Armenian e-Science Foundation

Instructions for requesting personal, server/host or service certificates from Armenian e-Science Foundation Certification Authority (ArmeSFo CA)

1 Introduction

This document describes the steps, which have to be done in order to request personal, server, host or service certificates from ArmeSFo CA. It is based on the ArmeSFo CA Certificate Policy and Certification Practice Statement (CP/CPS) document available at *http://www.escience.am/ca/policy/*.

Before starting the process of application for ArmeSFo CA certificate, you have to read the ArmeSFo CA CP/CPS, understand its policy, requirements to the certificate requestors, obligations of the subscribers of the ArmeSFo CA certificates and agree to follow the CP/CPS and all operational procedures derived from this document.

2 Who can request ArmeSFo CA certificate?

ArmeSFo CA issues certificates to physical persons, servers, hosts and services. The entities that are eligible for certification by the ArmeSFo CA are all those entities related to the organisations 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-organisational sharing of resources.

3 Choose the subject distinguished name (DN) of the certificate

Requesters of the certificate have to determine the subject DN of the certificate before they apply for a certificate. You can write down the subject DN on the paper to use it when generating certificate request.

***The use of printable characters in the DN*:** The following characters are allowed:

- Upper and lower case letters: '**a**'-'**z**', '**A**'-'**Z**',
- Numbers: '**0**'-'**9**',
- Characters: '**(**', '**)**', '**+**', '**,**', '**-**', '**.**', '**:**', '**?**', ' ','***/***', that is, left and right parentheses, plus, comma, minus/hyphen, dot (period), colon, question mark, space and forward slash.
  Note: In order the forward slash to be interpreted by openssl as a standard visible character it must be prefixed by the backslash ('\').

The subject DN must have the following form:

*"**/C=AM/O=ArmeSFo**/O=organisationName/OU=organisationalUnitName/CN=common Name".*

You have to replace *organisationName and organisationalUnitName* and *commonName* with relevant to your organisation and organisational unit names.
The value of the *commonName* will correspond either to your full name (for personal certificate) or to the server/host name (for server/host certificate), or to the service name (for service certificate)

3.1 *organisationName*

Use the official acronym of your organisation/institution.

For example, if you are working in the Yerevan Physics Institute, choose *'**O**=YerPhI'*

If your organisation has no official acronym, choose its full official name.

For example, *'**O**= Some Institute'*

3.2 *organisationalUnitName*

Put the official acronym or the full name of your division/department/laboratory in the organisation

For example, *'**OU**=Experimental Division'*

3.3 *commonName*

The *commonName* value in ***CN*** field differs in the case of personal, server/host and service certificates.

3.3.1 *commonName* for personal certificates

Put your common name in the form <FirstName LastName>

For example: *'**CN**=Hakob Hakobyan'*

Please note, that your first and last names must be identical to those in your passport. Do not write ***CN**=Hakob Hakobian* if you have *Hakob Hakob**y**an* in your passport.

3.3.2 *commonName* for server/host certificates

The value of *commonName* for a server/host is its fully-qualified domain name (FQDN).

For example, *'**CN=aligrid1.yerphi.am**'*

3.3.3 *commonName* for service certificate

The value of *commonName* for a service is the service name separated by slash from fully-qualified domain name (FQDN) of the server/host where the service runs

For example, *'**CN**=ldap/aligrid1.yerphi.am'*

4 Generate certificate request (CR)

Below the commands for generating key pair and CR for the user using OpenSSL software are given. OpenSSL software is included in modern UNIX-like OS distributions. Refer to http://www.openssl.org/related/binaries.html page if you are user of MS Windows OS, to get information about downloading and installation of OpenSSL under MS Windows. The example below assumes that you are using Unix-like OS. '***$***' represents the shell prompt (it should not be typed!).

If you are planning to have certificate for working in Grid, you have to generate your key pair and CR in the *~/.globus* directory:

$ *mkdir ~/.globus*
$ *cd ~/.globus*

If you are not planning to work in Grid, we advise you to generate your key pair and CR in the *~/.private* directory:

$ *mkdir ~/.private*
$ *cd ~/.private*

Generate a 1024-bit RSA key pair and CR. The private key will be stored in the file *userkey.pem*, while the request will be stored in the file *userreq.pem*. You will be asked for password – choose one with at least 12 characters long (see ArmeSFo CA CP/CPS, Section 1.1.1, Strong pass-phrase).

$ *openssl req -sha512 -newkey rsa:1024 -keyout userkey.pem -out userreq.pem -subj <SUBJECT>*

Note: This command should be typed as one line and you have to replace <SUBJECT> with actual subject DN string as described in the previous section.

Examples of subject DN strings:

for personal certificate: **"/C=AM/O=ArmeSFo/O=YerPhI/OU=Experimental Division/CN=Hakob Hakobyan"**

for server/host certificate: **"/C=AM/O=ArmeSFo/O=YerPhI/OU=Experimental Division/CN=aligrid1.yerphi.am"**

for service certificate: **"/C=AM/O=ArmeSFo/O=YerPhI/OU= Experimental Division/CN=ldap\/aligrid1.yerphi.am"**

Change the permissions of your private key file:

$ *chmod 400 userkey.pem*

5. Verify the subject DN of your CR:

$ *openssl req -in userreq.pem -subject –noout*

6. Your steps after generation of CR:

6.1 Read the 'Minimum Security Requirements of ArmeSFo CA' (*http://www.escience.am/ca/certreqs/index.html*)

6.2 If you are requesting <u>user certificate</u>, then

6.2.1 Copy the *userreq.pem* file to the USB flash or CD/DVD, or floppy disk.

6.2.2 Prepare following documents and data:

- Your passport,
- Copy of your passport,
- Official document from your organisation proving your relations with the organisation, signed and stamped by an official representative of the organisation. See Appendix for an example of such document.
- Your work e-mail address and personal phone number

Note: ArmeSFo CA does not accept the e-mail addresses at social mail servers like ***yahoo.com, gmail.com, mail.ru***, ***list.ru, rambler.ru, etc***. The CRs sent from these addresses will be rejected.

6.2.3 Send message to Registration Authority of ArmeSFo CA in ArmeSFo using the following e-mail address:

ra_armesfo_ca@escience.am

The subject of your message should be:

User certificate request from <put your full name>

The body of your message should be:

Dear RA,

I have read the ArmeSFo CA CP/CPS and 'Minimum Security Requirements of ArmeSFo CA' to subscribers and agree to follow these documents. I would like to meet with the personnel of ArmeSFo RA in order to present my CR and requested documents.

<put your full name>

The RA will appoint a face-to-face authentication meeting with you, where you will present the requested data, documents and CR.

6.3 If you are requesting server/host or service certificates (you can do that only if you have a valid ArmeSFo CA user certificate and you are the system administrator of the server/host), then your steps are as follows:

6.3.1 Using your private key and certificate, you have to generate the user certificate in pkcs#12 format, which is used for signing the message.

Create the pkcs#12-format certificate with the following command:

$ *openssl pkcs12 -export -in usercert.pem -inkey userkey.pem -out usercert.p12*

You will be asked for two passwords: the password of the private key, which was set when generating the key pair and the password for creating pkcs#12 file (asked twice)

6.3.2 Install a mail agent that handles with the certificates in pkcs#12 format (we recommend the Open Source mail agent Thunderbird available for both Windows and Linux platforms *http://www.mozilla.com/en-US/thunderbird/*) and import to the agent *usercert.p12* and ArmeSFo CA root certificate *(*from *http://www.escience.am/ca/).*

6.3.3 Send **digitally signed message** to **ra_armesfo_ca@escience.am**

The subject of your message should be: (***Host, Server, Service) certificate request for <put the CN of the (host, server, service)>.***

The message must contain short description of the purpose of the use of the (host, server, service) certificate.
The message must also contain the statement that you are the administrator of the host/server.

Note: The content of certificate request file has to be included in the body of the message.

7 Certificate delivery to subscribers

The accepted CRs will be sent to ArmeSFo CA for the certificate issuance. As soon as the certificate is issued, it will be sent to you by ArmeSFo CA via digitally signed e-mail.

Appendix: Example of official employment statement.

ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅՈՒՆ
ԱՌԵՎՏՐԻ ԵՎ ՏՆՏԵՍԱԿԱՆ ԶԱՐԳԱՑՄԱՆ
ՆԱԽԱՐԱՐՈՒԹՅՈՒՆ
Ա.Ի. ԱԼԻԽԱՆՅԱՆԻ անվան
ԵՐԵՎԱՆԻ ՖԻԶԻԿԱՅԻ ԻՆՍՏԻՏՈՒՏ
ՊԵՏԱԿԱՆ ՈՉ ԱՌԵՎՏՐԱՅԻՆ
ԿԱԶՄԱԿԵՐՊՈՒԹՅՈՒՆ

REPUBLIC OF ARMENIA
MINISTRY OF TRADE AND
ECONOMICAL DEVELOPMENT
YEREVAN PHYSICS INSTITUTE
After A.I. ALIKHANIAN
STATE NON COMMERCIAL
ORGANIZATION

«04» 10 2007 № 02-186

To Whom It May Concern:

This is to certify that Mr. Arsen Hayrapetyan is working in the Laboratory #143 of Yerevan Physics Institute after A.I.Alikhanian as Junior Researcher.

L.S. Mikaelyan
The Assistant of the Director for the [illegible]

375036 Երևան, Ալիխանյան եղբայրների 2
Հեռ. (37410) 341 500, Ֆաքս. (37410) 398 392

2 Brothers Alikhanyan street., Yerevan 375036
Phone: (37410) 341 500, Fax: (37410) 398 392