ArmeSFo

Armenian e-Science Foundation
Certification Authority

ArmeSFo CA update

Armenuhi Abramyan, Narine Manukyan

aabramya@escience.am nmanukya@escience.am

26th EUGridPMA and IGTF All Hands meeting, Lyon, France, 10-12 Sep 2012

About Narine Manukyan

This presentation was planned to be presented by Narine Manukyan.
However, after a bicycle accident, happened ten days ago at CERN, she was strongly advised by physicians not to travel for some time.

Contents

- *Updates after January 2010, last presentation of ArmeSFo CA to EUGridPMA (in Dublin)*
- *Status of self- and external audits*
- *OCSP responder implementation*
- *SHA-2 based certificate profile*
- *Educational programme of ArmeSFo CA*
- *Next steps*

Updates: ArmeSFo CA personnel

The actual personnel of ArmeSFo CA:

- ***Ara Grigoryan*** – *manager*
- ***Arsen Hayrapetyan*** – *alternate manager*
- ***Narine Manukyan*** – *senior operator*
- ***Armenuhi Abramyan*** – *operator*
- ***Vardanush Papikyan*** – *operator*

Updates: New RA and new instructions

- In August 2007 ArmesFo CA established first RA unit for the users working in any structure of National Academy of Sciences of the Republic of Armenia (NAS RA), the largest in Armenia network of scientific institutions – **RA of ArmeSFo CA in NAS RA**

- **In October 2010 ArmeSFo CA established second RA unit for the users working in the other Armenian organizations – RA of ArmeSFo CA in ArmeSFo**

For each RA, detailed certificate request instructions for subscribers have been published.

ArmeSFo CA does not fulfill anymore the duties of RA.

Updates: Next version of CP/CPS

***Major** changes concern a very detailed specification of:*

- **RA obligations;**
- **Subscriber obligations;**
- **Re-keing procedure;**
- **Revocation request procedure.**

These changes reflect the experience of our work with Armenian RAs and subscribers.

The new CP/CPS is ready, however its publication is pending mainly because of a necessity to prepare and publish simultaneously the corresponding detailed instructions for ArmeSFo CA operators, RAs and subscribers.

Status of self- and external audits

- **ArmeSFo CA self-audit was done back in December 2007 following to audit guidelines version 1.0-b4** (https://forge.gridforum.org/sf/go/doc4858)

- **The results were presented at 12th EUGridPMA meeting in Amsterdam in January 2008** (https://www.eugridpma.org/agenda/archive-a073/ArmeSFo_CA_updates_and_self-audit.ppt)

- **In 2008 EUGridPMA appointed David O'Callaghan as a reviewer of ArmeSFo CA audit results**

- **In June 2009, the self-audit results were discussed in length with Jens Jensen who visited Armenia. Before the visit, it was agreed with David Groep that Jens would be a co-reviewer for the self-audit.**

- **Comments and suggestions by Jens have been taken into account and Arsen Hayrapetyan presented a status update at 18th EUGridPMA meeting in Dublin in January 2010 via videolink** (http://agenda.nikhef.nl/getFile.py/access?contribId=9&resId=1&materialId=slides&confId=914). **Jens commented on the self-audit after the talk and gave (orally) a (positive) short summary of his review.**

OCSP Configuration

In the CA's openssl.cnf new section is added:

```
[ v3_OCSP ]
basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
extendedKeyUsage = OCSPSigning
```

The following extension:

```
authorityInfoAccess = OCSP;URI:http://armgrid3.yerphi.am:8888
```

is added to the sections

```
[ usr_cert ],[ srv_cert ],[ service_cert]
```

One has the following extension in EE certificates:

```
Authority Information Access:
            OCSP - URI:http://armgrid3.yerphi.am:8888
```

Test certificate with SHA256 and OCSP

Version: 3 (0x2)
Serial Number: 181 (0xb5)
Signature Algorithm: **sha256WithRSAEncryption**
Issuer: C=AM, O=ArmeSFo, CN=ArmeSFo CA
Validity
Not Before: Jun 14 12:17:43 2012 GMT
Not After : Jun 14 12:17:43 2013 GMT
Subject: C=AM, O=ArmeSFo, O=YerPhI, OU=Experimental Division, CN=Hakob Hakobyan
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Modulus (1024 bit):
…
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Basic Constraints: critical
CA:FALSE
X509v3 Key Usage: critical
Digital Signature, Key Encipherment, Data Encipherment
X509v3 Extended Key Usage:
TLS Web Client Authentication, E-mail Protection
X509v3 Subject Alternative Name:
email:hakob@gmail.com
X509v3 Certificate Policies:
Policy: 1.3.6.1.4.1.17306.8.1.0.7
Policy: 1.2.840.113612.5.2.2.1
X509v3 CRL Distribution Points:
URI:http://armesfoca-crl.fzk.de/crl.pem

Authority Information Access:
OCSP - URI:http://armgrid3.yerphi.am:8888

Signature Algorithm: sha256WithRSAEncryption
……..

Educational programme

- **An educational web portal *WhyPKI* dedicated to the security in cyberspace has been created (http://www.escience.am/whypki/). The portal is bilingual, in Armenian and English, which is important for the development of the Armenian cybersecurity vocabulary**
- **An educational CA, *ToyCA*, providing certificates for any requestor has been created**
- **The *WhyPKI* portal provides for *ToyCA* an interface for generation of private keys and certificate requests (http://www.escience.am/whypki/?q=node/135)**
- A Bachelor student has been actively involved in the creation of ***WhyPKI*** and ***ToyCA***

Next steps

- ✓ **Transition to the issuance of SHA-2 based certs and preparation of appropriate user explanatory documents (by January 1, 2013);**
- ✓ **Deployment of a production OCSP responder on ArmeSFo CA server (by January 1, 2013);**
- ✓ **Enabling IPv6 for the end-point of CRL and OCSP responder;**
- ✓ **Generation of a new 4096-bit ArmeSFo CA private key;**
- ✓ **Issuance of new version of the CP/CPS;**
- ✓ **Preparation of the new instructions for ArmeSFo CA operators, RAs and subscribers compatible with new CP/CPS.**

Armenian e-Science Foundation
Certification Authority

THANK YOU!