Tuesday notes

Belarussian CA self audit Yury Ziamtsou

Ursula: Is Yury going to change the RA's, or leave them as they are? He is not going to change them now, but in the next audit.

No questions and comments

Reviewer: Ursula Epting

TR Gris self audit (Onur Temizsoylu)

Onur has already implemented all of the issues in the new version of CP/CPS

No comments

Reviewer: Jean-Cristophe Real

New CA TNgrid (Tunisia)

CP/CPS reviewers: Feyza Eryol and Alexandru Bobe

David Groep

Introduction to large-scale issuing of host certs: the data centre use case

Ursula: Asked what about old hosts and rekeying, how that hosts would be identified? How would they guarantee that only one robot certificate can sign the requests?

Yury: Virtual hosts need to be considered. how can they be identified?

Alexey from CERN should explain this in more depth, and we should allow if it is secure in Ljubljana meeting.

Marco Bencivenni

On-line credential requesting and -storing portals, a risk analysis

Reimer: concerned about the storage of the private key (in non-swappable memory). User uploads the private key in use case 1. In use case 2, the MyProxy server stores the key. It is not consistent where the private key is held.
Marco said that is an issue, and it will be resolved

Use case 1. the users key is uploaded. that is not a good design.
Marco said that the point is that the key would be deleted, and the passphrase not stored.
David thinks that guidelines actually support that.

Marco: the idea is that portal is to upload the certificate to MyProxy server, to make it easier for the user.
David: The machine that handled the certificates is a trusted system?
Marco: there would a separate box handling the security functions.

Roberto: the CP/CPS complies with TCS

Conclusion: This structure, with the credential manager on the single box linked to TCS is fine with everyone.

Marko is to circulate the progress to the list.

Jens Jensen

Updates to the PKP Guidelines and management of credentials

The two questions Jens emphasized:
Should the subscriber acknowledge the receipt of a key?
Should the deployment of a key be a proxying step?

Reimer doesn't agree with: CA must not generate private keys. Current private key protection guidelines already allows for others to generate private keys.
How clear is the document on who is 2nd party and 3rd party? Should the CA be considered as 3rd party?

Who is going to draft a new piece of text which will be discussed in the next meeting in Ljubljana, where we will decide whether we like it or not? Jens will do it.

CA Update: UKeScience roll-over (Jens Jensen)

No questions or comments
