EUGridPMA meeting, Rome, 14-16 January 2013

Monday 14 January

Agenda: http://www.eugridpma.org/meetings/2013-01/

TAGPMA update by David Groep based on slides sent by Derek Simmel

IGTF Risk Assessment Teams actions and future - Jens Jensen
No risk assessments since last meeting.
A more proactive approach proposed. Jens doesn't have the time to put much effort in this. Others should step in. Also a secretary would be welcome.
Are there tools available for automatic tests? Some tooling is available through the IGTF RAT pages.
How do we learn about risks? How do commercial providers handle this?
Ursula Epting offered to be an active member.
We should monitor cryptographic communities.

Self audit review status - David Groep
Some are still pending.
Status of Belnet CA is unclear. Did they move to TCS completely and can the BELNET CA be removed? Will be clarified.
Response needed from MARGI CA.
No reviewers anymore for Turkish CA. New volunteers?
BalticGrid did sent an update last Friday.
Romanian CA has been reviewed by Ursula. All is ok.
Reimer: DFN passed audit by ETSI for their PKI facilities.
David: attendance required in principle once a year, but can be two years if attended by video in between physical attendances.

CA Update I: SlovakGrid - Miroslav Dobrucky

CRL published now in DER format (Browsers need CRLs in DER format).

The only MUST change (D) implemented now: inclusion of classic profile OID

Discussion about the identity checking of persons by RAs, especially checking that it's still the same person. Must prevent issuing the same DN to different persons, but privacy must be guaranteed.

Discussion on changing DN of CA. Jens: experience with renaming of CA; E.g. same DN for issued certs cannot be used by the two CAs. Anders: storage systems may give problems because file ownership may be based on DNs. In general users may be confronted with problems.

New CP/CPS version 2.2 will be proposed in 2013.

Plan is to write an Operations manual (for use by RAs).

User manual will be updated,

Peer reviewers: Pavel Wolniewicz (PSNC), Emir Imamagic (SRCE CA)

SHA-2 availability status and issues

TAGPMA discussed the change. Several issues. A new timeline is proposed.

One of the changes discussed: What to do if SHA-1 is broken. TAGPMA proposes not to remove CAs automatically but first assess the risk.

Anders: what problems do we have with SHA-1. David: In general software built with old crypto libraries (e.g. jGlobus version 1, Bouncy castle) will experience problems with SHA-2. Vincent (IDRIS): is there a place where known problems are published? Some suggestions: HASH RAT document and TAGPMA.

gsisshTERM tested by Cerlane (Siew Hoon Leong) (LRZ).

dCache status: evaluation in progress. Using jGlobus version 2 is planned, also supporting old style proxies.

Willy: old secure tokens won't support SHA-2.

Intermediate CAs should have both types in the transition period with different serial numbers.

Proposal is that users can have certs for both sha-1 and sha-2 for same key, pair provided different serial numbers are used.

David: what is the status of using a key length of 2048? Willy: forces the use of 2048. David: Who doesn't have a 2048 capability? Ursula: IE shows a problem generating the 2048 keys with the browser.

Only a few hands showing up if asked who cannot issue sha-2 certs.

SHA-2 certs at the moment are basically used for testing only.

Conclusion: the timeline proposed by TAGPMA is accepted. Some of the above discussed recommendations are proposed to be added.

IPv6 readiness is shortly discussed.

Lunch

Updates from the APGridPMA – Eric Yen

Big changes planned for CA members from Australia and Japan.

SHA-2 transition is on track

David: asks about status of removal of e-mail address from IAPG CA root cert. Eric: will take some time.

OCSP status – David Groep

(see material on agenda page)

In order to push the deployment of OCSPs two profiles are proposed, one for CAs and one for RPs. The latter can be used by RPs to drive software development. Both profiles are discussed.

"OCSP Profile for CAs" discussed/edited in EUGridPMA wiki:

TWiki> Main Web>TechInfo>OCSPProfileForIGTFCAs (2013-01-09, DavidGroep) EditAttach

There is discussion on validity period for responses. 30 hours is proposed by David based on what some commercial providers do. Reimer: may be worse than using fetchcrl. David: in case of a revocation new OCSP response must be issued immediately.

For off-line CAs a validation cert can be used for on-line signing. Problem is that validation certs itself are not supposed to be checked for revocation. These certs should be "short" lived (~ 30 – 100 days?).

Maximum time for pre-computed responses: the responses may be pre-computed for 30 hours ahead but must not be cached for more than one hour.

Section on Running an OCSP server: several examples are given in the document, but no script found to generate responses.

Discussion/editing of "**OCSP Deployment Guidelines for Relying Parties**":

TWiki> Main Web>TechInfo>OCSPDeploymentGuidelines (2013-01-12, DavidGroep) EditAttach

RFC 6277 includes the requirement for the acceptance of SHA-256 signed statements.