



Armenian e-Science Foundation

Only for users from National Academy of Sciences of the Republic of Armenia!

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 latest version of ArmeSfo CA Certificate Policy and Certification Practice Statement (CP/CPS) document available at <http://www.escience.am/ca/policy>.

Before applying for the certificate please read carefully Section 2.1.2 “Subscriber obligations” of ArmeSfo CA CP/CPS.

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 Choosing 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 DN on the paper to use it when generating certificate signing 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 DN must have the following form:

"/C=AM/O=ArmeSFo/O=organisationName/OU=organisationalUnitName/CN=commonName".

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 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 Byurakan Astrophysical Observatory, choose 'O=BAO NAS RA'

3.2 organisationalUnitName

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

For example, 'OU=Department of Galaxies'.

3.3 commonName

The *commonName* value in **CN** field differs in the case of personal, host or 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 Hakobyan* in your passport.

3.3.2 commonName for host certificates

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

For example, *'CN=gridhost.bao.am'*

3.3.3 commonName for service certificates

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/gridhost.bao.am'*

4 Generating certificate signing request (CSR)

Below the commands for generating key pair and certificate signing request (CSR) 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.

- Create a private directory to store your key pair:

```
$> mkdir .private
```

```
$> cd .private
```

Generate a 1024-bit RSA key pair and certificate request. 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 16 characters long (see ArmeSFo CA CP/CPS, Section 1.1.1, Strong pass-phrase).

```
$> openssl req -sha1 -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.

Note: If you want the slash to be interpreted by *openssl* as a standard visible character in the values of the DN fields, it should be prefixed by the backslash ('\').

Examples of subject DN strings:

for personal certificate: **"/C=AM/O=ArmeSFo/O=BAO NAS RA/OU=Department of Galaxies/CN=Hakob Hakobyan"**

for host certificate: **"/C=AM/O=ArmeSFo/O=BAO NAS RA/OU=Department of Galaxies/CN=gridhost.bao.am"**

for service certificate: **"/C=AM/O=ArmeSFo/O=BAO NAS RA/OU= Department of Galaxies/CN=ldapVgridhost.bao.am"**

- Change the permissions of the private key file:

```
$> chmod 400 userkey.pem
```
- Verify the subject DN of the requested certificate:

```
$> openssl req -in userreq.pem -subject -noout
```
- Copy the *userreq.pem* file to the floppy disk or CD or USB flash.

Note: Under no circumstances will the ArmeSFo CA have access to the private keys of any subscriber to whom it issues a certificate. (ArmeSFo CA CP/CPS, Section 2.8.2) The ArmeSFo CA does not generate private keys for entities and hence does not deliver private keys. (ArmeSFo CA CP/CPS, Section 6.1.2)

5. Your steps after generation of CSR:

5.1 If you are requesting user certificate, then

5.1.1 Prepare following documents and copies:

- Your passport
- Copy of your passport
- Official document from your Organisation stating that you are its employee, signed by an official representative of the Organisation and stamped by the seal of the Organisation. An example is given in Appendix

5.1.2 Send a message to Registration Authority of ArmeSFo CA in NAS RA using the following e-mail address: ra_nas_ra_ca@escience.am

The message should state that

- you have read the *ArmeSFo CA CP/CPS* and *Instructions for requesting personal, server/host or service certificates from Armenian e-Science Foundation Certification Authority (ArmeSFo CA)*
- you agree to follow the requirements to the users stated in these documents and
- you would like to meet with the personnel of Registration Authority of ArmeSFo CA in NAS RA in order to present your CSR and requested documents.

5.2 If you are requesting 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:

5.2.1 Using your private key and certificate, you have to generate the user certificate in pkcs#12 format, which is used for signing the message. Provided you have your private key in *MyPrivkey.pem* file and your certificate in *MyCert.pem* file, you can create the pkcs#12-format certificate with the following command:

```
$> openssl pkcs12 -export -in MyCert.pem -inkey MyPrivkey.pem -out MyFile.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)

5.2.2 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 *MyFile.p12* and ArmeSFo CA root (from <http://www.escience.am/ca/>) certificates.

5.2.3 Send signed message to ra_nas_ra_ca@escience.am

The message must contain short description of the purpose of the use of the host or service certificate.

In the case of requesting host certificate, the message must also contain the statement that you are the administrator of the host.

In the case of requesting service certificate, the message must also contain the additional statement that you are the administrator of the host on which the service is running.

Important note! The content of the host or service certificate request file has to be included in the body of the message.

6 Certificate delivery to subscribers

As soon as the certificate is issued, it will be sent to the subscriber by ArmeSFo CA in digitally signed e-mail.

Appendix: Example of official employment statement.

