ArmeSFo CA update (including self-audit)

Armenian e-Science Foundation
Certification Authority

Arsen Hayrapetyan

Status since January 2008…

- Last presented at 12th EUGridPMA meeting, January 2008, Amsterdam, Netherlands
- Since then…
  - 3 new versions of CP/CPS issued
  - EE certificate profile harmonised with Grid Certificate Profile v0.25
  - Publication of issued EE certificates discontinued: LDAP repository is no longer maintained
  - Switched to CRL v2
  - Audited by external auditor - Jens Jensen, UK e-Science CA.

CP/CPS changes

- Chiefly certificate profile changes - GCP v0.25 is implemented for EE certificates.
- CA root certificate had been accorded with GCP v0.25 prior to January 2008

Certificate profile changes

- Extensions removed from EE certificates: *nsCertType*, *nsBaseUrl*, *naCaPolicyUrl*, *nsComment*, *nsCaRevocationUrl*, *subjectKeyIdentifier*, *authorityKeyIdentifier*, *issuerAltName*
- Extensions added to **user** certificate: *extendedKeyUsage: clientAuth*
- Extensions added to **host** and **service** certificates: *extendedKeyUsage: clientAuth, serverAuth*
- Bits unset in *keyUsage* extension in **user** and **host/server** certificates: *nonRepudiation*, *keyAgreement*
- Bits set in *extendedKeyUsage* extension in **user** certificate: *emailProtection*
- Changes can be traced through *Revision History* of CP/CPSes (vv 0.5, 0.6, 0.7): http://www.escience.am/ca/policy

CRL v2

- Issuing CRL v2 is recommended by IETF PKIX - RFC 5280
- Switching to CRL v2 was rated as high-priority issue by the Auditor (mark D) during external audit

- So, starting with CP/CPS v0.7 (came into effect on 12 June 2009), we are issuing CRL v2.
  - Following CRL extensions are set: *cRLNumber* and *authorityKeyIdentifier*

Self and external audits

- Self-audit performed in December 2007
- Results sent to EUGridPMA
- Auditor appointed by PMA: David O'Callaghan
- Audited by Jens Jensen during his visit to Armenia (to work on NATO Collaborative Linkage Grant "Improved Cybersecurity for NATO Partner Countries"), 04-07 June 2009
- Some of the audit issues fixed

Results of the self-audit

- The issues were rated on the scale **A** (“it is OK”), **B** (“minor recommendation”, would be nice to change), **C** (“major recommendation”, this really ought to be changed), **D** (“Advice”, MUST be actually changed), X (“not applicable”)
- Identified:
  - 3 issues of type D
  - 10 issues of type C
  - 5 issues of type B

Results of the external audit

- Identified by external Auditor:
  - 4 issues of type D
  - 8 issues of type C
  - 5 issues of type B

Comparison of the results

Self-audit **C** ↑ external audit **D**	2 items
Self-audit **A** ↑ external audit **C**	1 item
Self-audit **B** ↑ external audit **C**	1 item
Self-audit **A** ↑ external audit **B**	1 item
Self-audit **D** ↓ external audit **C**	1 item
Self-audit **C** ↓ external audit **B**	1 item
Self-audit **C** ↓ external audit **A**	1 item

Items rated differently (1)

- *Self-audit **C** ↑ external audit **D***
  - Adding RAs to the list of entities who can request revocation
  - Separating CA encrypted private key from the pass phrase
- *Self-audit **A** ↑ external audit **C***
  - CRLs were issued in v1 format. V2 format was recommended by Auditor
- *Self-audit **B** ↑ external audit **C***
  - Defining the role of RA in proper section of the CP/CPS
- *Self-audit **A** ↑ external audit **B***
  - crlDistributionPoints extension points to PEM-formatted certificate

Items rated differently (2)

- *Self-audit **D** ↓ external audit **C***
  - Moving the safe with CA machine to the room where the physical access is restricted to CA personnel solely (access to the safe itself **is** restricted to CA personnel solely)
- *Self-audit **C** ↓ external audit **B***
  - Restructuring CP/CPS according to RFC 3647
- *Self-audit **C** ↓ external audit **A***
  - CP/CPS does not include the CA obligation to maintain the archive of records collected by RA, but it is included in ArmeSFo CA agreement with its RAs

Work on identified issues (1)

- Issues related to physical security
  - Moving CA machine safe to more protected area (D or C): *pending (we will probably move it in spring)*
  - Separating encrypted key from its password (D or C): *pending, will be fixed together with previous issue*
- CP/CPS-related issues – not fixed yet (planned for March-April)
  - CA policy approval procedure (C)
  - RAs are not specified as entities who can request revocation (D or C)
  - RA operation is nor described in sufficient detail (C)

Work on identified issues (2)

- Compromise and disaster recovery
  - No document detailing the procedure for CA personnel (D)
- CRL format
  - crlDistributionPoints extension in EE certificates points to PEM-formatted CRL. Should be DER-formatted (C)
- CRL version (D)
  - Fixed, we issue v2 CRL now
- Publication of SHA1 and MD5 sums of CA root certificate in the CA repository along with instructions how to verify them (C)
  - Fixed, the info is published in CA repository