EE-RA Communications - General Guidance

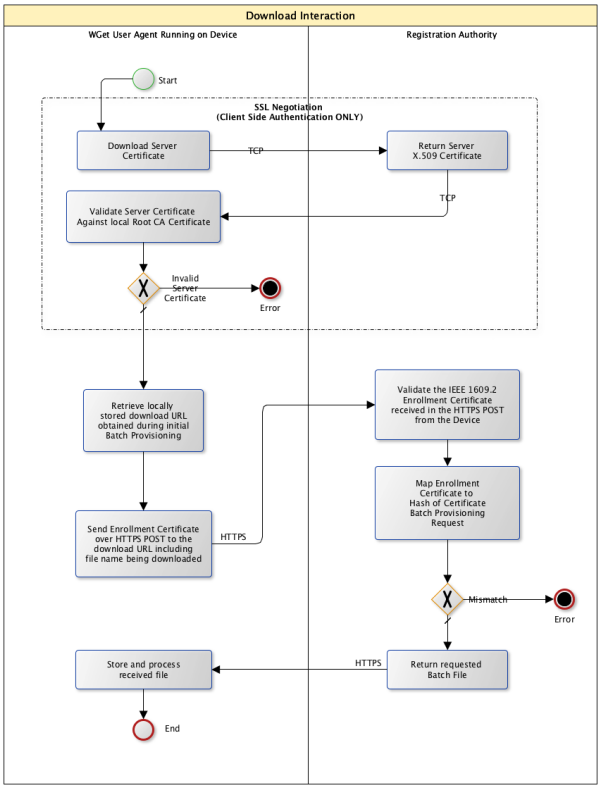
The following is provided as general guidance for EE-RA messaging. For specific messaging, refer to the RA - Services View.

EE initiates all communication between EE and RA. All communications between EE and RA fall into one of two categories: 1) (Non-)Authenticated Download Requests 2) SCMS Protocol Messages.

EE-RA Authentication and RA-EE Authentication

1. EE establishes a secure server-authenticated TLS connection with RA (RA authenticates to EE).
2. EE then digitally signs the current time of type IEEE 1609.2 Time32 with EE's enrollment certificate.
3. EE uses POST to include the IEEE 1609.2 enrollment certificate, the current time of type IEEE 1609.2 Time32, the digital signature over the current time, and the ASN.1 request. Note that this payload is TLS protected.
4. RA validates the enrollment certificate against the internal blacklist, and then verifies the enrollment certificate.
5. RA validates the time-stamp against a configurable time tolerance (default value is defined in SCMS-1203), and then digitally verifies the signature of the current time.
6. RA grants access to the file to download, if all verifications were successful. Otherwise, RA closes the connection.

A simplified version is displayed in the diagram below. Note that the diagram does not include the digitally signed time-stamp of Step 2 and the verification of Step 5.



EE-RA Download Interaction

RA Revocation

An X.509 root CA certificate that EEs install during bootstrapping issues RA's X.509 certificate. EE will perform the following check before Step 2 in above EE-RA mutual authentication:

- EE validates whether the X.509 root CA issued RA's X.509 certificate, and whether RA's X.509 certificate is valid.

In order to revoke an RA, the operator will modify the DNS entry for the RA (e.g. ra.ra-hoster.com) to point to the new RA (or RA's load-balancer/firewall, depending on RA's architecture). Attacks might be still possible; an attacker can compromise the RA X.509 certificate, implement DNS spoofing, and compromise the LOP. However, the adversary's gain is limited to learning enrollment certificates. Therefore, the RA may or may not support a revocation mechanism for RA's TLS certificate (e.g. the certificate status request extension, colloquially known as OCSP stapling and specified in RFC 6066, Section 8). The EE (both OBE and RSE) may or may not support the TLS revocation mechanism.

Download Request

Download requests are used by the EE to download a file from the RA.

The EE uses HTTP GET to make download requests. There are two different kind of download requests: authenticated and non-authenticated:

- In order to provide IEEE 1609.2 based authentication from EE to RA for authenticated download requests an APDU named SignedAuthenticatedDownloadRequest is included in the request. The filename of the file EE is attempting to download and the current time timestamp is included in the SignedAuthenticatedDownloadRequest. The EE uses its enrollment certificate's signing key to create the signature in the SignedAuthenticatedDownloadRequest. A HTTP header with Base64 encoded ASN.1 serialized SignedAuthenticatedDownloadRequest APDU is included in the HTTP GET message.
- Non-authenticated download are plain HTTP GET messages with an optional HTTP Header 'If-None-Match' to identify the version of an already downloaded file.

The HTTP GET Range option may be used to request a partial download for the purposes of resuming a previously interrupted download.

SCMS Protocol Messages

SCMS protocol messages are used by the EE to send SCMS protocol APDU messages to RA. The EE uses HTTP POST to send the SCMS protocol APDU to RA. The EE ASN.1 serializes the APDU and sends it as the HTTP POST Message Body in binary form.

Requirements

- Download requests include requests from EE to RA for the following files:
  - .info
  - Global Policy File (GPF)/Local Policy File (LPF)
  - Global Certificate Chain File (GCCF)/Local Certificate Chain File (LCCF)
  - OBE pseudonym certificate batch file
  - RSE application certificate files
  - OBE identification certificate files
- Download requests shall be sent from EE to RA via HTTP GET.
- Authenticated download requests shall include a HTTP Header with value equal to an ASN1 serialized Base64 encoded SignedAuthenticatedDownloadRequest message.
- APDUs sent from EE to RA via HTTP POST shall include:
  - SecuredRACertRequest
  - SecuredPseudonymCertProvisioningRequest
  - SecuredIdCertProvisioningRequest
- APDUs other than SignedAuthenticatedDownloadRequest shall be sent from EE to RA via HTTP POST.
- APDUs sent from EE to RA via HTTP POST shall sent Content-Type header equal to application/octet-stream.
- APDUs sent from EE to RA via HTTP POST shall be sent in the HTTP Message Body in binary ASN.1 serialized form.