Armenian e-Science Foundation Certification Authority

Ara A. Grigoryan [1,2], Artem Harutyunyan [1,2,3], Arsen Hayrapetyan [1,2,4]

[1] Armenian e-Science Foundation;
[2] Yerevan Physics Institute;
[3] Student at Department of Computer Science and Informatics, State Engineering University of Armenia;
[4] Student at Department of Applied Mathematics, Yerevan State University

Armenian e-Science Foundation

http://www.escience.am

Non-profit Institution, established in 2002.

Goals - introduction and dissemination of the e-Science technologies in Armenian scientific, educational and other organizations.

Sponsors:

- Swiss "Fonds Kidagan";
- Caloust Gulbenkian Foundation;
- "Link Ltd" software developing company (http://www.link.am);
- "Lans Ltd" computer hardware vending company (http://www.lans.am);
- "Web" Internet Service Provider (http://www.web.am).

ArmeSFo Certification Authority

http://www.escience.am/ca

- One of the main objectives of ArmeSFo is the deployment of the Grid infrastructures in Armenia.
- ArmeSFo CA is an Armenian Certification Authority maintained by ArmeSFo as a courtesy service to the Armenian Grid community.
- ArmeSFo CA is managed by the ArmeSFo team of the Yerevan Physics Institute (http://www.yerphi.am).

ArmeSFo CA

CP/CPS

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

The document is based on the following sources:

[RFC 2527], [RFC3280], [DOE CP/CPS], [DutchGrid CP/CPS], [INFN CP/CPS], [Grid-Ireland CP/CPS], [LIP CP/CPS], [UK CP/CPS], [EuroPKI CP], [ASGCCA CP/CPS], [CERN CP/CPS].

Object Identifier: 1.3.6.1.4.1.17306.8.1.0.1

01 December 2003, Version 0.1 (Draft-B)

ArmeSFo CA

Distinguished Names Scheme

Common fixed component: C=AM, O=ArmeSFo

Examples of the Distinguished Names:

For issuer: ***C=AM, O=ArmeSFo, CN=ArmeSFo CA***

For persons: ***C=AM, O=ArmeSFo, O= YerPhI, OU=Experimental Department, CN=Artem Harutyunyan***

For servers: ***C=AM, O=ArmeSFo, O= YerPhI, OU=Experimental Department, CN=aligrid.yerphi.am***

For grid hosts: ***C=AM, O=ArmeSFo, O= YerPhI, OU=Experimental Department, CN=host/aligrid.yerphi.am***

For services: ***C=AM, O=ArmeSFo, O= YerPhI, OU=Experimental Department, CN=ldap/aligrid.yerphi.am***

ArmeSFo CA

Certificates Extensions

Eight X.509 extension entries/attributes:

basicConstraints (critical), keyUsage (critical), subjectKeyIdentifier, authorityKeyIdentifier, subjectAltName, issuerAltName, certificatePolicies, crlDistributionPoints

Five Netscape extension entries/attributes:

nsCertType, nsBaseUrl, nsCaPolicyUrl, nsComment, nsCaRevocationUrl

Three sets of extensions (three sets of attribute values):

1. **ArmeSFo CA user certificate extensions;**
2. **ArmeSFo CA server/host and service certificate extensions;**
3. **ArmeSFo CA root certificate extensions;**

ArmeSFo CA

Root Certificate

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

Self-signed Certificate

Subject DN=Issuer DN: C=AM, O=ArmeSFo, CN=ArmeSFo CA

Date of issuance: 01.12.2003

Life time: 1096 days

Key length: 2048 bits

MD5 Fingerprint: 63:B3:08:9F:57:76:4A:B0:FC:D2:3D:26:15:14:CA:E7

Hash value: d0c2a341

ArmeSFo CA

End Entity Certificates

Life time: Not more than 1 year

Key length: At least 1024 bits

Authentication of the entity's identity:

For person requesting a certificate: In person presentation of valid official identification document

For server/host/service: Request is sent by e-mail, signed by a valid ArmeSFo CA certificate of the corresponding system administrator

Public key delivery to ArmeSFo CA: Signed e-mail, FDs, CDROMs

ArmeSFo CA

Certificate Revocation List

URI: http://www.escience.am/ca/crl.pem

CRL issuance frequency:

- The maximum (minimum) lifetime of the CRL is 30 (7) days;
- CRL is updated immediately after every revocation;
- CRL is reissued at least 7 days before expiration

Circumstances for revocation:

- **The private key has been lost or compromised;**
- **The information in the certificate is suspected to be inaccurate;**
- **The subscriber has failed to comply with the rules of ArmeSFo CA CP/CPS;**
- **The system to which the certificate has been issued has been retired.**
- **The subscriber of the certificate has ceased his relation with organization;**
- **At subscriber's request**

ArmeSFo CA

Security Standards

Private key security:

- Protected by strong (at least 16 characters) pass-phrase;
- Kept encrypted in multiple copies in FDs and CDROMS stored in secure places

Computer security:

- Operating systems of the ArmeSFo CA computers are maintained at a high level of security by applying all recommended and applicable patches;
- Operating systems configuration is reduced to the base minimum;
- Signing machine is kept in a safe and powered off between uses. Only the ArmeSFo CA personnel have access to the safe's keys.

ArmeSFo CA

Signing Machine

Location: Yerevan Physics Institute

ArmeSFo CA

Recorded and Archived Events

Types of events recorded:

- Certification requests;
- Issued certificates;
- Revocation requests;
- Issued CRLs;
- CA machine boots/logins/logouts.

Types of events archived:

- Certification requests;
- Issued certificates;
- Revocation requests;
- Issued CRLs;
- CA machine boots/logins/logouts;
- All electronic messages sent to and by the ArmeSFo CA.

ArmeSFo CA

Personnel Control

Background, qualification and experience requirements:

The ArmeSFo CA personnel is recruited from the ArmeSFo team of the Yerevan Physics Institute. The recruited persons are familiar with the importance of PKI and are technically and professionally competent.

Documentation supplied to personnel:

- Copy of the ArmeSFo CA CP/CPS;
- The ArmeSFo CA Operations Manual.

ArmeSFo CA

Personnel

3-year experience of the work on the Grid issues, including certification (AliEn)

ArmeSFo CA

Contact Details

Address for operational issues:

Yerevan Physics Institute 2, Brothers Alikhanian Str.
375036 Yerevan Armenia

Phone: (+ 3741) 341500; Fax: (+ 3741) 350030
Email: ca@escience.am

Contact persons:

Ara A. Grigoryan (aagrigor@jerewan1.yerphi.am)
Artem Harutyunyan (hartem@moon.yerphi.am)

Yerevan Physics Institute 2, Brothers Alikhanian Str.
375036 Yerevan Armenia

Phone: (+ 3741) 341500; Fax: (+ 3741) 350030