ArmeSFo CA self-audit

Armenian e-Science Foundation Certification Authority

http://www.escience.am/ca/

Mariam Pilikyan, Narine Manukyan, Armenuhi Abramyan
mpilikya,nmanukya,aabramya@escience.am

Introduction

ArmeSFo CA was established by Armenian eScience Foundation in 2003.

Goal- courtesy service of the digital certificate issuance to Armenian academic community.

Member of EUGridPMA since December 2003

ArmeSFo CA statistics

ArmeSFo CA has 2 RA units:

RA of ArmeSFo CA in NAS RA (Serving to Institutions from National Academy of Sciences of the Republic of Armenia)

RA of ArmeSFo CA in ArmeSFo (Serving to other Armenian Institutions: Universities, Yerevan Physics Institute, etc)

Issued certificates: 366

- ✓ **Personal: 322**
- ✓ **Host: 44**

Revoked certificates : 46

- ✓ **Personal: 28**
- ✓ **Host: 18**

Valid certificates : 46

- ✓ **Personal: 35**
- ✓ **Host: 11**

Since May 2015, all EE certificates are issued using SHA-512 cryptographic hash function.

The last SHA-1 certificate expires on 12 May 2016

CP/CPS Version 1.0

We have introduced numerous changes to our previous CP/CPS (version 0.9).

The new, 1.0 , version has been sent to PMA assessment on 11 April

and has been published on 29 April 2016.

The updates were dictated by the results of previous self audits and ArmeSFo CA experience in the work with applicants and users.

In particular, the following major updates have been introduced in v1.0 :

- ✓ **Routine Re-key procedure;**
- ✓ **Detailed specification of the RA and subscriber obligations;**
- ✓ **Detailed description of certificate application and certificate issuance procedures;**
- ✓ **Detailed description of revocation request submission procedure.**

Self-Audit (what do we have with the last version of CP/CPS)

The Self-Audit followed the OGF GFD-I.169 document.

- **Total number of items: 68**
  - **65 issues of type A (“it is OK”)**
  - **1 issue of type C (“major recommendation”, this really ought to be changed)**
  - **2 issues of type X (“not applicable”)**

Issue of type C

3.1.1. CP/CPS
 # 6 from GFD-I.169
The CP/CPS document should be structured as defined in RFC 3647.

***Status*: ArmeSFo CA CP/CPS is structured according to RFC 2527.**
***Solution*: Current CP/CPS constitutes a reliable framework for our practices. Nonetheless, the updating will be done if strongly recommended by PMA and Relying Parties.**

Issues of type X

3.1.3. CA Key
 # 15 from GFD-I.169

The on-line CA architecture should provide for a (preferably tamper protected) log of issued certificates and signed revocation lists.

Status: **Not applicable. ArmeSFo CA is an offline CA.**

3.1.7. End Entity Certificates and Keys
 # 40 from GFD-I.169

Certificates associated with a private key restricted solely to hardware token may be renewed for a period of up to 5 years (for equivalent RSA key lengths of 2048 bits) or 3 years (for equivalent RSA key lengths of 1024 bits).

Status: **Not applicable. ArmeSFo CA does not have hardware token**

PEER REVIEWS?

THANK YOU

Backup slides

History of ArmeSFo CA audits (from Cosmin's presentation)

Self-audit	Lyon: 2012-09-11
Audit status	done
Peers	Jens Jensen, David O'Callaghan
Peer status	pending
Peer review status	14.04.2016: Ara: Suggests a) to use the new CP/CPS if approved and b) to perform the self-audit considering the new version. 11.04.2016: Mariam: Sends v.1.0 of ArmeSFo CA CP/CPS. It contains major modifications of the actual version. Intends to enter in production in 15 days. 07.04.2016: Narine: On behalf of ArmeSFo CA I confirm that we will remotely present our self-audit in Abingdon meeting. 17.12.2015: Narine: ArmeSFo CA will perform and remotely present self-audit to next PMA meeting following after Bratislava's. 04.09.2015: No answer, no update. 11.03.2015: Narine - ArmeSFo CA cannot present self-audit on upcoming meeting. 2014-09-08: Need new self-audit. Jens Jensen: ArmesFo? No, it's a long time ago I reviewed them. Probably due for another now, but I am not entirely convinced it should still be me who is a reviewer. I don't mind, but am fairly thinly sliced at the moment. David O'Callaghan: I'm also out of the CA business at the moment, so I would like to drop out of this...