SCMS MANAGER™
SECURITY CREDENTIAL MANAGEMENT SYSTEM

EE CERTIFICATE ROLLOVER (RE-ENROLLMENT) TECHNICAL STANDARD

VERSION 1.0

October 8, 2020

Author

SCMS Manager

TABLE OF CONTENTS

1 Description 2

2 Assumptions 3

3 Design 4

3.1 EE Initiates the Re-enrollment Request 4

3.2 RA Processes EE's Request and ECA's Response 5

3.3 ECA Processes New Enrollment Request 6

4 SCMS RA Routes 8

4.1 EE Re-enrollment Provisioning Request 8

4.1.1 Preconditions: 8

4.1.2 ASN Description 9

4.2 EE Re-enrollment Download Request 9

4.2.1 Preconditions 9

4.2.2 Postconditions 10

4.2.3 ASN Description 10

5 ASN 11

5.1 Re-Enrollment Request ASN 11

5.1.1 SecuredReEnrollmentRequest 11

5.1.2 SignedReEnrollmentRequest 11

5.1.3 SignedEeEnrollmentCertRequest 12

5.1.4 ScopedEeEnrollmentCertRequest 12

5.1.5 EeEcaCertRequest 13

5.2 Re-Enrollment ACK ASN 13

5.2.1 SecuredReEnrollmentCertProvisioningAck 13

5.2.2 SignedReEnrollmentCertProvisioningAck 13

5.2.3 ScopedReEnrollmentCertProvisioningAck 14

5.2.4 RaEeReEnrollmentCertProvisioningAck 14

6 Revision History 15

SCMS MANAGER EE ENROLLMENT CERTIFICATE ROLLOVER (RE-ENROLLMENT) TECHNICAL STANDARD

1 DESCRIPTION

This Technical Specification is intended to amend the CAMP protocol with re-enrollment to allow new and existing devices to renew their enrollment certificates as they expire. The design of this specification follows the work initiated by CAMP: (https://wiki.campllc.org/display/SCP/Step+20.1%3A+EE+Enrollment+Certificate+Rollover), and though CAMP laid the groundwork, this document fills in technical gaps, provides implementation recommendations and establishes ASN.1 to fully define the process. For ease of adoption and implementation, the structure of the ASN.1 and request-download pattern were modelled off of preexisting protocols. Please note that this specification is only intended to define re-enrollment within the CAMP protocol, as the newer version of the protocol, IEEE 1609.2.1, has its own definition but it is not backwards compatible.

During the bootstrap process, an end entity (EE) is issued an enrollment certificate by an Enrollment CA (ECA) via a DCM in a secure environment, which is used to authenticate communication between an EE and the RA. When an enrollment certificate approaches its expiration date, it must be rolled over to a new certificate so that the EE can continue to authenticate with the RA. This process does not take place in a secure environment, and no trusted DCM is available. Instead, the existing enrollment certificate is used to facilitate secure communication with the RA performing a similar task to the DCM.

Some EEs may not have reliable network access, so the request to re-enroll and the retrieval of the new enrollment certificate are separated into two individual transactions. This separation also allows the RA to choose the timing for when it will forward the request to the Enrollment CA. This time delay may be needed to ensure that the RA has access to an ECA with an expiration time that will allow for the validity period of the new enrollment certificate. When an EE requests re-enrollment, the RA will return a time estimate for when the new certificate will be ready for download. This procedure is similar to the process of requesting and downloading authorization certificates.

An EE may request re-enrollment at any time if it has a currently valid enrollment certificate and the EE has not been added to the RA's blacklist. The RA for the EE's current enrollment certificate will accept only one request and corresponding download for re-enrollment. However, if a new re-enrollment request is made before the download of an enrollment certificate from a previous request, the first certificate and request will be invalidated and added to the blacklist. As long as the device has not downloaded a new enrollment certificate from a previous request attempt, then a new request will be honored. The new enrollment certificate will have a validity period that begins when the current enrollment certificate expires (there is no overlap in the validity period for enrollment certificates).

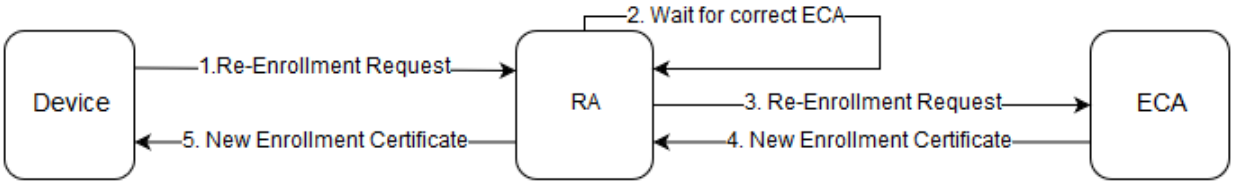

FIGURE 1: BASIC FLOW DIAGRAM

2 ASSUMPTIONS

- The EE possesses a valid enrollment certificate that has not been blacklisted by the RA.
- The EE has not previously completed the re-enrollment process using the currently valid enrollment certificate.
- An ECA is available to sign re-enrollment requests.
- The ECA's certificate will be valid for the entire duration of any re-enrollment request that it signs.
- The new enrollment certificate will have the same PSID/SSP and geographic region attributes, and will have a validity period starting at the expiry date of the old enrollment certificate (there is no overlap in the validity period for enrollment certificates).
- EEs have the ability to generate a new key pair for the new enrollment certificate (no key injection).
- Some EEs have limited network connectivity, therefore the steps of initiating a re-enrollment request, downloading the new enrollment certificate, and validating the new enrollment certificate shall be completed as asynchronous process.
- An EE may request re-enrollment at a time defined by the SCMS provider. The recommended timeframe is 12 – 24 months before the current enrollment certificate's expiration.
- An EE will only possess one valid enrollment certificate at a time, and may only download a single re-enrollment certificate using its currently valid enrollment certificate.
- The RA can store at least two enrollment certificates for each EE: The current enrollment certificate and the new enrollment certificate.
- The existence, or lack thereof, of a stored new enrollment certificate provides a mechanism to track the current stage of re-enrollment.

3 DESIGN

Due to the fact that some EEs may have limited network connectivity, the re-enrollment process takes place in two phases:

1. The EE contacts the RA to initiate a re-enrollment request. If the RA accepts the request, it will inform the EE of a time when it may come back to download the new enrollment certificate.

2. The EE returns to the RA to download a new enrollment certificate

This approach is meant to match the process used to request and download pseudonym certificates. In practice, a re-enrollment request can be sent and the new enrollment certificate retrieved at the same time the EE is requesting, downloading, or topping off its pseudonym certificates. Note that, an EE must update its LPF and LCCF files any time it connects to the RA. If multiple transactions are performed during the same session, then this step only needs to be performed once.

The following sections outline these steps in detail.

3.1 EE INITIATES THE RE-ENROLLMENT REQUEST

If an EE possesses a valid enrollment certificate and has not yet requested re-enrollment, then it may perform the following during its next transaction with the RA:

1. Create a new enrollment key pair and use it to construct an enrollment certificate request with the same properties (same PSID/SSP and region) used in the original enrollment certificate.
    a. The only changes allowed in the new CSR is the validity period for the certificate, with the start time of the new certificate being set to the expiry time of the existing certificate.
    b. The enrollment certificate request is signed using the new verification key.

2. Construct a new signed message containing the new enrollment certificate request and sign that message with the current enrollment certificate private key. This is a re-enrollment request.

3. Send the re-enrollment request to the RA, using the current enrollment certificate to authenticate to the RA. The RA will validate the request (see below) and reply to the EE with a time indicating when the EE can return to download the new certificate and a hash of the request which must be used to retrieve the new certificate. This mirrors the process used to schedule pseudonym certificate downloads. Note that after reconstructing the new enrollment private key, the EE shall delete the ephemeral key pair that was used in the request.

3.2 RA PROCESSES EE'S REQUEST AND ECA'S RESPONSE

Upon receiving a re-enrollment request from the EE, the RA performs the following steps:

1. Perform the following checks on the re-enrollment request:
    a. Validate that the EE's current enrollment certificate has not been blacklisted.
    b. Verify that the public key in the new enrollment certificate request is not the same key as in the current enrollment certificate.
    c. Ensure from the RA database that the EE has not downloaded a previously requested re-enrollment certificate using the current enrollment certificate.
    d. Validate the "outer" signature on the re-enrollment request message using the public key in the currently valid enrollment certificate.
        i. Note: The ECA will validate the "inner" signature on the enrollment certificate request (the payload of the message) using the new enrollment public key in the message. There is no need for the RA to check this signature.
    e. Verify that the requested start time in the re-enrollment request matches the expiration date of the currently active enrollment certificate.
    f. Verify that the re-enrollment request has the same PSID / SSP attributes as the current enrollment certificate.
2. Store the re-enrollment request in the database. The presence of a re-enrollment request in the database signifies that the EE has a re-enrollment request in progress. If this is the case, the RA shall invalidate this previous request if the new enrollment certificate has not been downloaded. If that previous re-enrollment request resulted in a new enrollment certificate, this new one shall be blacklisted.
3. Respond to the EE with a requestHash and eCertDLTime to schedule the download of the new enrollment certificate.
    a.
4. Schedule a time to activate the re-enrollment request shortly before the eCertDLTime that was calculated in step 3.
    a. The amount of time allotted for this procedure is implementation dependent. It is recommended that the RA design account for the work load of the RA and the accompanying ECA to ensure that the new enrollment certificate is available when the EE returns to download.
5. Sign the re-enrollment request using the RA private key and forward the signed request to the ECA.
6. Upon receiving the EE's new enrollment certificate from the ECA, store it in the database; or, if an error is returned, store the error message in place of the new certificate. Create a relation between the previous enrollment certificate and the new enrollment certificate for revocation and pseudonym certificate download purposes. There will be no impact on existing authorization certificates (pseudonym, application, etc); the same certificates that were provisioned by the original enrollment certificate, using the same request hashes, can be downloaded by the new enrollment certificate. Additionally, there is no need, nor ability, to submit another initial provisioning request with the new enrollment certificate, as top-offs will continue to be made for the EE, and can be downloaded using the new enrollment certificate.

7. At the time the EE attempts to retrieve the new EC, the RA shall verify that the EE has not been blacklisted before it allows the download of the new EC.
8. Shall increment the download count of the new enrollment certificate once the EE has downloaded it.
9. Once the current enrollment certificate has expired, the RA shall delete it from the database. After this happens, the RA will have only one enrollment certificate for the EE which makes it possible for the EE to request the next enrollment certificate.

3.3 ECA PROCESSES NEW ENROLLMENT REQUEST

Upon receiving an enrollment certificate request from the RA, the ECA performs the following steps:

1. Validate the RA signature.
2. Verify the signature that was created by the EE using the enrollment private key on the enrollment public key.
    a. This step proves that the entity that generated the request was in possession of the enrollment private key.
3. Validate the validity period of the certificate request.
    a. Note: The ECA may be issued under a new Root CA and ICA than the EE's current enrollment certificate or the RA certificate. This is OK as long as the ECA can validate the RA signature and the validity periods of the new enrollment certificate are within the ECA's validity period.
4. Generate a new enrollment certificate and sends it back to the RA for delivery to the EE; or, return an error to the RA.

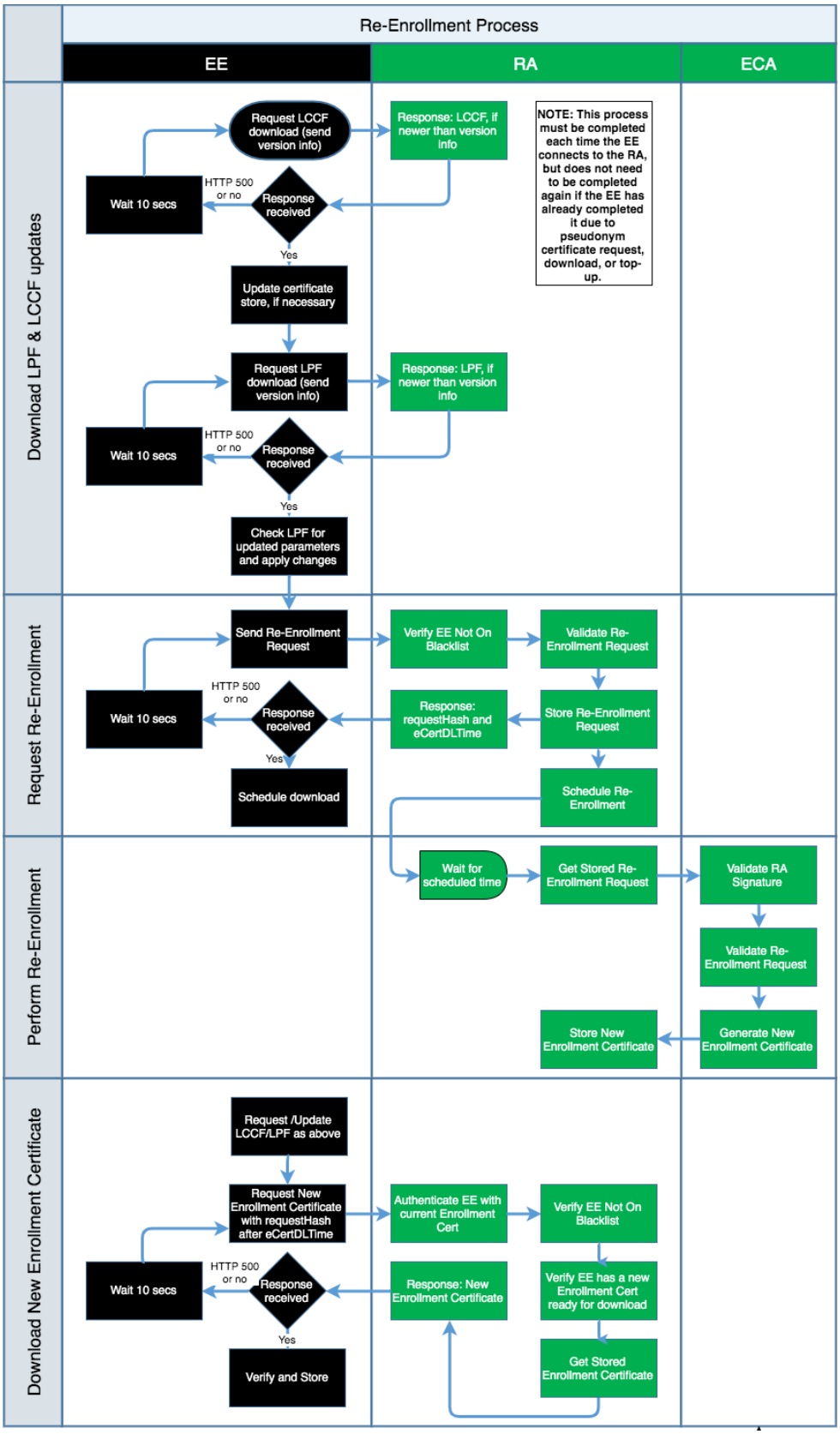

FIGURE 2: DETAILED FLOW DIAGRAM
(https://wiki.campllc.org/display/SCP/Step+20.1%3A+EE+Enrollment+Certificate+Rollover)

4 SCMS RA ROUTES

Re-Enrollment introduces two new routes: one for requesting and one for downloading the generated certificate zip. Both are described below.

4.1 EE RE-ENROLLMENT PROVISIONING REQUEST

A device sends a re-enrollment request for its next enrollment certificate, once in each enrollment certificate's lifetime.

PORT	8892
PATH	/ee-re-enrollment-request
HTTP Method	POST
HTTP Request Body	ASN.1 serialized SecuredReenrollmentRequest
HTTP Response Body	SecuredReenrollmentCertProvisioningAck with a *requestHash* property containing the lower 8 bytes of the request hash. This value will identify this device for the download of the requested certificate. The reply property contains a RaEeReenrollmentCertProvisioningAck with a *certDLTime* property containing the expected time for download of the requested batch, and a *certDLURL* property containing the URL where the ReEnrollmentResponse can be downloaded.

4.1.1 PRECONDITIONS:

1. Requested re-enrollment region is the same as original enrollment region
2. Requested re-enrollment permissions are the same as the original enrollment permissions
3. Requested re-enrollment start time is the same as the expiration time of the current enrollment

4.1.2 ASN DESCRIPTION

Just as a pseudonym provisioning request is wrapped in an Ieee1609Dot2Data signed data (signed by the device's enrollment) and ultimately encrypted to the RA, likewise is the re-enrollment request. The signed data in this case is a 'SignedEeEnrollmentCertRequest', which is the same ASN type used in first-time enrollment.

4.2 EE RE-ENROLLMENT DOWNLOAD REQUEST

PORT	8892
PATH	/ee-re-enrollment-download
HTTP Method	GET
HTTP Request Body	Empty
HTTP Request Headers	HTTP Header 'Download-Req' containing a Base64 encoded ASN.1 serialized *SecuredAuthenticatedDownloadRequest*, containing a *SignedAuthenticatedDownloadRequest*, containing a *ScopedAuthenticatedDownloadRequest*, containing an *AuthenticatedDownloadRequest* with a filename property of the form [0-9A-F]{16}.zip, where the group of 16 hexadecimal digits is the device's request hash obtained from the re-enrollment request.
HTTP Response Body	The corresponding ReEnrollmentResponse (SignedEeEnrollmentCertResponse)

4.2.1 PRECONDITIONS

1. The requested batch has already been generated
2. The requesting device has not been previously revoked

3.

4.2.2 POSTCONDITIONS

1. The file corresponding to the certificate specified in the request URL is returned. Type is a SignedEeEnrollmentCertResponse which can be processed the same way as first time enrollment responses.

4.2.3 ASN DESCRIPTION

SecuredAuthenticatedDownloadRequest are used to make download request and they are already well defined by other use cases.

5 ASN

The re-enrollment download request uses a SecuredAuthenticatedDownloadRequest and its response uses a SignedEeEnrollmentCertResponse which are both used elsewhere in SCMS and thus not redefined by this document. The new structures defined here relate to the re-enrollment request and ack only. These structures pull heavily from existing structures, just with new names.

Re-Enrollment requests:

1. SecuredReEnrollmentRequest (NEW)
2. SignedReenrollmentRequest (NEW)
3. SignedEeEnrollmentCertRequest (EXISTING)
4. ScopedEeEnrollmentCertRequest (EXISTING)
5. EeEcaCertRequest (EXISTING)

Re-Enrollment acks:

1. SecuredReEnrollmentCertProvisioningAck (NEW)
2. SignedReEnrollmentCertProvisioningAck (NEW)
3. ScopedReEnrollmentCertProvisioningAck (NEW)
4. RaEeReEnrollmentCertProvisioningAck (NEW)

5.1 RE-ENROLLMENT REQUEST ASN

5.1.1 SecuredReEnrollmentRequest

```
-- @class SecuredReEnrollmentRequest
-- @param content contains encrypted SignedReEnrollmentRequest sent to RA
--              decrypts to a SignedReEnrollmentRequest.
SecuredReEnrollmentRequest ::= SecuredScmsPDU (WITH COMPONENTS {...,
  content (WITH COMPONENTS {...,
    encryptedData
  })
})
```

5.1.2 SignedReEnrollmentRequest

```
-- @class SignedReEnrollmentRequest
-- @param content contains standard SignedEeEnrollmentCertRequest
```

```
--              ** signed by device's current enrollment certificate **
SignedReEnrollmentRequest ::= Ieee1609Dot2Data( WITH COMPONENTS{...,
   content( WITH COMPONENTS{...,
     signedData( WITH COMPONENTS{...,
       tbsData( WITH COMPONENTS{...,
         payload( WITH COMPONENTS{...,
           data( WITH COMPONENTS{...,
             content( WITH COMPONENTS{...,
               unsecuredData( CONTAINING SignedEeEnrollmentCertRequest)
             })
           })
         })
       })
     })
   })
})
```

5.1.3 SignedEeEnrollmentCertRequest

```
SignedEeEnrollmentCertRequest ::= SecuredScmsPDU (WITH COMPONENTS {...,
  content (WITH COMPONENTS {...,
    signedCertificateRequest  (CONTAINING
      SignedCertificateRequest (WITH COMPONENTS {...,
        tbsRequest (ScopedEeEnrollmentCertRequest),
        signer (WITH COMPONENTS {
          self
        })
      })
    )
  })
})
```

5.1.4 ScopedEeEnrollmentCertRequest

```
ScopedEeEnrollmentCertRequest ::=
  ScmsPDU  (WITH COMPONENTS {...,
    content (WITH COMPONENTS {
      eca-ee (WITH COMPONENTS {
        eeEcaCertRequest
      })
    })
```

})

5.1.5 EeEcaCertRequest

```
EeEcaCertRequest ::= SEQUENCE {
   version              Uint8(1),
   currentTime          Time32,
   tbsData              ToBeSignedCertificate (WITH COMPONENTS { ...,
            id(WITH COMPONENTS {  # unused in all enrollments
            linkageData ABSENT }),
            region PRESENT, # must be same as original enrollment region
            appPermissions ABSENT,
             certIssuePermissions ABSENT,
            certRequestPermissions PRESENT, # must be same as original permissions
            verifyKeyIndicator (WITH COMPONENTS {
            verificationKey }) }),
            ...
}
```

5.2 RE-ENROLLMENT ACK ASN

ASN structures are the same as pseudonym provisioning acks, just renamed

5.2.1 SecuredReEnrollmentCertProvisioningAck

```
SecuredReEnrollmentCertProvisioningAck ::= SecuredScmsPDU (WITH COMPONENTS {...,
  content (WITH COMPONENTS {...,
    encryptedData  -- decrypts to a SignedReEnrollmentCertProvisioningAck
  })
})
```

5.2.2 SignedReEnrollmentCertProvisioningAck

```
SignedReEnrollmentCertProvisioningAck ::= SecuredScmsPDU (WITH COMPONENTS {...,
  content (WITH COMPONENTS {...,
    signedData  (WITH COMPONENTS {...,
      tbsData (WITH COMPONENTS {...,
```

```
    payload (WITH COMPONENTS {...,
      data (WITH COMPONENTS {...,
        content (WITH COMPONENTS {
          unsecuredData (CONTAINING ScopedReEnrollmentCertProvisioningAck)
        })
      })
    }),
    headerInfo (WITH COMPONENTS {...,
      psid (SecurityMgmtPsid),
      generationTime ABSENT,
      expiryTime ABSENT,
      generationLocation ABSENT,
      p2pcdLearningRequest ABSENT,
      missingCrlIdentifier ABSENT,
      encryptionKey ABSENT
    })
  })
 })
})
```

5.2.3 ScopedReEnrollmentCertProvisioningAck

```
ScopedReEnrollmentCertProvisioningAck ::=
 ScmsPDU  (WITH COMPONENTS {...,
  content (WITH COMPONENTS {
   ee-ra (WITH COMPONENTS {
    RaEeReEnrollmentCertProvisioningAck
   })
  })
 })
```

5.2.4 RaEeReEnrollmentCertProvisioningAck

```
-- @brief This structure represents the acknowledgement of the RA that it has
--        received an EE's re-enrollment certificate provisioning request.
-- @class RaEeReEnrollmentCertProvisioningAck
RaEeReEnrollmentCertProvisioningAck ::= RaEePseudonymCertProvisioningAck
```

6 REVISION HISTORY

V1.0	October 8, 2020	Release