Monday 12th

MARWAN Presentation

No questions or comments

They cannot have multiple internet links, but can only use one which is a private provider.

APGridPMA update (Eric Yen)

No questions or comments

TAGPMA update Scott Rea

No questions or comments

IGTF RAT assessments (Jens Jensen)

No questions

A quick discussion about recent attacks on CA's led by David

The issuing machines with HSM had no antivirus and anti malware software, so they were attacked with conventional virus and malware software, and the hackers happily issued certs

The conclusion was that CA implementation should really match what is written in CP\CPS.

David: Should we travel a lot and audit everyone? No we should trust ourselves.

Self-audit reviews:

IUCC

Must appear in Ljubljana or be removed from PMA. Self-audit was in Amsterdam 2008.

-

UK eScience CA

Self-audit in Berlin 2009, new CP/CPS presented in Marrakesh.

-

pkIRI

presented in Dublin 2010

Jens didn’t get any feedback. He should ask for feedback and check on status of review.

-

AEGIS CA

David commented on changes and new CP/CPS should go into effect.

-

Grid Ireland

Presented in Zagreb 2010. David O’Callaghan has no update as data protection section needs to be completed, and then the update should be sent to the reviewers.

-

DFN

Presented in Utrecht 2011. Reimer implemented the minor changes and new CP/CPS should be ready (Maybe in Ljubljana).

-

Belnet

Presented in Utrecht 2011. Their CA is not offline as it should be, and Christos pulled the plug on it. They still need to do a self-audit.

Tunisia CA review.

David will ask for reviewers on the list.

Ankabut-GRID UAE CA

First step to final accreditation, a presentation of UAE CA.

No questions or comments

--

Junet CA presentation (Anwar Al-Yousef)

Questions:

David:

How is he sure that JUNet name is unique in Jordan? They have a registry for all of the companies, and JUNet is registered there

Milan:

CA CERT:
Alt names do not appear in CA cert, but that is good, remove them from CP/CPS if they exist

User certs:
Remove issuer alt name, and subject alt name from user certs.

Service certs:
Don't use alt names
Host keys aren't protected with passphrase, and Anwar wrote in his presentation that they are.
How do you link identity vetting to the original request? They do it using a PIN code.

Host/service enrollment:
How do you link the subscriber to the common name? They are using the domain name database.

Circumstances for revocation:
The first and the last circumstance are the same, remove the last one.

Certificate revocation:
If someone else finds the private key of the certificate, there should be some mechanism for them to request revocation.
Machine security:
How will you patch offline machine? They connected it to internet for updating. They should initialize it from live cd.

CA/RA machine security:
"Any unauthorised software change is monitored", add the text that someone will act on it.

Records archival:
They should record activation of signing key.

Assesment and audit:
Add that CA should be audited by a relying parties as well.

Conclusion:

Anwar will update CP/CPS and circulate it to the group. David and Milan will look in to changes in his comments.

The new CP/CPS will be made available in two weeks.

MaGrid CA update (Karim Oustouh)

They want to create another ca.
If they create another one for the name change, they should retire the old one.

Romanian CA self audit (Cosmin Nistor)

Reviewers:

Ursula Epting and Yurij.

CA update Belnet

No questions or comments

New TACAR registration policy (Milan Sova)

Ursula requested the statistics of how many people are using the TACAR repository

Milan asked the members to read the new policy, and to vote on Wednesday.
