CA Status Update: CERN CA

Paolo Tedesco
CERN - IT/OIS

33rd EUGridPMA meeting, Berlin

12/01/2015

Agenda

- Status of SHA2 migration
- Policy changes
- Self-audit results

SHA-2 migration

- No more valid SHA1 certificates
- Issued last CRLs
  - 2 years validity
- Remove SHA1 CERN CA from IGTF
  - Any particular procedure?

Policy: Identity Verification

- Change user identity verification
  - Goal: simplify procedures
  - Especially for mobile devices
- User certificate: password + birth date
  - Asks for password outside login page
  - Looks like phishing
- Host certificate: certificate authentication
  - No added security

Identity Verification: Proposal

- Standard authentication only
  - Same security
  - Same conditions
  - Improved user experience
  - Avoid support tickets

Policy: Autoenrollment

- Context: OpenStack cloud infrastructure
  - Very high number of machines
  - Manual certificate requests do not scale
- Currently internal CA allows autoenrollment
  - Machine gets certificate without user intervention
  - Based on machine Kerberos credentials
- Proposal: autoenroll Grid certificates
  - Must provide solution suitable for future scenarios

OIS

Self-Audit Results

Section	Score	Max
1. CP/CPS	6	6
2. CA system	4	4
3. CA Key	6	8
4. CA Certificate	5	6
5. Certificate revocation	4	4
6. Certificate revocation list	7	8
7. End entity certificates and keys	8	10 (12)
8. Records archival	2	3
9. Audits	3	3
10. Publication and repository responsibilities	6	6
11. Privacy and confidentiality	0	0 (1)
12. Compromise and disaster recovery	1	1

Documents used:

- Guidelines for auditing Grid CAs, version 1.1 (27 Oct 2010)
- Authentication Profile for Classic X.509 Public Key Certification Authorities with secured infrastructure, version 4.4 (29 Feb 2012)

Self-Audit: CA Key

- CA re-key policies were missing
  - Items 17, 18
  - Score: D
- Not occurred yet
- Added in CP/CPS section 5.6
  - Needs approval

Self-Audit: CA Certificate

- In the CA certificate, the “key usage” extension is not marked as critical
  - Item 22
  - Score: B
- Cannot be changed at this point

Self-Audit: CRL

- CRL re-issued immediately only if certificate compromised
  - Item 30
  - Score: B
- No security problem
- Improves performance
- Not modified

Self-Audit: End Entity Certificates and Keys

- No user certificate may be shared
  - Item 35
  - Score:B
- Stated more explicitly in section 4.5.1

- Policy identifier certificate extensions
  - Item 38
  - Score: B
- Will fix when releasing new CP/CPS
  - Need new OID

Self-Audit: Records Archival

- All needed items archived, but not stated in CP/CPS
  - Item 43
  - Score: B
- Added in section 5.5.1

Self-Audit: summary

- Will provide new CP/CPS document
  - With modifications for self-audit only
  - Please comment
- Need 2 reviewers