EUGridPMA, Amsterdam. Jan 2008

Monday 14/1/2008

09.30 Welcome, agenda, minutes last meeting, note taker, introductions

10.00 Round - table update

Milan – changing to EJBCA gives Shib i/f

Ireland – discussing federations and may be some news maybe SLCS in future.

UK – after incident decided safest to change key.

DFN – statistics issued altogether 1300 cetrs and RAs in 56 orgs. Hosting non-grid CAs – 14K certs (11K valid). Office/CDP relocation went well without problem. 2008 expect EE cert issuing for rollover in hierarchy, thinking about removing grid CA and let root issue EE certs to avoid rollover. Policy change not big, will post for agreement on mailing list. Also setting SLCS CA for presentation in Copenhagen – looking for volunteers for review (MikeH)

Spain – old CA has expired, new certs have been issued. Stats - ~!300 (500user)

Austria – no change. HSM work still underway. Fewer certs due to funding problems hopefully now sorted out. 177 valid certs. Will present new CP/CPS

Switzerland/SWITCH – SwissSign upgrade infrastructure short outage.

???Cyprus –

Christos(Greece) – second phase HellasGrid transitioning to new CA after summer. Experimenting with OpenID and Shib thinking about SLCS CA. SeeGrid CA will die soon but have request from Georgia, expires in Aug 2009 hopefully all will have national CA. Some info on Georgia talking later.

Italian – will issue robot certificates, new CP/CPS already on mailing list. Old CA cert expired but 3000 hosts still attempting to download CRL. David – sees also strange patterns. Emir - Can use GGUS to chase this. Jens – want mechanism to flag problems in distribution mechanism where sites don't upgrade. **ACTION** Roberto can put list of bad hosts on mailing list give to individuals. Jens – could put 'bomb' in each release? Mike – another case of lack of action on notification. DOEGrids also rolled over but had problems, mainly in browsers.

Tamas/NIIF – normal ops. 400 certs. One or two more RAs coming.

Baltic – new software for request and certs – home made but procedures remain the same. 6 new RAs . 202 valid certs and preparing self audit and expect some CP/CPS changes.

CERN – 2000 personal certs, 2700 certs for hosts. Vista had a bug but now fixed in service pack. Mid-term goal for smartcards for CERN staff – Windows and Linux and testing.

Croatia – 110 certs with expected self audit. Looking and MICS and SLCS because of difficulty establishing RAs - ~6month timescale. Maybe present next time.

???? – introduction of separate RA (used to be CA operator). Roving RA. Have performed self audit and

Portugal – no news 350 valid certs.

France/GridFR – machine will move to Toulouse. Do we have to renew CP/CPS? Should be trivial change

Emir question – to change to improve compliance (throw out Netscape). David – should just post to list and wait for 2 weeks.

Jens – what about presentation from Morroco? David – are operational, were they not provisionally accepted? Jens has completed full audit. And it's OK.

10.30 Updates from the TAGPMA (Vinod Rebello)

Update since Thessaloniki. Details on slides. Thanks to Darcy Quesnel, now left. Question – is there a protocol for migration from one PMA to another. David – not formal.

EELA-II project driving growth in S. America. Not much change in Central Am. – maybe Cuba coming.

Biggest issue is SLCS profile. Unchanged since 2005 – out of date. Recent security incidents prompted asking if CRLs are needed for SLCS, no other way to restrict/block certs.

11.00 Coffee

11.30 Accreditation of new CAs: Ukraine (Sergey Velichkevych)

Details on slides now positive results from reviewers.

Mike – So, it's a good thing to write own CP/CPS rather than template? Sergey – using template for 90% of content removes a lot of experience responding to small but important details. IS a good experience. Jens - will speak tomorrow on this. David – thanks to reviewers and now accredited ☺

11.45 Accreditation of new CAs: MARGI CA (Aleksandar Dimeski)

Details on slides. Emir – done review looks mainly OK. Similar to other CP/CPS's. Christos – has to request/insist this group use official name registered in the UN. ?? – could strike fro document but probably not website. Political discussions. David – PMA official will refer to UN registered name. Technical comments on lack of separation of RA and CA duties. Suggest better to clearly separate. Other issues minor. Emir – list of obligations has moved to sect. 9.6 and missing in 3 CP/CPSs (Macedonian, SEEGrid, ??)

Milan – clarify crl 'within 1 working day' , from what starttime ? Aleks. – from receipt of request. Milan – suggest clarify in CP/CPS. What software? – CSP. Maybe problems with V2 crls?

David – can we do rest of process by email? No objections.

17.30 Continuous Audit Process III: BEgrid

After approval since 2004 now out of date. Needed review.

OpenCA with home-made scripts not very good. Also poor separation between CA and RA. Audit lead to choosing completely new solution. Put out call for tender for PKI solution. May be external (compliant with this group) or local operation offering part of cover to grid users.

Will update the dead urls as soon as possible and update cert. extensions not critical. Other work will be left to new solution. Add OID (BELNET had one)

Q Jules – cp/cps not found. A: yes update asap.

Interested in feedback on solution evaluations. Did not feel comfortable with OpenCA.

12.45 Lunch

14.00 The DoEGrids in‐depth Updates and Audit special

Details in slides….

14.00 DoEGrids CA and PKI Architecture (Mike Helm, Bob Cowles)

14.45 Continuous Audit Process: DoEGrids results (Mike Helm)

Reminder of NIST process (800-53). In LBNL's view - LOW – something bad, MEDIUM – the building burned down, HIGH – somebody got killed.

DOEGrids CA Audit

Wanted to get involved early in audit process. Details in slides, introduction of auditors and their experience.

Milan – min. reqs. Make RA involvement in renewal? Mike – not in DOEGrids. Do need to provide improved information/notices to RAs. DaveK – yearly vetting sounds right. (Later discussion)

DougO – RA auditing. Investigated 20 user + service certs at random. Mike showed ?twiki with summary results. IanN – all records are either server logs or email archive? Doug – yes have not records of actual identity. Mike Could show another time?

CRL history was deleted by upgrade.

DaveK – is it strange that discussion of functionality comes up in audit? Mike – herding cats?

DaveK – happy to see such extensive audit.

RaimerK – overlap in community in TAGPMA. Mike – yes overlap exists.

DavidG – for all CA audits should have one or two people in this group to review?

Christos – confusion, audit results are not addressed. Mike - only 2 issues – id verification and cps rfc version. Christos – does not make sense to set the bar high if CAs don't update

to compliance. Mike – most issues will be addressed. with conservative community tp bring inline.

IanN – requirements doc. with ‘shoulds’ discussion. Jens – CAs do do things for understood reasons and should be allowed.

Mike – NIST audit is a little different from a compliance audit.

??? – maybe a second audit is necessary after update to compliance. DavidG/Jens – update to cps rfc is not mandatory but is a noted non-compliance.

15.30 Tea

16.00 NIST 500‐53 audit results for the DoEGrids PKI (Bob Cowles)

17.00 Identity in US Science Environments (Doug Olson)

Details in slides.

Mike – NERSC example is pretty similar to NSF and DOEGrids delegation. DaveK – is PI legally responsible. Doug – not exactly what ‘legally’ is but some responsibility.

DavidG – reactions, relying parties? Mike – TAGPMA has already approved NSF process. (same time and NERSC and NCSA MICS process). DavidG – sees lot of similarity with PI and RA roles. And see lot of interactions with end-user which would be hard to fake.

Mike – in USA senior managers have considerable freedom and sometimes problems arise from this.

US Research ID – a simple proposal – Give Up ! We are in deadlock. US Research science vs Europe. Ask this group allow US exception. DaveK – not just US/EU exception it’s project versus institution.

Emir – same isues with growth of NGI

Jens – STFC talking about same things in user offices. Profs are like PIs here. Need management of users in databases with something like LoA. Data protection compliance issues but PI can only be ‘second rate’ to RA. Mike – LoA will never (effectively) happen in US – too long. Jens – robots to be owned by projects so not tied to individual for continuity.

18.00 End, back to the hotel and the Girassol restaurant

12.15 Accreditation of new CAs: IR‐GRID (Remote: Majid Arabgol)