Armenian e-Science Foundation

ArmeSFo CA

Certificate Policy and Certification Practice Statement

Version 1.0
11 April 2016

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. Among the objectives of ArmeSFo are the deployment of the Grid infrastuctures in Armenia and promotion of the involvement of national specialists in the international Virtual Organizations.
ArmeSFo CA is maintained by ArmeSFo as a courtesy service to national academic community.
This document is structured according to the memo "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", RFC 2527 [1]. It describes the set of rules and operational practices used by ArmeSFo CA.
Throughout this document, the words 'must', 'must not', 'required', 'shall', 'shall not', 'should', 'should not', 'recommended', 'may', may not', 'optional' are to be interpreted as in RFC 2119 [2].

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).

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.

CA - Certification Authority

An authority trusted by one or more subscribers to create and assign certificates.

Certificate (Entity certificate)

A data structure, containing the public key and identity information of an entity digitally signed with the private key of the CA.

CP - Certificate Policy

A set of rules that indicates the applicability of a certificate to a particular community and/or class of applications with common security requirements.

CPS - Certification Practice Statement

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

CRL - Certificate Revocation List

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

CR - Certificate request

A request for a digital certificate made by requestor. CR consists of an e-mail message, request file, documents and data required for the authentication of the requestor.

CRR - Certificate revocation request

A request for revocation of a certificate made by subscriber, RA, CA or anyone else.

'Host'

Common denotation/naming for server, host and service.

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.

Policy qualifier

Policy-dependent information that may accompany the CP identifier in an X.509 certificate.

RA - Registration Authority

An entity that is responsible for identification and authentication of certificate or certificate revocation requestors and verification of their requests. The RA does not issue certificates.

Re-keying

Re-keying refers to a process of generation by a subscriber of a new key pair, request of a new personal certificate before expiration of the current certificate and issuance of the new certificate. The re-keying procedure requires the identity data in the subscriber's new certificate to be the same as those in the current one.

Relying party

A recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate.

Repository

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

Requestor

A person who is requesting from CA a certificate or revocation of a certificate issued by CA.

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 12 characters long and it 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 characters outside this range.

Subscriber

A person to whom a digital certificate is issued.

1.2 Identification

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

Version: **1.0**

Date: 11 **April 2016**

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

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

1.3.6.1.4.1.17306.8.1.1.0

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
1	Major version
0	Minor version

1.3 Community and Applicability

1.3.1 Certification authorities

ArmeSFo Certification Authority is a root certification authority. It does not have subordinate CAs.

1.3.2 Registration authorities

Registration authorities are established in Armenian organizations by the ArmeSFo CA as required, in order to support the growth of the demand for certificates. RAs are created on the base of official agreements between organizations and ArmeSFo.
A Registration Authority consists of an RA manager and one or more RA operators. The RA manager is appointed within the organization where (s)he is employed, and is in turn responsible for appointing RA operators. RA manager ensures that the RA personnel operate in accordance with the procedures defined by this CP/CPS. RA does not issue certificates. ArmeSFo CA may also perform the role of RA.
In case of substantial violations by RA personnel of their obligations and security requirements, the ArmeSFo CA may decide to suspend or terminate the RA operation.

1.3.3 End entities

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

1.3.4 Applicability

The issued certificates can be used for:
- e-mail signing and encryption (S/MIME);
- 'host' authentication (SSL/TLS, GSI);
- client authentication (SSL/TSL, GSI);

- generation of proxy certificates, as specified in RFC3820 [3].

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

1.4 Contact Details

1.4.1 Specification administration organization

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

Armenian e-Science Foundation
49 Komitas Avenue
0051 Yerevan Armenia

Phone: (+37410) 230510
Fax: (+37410) 230510
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
Narine Manukyan
Mariam Pilikyan
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 validated requests from authenticated entities;
- Notify the subscriber of certificate issuance;
- Accept revocation requests from authenticated entities;
- Issue CRLs;
- Publish the issued CRLs;
- Follow the policies and procedures described in this document.

2.1.2 RA obligations

The Registration authority (RA) of ArmeSFo CA is entitled by ArmeSFo CA to the authentication of the certificate and certificate revocation requestors and validation of their requests in accordance with all provisions specified in this CP/CPS. To this end, the RA must agree to follow this CP/CPS and all operational procedure derived therefrom.

The personnel (manager and operators) of RA:

- Must have necessary background of the fundamentals of PKI and knowledge of management with CRs, certificates and CRRs;
- Must be familiar with ArmeSFo CA policy and practice defined in this CP/CPS and all the relevant documentation published on the ArmeSFo CA web pages;
- Must have valid ArmeSFo CA personal certificate;

- Must digitally sign (by the private key associated with her/his personal certificate issued by ArmeSFo CA) all electronic messages communicated to ArmeSFo CA personnel, requestors and subscribers.

The RA must authenticate the requestors and check the validity of their CRs and CRRs

For personal (user) CR, the RA:

- Must check that the requestor has presented all documents and data listed in Section 3.1.9 of this CP/CPS and decide if the requestor has the right to have an ArmeSFo CA certificate;
- Must verify that the subject distinguished name (DN) of the CR is constructed according to the rules defined in Section 3.1.1 of this CP/CPS and reflects correctly the affiliation and common name (CN) of the requestor;
- Must verify the uniqueness of the subject DN by checking the archived documents and certificates. If it is not unique, the RA does not reject the CR, but notifies the CA about duplication of the subject DN, when sending the approved CR;
- Must instruct the requestor on the proper care and protection of the private key associated with the request.

In case of receiving CR within the re-keying procedure (see Section 3.2), the RA

- Must check that the requestor possesses valid ArmeSFo CA personal certificate;
- Must check that the subject DN and e-mail address of the CR coincide with those of the personal certificate of requestor;
- Must re-verify the subscriber data and affiliation, the right of the requestor to a certificate;
- Must check that the last authentication of the requestor (according to the procedures in Section 3.1.9) was done not more than 4 years ago.

For 'host' (host, server or service) CR, the RA:

- Must check that the requestor possesses valid ArmeSFo CA personal certificate;
- Must check that the requestor is the main or alternate administrator of the 'host', whose Fully Qualified Domain Name (FQDN) is contained in the subject DN of the CR;
- Must verify that the subject DN of the 'host' CR is constructed according to the rules defined in the Section 3.1.1 of this CP/CPS;
- Must verify the uniqueness of the subject DN by checking the archived documents and CRs. If it is not unique, the RA does not reject the CR, but notifies the CA about duplication of the subject DN, when sending the approved CR.

The approved CRs must be sent to ArmeSFo CA. The CRs must be enclosed in the message body and the message should also contain the work e-mail address and phone number of the requestor.

Procedure of authentication and sending approved CRs to ArmeSFo CA must last not more than five working days.

In case of CR rejection, the RA personnel must send to the requestor a message explaining the reasons of rejection.

Certificate revocation requests

The RA receives, checks the CRRs and sends the validated CRRs to ArmeSFo CA.

- In case of receiving from a subscriber a request for revocation of her/his personal certificate, the RA must authenticate the subscriber at a face-to-face meeting using: 1) The (archived) documents and data which had been presented by subscriber at the last of the preceding authentication meetings and 2) The passport to be presented by subscriber.

- In case of receiving a CRR from any other person the RA must authenticate the requestor following the procedure described in Section 3.1 and validate the revocation request.

The RA must process the CRR and send the validated CRR to ArmeSFo CA within one working day.

The RA must archive:

- Documents and data presented by requestors;
- CRs and corresponding issued certificates;
- CRRs;
- Correspondence with ArmeSFo CA and its personnel;
- Correspondence with subscribers and requestors.

The RA archive is considered as a part of the ArmeSFo CA archive and must be given (or sent) to ArmeSFo CA personnel upon their request. Before giving or sending archived documents the RA must make and keep their copies.

RA personnel must agree with all audits requested by the ArmeSFo CA personnel and must assist in these audits.

2.1.3 Subscriber obligations

Subscriber must:

- Read and adhere to the policy and procedures outlined in this document;
- Generate key pair using trustworthy methods;
- Take reasonable precautions to prevent a loss or disclosure of the private key associated with the certificate;
- Use a strong pass-phrase (Section 1.1.1) to protect the private key of the personal certificate. Keys used by hosts, servers, and services may be stored in an unencrypted form, in which case the private key should be accessible only by relevant applications, services or systems and should be protected by appropriate operating system file permissions;
- Send immediately e-mail to CA with request for the personal certificate revocation in case the associated private key is disclosed or suspected to be disclosed
- Contact immediately RA (by e-mail or any other communication way) in case of her/his private key loss, corruption. Present her/his passport at the authentication meeting, which will be appointed by RA;
- Send e-mail to CA with CRR in case when the certificate is no longer needed or the personal information in the certificate has become wrong or inaccurate;
- The administrator of ‘host’ must send e-mail to CA for revocation of the ‘host’ certificate in the following cases: 1) The ‘host’ private key is lost, corrupted, disclosed (or suspected to be disclosed) or compromised in other way; 2) Certificate is no longer needed or the ‘host’ information in the corresponding certificate has become wrong or inaccurate.

All e-mails sent to CA by must be digitally signed by subscriber’s private key.

In case subscriber requests the personal certificate re-keying (see Section 3.2) (s)he must send CR not sooner than 30 days before and not later than 10 days before expiration of the current certificate.

In case administrator requests new certificate for the ‘host’ (s)he must send CR not sooner than 30 days before and not later than 10 days before expiration of the current ‘host’ certificate.

Each time subscriber (administrator) creates a request for personal (‘host’) certificate, (s)he must generate a new key pair. The reuse of old private key for generation of a new CR is not allowed.

2.1.4 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.

2.1.5 Repository obligations

- The ArmeSFo CA will keep web site at http://www.escience.am/ca/;
- The ArmeSFo CA will publish on its web site a copy of this document;
- The ArmeSFo CA will publish on its web site the ArmeSFo CA public key certificate;
- The ArmeSFo CA will publish CRL with URI http://armesfoca-crl.scc.kit.edu/crl.pem;
- The ArmeSFo CA will publish on its web site the list of RAs and their contact details
- The ArmeSFo CA will publish on its web site guidelines, instructions and other necessary documentation

2.2 Liability

- 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 from the use 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

If any part or any provision of this document shall to any extent prove invalid or unenforceable in laws of Republic of Armenia, such part or provision shall be deemed to be omitted from this document. The omitted part or provision shall be replaced with a valid, legal and enforceable part or provision, which have an effect as close as possible to the part or provision being replaced. The remainder of this document shall remain valid and enforceable to the fullest extent permissible by laws of Republic of Armenia.
In the event that the ArmeSFo CA ceases operation, it will apply all reasonable efforts to notify on such termination all its subscribers, RAs, cross-certifying CAs and any other relying parties known to 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 President of 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.scc.kit.edu/crl.pem;
- All versions of ArmeSFo CA CP/CPS document – http://www.escience.am/ca/policy/;
- The list of its RAs – http://www.escience.am/ca/ras/;
- Other information.

2.6.2 Frequency of publication

- The ArmeSFo CA root certificates will be published as soon as issued;
- The CRL's will be published as soon as issued;
- 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 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/;
- The URI of ArmeSFo CA CRL is http://armesfoca-crl.scc.kit.edu/crl.pem;

2.7 Compliance Audit

A self-assessment will be done at least once per year by the ArmeSFo CA to verify that its operation complies with 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 ArmeSFo CA and its RAs collect the following information that is considered confidential:
- The photocopy of the requestor's passport;
- The official document proving the relation of the requestor with the organization;
- The requestor's phone number.

2.8.2 Types of information not considered confidential

The following collected information is not considered confidential:
- The requestor's full name;
- The requestor's work e-mail address;
- The requestor's organization and organizational unit names;
- The requestor's CR file.
- Statistics regarding certificates issuance and revocation.

Under no circumstances will the ArmeSFo CA have access to the private key of any entity to whom it issues a certificate.

2.8.3 Disclosure of certificate revocation/suspension information

No details about the revocation are currently disclosed in a public repository. Subscribers (administrators) may be notified about the reason for revocation of personal ('host') certificate. Qualified relying parties may inquire about the reason for revocation, and will be notified of such reason. See also Section 2.8.4

2.8.4 Release to law enforcement officials

The law enforcement officials will be allowed to inspect, upon their request and exhibition of regular warrant, the information collected by the ArmeSFo CA.

2.8.5 Release as part of civil discovery

In case of civil discovery, personal information will not be released.

2.8.6 Disclosure upon owner's request

Personal information requested by a subscriber in an authenticated request and upon presentation of proper proof of identity will be disclosed to the subscriber at a face-to-face meeting with CA or RA personnel.

2.8.7 Other information release circumstances

An auditor doing a formal compliance audit may have access to confidential data collected by ArmeSFo CA. The auditor will not have access to cryptographic keys that are part of the CA infrastructure. Any auditor will be required in writing to agree keeping all confidential data secret and not to publish them in any reports.
There are no other circumstances for the release of confidential information.

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:

- RFCs 2527 [1], 2119 [2], 3820 [3] and 3280 [4];
- Guidelines and Authentication Profiles of EUGridPMA [5];
- Grid Certificate Profile of OGF [6];
- CPs and CPSs of: DutchGrid CA [7], UK e-Science CA [8], GridKa-CA [9] and RDIG CA [10].

3 Identification and Authentication

3.1 Initial Registration

3.1.1 Types of names

Name components vary depending on the type of certificate. Names are consistent with the name requirements specified in RFC3280 [4].
The ArmeSFo CA certificate subject name is an X.500 subject DN. Any DN under this CP/CPS starts with the following fixed component

C=AM, O=ArmeSFo

The variable part of subject DN begins with the name of the organization (O) the subject is officially related to. The next, optional, field is the organization unit name (OU), which specifies the subject's department/division of the organization. The last field of subject DN is the common name (CN) of the subject. The CN must be obtainable from the subject real name as stated in Section 3.1.2. For a person, the CN is the person's Full Name. For a server/host, the CN is the Fully Qualified Domain Name (FQDN) of the server. For a service, the CN has the form "service/FQDN of the server (host) where the service runs".
Following this, the subject DN 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 (hosts)

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

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

For services

C=AM, O=ArmeSFo, O=*organizationName*, OU=*organizationUnitName*, CN=*serviceName/server(host) 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 CN, in the organization name and in the organization unit name must be meaningful. The names must be related with the subject organization and with the subject real name.
- For a person, the CN must be obtainable from the legal person name as presented in her/his passport.
- For servers and 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 subject DN for each certificate must be unique. It will never be assigned to more than one entity. To ensure the uniqueness of each subject DN, ArmeSFo CA can add letters, digits and other allowed ASCII characters to the CN part of the subject DN.

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

ArmeSFo CA and its RAs verify the identity of organizations by checking that:
- the organization is involved in the activities mentioned in Section 1.3.3;
- the organization is operating in Armenia (by verifying the organization official contact information).

The relation between the requestor and the organization mentioned in the subject DN of the CR must be proved by the document signed and stamped 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

All entities are authenticated and corresponding CRs are validated by RAs of ArmeSFo CA.

The authentication procedure is different for persons and ‘hosts’.

Authentication of persons

The authentication of a requestor and validation of her/his CR is performed by RA at a face-to-face meeting with the requestor.

The following documents and data have to be presented by the requestor:

- Passport;
- Copy of passport;

- Official document proving the relation of requestor with the organization specified in the subject DN of the CR. The document has to be signed and stamped by an official representative of the organization (the document is not needed in case of CRR);
- The work e-mail address;
- The phone number.

Authentication of 'hosts'

The CRs must be sent by 'host' administrator by e-mail to RA. The e-mail must be signed with the private key associated with the valid ArmeSFo CA personal certificate of the sender. The CR must be enclosed in the message body.

Consequently, the RA validates the CR following the procedure described in Section 2.1.2.

3.2 Routine Re-key

Re-keying is allowed to subscribers of ArmeSFo CA before the expiration of their current personal certificate. Subscribers must generate a new key pair and send the CR to RA via e-mail, signed by the private key associated with the current valid certificate.

The subject DN and e-mail address in the CR must be the same as those in the current valid certificate. The re-keying is allowed provided the last authentication of the requestor according to the procedures in Section 3.1.9 was done not more than 4 years ago.

The personal certificate re-keying request must be sent not sooner than 30 days before and not later than 10 days before expiration of the current certificate.

The re-keying process does not require the identity verification of the subscriber. However the RA will perform checks described in Section 2.1.2 for certificate re-keying.

3.3 Re-key After Revocation

There is no re-keying after revocation. A new certificate request should be submitted following the procedure specified in section 3.1.

3.4 Revocation Request

Anyone can submit CRR to ArmeSFo CA. However, any CRR requestor must be authenticated and her/his CRRs must be validated, unless the ArmeSFo CA can independently verify that security requirements to the key protection have been violated.

ArmeSFo CA accepts the following authentication and validation procedure for CRRs:

In case of the personal certificate revocation requested by subscriber:

- If the subscriber has access to the key associated with her/his certificate, (s)he must send to ArmeSFo CA an e-mail with CRR, signed with the private key associated to the certificate requested to revoke;
- If the private key is lost or corrupted, (s)he must send CRR to RA by e-mail or by any other way. The RA appoints a face-to-face meeting with subscriber. The subscriber presents at the meeting her/his passport.

In case of the 'host' certificate revocation requested by administrator: By e-mail to ArmeSFo CA signed with the personal private key of the 'host' administrator;

In all other cases: The CRR must be submitted to RA by e-mail or any other method and the authentication of the revocation requestor and validation of her/his CRR must be done as per Section 3.1.9.

4 Operational Requirements

4.1 Certificate Application

- The requestor must generate her/his own key pair as per Section 6;
- The requestor must register with the ArmeSFo CA as per Section 3.1;
- The subject DN must be as per Section 3.1;

- The minimum key length for all the requested certificates must be 1024 bits;
- The maximum validity time for each certificate is one year.

On initial application, and subsequently every 5 years the requestor of a personal certificate must pass authentication procedure at a face-to face meeting with RA (as per Section 3.1). In case the entity is 'host', the corresponding administrator will be authenticated based on the requirements detailed in Section 3.1.

In case a re-keying is requested, the CR must be submitted to RA by electronic mail following the procedure described in Section 3.2.

The RA, after authenticating the requestor identity and validating her/his request, sends the CR to CA.

ArmeSFo CA will reject all non-legitimate CRs; in the case of rejection the requestor will be notified by electronic mail. Obviously nonsensical requests will be discarded without notification.

4.2 Certificate Issuance

- The ArmeSFo CA issues the certificate if, and only if, the authentication of the entity, for whom the certificate is requested and verification of the CR were successful;
- The request for certification is normally handled within five working days after receipt of validated CR from RA;
- The requestor will be notified by e-mail about the certificate issuance or rejection. In 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 disclosed, lost, corrupted or misused;
- The entity data as represented in the certificate have changed (name changed, machine decommissioned, organization dissolved or no longer eligible under the criteria detailed in section 1.3.3);
- The subscriber is known to have violated his obligations with regard to the ArmeSFo CA;
- The subscriber of the certificate has ceased his relation with organization;
- At subscriber's request;
- At administrator's request (for revocation of the 'host' certificate).

4.4.2 Who can request revocation

The revocation of a certificate can be requested by:
- Subscribers;
- Administrators of certified 'hosts';
- The RA which performed the validation of the request for the certificate;
- The ArmeSFo CA;
- Any other entity presenting proof of knowledge of the private key disclosure, loss, misuse, or of the modification of the data recorded in the certificate.

4.4.3 Procedure for revocation request

The ArmeSFo CA will handle request for revocation that reaches it by any means, authenticated or unauthenticated. A CRR will be accepted if:
- The ArmeSFo CA can independently verify that the private key has been lost, corrupted, disclosed or misused;

- It is signed with the private key associated to the certificate whose revocation is requested;
- It is signed with the private key associated with the certificate of the administrator of the 'host' whose certificate revocation is requested;
- It is signed by the RA who originally approved the CR.

Any other CRR will be accepted only if the entity requesting the revocation is authenticated as described in Section 3.4

4.4.4 Revocation request grace period

If a subscriber or administrator of the certified 'hosts' discovers that his/her or 'host' private key is lost, corrupted or disclosed, (s)he should request revocation immediately as per Sections 2.1.3 and 3.4.

The RA should authenticate the revocation requestor, validate her/his CRR and send CRR to ArmeSFo CA within one working day.

The ArmeSFo CA will process the validated CRRs within one working day.

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 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 event recorded

The ArmeSFo CA records the following events:
- CRs;
- Issued certificates;
- CRRs;
- Issued CRLs;
- CA machine boots/logins/logouts;
- All electronic messages sent to and by the ArmeSFo CA.

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.

4.5.4 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 event recorded

- CRs;
- Issued certificates;
- CRRs;
- 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 3 years.

4.6.3 Protection of archive

Archives are copied to an off-line medium 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 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

No stipulation.

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, cross-certifying CA's and any other relying parties;
- Terminate distribution services for certificates and CRLs issued using the compromised key;
- Generate a new CA key pair and new root certificate and make the certificate immediately available in the public repository;
- All entities certified with compromised key will be re-certified, following the procedure defined in Section 3.1.9;
- If the private key of an RA personnel member has been lost, corrupted, disclosed or misused, the ArmeSFo CA will investigate the circumstances. In case the event has affected the security, the ArmeSFo CA may terminate the RA operation and revoke all certificates issued by the request of the RA.

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 signing 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 all subscribers, RAs, cross-certifying CAs and all other known relying parties;
- Cease the issuance of certificates and CRLs;
- Destroy all copies of private keys;
- Make publicly available the information of its termination.

5 Physical, Procedural and Personnel Security Controls

5.1 Physical Controls

5.1.1 Site location and construction

No stipulation.

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 USB flash drives and CD/DVD disks.

5.1.7 Waste disposal

Waste carrying potentially confidential information is 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 maintenance of the CA requires suitably trained persons who are familiar with the fundamentals of PKI and who are technically and professionally competent. The actual personnel are recruited from specialists of Armenian e-Science Foundation.

5.3.2 Background check procedures

See Section 5.3.1.

5.3.3 Training requirements

No stipulation.

5.3.4 Retraining frequency and requirement

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 personnel on dedicated machine not connected to any kind of computing network. The requestors must generate their key pair themselves. The key pairs for 'hosts' must be generated by administrators.

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' CRs may be delivered to the ArmeSFo CA by signed e-mail, floppy disks, CD/DVD disks, USB flash drives, SSL protected web interface.

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 user, server, host and service certificates 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* and *extendedKeyUsage* extensions are 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

Private keys must not be escrowed.

6.2.4 Private key backup and archival

The ArmeSFo CA private key is kept encrypted in multiple copies in removable media kept 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 and private keys, the maximum usage 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

Only ArmeSFo CA personnel know the activation data for the ArmeSFo CA private key. The ArmeSFo CA private key and its activation data are kept in separate locations. The private keys of subscribers are protected by strong pass-phrases.

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 this CP/CPS**
- crlDistributionPoints: **URI:http://armesfoca-crl.scc.kit.edu/crl.pem**

The following extensions are set in the ArmeSFo CA 'host' certificates:

- basicConstraints: **critical**, **CA:FALSE**
- keyUsage: **critical**, **digitalSignature**, **keyEncipherment**, **dataEncipherment**
- extendedKeyUsage: **clientAuth**, **serverAuth**
- subjectAltName: ***'host''s Fully Qualified Domain Name***
- certificatePolicies: **The OID of this CP/CPS**
- crlDistributionPoints: **URI:http://armesfoca-crl.scc.kit.edu/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

Minor changes, e.g. editorial updates of the CP/CPS that do not affect security and policy, will be announced to the RAs and cross-certifying CAs through mailing lists, but no advance warning will be given. The CP/CPS with major changes will be sent to EUGridPMA for approval before publication.

Subscribers will not be warned in advance of changes to the ArmeSFo CA CP and CPS.

8.2 Publication and Notification Policies

All versions of ArmeSFo CA CP/CPS are available at http://www.escience.am/ca/policy/.

8.3 CPS Approval Procedures

No stipulation.

9 Bibliography

1. S. Chokani and W. Ford ***"Internet X.509 Infrastructure Certificate Policy and Certification Practices Framework"***, http://www.ietf.org/rfc/rfc2527.txt
2. S. Bradner, ***"Key words for use in RFCs to Indicate Requirement Levels"***, http://www.ietf.org/rfc/rfc2119.txt
3. S. Tuecke et al***.,"Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile"***, http://www.ietf.org/rfc/rfc3820.txt
4. R. Housley et al., ***"Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"***, http://www.ietf.org/rfc/rfc3280.txt
5. ***EUGridPMA Guidelines and Authentication Profiles,*** http://www.eugridpma.org/guidelines/classic/
6. David L. Groep et al., ***"Grid Certificate Profile"***, GFD-C.125, CAOPS-WG, http://www.ogf.org/documents/GFD.125.pdf
7. ***DutchGrid and NIKHEF Medium-security X.509 CA Certification Policy and Practice Statement,*** http://ca.dutchgrid.nl/medium/policy/
8. ***UK e-Science CA Certificate Policy and Certification Practices Statement,*** http://www.ngs.ac.uk/ukca/certificates/cpcps
9. ***GridKa-CA Certificate Policy and Certification Practice Statement,*** http://grid.fzk.de/ca/gridka-cps.pdf
10. ***RDIG CA Certificate Policy and Certification Practice Statement***, http://ca.grid.kiae.ru/RDIG/policy/

Appendix: Revision Logs

A.1 Version 0.1 (20 March 2004) Initial release

A.2 Version 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

A.3 Version 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

A.4 Version 0.4 (27 November 2007)

The following sections are updated:

1.1 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, sCaRevocationUrl.*

A.5 Version 0.5 (29 July 2008)

The following sections are updated:

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.

A.6 Version 0.6 (07 October 2008)

The following sections are updated:

Added *emailProtection* bit to *extendedKeyUsage* extension of user certificates for e-mail signing.

A.7 Version 0.7 (12 June 2009)

The following sections are updated:

2.1 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 (RFC5280), ArmeSFo CA issues now the CRLs version 2.

7.2.2 Two CRL extensions, *cRLNumber and authorityKeyIdentifier,* are set

A.8 Version 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'

A.9 Version 0.9 (28 June 2013)

The following sections are updated:

1.2 The OID of the document is changed to 1.3.6.1.4.1.17306.8.1.0.9
2.6.1 The URL of the latest CRL is changed to http://armesfoca-crl.scc.kit.edu/crl.pem
7.1.2 The URI of crlDistributionPoints is changed to http://armesfoca-crl.scc.kit.edu/crl.pem

A.10 Version 1.0 (11 April 2016)

The following sections are updated:

1.1 The Introductory paragraph is edited.
1.1.1 Some definitions are removed or modified. A few definitions are added*.*

1.2 The OID of the document is changed to: 1.3.6.1.4.1.17306.8.1.1.0

1.3.1 The text is edited.
1.3.2 The text is rewritten. Details are added.
1.3.3 The text is edited.
1.3.4 The applicability of certificates is specified in more detail.

1.4.1 The first sentence is rewritten as **'**The ArmeSFo CA is managed by the ArmeSFo'.
The postal code is changed to: 0051; The fax number is changed to: +(37410) 230510
1.4.2 The name of Arsen Harypatyan is removed the names of Narine Manukyan and Mariam Pilikyan are added.

2.1 Subsection 2.1.2 'RA obligations' is introduced. Correspondingly, the numbering of the next subsections of Section 2.1 is changed.
2.1.3 The subscriber obligations are specified in more detail.
2.1.5 More details are added.

2.2 The first bullet is removed.

2.4.2 The text is rewritten to specify the severability.
2.4.3 The text is changed for **'**All disputes related to the interpretation and enforcement of the conditions and rules described in this document will be resolved by the President of the ArmeSFo'.

2.6.1 Two bullets are added: 'The list of its RAs – http://www.escience.am/ca/ras/' and 'Other information'
2.6.2 Bullet 1 is replaced by 'The ArmeSFo CA root certificates will be published as soon as issued'; Bullet 2 is replaced by 'The CRL's will be published as soon as issued'.
2.6.3 The first bullet is removed.
2.6.4 A bullet 'The URI of ArmeSFo CA CRL is http://armesfoca-crl.scc.kit.edu/crl.pem' is added.

2.7 The first sentence is modified for 'A self-assessment will be done at least once per year by the ArmeSFo CA to verify that its operation complies with this CP/CPS'.

Sections 2.8.1 - 2.8.7 are rewritten.

2.9 The list of sources on which this CP/CPS is based is given.

Sections 3.1.1, 3.1.2, 3.1.4, 3.1.8 and 3.1.9 are rewritten.

3.2 Routine Re-key is specified

3.3 The text is replaced by 'There is no re-keying after revocation. A new certificate request should be submitted following the procedure specified in section 3.1'.

3.4 A detailed description of revocation request submission procedure is given.

4.1 The procedure of certificate application is described in more detail

4.2 More details on the certificate issuance procedure are given.

Sections 4.4.1 - 4.4.4 are rewritten.
4.4.6 Second bullet is removed.

4.5.1 A bullet is added 'All electronic messages sent to and by the ArmeSFo CA'.

4.6.1 The bullets are rearranged

4.6.3 The sentence is changed to 'Archives are copied to an off-line medium and stored in a safe place'.

4.7 The first sentence now reads as 'The ArmeSFo CA's private signing key is changed periodically; from that time on, only the new key will be used for signing purposes'.

4.8.2 Changed for 'No stipulation'.
4.8.3 The actions of ArmeSFo CA in case of entity key compromise are written in more detail.
4.8.4 The word 'signature' is replaced by 'signing'

4.9 The first bullet is replaced by 'Inform all subscribers, RAs, cross-certifying CAs and all other known relying parties'.

5.1.1 Is replaced by 'No stipulation'.
5.1.6 Bullet 2 is changed for 'Backup copies of the CA related information are kept in USB flash drives and CD/DVD disks'.
5.1.7 The text is edited.

5.3.1 Is replaced by 'The maintenance of the CA requires suitably trained persons who are familiar with the fundamentals of PKI and who are technically and professionally competent. The actual personnel are recruited from specialists of Armenian e-Science Foundation'.

6.1.1 Is changed for 'Keys for the ArmeSFo CA are generated by the ArmeSFo CA personnel on dedicated machine not connected to any kind of computing network. The requestors must generate their key pair themselves. The key pairs for 'hosts' must be generated by administrators'.
6.1.3 Is changed to 'The entities' CRs may be delivered to the ArmeSFo CA by signed e-mail, floppy disks, CD/DVD disks, USB flash drives, SSL protected web interface'.

6.1.5 The first bullet is changed to 'The minimum key length for user, server, host and service certificates is 1024 bits'.

6.1.9 Is modified to 'For certificates issued by the ArmeSFo CA under this policy, the *keyUsage* and *extendedKeyUsage* extensions are defined in Section 7.1.2'.

6.2.3 'No stipulation' is changed for 'Private keys must not be escrowed'.

6.2.4 Is replaced by 'The ArmeSFo CA private key is kept encrypted in multiple copies in removable media kept in secure places'.

6.4.2 Is modified to 'Only ArmeSFo CA personnel know the activation data for the ArmeSFo CA private key. The ArmeSFo CA private key and its activation data are kept in separate locations. The private keys of subscribers are protected by strong pass-phrases'

7.1.2 Editorial corrections:

- Sentence 'The OID of ArmeSFo CA CP/CPS' is replaced by 'The OID of this CP/CPS';
- Instead of terms server, host and service, their common denotation 'host' is used.

8.1 Specification Change Procedures are specified in more detail.

8.2 The following modification is made 'All versions of ArmeSFo CA CP/CPS are available at http://www.escience.am/ca/policy/

9 The list of references is substantially updated.