with various suggestions from meeting, sent around for 2-week last call [actual items similar to mwh's mail but need other notetakers to fill in]
* SWITCH to send signing certs &c to DG when ready

[break]

LIPCA – Nuno C update

Replacement
OpenCA 0921 – discussion of pros & cons
Classic CA profile …
Future plans:
discontinue old LIP CA
More RAs in universities &c
Is openca the right software?
[Too much work to do all the customization, basically, given time/resources]
Has to extend root CA, but has authority key identifier with serial number in it.
Q: about openCA status
See www.ccc.org
Also various changes in one of the split branches will be available later this year (openxpki)
Remark: Exciting features are good, but we spend a lot of time turning off features, and putting in our necessary features & policy, so it may not be worth the burden to switch.

Decided to go thru

Certificate Profile Document (OGF) / D Groep

Idea here is to review it in the next 2 weeks, and go to last call at OGF-Chapel Hill

Has authority key id / ca cert replacement issue cases

Q: has comparison w/ RFC 3280 been done? We may contradict/differ.
Correct authority key id for EE & CA is a MUST unless self-signed (section 2.4.6).
Suggested to omit this RFC-conforming language (already in RFC) but mention in footnote that these can be omitted &c.
* Need text to describe serial number usage in authority key id – JJ will do this.
* Need text about security considerations – disclaimers for misinterpretations of attributes by services, and known divergences of opinion.

What kind of document? Informational, BP, Recommendation? Probably BP?

Name constraints …

Should we cover Mozilla & Microsoft?
We have to some extent – perhaps say, included where relevant
* mwh will write alternative nameconstraint text, send to DG for consideration