Step 20.1: EE Enrollment Certificate Rollover

Target release	Post PoC
Document owner	Brian Romansky
Reviewer	

Goals

Define a procedure to securely re-enroll a non-revoked EE when its enrollment certificate is about to expire.

During the bootstrap process, an 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 procedures is similar to the process of requesting and downloading pseudonym 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 for re-enrollment. 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).

Assumptions

- The EE possesses a valid enrollment certificate that has not been blacklisted by the RA.
- The EE has not previously requested re-enrollment 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.
- For any EE, only one enrollment certificate may be issued for a particular PSID/SSP combination at a time (see Certificate Types for details).
    - An EE should only be allowed to initiate one re-enrollment request for a particular PSID/SSP combination.
    - The new enrollment certificate will have the same PSID/SSP, 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 verification 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 any time
- An EE will only possess one valid enrollment certificate at a time, and may only make a single re-enrollment request 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.

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 (see Use Case 3: OBE Pseudonym Certificates Provisioning). 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, as described in Step 3.1: Request for Pseudonym Certificates, 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.

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 verification key pair and use it to construct an enrollment certificate request with the same properties (same PSID/SSP) used in the original enrollment certificate.
    a. The only changes allowed in the 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. See Use Case 2: OBE Bootstrapping (Manual) for details on formatting the CSR.
    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 (Use Case 3: OBE Pseudonym Certificates Provisioning). Note that after reconstructing the new enrollment private key, the EE shall delete the ephemeral key pair that was used in the request.

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. Ensure that the RA database does not already contain a new enrollment certificate or scheduled re-enrollment request for the EE.
    c. 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 verification public key in the message. There is no need for the RA to check this signature.
    d. Verify that the requested start time in the re-enrollment request matches the expiration date of the currently active enrollment certificate.
    e. 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.
3. Respond to the EE with a requestHash and eCertDLTime to schedule the download of the new enrollment certificate.
    a. The eCertDLTime may be any time that is less than three (3) years prior to the expiration date of the current enrollment certificate. This ensures that the currently active ECA used by the RA for re-enrollment will have a valid life span sufficient to generate a new enrollment certificate with a full life span. See PoC Certificate Expiration Timelines for details on the relationship of these certificate validity periods.
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 (replacing or removing the pending re-enrollment request and storing the new enrollment certificate); 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.
7. 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.

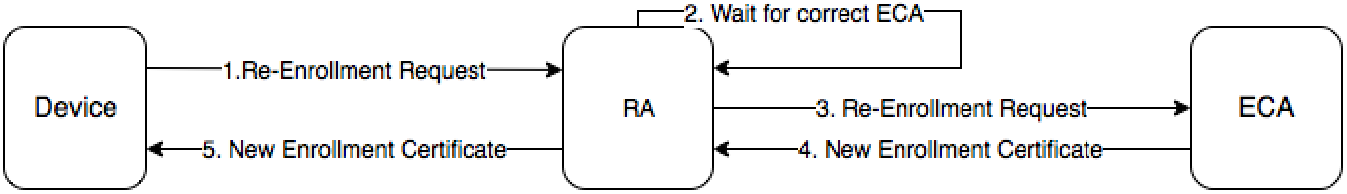
ECA Processes New Enrollment Request

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

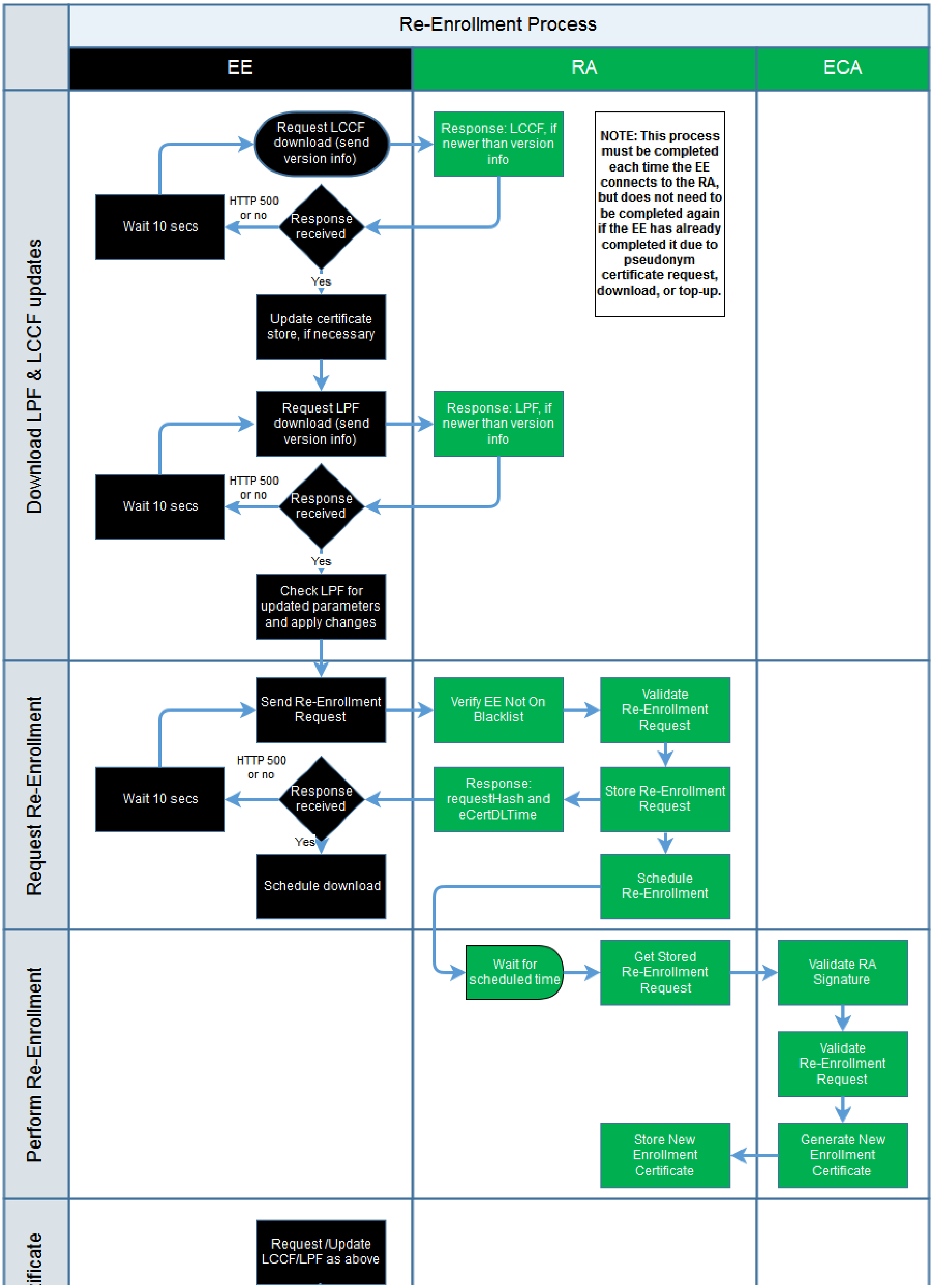
1. Validate the RA signature.
2. Verify the signature that was created by the EE using the validation private key on the validation public key.
    a. This step proves that the entity that generated the request was in possession of the validation private key.
3. Validate the validity period of the certificate 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.

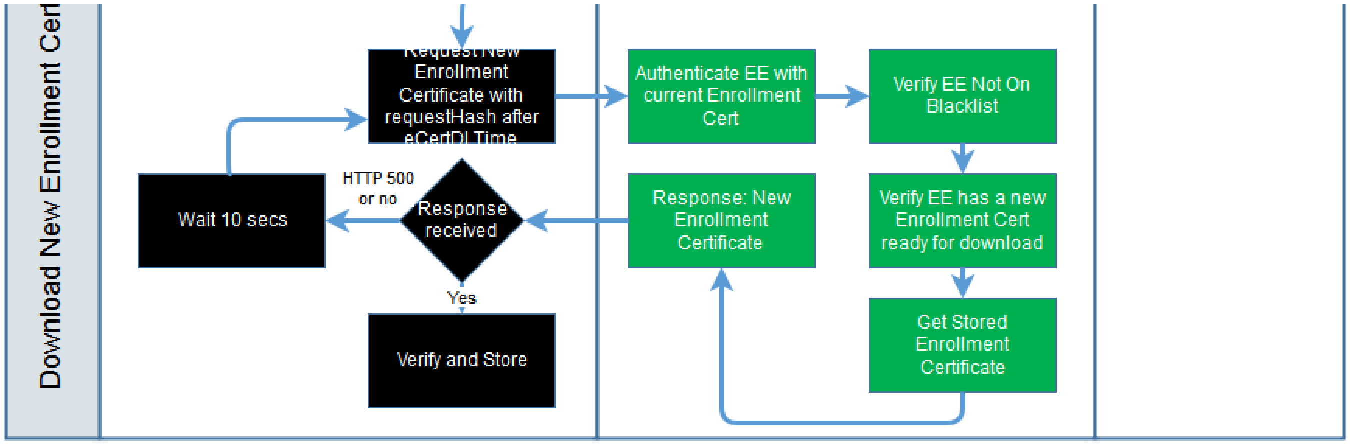
Diagrams

The figure below shows the relationship of the RA and ECA in the re-enrollment process. The next figure is a process diagram that outlines the overall re-enrollment procedure.



Role Of The RA And ECA In Re-enrollment


Re-Enrollment Process
EE
RA
ECA
Download LPF & LCCF updates
Request LCCF download (send version info)
Response: LCCF, if newer than version info
NOTE: This process must be completed each time the EE connects to the RA, but does not need to be completed again if the EE has already completed it due to pseudonym certificate request, download, or top-up.
Wait 10 secs
HTTP 500 or no
Response received
Yes
Update certificate store, if necessary
Request LPF download (send version info)
Response: LPF, if newer than version info
Wait 10 secs
HTTP 500 or no
Response received
Yes
Check LPF for updated parameters and apply changes
Request Re-Enrollment
Send Re-Enrollment Request
Verify EE Not On Blacklist
Validate Re-Enrollment Request
Wait 10 secs
HTTP 500 or no
Response received
Response: requestHash and eCertDLTime
Store Re-Enrollment Request
Yes
Schedule download
Schedule Re-Enrollment
Perform Re-Enrollment
Wait for scheduled time
Get Stored Re-Enrollment Request
Validate RA Signature
Validate Re-Enrollment Request
Store New Enrollment Certificate
Generate New Enrollment Certificate
ificate
Request /Update LCCF/LPF as above


Download New Enrollment Cert
Request New Enrollment Certificate with requestHash after eCertDlTime
Wait 10 secs
HTTP 500 or no
Response received
Yes
Verify and Store
Authenticate EE with current Enrollment Cert
Verify EE Not On Blacklist
Response: New Enrollment Certificate
Verify EE has a new Enrollment Cert ready for download
Get Stored Enrollment Certificate

Re-enrollment Process Diagram

Requirements

<table>
<tr><th>Key</th><th>Status</th><th>Summary</th><th>Description</th><th>Justification</th><th>Notes</th><th>Component/s</th></tr>
<tr><td>SCMS-341</td><td>EE REQUIREMENT</td><td>EE TLS Cipher Suite</td><td>The EE shall support at least the following TLS cipher suites for all communications to SCMS components:
<table>
<tr><th>IANA Value</th><th>Description</th><th>Reference</th></tr>
<tr><td>0xC0, 0x23</td><td>TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256</td><td>RFC5289</td></tr>
<tr><td>0xC0, 0x24</td><td>TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384</td><td>RFC5289</td></tr>
<tr><td>0xC0, 0x2B</td><td>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256</td><td>RFC5289</td></tr>
<tr><td>0xC0, 0x2C</td><td>TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384</td><td>RFC5289</td></tr>
<tr><td>0xC0, 0xAC</td><td>TLS_ECDHE_ECDSA_WITH_AES_128_CCM</td><td>RFC7251</td></tr>
<tr><td>0xC0, 0xAD</td><td>TLS_ECDHE_ECDSA_WITH_AES_256_CCM</td><td>RFC7251</td></tr>
</table></td><td>This is the requirement for the SSL transport tunnel.</td><td>This is out of scope as it defines EE behavior.</td><td>On-board Equipment (OBE), Road-side Equipment (RSE)</td></tr>
<tr><td>SCMS-411</td><td>EE REQUIREMENT</td><td>EE Authentication to RA for Request</td><td>The EE shall authenticate its requests with its enrollment certificate and signed timestamp to avoid replay attacks on the RA.</td><td>Messages from EEs to an RA must be secure against replay attacks. The signed time stamp from the EE enables the RA to validate the freshness of EE requests.</td><td>This is out of scope since it defines EE's behavior.
In the case of re-enrollment (Use Case 22), the EE must use the current, active enrollment certificate to authenticate to the RA.</td><td>On-board Equipment (OBE), Road-side Equipment (RSE)</td></tr>
</table>

SCMS-459	CLOSED	OCSP: Stapled for RA to OBE	The RA shall respond to an OBE request for an OCSP stapled certificate.	Most OBEs do not have access to CRL updates or a reliable network connection to an OCSP server, so the RA must provide an OCSP stapled response so that the OBE can validate the RA's TLS certificate.	OCSP stapling provides improved performance compared to CRLs. OCSP stapling is specified in RFC 6066, Section 8. The RA will be able to respond to the OBE's request for an OCSP stapled certificate. The RA itself will rely on an OCSP service to sign its certificate validation request, which it will return to the EE. For the PoC, the RA will refer to an X.509 CRL to validate certificates of SCMS back-end components (MA, LA, and PCA). OCSP will not be used for back-end component certificate validation.	RA
SCMS-507	TESTS PASSED	Maintain an Internal Blacklist	RA shall maintain an Internal Blacklist and keep it updated based on the communications with the MA.	So that revoked EEs are not able to authenticate with the RA anymore	Every logical RA has its own internal blacklist that is not shared with anyone else. To prevent compromised components to speak with the RA, the RA needs to validate against the SCMS component CRL (compare ~~SCMS-859~~, SCMS-504) and the X.509 CRL (~~SCMS-405~~).	RA
SCMS-512	CLOSED	Policy file	RA shall always provide a local policy file (LPF) available for download by EE.	There is always a global configuration available, and that configuration shall be current.	Note that LPF might have the same content as the global policy file (GPF).	RA
SCMS-513	CLOSED	RA downloads via TCP/IP	RA shall provide downloads over TCP/IP.	To utilize standard internet protocols for the download process.	Downloads could be e.g., policy file, Global Certificate Chain File, certificates, .info file etc.	RA
SCMS-514	CLOSED	RA download via HTTPS	RA shall provide downloads over HTTPS (TLS).	To utilize standard internet protocols for the download process.	Downloads could be e.g., policy file, Global Certificate Chain File, certificates, .info file etc. TLS will provide encryption (~~SCMS-537~~) and RA-EE authentication (~~SCMS-539~~). IEEE 1609.2 certificates within a TLS session will be used for EE-RA authentication (SCMS-538).	RA
SCMS-515	CLOSED	RA requires EE authentication	The RA shall require EE authentication for authenticated transactions.	To ensure that only a proper EE can send requests, download certificates or files.	It is not cost effective to provide OBEs with TLS certificates currently. Instead, the OBE will use TLS to authenticate the other endpoint (as a server) and will use its SCMS certificate to identify itself. EE authenticates via its IEEE 1609.2 enrollment certificate. The details of the authentication process are defined EE-RA Communications - General Guidance	RA
SCMS-517	CLOSED	Tunneling through LOP	RA shall provide downloads only via a LOP interface, which removes all location information from the incoming request.	to anonymize the location of EEs.		RA
SCMS-521	CLOSED	Acknowledge request	RA shall acknowledge the receipt of EE's request with a TCP ACK within a specified amount of time, currently set to be 1 sec.	So that EEs know that RA received their request.		RA

SCMS-522	EE REQUIREMENT	Retry request	EE shall retry, if it does not receive a response from RA (file download, TCP ACK, RA accept request ACK, HTTP 500, or HTTP 304) within a specified amount of time, currently set to be 10 sec from the time of request.	To ensure that the request is received by the RA.	This is out of scope as it defines EE behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-523	EE REQUIREMENT	Number of retries	EE shall limit the number of retries to a maximum of 10 in a 60 minute period	To reduce resource usage, EEs shall limit the number of retries.	This is out of scope as it defines EE behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-529	CLOSED	Store enrollment certificate and butterfly parameters	RA shall store enrollment certificate and butterfly parameters for each OBE for its lifetime.	so that OBE can be revoked properly. Arbitrary number based on historical trends for vehicle ownership. For example, collector vehicles that are kept on the road for longer than typical vehicles.	PoC will only store 3 years	RA
SCMS-537	CLOSED	RA-to-EE encryption	The RA-to-EE communication shall be encrypted.	To avoid that an adversary is able to read EE's enrollment certificate (protect location privacy) or, in case of pseudonym certificates, that an adversary is able to read PCA-encrypted pseudonym certificates.	For pseudonym certificates, this counters a somewhat exotic attack: if an attacker eavesdrops all individually encrypted pseudonym certificates (encrypted by PCA to EE), and then later extracts the Butterfly keys (e.g., after the car arrived on the junk yard), the attacker is able to track the target vehicle in a retrofit manner assuming that attacker has access to a large database of tracking data. For other certificates, this is just an add-on security layer.	RA
SCMS-539	EE REQUIREMENT	RA authentication to EE	The EE shall require RA Authentication before any communication starts.	EE checks whether it talks to proper RA before communication starts and to avoid sending its enrollment certificate to a malicious RA. RA authenticates via its TLS X.509 certificate. The details of the authentication process are defined in EE-RA Communications - General Guidance	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-541	EE REQUIREMENT	OCSP stapling - EE	The EE shall use the TLS Certificate Status Request extension (OCSP stapling) to verify RA revocation status.	To avoid connecting to a revoked and potentially rogue RA.	This is out of scope since it specifies EE's behavior. If EE does not support this feature, the following might happen: An adversary that extracted the RA's private key and that successfully spoofed DNS is able to learn EE's enrollment certificate (but not EE's private key). OCSP stapling is specified in RFC 6066, Section 8.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-709	EE REQUIREMENT	Check for and Download Policy Updates	EE shall check for and download policy updates upon establishing communications with the RA	It is necessary to ensure that the EE is always using the latest policy for new downloaded certificates. Policy definition details are available at Use Case 18: Provide and Enforce Technical Policies.	If no policy file is available on the EE, the EE is allowed to make a download attempt at any time. This is out of scope since it defines EE behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-754	EE REQUIREMENT	Sign certificate request	The EE shall sign certificate requests with its enrollment certificate.	So that RA can verify that the certificate request was not been modified in transit and to verify that the certificate request is originating from a valid EE	This is out of scope since it defines EE behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

SCMS-768	CLOSED	RA - Local Certificate Chain File	RA shall provide a Local Certificate Chain File to EEs for download.	To enable EEs to verify certificates without further CA certificate downloads. If the file name of the Global Certificate Chain File indicates a new version, the RA will update its Local Certificate Chain File with the new chain information, as appropriate for the EEs under its jurisdiction. EEs send their current LCCF's version number in the download request to RA and the response will include a newer LCCF if available.		RA
SCMS-776	EE REQUIREMENT	Encrypt certificate request	The EE shall encrypt the request using the RA certificate.	So that the request is shared confidentially between the EE and RA.	This is out of scope since it defines EE behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-952	EE REQUIREMENT	Error code: eePolicyFileDownloadFailed	EE shall log the error code in EE's error log file, if EE is not able to download the local policy file (e.g., because there is none or it is corrupted).	As the policy file is essential for the system to work correctly and contains security relevant information, it is important to have an error handling whenever the EE is not able to get the latest version of that file.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1189	EE REQUIREMENT	Trust Chain Broken - EE	The EE shall not attempt to request or download pseudonym certificate batches, OBE identification certificate files, RSE application certificate, or a new enrollment certificate, if any component in the trust chain of EE's enrollment certificate is revoked. In this case, EE also shall not attempt to download a local policy file or local certificate chain file from RA.	To reduce resources, since RA will reject request.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1203	CLOSED	Check time stamp	RA shall check the signed (by EE) time-stamp and allow a tolerance of 5 seconds.	To counter replay or delay attacks.		RA
SCMS-1204	CLOSED	Check blacklist	RA shall reject EE request and respond with HTTP 500, if EE is listed on its blacklist.	To reject request, and not provide any useful information to EE.	If EE is listed, RA will reject the connection. Otherwise, RA will proceed with the authentication process. The Internal Blacklist Manager (IBLM) of the Misbehavior Authority (MA) updates the RAs on which devices to exclude from granting certificates. Therefore, it sends out revocation information (e.g., linkage information, certificate digest, etc.) that allows the RA to identify the enrollment certificate of the corresponding device and put it on the internal blacklist. The RA does not send out enrollment certificates to the IBLM.	RA
SCMS-1353	EE REQUIREMENT	EE request LCCF from RA	The EE shall check for an updated Local Certificate Chain File (LCCF) upon establishing communications with the RA	To be able to verify SCMS certificates based on their certificate chain.	All the certificate chains will contain certificates up to the root CA including elector endorsement for the root CA certificate. This is out of scope since it defines EE behavior	On-board Equipment (OBE), RA, Road-side Equipment (RSE)
SCMS-1377	CLOSED	RA check whitelisted ECA	RA shall validate that the enrollment certificate used by the EE for authentication is issued by a whitelisted ECA.	To ensure that only a proper EE can send requests, download certificates or files.	Whitelist defined in SCMS-1371	RA

SCMS-1419	CLOSED	ECA issues implicit certificates	ECA shall issue implicit OBE and RSE enrollment certificates	To save storage space and over-the-air bytes		ECA
SCMS-1600	CLOSED	Enrollment certificate lifetime	ECA shall issue Enrollment Certificates with an expiration date on or before 00:00:00 UTC January 1, 2025.	To avoid any need to update enrollment certificates during the CV-Pilot project.	Maximum life span 1,084 sixtyHours. This is for CV-Pilot only.	ECA
SCMS-1906	EE REQUIREMENT	Enrollment certificate corresponds to the private key	The enrollment key-pair generator (OBE, RSE, or DCM) shall check that the enrollment certificate corresponds to the private key	This is necessary because otherwise the device won't be able to use the enrollment certificate for requesting pseudonym/identification /application certificates.	If re-enrolling, no DCM is available and this check must be done by the EE.	DCM, On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1907	EE REQUIREMENT	Enrollment certificate verification	The enrollment key-pair generator (OBE, RSE, or DCM) shall check that the enrollment certificate correctly verifies, including building a chain back to the root CA.	This is necessary because otherwise the device won't be able to use the enrollment certificate for requesting pseudonym/identification /application certificates.		DCM, On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1910	EE REQUIREMENT	Verification key pair generation algorithm	EE shall shall generate the verification key pair using an algorithm approved for use within the SCMS.	Because only those algorithms will be supported by the SCMS.	See Approved Cryptographic Algorithms This is out of scope as it defines EE behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-2475	REVIEW	Re-Enrollment Validate Current Enrollment Cert	RA shall validate the signature of the current enrollment certificate in order to initiate a re-enrollment request.	The re-enrollment process requires a currently valid enrollment certificate.	When an EE is initially enrolled we require a secure connection to the DCM. For re-enrollment, this is replaced by the authenticated, current enrollment certificate.	RA
SCMS-2476	REVIEW	Store new enrollment cert for download	The RA shall store the new enrollment certificate until it is fetched by the EE.	The new enrollment certificate is not necessarily generated at the time of request by the EE.		RA
SCMS-2477	REVIEW	Keep new enrollment cert	The RA shall allow the EE to re-download its new enrollment certificate provided the device's credentials are still valid and not expired.	To allow for recovery after data loss.		RA
SCMS-2478	REVIEW	PSID in re-enrollment request must match current enrollment PSID	RA shall verify that the PSID in the re-enrollment request matches the PSID in the current enrollment certificate.	New enrollment certificate must have have identical permissions.		RA
SCMS-2479	REVIEW	Re-Enrollment certificate lifetime	RA shall ensure that the new enrollment certificate has the same validity period as the current enrollment certificate, with the start time of the new enrollment certificate equal to the expiry time of the current enrollment certificate.	The certificate validation chain for the new enrollment certificate must be valid for it's entire lifetime.		RA
SCMS-2480	REVIEW	Store all re-enrollment requests / certificates	The RA shall keep a record of all pending enrollment requests /certificates. Once an enrollment certificate expires, there is no need to store it.	To track the status of enrollment and to detect duplicate re-enrollment requests.		RA

SCMS-2481	REVIEW	Schedule generation of new enrollment certificate	RA shall schedule a time to forward the re-enrollment request to the ECA at a t time that is no sooner than two years after the start date of the current enrollment certificate.	ECA at time of request may not have validity period that covers new enrollment cert. Must wait for new ECA to come online.	The 2 year overlap is based on the current design of a 6 year enrollment cert and an 11 years ECA cert with 2 year overlap (for ECA certificates).	ECA, RA
SCMS-2482	REVIEW	Delete pending re-enrollment requests upon blacklisting	RA shall delete any pending re-enrollment request or stored new enrollment certificate, if the corresponding EE becomes blacklisted.	A blacklisted EE cannot authenticate with the RA and should not be able to obtain a new enrollment certificate.		RA
SCMS-2483	EE REQUIREMENT	Secure Key Generation	EE shall generate the private key for use in a new enrollment certificate in a hardware secure module.	The maintain confidentiality of private keys.		On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-2610	EE REQUIREMENT	Use FQDN found in certificate	EEs shall use the FQDN specified in the "id" field of the SCMS component certificate to contact the component.	The IP address of SCMS components are not guaranteed to be static and may change at any time.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-2611	REVIEW	Store enrollment certificate	RA shall store the following for each OBE: • All non-expired enrollment certificates • The most recent expired enrollment certificate	So that OBEs can be revoked or re-enrolled properly.		RA

42 issues

Use Case 20.1 - Requirements