Effective as from 29 April 2016

Armenian e-Science Foundation

Instructions on Certificate Revocation Request (CRR)

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 user:

- 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:

Send an e-mail to ArmeSFo CA signed with the personal private key of the 'host' administrator;

Below is the example of CRR for the user in case of lost or corrupted private key.

Send message to Registration Authority who has performed your authentication
The subject of your message should be: Certificate revocation request from <your full name>
The body of your message should be:
Dear RA,
<the reason of your revocation request>
<your full name>

Below is the example of CRR for server/host or service.

Send digitally signed message to Registration Authority of ArmeSFo CA.
The subject of your message should be: Certificate revocation request of <the CN of the host/server/service>
The body of your message should be:
Dear RA,
<the reason of your revocation request>
<your full name>