ArmeSFo CA

Armenian e-Science Foundation CA: Status and Updates

Ara A. Grigoryan

ArmeSFo CA

Contents

1 Contact info and personnel

ArmeSFo CA

Armenian e-Science Foundation

49 Komitas Avenue

375051 Yerevan Armenia

Phone: (+37410) 230510

Fax: (+37410) 282951

e-mail: ca@escience.am

http://www.escience.am/

Contact persons:

Ara Grigoryan

Arsen Hayrapetyan

e-mail: ca@escience.am

The actual personnel are recruited mainly from young specialists of Yerevan Physics Institute.

The ArmeSFo CA team:

- ✓ Ara Grigoryan
- ❑ Artem Harutyunyan
- ➢ Arsen Hayrapetyan
- ❖ Tatevik Poghosyan

ArmeSFo CA

2 Current CA root certificate

Issuer:
C=AM, O=ArmeSFo, CN=ArmeSFo CA
Validity
Not Before: Dec 1 23:29:21 2003 GMT
Not After : Dec 1 23:29:21 2006 GMT
RSA Public Key: (2048 bit)

X509v3 extensions:

X509v3 Basic Constraints: critical
CA:TRUE
X509v3 Key Usage: critical
Digital Signature, Non Repudiation, Certificate Sign, CRL Sign
X509v3 Subject Alternative Name:
email:ca@escience.am
X509v3 Issuer Alternative Name:
email:ca@escience.am
X509v3 Certificate Policies:
Policy: 1.3.6.1.4.1.17306.8.1.0.1
CPS: http://www.escience.am/ca/policy/
X509v3 CRL Distribution Points:
URI:http://www.escience.am/ca/crl.pem

Netscape extensions

Netscape Cert Type:
SSL CA, S/MIME CA, Object Signing CA
Netscape Base Url:
http://www.escience.am/ca/
Netscape CA Policy Url:
http://www.escience.am/ca/policy/
Netscape Comment:
This is the root certificate of the ArmeSFo Certification Authority
Netscape CA Revocation Url:
http://www.escience.am/ca/crl.pem

ArmeSFo CA

3 End entities

The ArmeSFo CA issues certificates to physical persons, servers and services. The entities that are eligible for certification by the ArmeSFo CA are all those entities related to the organizations, formally based in and/or having offices inside the Republic of Armenia, that are involved in the research or deployment of multi-domain distributed computing infrastructures, intended for cross-organizational sharing of resources.

ArmeSFo CA

4 EE certificates

Issuer:
C=AM, O=ArmeSFo, CN=ArmeSFo CA
Validity:
Not Before: Jun 21 11:25:44 2005 GMT
Not After : Jun 21 11:25:44 2006 GMT
Subject:
C=AM, O=ArmeSFo, O=YerPhI, OU=Theoretical Department, CN=Ara Grigoryan
RSA Public Key: (1024 bit)

X509v3 extensions:

X509v3 Basic Constraints: critical CA:FALSE
X509v3 Key Usage: critical
Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment, Key Agreement
X509v3 Subject Alternative Name:
email:aagrigor@mail.yerphi.am
X509v3 Issuer Alternative Name:
email:ca@escience.am
X509v3 Certificate Policies:
Policy: 1.3.6.1.4.1.17306.8.1.0.1
CPS: http://www.escience.am/ca/policy/
X509v3 CRL Distribution Points:
URI:http://www.escience.am/ca/crl.pem

Netscape extensions

Netscape Cert Type:
SSL Client, S/MIME, Object Signing
Netscape Base Url:
http://www.escience.am/ca/
Netscape CA Policy Url:
http://www.escience.am/ca/policy/
Netscape Comment:
This is a user certificate issued by the ArmeSFo Certification Authority
Netscape CA Revocation Url:
http://www.escience.am/ca/crl.pem

ArmeSFo CA

5 EE certificates (statistics)

Bad network connection of Armenian scientific and educational institutions with the outer world!

No possibility to exploit International Grid functionalities

However, the ArmeSFo and Yerevan Physics Institute teams are actively involved in the development of the ALICE Environment on the Grid (AliEn)

Total: 9 certificates issued since the beginning of 2004

6 – users

3 – hosts

ArmeSFo CA fulfils itself the functions of RA

6 inCompliances with Minreqs

Configuration file

X509v3 Certificate Policies:
Policy: 1.3.6.1.4.1.17306.8.1.0.1
:-(CPS: http://www.escience.am/ca/policy/

:-(Default message digest is MD5

Security control

The ArmeSFo CA signing machine is kept in a safe. Physical access to the ArmeSFo CA signing machine is restricted to the authorized ArmeSFo CA personnel
:-(The safe still not in a dedicated room

Actions

Updates to .cnf. Renewal of the root certificate

Actions

The safe will be moved to a closed office by the end of the Winter 2006

ArmeSFo CA

7 Renewing the root certificate

1. The ArmeSFo CA root certificate expires on 01.12.2006
   Signing key changeover is needed
2. The CP and CPS, structured in accordance with rfc3647, have to be prepared

In order to provide:

- **>than one year overlap between old and new keys (1 year lifetime of the EE certificates)**
- **enough time for the fulfilment of 2,**

we need to renew our certificate with the extension of its lifetime for 1 year (+ a few months more?).

ArmeSFo CA

8 Updates to CP/CPS

The following sections are updated:

1.4 (Contact details are specified, missing rfc2527 entries are added);

2.6.1, 2.6.4 (URLs of the CA certificate, EE certificates, crl and CP/CPS are added. The address of ArmeSFo CA LDAP server is added);

3.1.9 (Added that the server and service certificate requests must be enclosed in the message body);

4.4.2, 4.4.4 (ArmeSFo CA is added to the revocation requestors. Revocation request grace period is set to one working day);

5.1.2 (The location of the CA signing machine is specified);

5.3.1, 5.3.8 (The issues concerning the qualification and recruitment of the CA personnel are specified);

6.5.1 (Last bullet is moved to 5.1.2);

9 (Bibliography. Some references are refreshed).

New OID: **1.3.6.1.4.1.17306.8.1.0.2**

ArmeSFo CA

9 Main plans for the nearest future

- Preparations for the ArmeSFo CA key changeover. CP and CPS according to rfc3647
- Introduction of the RA status: Signing the agreements with collaborating institutions (Yerevan Physics Institute, Yerevan State University, State Engineering University of Armenia, …)
- Study of the ArmeSFo CA status in relation to the recently approved Armenian law on digital signature
- Finding of a full-value funding. Actually the ArmeSFo CA is partially supported by the Swiss 'Fonds Kidagan' and Calouste Gulbenkian Foundation (Lisbon)