PKGrid CA Self-Audit 2015 (33rd EU-Grid-PMA Meeting, Berlin)

Managers
Adeel-ur-Rehman
Mansoor Sheikh

Brief History

- PK-Grid-CA was first presented and accredited during 2nd EuGridPMA meeting (held in September 2004) at Brussels
  - Since then, running the CA
- Initially run by Sajjad Asghar and Usman A. Malik
- Now taken care by Mansoor-ul-Islam Sheikh and myself

Previous Physical Attendances

- 5th meeting (Poznan), May 2005
- 8th meeting (Karlsruhe), Oct 2006
- 13th meeting (Copenhagen), May 2008
- 15th meeting (Nicosia), Jan 2009
- 25th meeting (Karlsruhe), May 2012
- Other times, mostly remote attendance!

Audit Results

- Last self-audit was presented during the 26th Meeting held in Lyon.
- Audit guidelines used:
  - GFD.169
  - version 1.1
  - dated: October 28, 2010
- According to doc, our audit summary:
  - B: 7
  - C: 0
  - D: 1
  - X: 3

“B”: 1/7

- The profile of the CA certificates must comply with the Grid Certificate Profile as defined by the Open Grid Forum GFD. 125? (CA item 22)
  - Check the profile of the CA certificate (details are described in the OGF Grid Certificate Profile Document, GFD. 125
    - Subject key identifier and authority key identifier will be valid from Dec 2016 when new Root Cert will be issued

“B”: 2/7

- Is a CRL issued at least 7 days before expiration (for off-line) or 3 days before expiration (for on-line)? (CA item 29)
    - We missed it a couple of times.

“B”: 3/7

- The CRLs must be compliant with RFC 5280 (32 of CA)
  - Is the CRL compliant with RFC 5280?
    - Subject key identifier and authority key identifier will be valid from Dec 2016 when new Root Cert will be issued

“B”: 4/7

- The repository must be run at least on a best-effort basis, with an intended availability of 24x7. (CA item 49)
    - We had a few un-announced downtimes.

“B”: 5/7

- Over the entire lifetime of the CA it must not be linked to any other entity. How does the CA guarantee this requirement? (RA item 8)
    - This guarantee is not explicitly mentioned in the CP/CPS.

“B”: 6/7

- The RA must record and archive all requests and confirmations. (11 of RA)
  - Does the RA record and archive all requests and confirmations?
    - NO RA other than NCP itself archive all records due to our small user community

“B”: 7/7

- The CA is responsible for maintaining an archive of these records in an auditable form. (12 of RA)
  - Does the RA maintain the archive of these records in an auditable form?
    - Archival for requests and confirmations is currently done by the CA, as we have a small user community

“D”: 1/1

- Does the CA or RA have documented evidence on retaining the same identity over time? (RA item 6)
  - We need to have a documented evidence on retaining the same identity over time.

“X”: 1/3

- Does the on-line CA provide a log of issued certificates and a signed revocation list? Is the log tamper-protected? (CA item 16)
  - CA server is not an online machine.

“X”: 2/3

- Are new EE certificates signed by a new cryptographic data? (CA item 18)
  - Yes, new certificates are signed by new cryptographic data.
- Is the old but still valid certificate available if there are still valid certificates signed by the old private key? (CA item 18)
  - NO, as the transition period is not due yet!
  - Also, old certificates and old key is not valid any more.

“X”: 3/3

- How is the re-new process described? (CA item 41)
  - We do not have a renewal policy for certificates as PK-GRID CA does not renew certificates rather it only rekeys…

My Questions

- Is the GFD document 169 (version 1.1, dated 28th October 2010 still the most appropriate)?
- Is the GFD document 125 still the latest?

Your Questions/Suggestions are Welcome!