Armenian e-Science Foundation

ArmeSFo CA

Certificate Policy and Certification Practice Statement

Version 0.8

29 December 2012

Table of Contents

1 Introduction

1.1 Overview

Armenian e-Science Foundation (http://www.escience.am/) is an Armenian non-profit institution aimed at the introduction and dissemination of e-Science technologies in Armenian scientific, educational and other organizations. One of the main objectives of ArmeSFo is the deployment of the Grid infrastuctures in Armenia. ArmeSFo CA is an Armenian Certification Authority maintained by ArmeSFo as a courtesy service to the e-Science activities in Armenia.
This is a draft document structured according to the memo “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practice Framework” [RFC 2527]. This document describes the set of rules and operational practices used by the ArmeSFo CA.

1.1.1 General definitions

Activation data

Data values, other than keys, that are required to operate cryptographic modules and that need to be protected (e.g., a PIN, a pass phrase, or a manually-held key share).

ArmeSFo

Armenian e-Science Foundation

Authentication

The process of establishing that individuals, organizations, or things are who or what they claim to be. In the context of a PKI, authentication can be the process of establishing that an individual or organization applying for or seeking access to something under a certain name is, in fact, the proper individual or organization. This process corresponds to the second process involved with identification as shown in the definition of the “identification” below. Authentication can also refer to a security service that provides assurances that individuals, organizations, or things are who or what they claim to be or that a message or other data originated from a specific individual, organization, or device. Thus, it is said that a digital signature of a message authenticates the message’s sender.

Certificate

Synonymous with Public Key Certificate

Certification Authority (CA)

An authority trusted by one or more subscribers to create and assign public key certificates and to be responsible for them during their whole lifetime.

Certificate Policy (CP)

A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range.

Certification Practice Statement (CPS)

A statement of the practices, which a CA employs in issuing certificates.

Certificate Revocation List (CRL)

A time stamped list identifying the revoked certificates, which is signed by a CA and made freely available in the CA public repository.

Host certificate

A certificate for server certification and encryption of communications (SSL/TLS). It will represent a single machine.

Identification

The process of establishing the identity of an individual or organization, i.e., to show that an individual or organization is a specific individual or organization. In the context of a PKI, identification refers to two processes: (1) establishing that a given name of an individual or organization corresponds to a real world identity of an individual or organization, and (2) establishing that an individual or organization applying for or seeking access to something under that name is, in fact, the named individual or organization. A person seeking identification may be a certificate applicant, an applicant for employment in a trusted position within a PKI participant, or a person seeking access to a network or software application, such as a CA administrator seeking access to CA systems.

Person Certificate

A certificate used for authentication to establish a person identity. It will represent an individual person.

Policy qualifier

The policy-dependent information that accompanies a certificate policy identifier in an X.509 certificate.

Public Key Certificate (PKC)

A data structure containing the public key of an entity and some other information, which is digitally signed with the private key of the CA, which issued it.

Registration Authority (RA)

An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA).

Relying party

A recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate. In this document, the terms “certificate user” and “relying party” are used interchangeably.

Repository

A storage area, usually on-line, where a CA stores its root certificate, issued certificates, CRLs, policy documents etc.

Service certificate

A certificate for a particular service running on a host. It will represent a single service on a single host.

Strong pass-phrase

In this document, “strong pass-phrase" refers to a pass phrase protecting a private key and satisfying the following: it is at least 16 characters long and contains upper and lower case letters. The pass-phrase should also contain some non-letter characters in the US-ASCII range (0x20-0x7e) and no letters outside this range.

Subscriber

A person or server to whom a digital certificate is issued.

1.2 Identification

Title: **ArmeSFo CA Certificate Policy and Certification Practice Statement**

Version: **0.8**

Date: **29 December 2012**

Expiration: **This document is valid until further notice.**

OID**: The following unique Object Identifier (OID) identifies this CP/CPS:**

1.3.6.1.4.1.17306.8.1.0.8

The following Table clarifies the meaning of this OID

1	International Organization for Standardization (ISO) assigned OIDs
3	Organizations acknowledged by ISO
6	United States Department of Defense (DOD)
1	Internet
4	Private
1	Internet Assigned Numbers Authority (IANA) registered private enterprises
17306	Armenian e-Science Foundation (ArmeSFo)
8	ArmeSFo CA
1	ArmeSFo CA CP/CPS
0	Major version
8	Minor version

1.3 Community and Applicability

1.3.1 Certification authorities

The ArmeSFo CA does not issue certificates to subordinate certification authorities.

1.3.2 Registration authorities

The ArmeSFo CA also performs the role of RA. Further registration authorities may be created by the ArmeSFo CA as required in order to support both the growth of the organizations and the demand for certificates.

1.3.3 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.

1.3.4 Applicability

The issued certificate can be used for:

- e-mail signing and encryption (S/MIME);
- authentication and encryption of communication (SSL/TLS)
- object-signing

Certificates issued by the ArmeSFo CA are only valid in the context of the ArmeSFo computing infrastructure research and deployment activities, any other usage including financial transactions is strictly forbidden.

1.4 Contact Details

1.4.1 Specification administration organization

The ArmeSFo CA is managed by the ArmeSFo team. The ArmeSFo CA address for operational issues is:

Armenian e-Science Foundation
49 Komitas Avenue
375051 Yerevan Armenia

Phone: (+37410) 230510
Fax: (+37410) 282951
Email: ca@escience.am

1.4.2 Contact person

The contact persons for questions related with this document or any other ArmeSFo CA related issues are:

Ara Grigoryan
Arsen Hayrapetyan
Email: ca@escience.am

1.4.3 Person determining CPS suitability for the policy

No stipulation

2 General Provisions

2.1 Obligations

2.1.1 CA obligations

The ArmeSFo CA will:

- Authenticate entities according the procedure outlined in this document;
- Issue certificates based on requests from authenticated entities;
- Notify the subscriber of the issuing of the certificate;
- Accept revocation requests from authenticated entities;
- Issue CRL according to the procedure outlined in this document;
- Publish the issued CRL;
- Follow the policies and procedures described in this document.

2.1.2 Subscriber obligations

Subscriber must:

- Read and adhere to the policy and procedures outlined in this document;
- Generate a key pair using a trustworthy method;
- Take reasonable precautions to prevent any loss, disclosure or unauthorized use of the private key associated with the certificate;
- Use a strong pass-phrase (see in General Definitions) to protect the private key of the personal certificate;
- Notify the ArmeSFo CA immediately in case of possible private key compromise;
- Notify the ArmeSFo CA immediately in case of key destruction and loss;
- Notify the ArmeSFo CA when the certificate is no longer required;
- Notify the ArmeSFo CA when the information in the certificate becomes wrong or inaccurate.

2.1.3 Relying party obligations

Relying parties must:

- Read and accept the policy and procedures published in this document;
- Verify the CRL before validating a certificate;
- Use the certificates for permitted uses only.

2.1.4 Repository obligations

- The ArmeSFo CA will keep a web server page at http://www.escience.am/ca/;
- The ArmeSFo CA will publish on its web server a copy of this document;
- The ArmeSFo CA will publish on its web server the ArmeSFo CA public key certificate;
- The ArmeSFo CA will publish on its web server the CRLs as soon as issued.

2.2 Liability

- The ArmeSFo CA only guarantees to control the identity of the subjects requesting a certificate according to the practices described in this document;
- The ArmeSFo CA is run on a best effort only basis and does not give any guarantees about the service security or suitability;
- The ArmeSFo CA does not warrant its procedures and it will take no responsibility for problems arising from its operation or for the use made of certificates it issues;
- The ArmeSFo CA denies any financial or any other kind of responsibilities for damages or impairments resulting from its operation.

2.3 Financial Responsibility

The ArmeSFo CA denies any financial responsibilities for damages or impairments resulting from its operation.

2.4 Interpretations and Enforcement

2.4.1 Governing law

This document is subject to all applicable laws of the Republic of Armenia.

2.4.2 Severability, survival, merger, notice

The ArmeSFo CA shall be entitled to terminate the certification services at any time. The ArmeSFo CA will make all reasonable efforts to notify on such termination all its subscribers and any relying parties known to the ArmeSFo CA to be currently and actively relying on certificates issued by the ArmeSFo CA. All certificates issued by the ArmeSFo CA that reference this document will be revoked no later than the time of termination.

2.4.3 Dispute resolution procedure

All disputes related to the interpretation and enforcement of the conditions and rules described in this document will be resolved by the Chairman of the ArmeSFo.

2.5 Fees

No fees are charged.

2.6 Publication and Repository

2.6.1 Publication of CA information

The ArmeSFo CA publishes the following information through its online repositories:

- The ArmeSFo CA root certificate – http://www.escience.am/ca/cacert/;
- The latest CRL – http://armesfoca-crl.fzk.de/crl.pem
- All versions of ArmeSFo CA CP/CPS document – http://www.escience.am/ca/policy/;
- Other relevant information.

2.6.2 Frequency of publication

- The certificates will be published as soon as issued;
- The CRL's will be published as soon as issued and at least every 30 days;
- New versions of the ArmeSFo CA CP/CPS will be published as soon as they have been approved.

2.6.3 Access controls

- The ArmeSFo CA online repository is maintained on a best effort basis. Excluding maintenance shutdowns and unforeseen failures the site should be available most of the time.
- The ArmeSFo CA does not impose any access control on its policy, its certificate, issued certificates and CRLs

2.6.4 Repositories

- The ArmeSFo CA web server is at http://www.escience.am/ca/

2.7 Compliance Audit

A self-assessment will be done at least once per year by the ArmeSFo CA to verify that its operation is according to this CP/CPS.
The ArmeSFo CA compliance with the rules and procedures specified in this CP/CPS may also be audited by other trusted CA at their own expense.

2.8 Confidentiality

2.8.1 Types of information to be kept confidential

The only confidential information kept by ArmeSFo CA is a photocopy of the subscriber's organization identity card or organization official document proving the relation of the subscriber with the organization.

2.8.2 Types of information not considered confidential

The ArmeSFo CA collects the following information that is not considered confidential:

- The subscriber's full name;
- A photocopy of the subscriber passport;
- The subscriber's e-mail address;
- The subscriber's organization address;
- The subscriber's certificate request file;
- The subscriber's public key file.

The information included in issued certificates and CRLs is not considered confidential. Under no circumstances will the ArmeSFo CA have access to the private keys of any subscriber to whom it issues a certificate.

2.8.3 Disclosure of certificate revocation/suspension information

The ArmeSFo CA will notify and inform the following entities:

- The subject of the personal certificate;
- The requestor of the server or service certificate.

2.8.4 Release to law enforcement officials

The information collected by the ArmeSFo CA will be made available to the law enforcement officials upon their request.

2.8.5 Release as part of civil discovery

The information collected by the ArmeSFo CA will be subject to the law of the Republic of Armenia.

2.8.6 Disclosure upon owner's request

The information collected by the ArmeSFo CA will be subject to the law of the Republic of Armenia.

2.8.7 Other information release circumstances

The information collected by the ArmeSFo CA will be subject to the law of the Republic of Armenia.

2.9 Intellectual Property Rights

No IPR are claimed on the certificates or CRLs issued by the ArmeSFo CA.
This 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].
This text may be used by anybody without prior approval; acknowledgments are welcomed but not required. Unmodified copies may be published without permission.

3 Identification and Authentication

3.1 Initial Registration

3.1.1 Types of names

Name components vary depending on the type of certificate. Names will be consistent with the name requirements specified in [RFC3280].
The certificate subject name is an X.500 distinguished name. Any name under this CP/CPS starts with a fixed component common to all certificates issued by ArmeSFo CA

C=AM, O=ArmeSFo

The variable component contains the name of the organization (O) with which the subject is officially related. A second optional organizational unit name (OU) must be specified when the certificate subject is related with a sub-organization as branch or department of the main organization. A common name (CN) that uniquely identifies the subject name must follow the organization name. The CN must be obtainable from the subject real name as stated in Section 3.1.2. For a server, the CN is the fully qualified domain name (FQDN) of the server. For a grid host, the CN is the FQDN of the server prefixed with the qualifier “host/”. For a service, the CN is the FQDN of the server prefixed with the service name followed by a slash.
Following this, the distinguished name has one of the following forms:

For issuer

C=AM, O=ArmeSFo, CN=ArmeSFo CA

For persons

C=AM, O=ArmeSFo, O=*organizationName*, OU=*organizationunitName*, CN=*commonName*

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

For servers

C=AM, O=ArmeSFo, O=*organizationName*, OU=*organizationunitName*, CN=*server FQDN*

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

For grid hosts

C=AM, O=ArmeSFo, O=*organizationName*, OU=*organizationunitName*, CN=*host/server FQDN*

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

For services

C=AM, O=ArmeSFo, O=*organizationName*, OU=*organizationunitName,* CN=*serviceName/server FQDN*

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

3.1.2 Need for names to be meaningful

- The names specified in the common name, in the organization name and in the organizational unit name must be meaningful. The names must be related with the subject organization and with the subject real name.
- For persons, the CN must be obtainable from the legal person name as presented in an official governmental identity document such as a passport or identity card.
- For servers and grid hosts, the CN must be formed from the FQDN.
- For a service, the CN must be related to the type of service and the FQDN of the server where the service is running.

3.1.3 Rules for interpreting various name forms

See Sections 3.1.1 and 3.1.2.

3.1.4 Uniqueness of names

The distinguished name for each certificate must be unique. In case of real subject name duplication, additional numbers and/or letters will be appended to the distinguished name to guarantee uniqueness.

3.1.5 Name claim dispute resolution procedure

No stipulation.

3.1.6 Recognition, authentication and role of trademarks

No stipulation.

3.1.7 Method to prove possession of private key

No stipulation.

3.1.8 Authentication of organization identity

The relation between the subscriber and the organization or organizational unit mentioned in the subject name must be proved through an organization identity card or organization official document stamped and signed by an official representative of the organization. In case of doubt the CA may take any required steps to inquire about the relation of the subscriber with the organization.

3.1.9 Authentication of individual identity

Procedure differs if the subject is a person, server or service:

For person requesting a certificate:

The certificate must be requested from the ArmeSFo CA in person. The person authentication is performed through the presentation of valid official identification documents proving that the subject is an acceptable end entity as defined in the Section 1.3.3 of this CP/CPS:

For server or service:

Certificate requests must be sent by e-mail, signed by a valid personal ArmeSFo CA certificate of the corresponding system administrator. The requests must be enclosed in the message body.

3.2 Routine Rekey

- Rekeying of the certificates before their expiration is not allowed
- Rekeying of the expired certificates will follows the same rules as an initial registration.

3.3 Rekey After Revocation

There is no rekey after revocation. Subscribers must apply for a new certificate.

3.4 Revocation Request

Certificate revocation requests should be submitted in the following ways:

- By an e-mail sent to ca@escience.am and signed with a valid ArmeSFo CA certificate; When the e-mail is not an option, the request will be authenticated using the procedure described in Section 3.1.9.

4 Operational Requirements

4.1 Certificate Application

- The subscriber must generate his own key pair as per Section 6.
- The subscriber must register with the ArmeSFo CA as per Section 3.1.
- The Distinguished Name must be as per Section 3.1.

4.2 Certificate Issuance

- The ArmeSFo CA issues the certificate if, and only if, the authentication of the subject is successful.
- The subject will be notified by e-mail about the certificate issuance or rejection. In the case of rejection, the e-mail will state the reason.

4.3 Certificate Acceptance

No stipulation.

4.4 Certificate Suspension and Revocation

4.4.1 Circumstances for revocation

A certificate will be revoked in the following circumstances:

- 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 in this 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.

4.4.2 Who can request revocation

The revocation of the certificate can be requested by:

- ArmeSFo CA;
- The certificate holder;
- Any other entity presenting proof of knowledge of the private key compromise, of the certificate misuse, or of the modification of the subscriber's data.

4.4.3 Procedure for revocation request

The revocation request will be authenticated as per Section 3.1.9.

4.4.4 Revocation request grace period

The ArmeSFo CA will response to revocation requests within one working day, except weekends and public holidays.

4.4.5 Circumstances for suspension

The ArmeSFo CA does not suspend the certificates.

4.4.6 CRL issuance frequency

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

4.4.7 CRL checking requirements

A relying party must verify a certificate against the most recent CRL issued, in order to validate the use of the certificate.

4.4.8 On-line revocation/status checking availability

No stipulation.

4.4.9 On-line revocation checking requirements

No stipulation.

4.4.10 Other forms of revocation advertisement available

No stipulation.

4.4.11 Checking requirements for other forms of revocation advertisement

No stipulation.

4.4.12 Special requirements re key compromise

No stipulation.

4.5 Security Audit Procedures

4.5.1 Types of events recorded

The ArmeSFo CA records the following events:

- Certification requests;
- Issued certificates;
- Requests for revocation;
- Issued CRLs;
- CA machine boots/logins/logouts.

4.5.2 Frequency of processing log

No stipulation.

4.5.3 Retention period for audit logs

Logs will be kept for a minimum of 3 years.

4.5.4 Protection of Audit Log

Only authorized ArmeSFo CA personnel is allowed to view and process audit logs. Audit logs are copied to an off-line medium.

4.5.5 Audit log backup procedures

Audit events are copied to an off-line medium, which is kept in a safe storage.

4.5.6 Audit collection system (internal vs. external)

The audit log accumulation system is internal to the ArmeSFo CA.

4.5.7 Notification to event-causing subject

No stipulation.

4.5.8 Vulnerability assessments

No stipulation.

4.6 Records Archival

4.6.1 Types of events recorded

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

4.6.2 Retention period for archive

Minimum retention period is three years.

4.6.3 Protection of archive

Archives are copied to an off-line medium in encrypted form and stored in a safe place.

4.6.4 Archive backup procedures

See Section 4.6.3.

4.6.5 Requirements for time-stamping of records

No stipulation.

4.6.6 Archive collection system (internal or external)

The archive system is internal to the ArmeSFo CA.

4.6.7 Procedures to obtain and verify archive information

No stipulation.

4.7 Key Changeover

The ArmeSFo CA's private signing key is changed periodically; from that time on, only the new key will be used for certificate signing purposes.
The older, but still valid, certificate will be available to verify old signatures until all of the certificates signed using the associated private key have also expired.

4.8 Compromise and Disaster Recovery

4.8.1 Computing resources, software, and/or data are corrupted

If the ArmeSFo CA equipment is damaged or rendered inoperative, but the CA private key is not destroyed, CA operation will be reestablished as quickly as possible. If the private key is destroyed, the case will be treated as per Section 4.8.3.

4.8.2 Entity public key is revoked

As per Section 4.8.3.

4.8.3 Entity key is compromised

If the private key of the ArmeSFo CA is, or suspected to be, compromised, the ArmeSFo CA will:

- Inform subscribers and any known relying party;
- Terminate the certificates and CRL distribution services for certificates and CRLs issued using the compromised key;
- Generate a new CA key pair and make the public key immediately available in the public repository.

New certificates will be issued only in accordance with the entity identification procedure defined in Section 3.1.

If an entity private key is compromised or suspected to be compromised, the entity must request a revocation of the certificate and make all reasonable efforts to inform any known relying parties.

4.8.4 Secure facility after a natural or other type of disaster

In the case of a disaster whereby the CA installation is physically damaged and all copies of the CA signature key are destroyed as a result, the ArmeSFo CA will take whatever action it deems appropriate.

4.9 CA Termination

Before the ArmeSFo CA terminates its services, it will:

- Inform the subscribers and all relying parties;
- Cease the issuance of certificates and CRLs;
- Destroy all copies of private keys;
- Make widely available the information of its termination.

5 Physical, Procedural and Personnel Security Controls

5.1 Physical Controls

5.1.1 Site location and construction

The ArmeSFo CA signing machine is housed in the Yerevan Physics Institute in Yerevan.

5.1.2 Physical access

- The ArmeSFo CA signing machine is kept in a safe. Only the ArmeSFo CA personnel have access to the safe's keys;
- Physical access to the ArmeSFo CA signing machine is restricted to the authorized ArmeSFo CA personnel.

5.1.3 Power and air conditioning

- The ArmeSFo CA signing machine and the ArmeSFo CA web server are both protected by uninterruptible power supplies;
- Environment temperature in rooms containing CA related equipment is maintained at appropriate levels by suitable air conditioning systems.

5.1.4 Water exposures

Due to the location of the ArmeSFo CA facilities, floods are not expected.

5.1.5 Fire prevention and protection

The ArmeSFo CA facilities obey to the Republic of Armenia law regarding fire prevention and protection in buildings.

5.1.6 Media Storage

- The ArmeSFo CA key is kept in several removable storage media;
- Backup copies of the CA related information are kept in floppies and CD-ROMs.

5.1.7 Waste disposal

Waste carrying potentially confidential information such as old floppy disks, are physically destroyed before being trashed.

5.1.8 Off-site backup

No stipulation.

5.2 Procedural Controls

No stipulation.

5.3 Personnel Controls

5.3.1 Background, qualifications, experience and clearance requirements

The role of the CA requires a suitably trained person that is familiar with the importance of a PKI, and who is technically and professionally competent. The actual personnel are recruited from specialists of Yerevan Physics Institute. There are no background checks of clearance procedures for trusted or other roles.

5.3.2 Background check procedures

See Section 5.3.1.

5.3.3 Training requirements

No stipulation.

5.3.4 Retraining frequency and sequence

No stipulation.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

No stipulation.

5.3.7 Contracting personnel requirements

No stipulation.

5.3.8 Documentation supplied to personnel

- Copy of this document;
- The ArmeSFo CA operations internal documents.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key pair generation

- Keys for the ArmeSFo CA are generated by the ArmeSFo CA managers on dedicated machine not connected to any kind of network. The software package is OpenSSL;
- Each entity must generate its key pair. The ArmeSFo CA does not generate private keys for entities.

6.1.2 Private key delivery to entity

The ArmeSFo CA does not generate private keys for entities and hence does not deliver private keys.

6.1.3 Public key delivery to certificate issuer

The entities' public keys are delivered to the ArmeSFo CA by signed e-mail, floppy disks, CDROMs.

6.1.4 CA public key delivery to users

The ArmeSFo CA certificate can be downloaded from the ArmeSFo CA web site.

6.1.5 Key sizes

- The minimum key length for a user or host/service certificate is 1024 bits;
- The ArmeSFo CA key length is 2048 bits.

6.1.6 Public key parameters generation

No stipulation.

6.1.7 Parameter quality checking

No stipulation.

6.1.8 Hardware/software key generation

No stipulation.

6.1.9 Key usage purposes (as per X.509 v3 key usage field)

For certificates issued by the ArmeSFo CA under this policy, the *keyUsage* extension is defined in Section 7.1.2.

6.2 Private Key Protection

6.2.1 Standards for cryptographic module

No stipulation.

6.2.2 Private key (n out of m) multi-person control

No stipulation.

6.2.3 Private key escrow

No stipulation.

6.2.4 Private key backup and archival

The ArmeSFo CA private key is kept encrypted in multiple copies in floppy disks and CDROMs stored in secure places.

6.2.5 Private key entry into cryptographic module

No stipulation.

6.2.6 Method of activating private key

The ArmeSFo CA private key is activated by a pass-phrase.

6.2.7 Method of deactivating private key

No stipulation.

6.2.8 Method of destroying private key

No stipulation.

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archival

All issued certificates are archived.

6.3.2 Usage periods for the public and private keys

The ArmeSFo CA root certificate has a validity of no more than twenty years. For other entity certificates, the maximum validity period is one year.

6.4 Activation Data

The ArmeSFo CA private key is protected by a strong pass-phrase.

6.4.1 Activation data generation and installation

No stipulation.

6.4.2 Activation data protection

All ArmeSFo CA operators know the activation data for the ArmeSFo CA private key. No other person knows the activation data. However, the activation data for the ArmeSFo CA private key is also kept in a sealed envelop in a safe in a separate location from the safe containing the private key and its backup copies.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific computer security technical requirements

- The operating systems of the ArmeSFo CA computers are maintained at a high level of security by applying all recommended and applicable patches;
- The operating systems configuration is reduced to the base minimum.

6.5.2 Computer security rating

No stipulation.

6.6 Life Cycle Security Controls

No stipulation.

6.7 Network Security Controls

Certificates are issued on a machine that is not connected to any kind of network.

6.8 Cryptographic Module Engineering Controls

No stipulation.

7 Certificate and CRL Profiles

7.1 Certificate Profile

7.1.1 Version number

X.509 v3.

7.1.2 Certificate extensions

The following extensions are set in the ArmeSFo CA user certificate:

- basicConstraints: **critical, CA:FALSE**
- keyUsage: **critical, digitalSignature, keyEncipherment, dataEncipherment**
- extendedKeyUsage: **clientAuth, emailProtection**
- subjectAltName: ***User's e-mail address***
- certificatePolicies: **The OID of ArmeSFo CA CP/CPS**
- crlDistributionPoints: **URI:http://armesfoca-crl.fzk.de/crl.pem**

The following extensions are set in the ArmeSFo CA server/host and service certificates:

- basicConstraints: **critical**, **CA:FALSE**
- keyUsage: **critical**, **digitalSignature**, **keyEncipherment**, **dataEncipherment**
- extendedKeyUsage: **clientAuth**, **serverAuth**
- subjectAltName: ***Server's Fully Qualified Domain Name***
- certificatePolicies: **The OID of ArmeSFo CA CP/CPS**
- crlDistributionPoints: **URI:http://armesfoca-crl.fzk.de/crl.pem**

The following extensions are set in the ArmeSFo CA root certificate:

- basicConstraints: **critical, CA:TRUE**
- keyUsage: **critical, keyCertSign, cRLSign**
- subjectKeyIdentifier: **hash**
- authorityKeyIdentifier: **keyid**

7.1.3 Algorithm object identifiers

No stipulation.

7.1.4 Name forms

See Section 3.1.1.

7.1.5 Name constraints

See Section 3.1.2.

7.1.6 Certificate policy object identifier

See Section 1.2.

7.1.7 Usage of policy constraints extensions

No stipulation.

7.1.8 Policy qualifier syntax and semantics

No stipulation.

7.1.9 Processing semantics for the critical certificate policy extensions

No stipulation.

7.2 CRL Profile

7.2.1 Version number

X.509 v 2.

7.2.2 CRL and CRL entry extensions

The following extensions are set in the CRL:

- cRLNumber: **The number of current CRL**
  CRL numbers are sequential, starting from 1.
- authorityKeyIdentifier: **Unique identifier for the private key of the CA**

Both extensions are non-critical.

8 Specification Administration

8.1 Specification Change Procedures

Subscribers will not be warned in advance of changes to ArmeSFo CA's policy and CPS.

8.2 Publication and Notification Policies

The ArmeSFo CA policy is available at http://www.escience.am/ca/policy/.

8.3 CPS Approval Procedures

No stipulation.

9 Bibliography

[ASGCCA CP/CPS] Academia Sinica Grid Computing Certification Authority (ASGCCA) Certificate Policy and Certification Practice Statement (Version 1.1, June 2003)

[CERN CP/CPS] CERN Certification Authority Certificate Policy and Certification Practice Statement (Version 2.0, August 18, 2002)

[DOE CP/CPS] DOE Grids Certificate Policy And Certification Practice Statement (Version 2.3, December 15, 2002)

[DutchGrid CP/CPS] DutchGrid and NIKHEF Medium-security X.509 Certification Authority Certification Policy and Practice Statement (Version 2.2, November 4, 2004)

[EuroPKI CP] EuroPKI Certificate Policy (Version 1.1, draft 4, October 2000)

[Grid-Ireland CP/CPS] Grid-Ireland Certification Authority Certificate Policy and Certification Practice Statement (Version 0.4, draft, June, 2002)

[INFN CP/CPS] INFN CA Certificate Policy and Certification Practice Statement (Version 1.0, December 2001)

[LIP CP/CPS] LIP CA Certificate Policy and Certification Practice Statement (Version 4.0, draft-F, 20 June 2003)

[RFC 2527] S. Chokani and W. Ford, “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practice Framework”, RFC2527

[RFC3280] R. Housley et. al., Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, RFC3280 (obsoletes: RFC2459) “

[UK CP/CPS] UK e-Science Certification Authority Certificate Policy and Certification Practice Statement (Version 1.2, 15 May 2005)

[Grid Certificate Profile] Grid Certificate Profile version 1.25 (published as Global Grid Forum document, GFD-C.125, CAOPS-WG)

Appendix: Revision History

Version	Major and minor numbers of OID	Date	Comments
0.1 (Draft-C)	0.1	20 March 2004	Initial approved release
0.2	0.2	10 November 2005	**The following sections are updated:** **1.1** (It is specified that ArmeSFo CA is maintained by ArmeSFo as a courtesy service to the e-Science activities in Armenia); **1.4** (Contact details are specified, missing rfc2527 entries are added); **2.6.1, 2.6.4** (URIs 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); **6.3.2** (The validity of ArmeSFo Ca root certificate is set to five years); **6.5.1** (Last bullet is moved to 5.1.2); **9** (Bibliography. Some references are refreshed).
0.3	0.3	31 March 2006	**The following sections are updated:** **2.6.1** and **7.1.2** (The URI of CRL is changed) **Appendix: Revision History:** (A few textual corrections are made)
0.4	0.4	27 November 2007	**The following sections are updated:** **1.2** (Minor version number of OID is changed to 4) **6.3.2** (The life time of CA root certificate is extended to ten years) **7.1.2** (The “digitalSignature” and “nonRepudiation” attributes are removed from *keyUsage* extension of CA root certificate. The “issuer:always” attribute is removed from *authorityKeyIdentifier* extension of CA root certificate. The following extensions are removed from CA root certificate: *subjectAltName, issuerAltName, certificatePolicies, crlDistributionPoints, nsCertType, nsBaseUrl, nsCaPolicyUrl, nsComment, nsCaRevocationUrl.*)

Version	Major and minor numbers of OID	Date	Comments
0.5	0.5	29 July 2008	**User and host/server certificate profiles agreed with Grid Certificate Profile v1.25 (GFD-C.125, CAOPS-WG):** **7.1.2** The following extensions are removed from **user** and **host/server** certificates: *nsCertType*, *nsBaseUrl*, *naCaPolicyUrl*, *nsComment*, *nsCaRevocationUrl*, *subjectKeyIdentifier*, *authorityKeyIdentifier*, *issuerAltName* The following extension is added to **user** certificate: extendedKeyUsage: **clientAuth** The following extension is added to **host/server** certificate: extendedKeyUsage: **clientAuth**, **serverAuth** The following values are removed from *keyUsage* extension in **user** and **host/server** certificates: *nonRepudiation*, *keyAgreement* **9** Reference to Grid Certificate Profile version 1.25 is added
0.6	0.6	07 October 2008	**The following sections are updated:** Added ***emailProtection*** bit to *extendedKeyUsage* extension of user certificates for e-mail signing.

Version	Major and minor numbers of OID	Date	Comments
0.7	0.7	12 June 2009	**The following sections are updated:** **1.2** ***The OID of the document is changed to*** 1.3.6.1.4.1.17306.8.1.0.7 **2.6.1** ***Bullet 1 is changed for:*** • The ArmeSFo CA root certificate – http://www.escience.am/ca/cacert/; PEM-formatted root certificate is moved to /ca/cacert web directory and DER-formatted root certificate is added ***Bullet 2 (URL of ldap server) is removed****. The LDAP server is no longer maintained.* ***The text for CP/CPS publication is changed*** to indicate that ArmeSFo CA publishes copies all versions of CP/CPS document **2.6.4** The URL of the ldap server is removed (the server is no longer maintained) **7.2.1** Following IETF PKIX recommendations (RFC 5280) - ArmeSFo CA issues now the CRLs version 2. **7.2.2** Two CRL extensions, *cRLNumber* and *authorityKeyIdentifier, are set*
0.8	0.8	29 December 2012	**The following sections are updated:** **1.2** **The OID of the document is changed to** 1.3.6.1.4.1.17306.8.1.0.8 **6.3.2** **The first sentence is replaced by** The ArmeSFo CA root certificate has a validity of no more than twenty years.