Effective as from 28 April 2016

Armenian e-Science Foundation

Obligations of Registration Authorities of ArmeSFo CA

This document defines the requirements which must be fulfilled by RAs of ArmeSFo CA. The document is subject to modifications. The RAs are requested to follow the latest version of the document published on http://www.escience.am/ca/ras/ Registration Authority (RA) personnel (Manager and Operator(s)) authenticate certificate signing requests (CRs), approve or reject them, and send the approved requests to ArmeSFo CA for signing them.

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 in the CP/CPS), 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 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 the 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 3.1in the CP/CPS 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.