Karlsruhe EUGridPMA and IGTF All Hands meeting, 07-09 May 2012

Notes by Cosmin Nistor, first 2 days

Monday, 07 May 2012

Updates from the APGridPMA, Eric Yen

- 15 accredited CAs, the newest one is Malaysia
- Mongolia re-starts accreditation, MAS takes over the process.
- issues from previous meeting: AU still looking for funding; discussion on the possibility of moving the New Zealand RA from the ARCS CA (AU) to ASGC CA (TW)
- still looking for volunteers for the F2F meeting from the 2nd half of 2012. If none, TW will host it again.

Updates from the TAGPMA, Derek Simmel

- 2 CAs pending accreditation (Peru - classic, and San Diego Super Computing - MICS)
- 1 RP suspended (NIH) - the person responsible was promoted, there is none else in charge now.
- TAGPMA website to be redefined by August
- TAGPMA voted to accept the updated classic profile (v. 4.4)
- Next TAGPMA meeting planned in Panama, week 27-31 August. Plans for a 1.5 days meeting, collocated with the CLCAR conference
- There is a collision with a conference in Argentina

IGTF RAT report, Jens Jensen

- RAT should be more proactive
- A co-chair is needed for sharing management and administrative jobs; waiting for a member of the RAT to volunteer
- There should be more than 1 member of the PMA per time zone
- Willy volunteered for the co-chair position

CA self-audit I: HellasGrid and SEE-Grid Catch-All, Christos Kanellopoulos, Christos Triantafyllidis

- Presentation of HellasGrid self audit
- Derek: time frame for addressing the found issues?
- Christos K: 1 work except for the archive issue

- Presentation of SEE-Grid
- David G: CA expire in 2014 - any plans for issue a new CA cert?
- Christos T: depends on the use of the CA. Hope not to, but it depends on the rest of the African countries from the project.
- Edgars and David G volunteered to review both CAs

RA transferral process and Registration Practices Statement, Eric Yen, Scott Rea

- short presentation from Eric
- scenario, goals, facts about moving user/host certs or the whole RA from a CA to another
- New Zealand issue again
- RPS (Registration Practices Statement) would be a solution?

- presentation from Scott - Standards for RPS
- Process recommendations, benefits
- long discussion
- Keith: we cannot accept registrations from any university - would lower the LoA
- Scott: overall you need CAs to every university - one for high LoA, one for medium LoA, one for low LoA
- Willy: CAs are in charge to checking the validity of the registration process, now you put it in the hands of the PMA - it would generate conflicts. CA should accredit the RAs.
- David K: we should consider the scale of the PMA meetings in the new frame
- Scott: CA must reference the RA
- Usman: most RAs are not capable of producing a RPS
- David K: there are some advantages of separating identity vetting from the CA
- Scott: An RA cannot be accredited unless the justification for moving from the CA
- Scott: An RA is typically project based
- Milan: No, not in all cases
- Irwin: RA can move to different projects and avoid identity vetting
- Scott: We decide. If they proved they need accredited, than it is OK. We want more communities not more CAs, and they can come as an RA.
- Irwin: It is hard to get a cert if you work for different projects. It is easier for universities to do the identity vetting.
- Alexandru: IS the RPS general enough for every CP/CPS?
- Scott: Yes, you can have a general document
- Keith: It's a transition period. There can be an RA for different CAs
- Ayman: It is a CA business to accredit RAs. Why should we go to the PMA?
- Scott: In commercial PKI the CAs don't accredit RAs. Browsers go to the RAs. The CA accreditation is not enough.
- Milan: RA procedures should be checked. RAs should not be members of the PMA, they belong to their CA group.
- Scott: Membership doesn't mean that they can vote
- Willy: Sooner or later there will be 2 groups in the PMA, CAs and RAs, producing different things.
- Derek: A separate group may choose to set different standards
- Scott: CA still have the responsibilities
- David G: **Changing the membership process is controversial. CA should remain responsible and members in the PMA. If a RA move from a CA to another and have a RPS, we could review this**
- Milan: There are IDPs with their own documents that will not be happy to provide a different RPS.
- Reimer: Why choose an RPS instead of an agreement? The responsibilities go from CA to PMA. There are different kind of operations between US and Europe. We have 1 CA per country.

SHA-2 risk assessment and implementation plan, HASHRAT team

- presentation by David G
- Derek: getting into the system wouldn't produce much damage except embarrassment
- Scott: an intruder can also change validation date, CRL, other stuff
- Scott: other thing - a blackmail can appear; force the CA to do stuff otherwise break stuff
- Derek: Are we prepared to publish all we know about the SHA-1 risk and force the middleware to react?
- Scott: No one will do anything if the consequences are too far.
- David G: SHA-1 is loosing bits. We cannot say when and if it will be broken.
- Scott: We don't have members in our community who have done assessments of their own exposures. Until you produce validation data for your algorithms you don't know what SHA-2 breaks.
- Keith: VOMS is not specified on the list of what SHA-2 breaks
- Milan: what pieces of the system were checked? And with what version of SHA-2?
- Jules: I don't think that there are any concerns. Is there any released software that has been tested against SHA-2?
- Scott: You have to get SHA-2 CRLs, certs, and install them in your normal operating environment
- Milan: In the future the main difference between SHA-2 and SHA-3 is the efficiency between environments.But what about the variation of the SHA-2?
- David G: The software producers should support at least 256 and 512
- Milan: we should create the panic
- Scott: We should say that after Jan 2013 you cannot issue SHA-1 certs. You can use them, but you cannot issue them
- David K: Who decide what SHA-2 to use?
- Milan: Let's tell the middleware producers that we are using all so they will support all
- Scott: Rekey rather than renew and sign certs with SHA-2 using the same key material
- Irwin: We cannot switch to SHA-2 now because we do not have software to test it
- Keith: When using VOMS, the latest version, there is no way I can select SHA-1 or SHA-2. There must be 2 independent investigations: we have to know that SHA-1 is in danger and we have to know that SHA-2 doesn't break anything

- The SHA1Risk-v.0.3.doc was edited and an improved version was uploaded to the Agenda pages
- The scope of the document for the software producers: what will taped if the SHA-1 is broken
- Christos K: Why should we take these measurements if, fo example, the Bank of America doesn't take them?

Tuesday, 08 May 2012

Locations and agenda for the next meetings

- next meeting will be hosted by RENATER in Lyon. 10-12 Sept 2012.
- for the Jan meeting there will be a poll asking the PMA members about the availability to travel to Abu Dhabi (UAE). There were talks about the price of the air tickets and about the possibility to travel outside EU for some of us. As a back up, there is the European choice, Firenze (It), hosted by INFN. The final decision will be taken after the poll. The dates are 14-16 Jan 2013.
- for the 2013 May meeting, tentative dates 13-15, the location is Kyiv, UA, hosted by NTU
- for the 2013 September meeting, tentative dates 9-11, the location is Bucharest, RO, hosted by ROSA

Authorization Service Operations profile: experience and endorsement, David Kelsey

- lots o discussions on the document
- Milan: Location of the service and the naming of the attributes are two different issues
- Scott: we need a clear definition of terms
- David K: the definition should define also the semantics of the attributes
- Irwin: the AA speaks for its community and defines the attributes accordingly
- David K: the attributes are meaningful only for the community they deserve
- David K: attributes assertions completions on the document and more.

RA Migration scenario for NZ, Eric Yen

- Eric: There should be a possibility for an RA to be associated to a national CA but also to other CA
- David G: do we require a new identity vetting?
- Derek: yes if the new CA doesn't accept the former CA id vetting
- Scott: CA2 has nothing to do with CA1. RA is managing the id vetting process. Does CP/CPS contain any wording on this topic?
- Eric: what if the connection between CA and RA is lost?
- Scott: CA1 either continues to issue CRLs and revoke certs or, if not, CA1 must revoke all certs. Users are affected
- Milan: are we able to support the transfer between the old CA and the new one?
- Keith: the users should be warned if they encrypted their data with the old key
- Eric: if the old CA is not terminated and keeps the services like issue CRLs could we allow an RA to be associated to 2 CAs?
- David G: yes, if the old CA keeps working as long as all user certs are valid
- David G: **RA serves 2 CAs. CA2 will be able to authenticate the users of the CA1 at the request stage for new name space.**

New CA presentation: EG-CA by EUN, Ayman Bahaa-Eldin

- presentation
- Usman and Feyza to review the final version
- after review, 2 weeks silence procedure

CA update presentation: INFN CA and IGI CA series and MICS CA, Roberto Cecchini

- presentation
- Roberto is still writing the CP/CPS

Updated CA and Robot presentation Grid-Ireland CA, David O'Callaghan

- presentation
- David O'C: Remote id vetting - OK by videoconference?
- Christos K: Turkey has an id vetting by VC very well organized
- David O'C: will submit CP/CPS in a few weeks

Revocation enhancements for PKI, Scott Rea

- presentation
- Ayman: OCSP not fully supported by this community
- Scott: Agree but still needs considered
- Scott: the man in the middle attacks the weakest point - the relationship between CA and RA

Updates to the PKP Guidelines and management of credentials, Jens Jensen

- Jens: first version of the document in 2 weeks

Soap box, Jens Jensen

- presentation