Security Credential Management System Proof–of–Concept Implementation

EE Requirements and Specifications Supporting SCMS Software Release 1.2.2

Made Available to the United States Department of Transportation

National Highway Traffic Safety Administration (NHTSA)

November 15, 2016

In Response to Cooperative Agreement Number

DTNH22-14-H-00449/0003

Table of Contents

1 Notice and Disclaimer 1

2 Introduction 2

3 Introduction for EE Developers 3

4 Environments documentation 6
4.1 SCMS Proof-of-Concept Connected Vehicle Pilot Environments Overview 6
4.2 SCMS Proof-of-Concept Connected Vehicle Pilot QA Environment 7
4.3 SCMS Proof-of-Concept Connected Vehicle Pilot PROD Environment 8

5 Requirements and Specifications 10
5.1 Common Requirements 10
5.1.1 SCMS PoC Supported V2X Applications 10
5.1.2 Certificate Types 22
5.1.3 Hardware, Software and OS Security Requirements 66
5.1.4 Elector-based Root Management 76
5.1.5 Cryptography 92
5.1.6 CRL Series Diagram 117
5.1.7 EE-RA Communications - General Guidance 118
5.1.8 EE-SCMS Core Communication Requirements 121
5.1.9 Overview of Used Error Codes 129
5.1.10 Re-enrollment 137
5.2 Requirements by Use Case 138
5.2.1 On-board Equipment (OBE) Use Cases 139
5.2.2 Road-side Equipment (RSE) Use Cases 139
5.2.3 Common EE Use Cases 139
5.2.4 Backend Use Cases 139
5.2.5 Requirement Status 140
5.2.6 Use Case 2: OBE Bootstrapping (Manual) 140
5.2.7 Use Case 3: OBE Pseudonym Certificates Provisioning 161
5.2.8 Use Case 5: Misbehavior Reporting 241
5.2.9 Use Case 6: CRL Download 253
5.2.10 Use Case 8: OBE Pseudonym Certificate Revocation 258
5.2.11 Use Case 11: Backend Management 266
5.2.12 Use Case 12: RSE Bootstrapping (Manual) 406
5.2.13 Use Case 13: RSE Application Certificate Provisioning 406
5.2.14 Use Case 16: RSE Application and OBE Identification Certificate Revocation 447
5.2.15 Use Case 18: Provide and Enforce Technical Policies 454
5.2.16 Use Case 19: OBE Identification Certificate Provisioning 490
5.2.17 Use Case 20: EE Re-Enrollment 565

6 Software Design Documents 586
6.1 Common - Services View 586
6.2 MA - Services View 586
6.2.1 General Notes 586
6.2.2 Services Summary for EE-MA Communications 587
6.2.3 MA - Download CRL 587
6.3 RA - Services View 587
6.3.1 General Notes 587
6.3.2 Services Summary for EE-RA Communications 588

6.3.3 RA - Request Pseudonym Certificate Batch Provisioning 588
6.3.4 RA - Download .info File 590
6.3.5 RA - Download Local Policy File 591
6.3.6 RA - Download Pseudonym Certificate Batch 593
6.3.7 RA - Retrieve Registration Authority Certificate 596
6.3.8 RA - Request Identification Certificate Provisioning 597
6.3.9 RA - Download Identification Certificate 598
6.3.10 RA - Request Application Certificate Provisioning 599
6.3.11 RA - Download Application Certificate 600
6.3.12 RA - Download Local Certificate Chain File 601
6.3.13 RA - Submit Misbehavior Report 603

7 Test Vectors 605
7.1 Purpose 605
7.2 Test Vectors Location 605
7.3 Overview 605
7.4 Crypto Test Vectors 605
7.4.1 Linkage Values lv(i,j) 605
7.4.2 Group Linkage Values glv(i,j,k) and Encrypted Indices ei(j,k) 605
7.4.3 Butterfly Expansion Function 606
7.4.4 Key Derivation Function, KDF2 [IEEE-1363a, ANSI X9.63] with SHA-256 606
7.4.5 Message Authentication Code, MAC1 (HMAC)[IEEE-1363a, ANSI X9.71, RFC 2104, 4231] with SHA-256 606
7.4.6 AES-CCM-128 Symmetric Authenticated Encryption [IEEE-1609.2, NIST SP 800-38C] 606
7.4.7 ECDH Key Agreement [SP800-56A Section 5.7.1.2] 606
7.4.8 ECIES Public-Key Encryption [IEEE-1609.2] 606
7.4.9 Implicit Certificate Generation and Public/Private Keys Reconstruction [SEC-4] 607
7.4.10 Hash-based Functions 607
7.4.11 AES-based Functions 607
7.4.12 ECC Functions 608
7.4.13 Linkage Values and Butterfly Key Expansion Functions 610
7.5 1602.2 and SCMS ASN.1 Objects 610
7.6 ECIES Encryption as in 1609.2-2016, Sec 5.3.5 612

8 Glossary 614

Table of Figures

Figure 1 The Three Environments of the SCMS POC Software 6
Figure 2 SCMS POC Connected Vehicle Pilot QA Environment 7
Figure 3 SCMS POC Connected Vehicle Pilot PROD Environment 8
Figure 4 Calculating In-use Lifetime of a Certificate Authority 31
Figure 5 Impact of Lag in Validity of Issued Certificates 32
Figure 6 Relationship Between Enrollment and CA Certificate Lifetimes 32
Figure 7 Example of Mid-Sequence Certificates 33
Figure 8 Summary of Elector and Root CA Activities, 1 of 2 42
Figure 9 Summary of Elector and Root CA Activities, 2 of 2 43
Figure 10 EE Enrollment Rollover Timeline 44
Figure 11 PoC Certificate Expiration Timelines - Overview Diagram, 1 of 3 45
Figure 12 PoC Certificate Expiration Timelines - Overview Diagram, 2 of 3 46
Figure 13 PoC Certificate Expiration Timelines - Overview Diagram, 3 of 3 47
Figure 14 PoC Certificate Expiration Timelines - Stackup, 1 of 3 48
Figure 15 PoC Certificate Expiration Timelines - Stackup, 2 of 3 49
Figure 16 PoC Certificate Expiration Timelines - Stackup, 3 of 3 50
Figure 17 Illustration of the Expiration Period of Various Certificate Types 61
Figure 18 Integrated Architecture 67
Figure 19 Connected Architecture 67
Figure 20 Networked Architecture 67
Figure 21 Endorsement Method Details 79
Figure 22 EE Storage Requirements 81
Figure 23 Day 1: Typical SCMS Operations 82
Figure 24 Day 2: Revoking an Elector 83
Figure 25 Day 3: SCMS Operating with Two Electors Only 84
Figure 26 Day 4: Replacing an Elector 85
Figure 27 Day 5: SCMS Returning to Typical Operation 86
Figure 28 Day 1: Typical SCMS Operations 87
Figure 29 Day 2: Standing Up a New Root CA Certificate 88
Figure 30 Day 3: Putting the SCMS Backend Trust Relationships in Place for the New Root CA Certificate 89
Figure 31 Day 4: Revoking the Existing and Adding the New Root CA Certificate 90
Figure 32 Day 5: Revoked Root CA, System Non-Functional 91
Figure 33 Day 6: System Functionality Restored 92
Figure 34 Butterfly Key Mechanism 113
Figure 35 Creation of Individual Linkage Values and Revocation of Individual Device 117
Figure 36 CRL Series Diagram 117
Figure 37 EE-RA Download Interaction 119
Figure 38 Overview of Methods 122
Figure 39 Overview of Multiple SCMS Components Served by Single LOP 122
Figure 40 Universal SCMS Handshake Processes, 1 of 5 123

Figure 41 Universal SCMS Handshake Processes, 2 of 5 124
Figure 42 Universal SCMS Handshake Processes, 3 of 5 125
Figure 43 Universal SCMS Handshake Processes, 4 of 5 126
Figure 44 Universal SCMS Handshake Processes, 5 of 5 126
Figure 45 Common Process for File Download Operations, 1 of 3 127
Figure 46 Common Process for File Download Operations, 2 of 3 127
Figure 47 Common Process for File Download Operations, 3 of 3 128
Figure 48 Common Process for Sending SCMS Messages, 1 of 2 128
Figure 49 Common Process for Sending SCMS Messages, 2 of 2 129
Figure 50 Pseudonym Certificate Provisioning Process 165
Figure 51 OBE-RA Communication 188
Figure 52 Download New Pseudonym Certificates 241
Figure 53 EE Misbehavior Reporting Process 252
Figure 54 SCMS Architecture 272
Figure 55 SCMS Root CA Trust Anchor Relationships - Overview 273
Figure 56 SCMS Root CA & Elector Trust Relationships 274
Figure 57 Elector A Revocation Process 275
Figure 58 SCMS Operational with Electors B & C Only 276
Figure 59 Introduce Elector D 277
Figure 60 SCMS Trust Relationships with Elector D 278
Figure 61 Create Replacement Root CA & Distribute to SCMS Servers 279
Figure 62 Introduce Replacement Root CA before Revoking Current Root CA 280
Figure 63 Revoke Root CA 281
Figure 64 Root Revoked - System Non-functional 282
Figure 65 Update EEs with New Certificates 283
Figure 66 CRLG Messaging Diagram 289
Figure 67 ECA Messaging Diagram 294
Figure 68 MA Messaging Diagram 304
Figure 69 PCA Messaging Diagram 309
Figure 70 PG Messaging Diagram 317
Figure 71 RA Messaging Diagram 323
Figure 72 Create Replacement Root CA & Distribute to SCMS Servers 338
Figure 73 Introduce Replacement Root CA Before Revoking Current Root CA 339
Figure 74 CRL Series Diagram 347
Figure 75 Revoke Root CA 401
Figure 76 Application Certificate Provisioning Process 407
Figure 77 RSE-RA Communication 425
Figure 78 Relationship GCCF-LCCF 480
Figure 79 GCCF/LCCF Structure 481
Figure 80 Identification Certificate Provisioning Process 491
Figure 81 OBE-RA Communication 514
Figure 82 Role Of The RA And ECA In Re-enrollment 570
Figure 83 Re-enrollment Process Diagram 571
Figure 84 SCMS-Protocol ASN.1 610
Figure 85 IEEE 1609.2 Schema ASN.1 610
Figure 86 SignedData ASN.1 611

Figure 87 SignedData Example ASN.1 611
Figure 88 ECIES Encryption 612

Table of Tables

Table 1 Supported V2X Applications 1
Table 2 Certificate Type Features 26
Table 3 PoC Certificate Expiration Timelines - Certificate Expiration and Renewal 34
Table 4 Expiration, In-use, and Overlap Requirements 36
Table 5 CV Pilot Certificate Expiration Timelines - Certificate Expiration 52
Table 6 CV Pilot Certificate Expiration Timelines - Certificate Expiration and Renewal Guidelines 54
Table 7 Renewal/Rollover Requirements 55
Table 8 Expiration, In-use, and Overlap Requirements 55
Table 9 CV Pilot Certificate Expiration Timelines - Certificate Expiration and Renewal 63
Table 10 EE Status through Addition/Revocation of Electors and Root CAs 78
Table 11 Butterfly Key 110
Table 12 Linkage Values 116
Table 13 RA-EE Errors 130
Table 14 SCMS Errors 131
Table 15 SCMS Error Log Values 133
Table 16 Standard HTTP Error Codes 135
Table 17 Document Header and Status 140
Table 18 Use Case 3 - Requirements 163
Table 19 Use Case 3.1 - Requirements 187
Table 20 Use Case 3.3 - Requirements 193
Table 21 Use Case 3.5 - Requirements 217
Table 22 Use Case 5 - Requirements 251
Table 23 Use Case 6 - Requirements 257
Table 24 Use Case 8.4 - Requirements 260
Table 25 Use Case 11 - Requirements 271
Table 26 Use Case 11.1.1 – Requirements 286
Table 27 CRLG Values 290
Table 28 MA Values 290
Table 29 CRL Store Values 290
Table 30 Step 11.1.1 Add CRLG - Requirements 292
Table 31 ECA Values 295
Table 32 DCM Values 295
Table 33 RA Values 295
Table 34 Use Case 11.1. Add ECA - Requirements 297
Table 35 Use Case 11.1.1 Add ICA - Requirements 301
Table 36 MA Values 304
Table 37 RA Values 304
Table 38 DCM Values 305
Table 39 Use Case 11.1.1 Add MA - Requirements 306
Table 40 PCA Values 309
Table 41 RA Values 309

Table 42 MA Values 310
Table 43 LA Values 310
Table 44 Use Case 11.1.1 Add PCA - Requirements 312
Table 45 PG Values 318
Table 46 RA Values 318
Table 47 Use Case 11.1.1 Add PG - Requirements 320
Table 48 RA Values 324
Table 49 DCM Values 324
Table 50 MA Values 324
Table 51 Use Case 11.1.1 Add RA - Requirements 326
Table 52 Use Case 11.1.2 Add Root CA - Requirements 334
Table 53 Use Case 11.1.3: Add Elector - Requirements 342
Table 54 Requirements 349
Table 55 Use Case 11.2.1 Revoke CRLG - Requirements 353
Table 56 Use Case 11.2.1 Revoke ECA - Requirements 359
Table 57 Use Case 11.2.1 Revoke ICA - Requirements 365
Table 58 Use Case 11.2.1 Revoke MA - Requirements 371
Table 59 Use Case 11.2. Revoke PCA - Requirements 375
Table 60 Use Case 11.2.1 Revoke PG - Requirements 384
Table 61 Use Case 11.2.1 Revoke RA - Requirements 389
Table 62 Use Case 11.2.2 Revoke Root CA - Requirements 394
Table 63 Use Case 11.2.3 Revoke Elector - Requirements 404
Table 64 Use Case 13.1 - Requirements 409
Table 65 Use Case 13.3 - Requirements 429
Table 66 Use Case 16.4 - Requirements 450
Table 67 List of Global Configuration Options 457
Table 68 List of Local Configuration Options 461
Table 69 Use Case 18.1 - Requirements 465
Table 70 Use Case 18.2 - Requirements 469
Table 71 Use Case 18.3 - Requirements 474
Table 72 GCCF Structure Elements 482
Table 73 LCCF Structure Elements 483
Table 74 Use Case 18.4 - Requirements 485
Table 75 Use Case 19.1 - Requirements 495
Table 76 Use Case 19.3 - Requirements 519
Table 77 Use Case 19.5 - Requirements 546
Table 78 Use Case 20.1 - Requirements 572
Table 79 Services Summary For EE-RA Communications 588

1 Notice and Disclaimer

This material is based upon work supported by the U.S. Department of Transportation under Cooperative Agreement No. DTNH22-14-H-00449/0003.

Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the Author(s) and do not necessarily reflect the view of the U.S. Department of Transportation.

2 Introduction

The Security Credential Management System (SCMS) Proof-of-Concept (POC) Implementation Project (SCMS POC Project) is being conducted by the Crash Avoidance Metrics Partners LLC (CAMP LLC) Vehicle Safety Communications 5 (VSC5) Consortium. Members of the Consortium are Ford Motor Company, General Motors LLC., Honda R&D Americas, Inc., Hyundai-Kia America Technical Center, Inc., Mazda, Nissan Technical Center North America, Inc., and Volkswagen Group of America. The goal of the SCMS POC design is to provide security services to support Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications at current production levels of passenger vehicles (up to 17 million annually) for the first year of deployment. An important goal of the SCMS POC system is to provide a flexible architecture that is capable of scaling to support larger numbers of V2V and V2I devices in the years following initial deployment. It is also anticipated that the SCMS POC design will provide both a stable platform and a research platform to support the USDOT and industry research needs prior to deployment. The work is sponsored by the National Highway Traffic Safety Administration (NHTSA) through Cooperative Agreement DTNH22-14-H-00449/0003.

Work in Task 4 of the project focuses on the design of the SCMS core components and protocols. Four software releases are planned during the course of the project. This document presents the requirements and specifications for the **SCMS POC System Release 1.2** from the perspective of an **End Entity (EE)**. This document is a work-in-progress. Future refinements and revisions to the requirements and specifications are anticipated as SCMS refinement is an ongoing task across multiple projects.

3 Introduction for EE Developers

The following paragraph will guide you as an EE developer through this documentation highlighting requirements and API documentation in the order of an EE's lifecycle. If you implement your EE software following this guide, you should have a device at the end that is able to communicate with the SCMS throughout the whole lifecycle.

1. First of all you need a Secure Environment for Device Enrollment where initialization and bootstrapping of your device will be executed
2. You need to have a device that applies to the requirements and descriptions laid out in Hardware, Software and OS Security Requirements
3. You need to have a True Random Number Generator
4. Your device needs to support in either hardware or software Approved Cryptographic Algorithms
5. You need to have an HTTP client that is able to communicate securely (HTTPS) to the SCMS as described in EE-RA Communications - General Guidance and EE-SCMS Core Communication Requirements
6. You need to know which Certificate Types you need to have on your device, which depends on the SCMS PoC Supported V2X Applications that you want to run on your device
7. The EE lifecycle starts with Use Case 2: OBE Bootstrapping (Manual), respectively Use Case 12: RSE Bootstrapping (Manual) depending on your EE type (OBE vs. RSE). Currently both processes are exactly the same.
8. Based on the EE type you are developing, you then create and send one of the following requests. All devices should always check for a new local certificate chain file (API: RA - Download Local Certificate Chain File) and a new local policy file (API: RA - Download Local Policy File) before sending subsequent request. All requests in this step #8 should be sent within the same HTTPS session.
    a. Pseudonym Certificates:
        i. Following the process in Use Case 3: OBE Pseudonym Certificates Provisioning, your OBE should create a pseudonym certificate batch request as described in Step 3.1: Request for Pseudonym Certificates and send it to the RA API as documented in RA - Request Pseudonym Certificate Batch Provisioning. Your OBE needs to create the butterfly seed pairs as described in SCP1: Butterfly Keys. Your OBE will get a response from RA with an *URL* and a *download time*.
        ii. Once your OBE's clock reaches *download time*, your OBE can download the initial pseudonym certificate batch at *URL* following the process in Step 3.3: Initial Download of Pseudonym Certificates using the RA API as documented in RA - Download Pseudonym

Certificate Batch and the .info file using RA's API documented in RA - Download .info File.

b. Application Certificate:

   i. Following the process in Use Case 13: RSE Application Certificate Provisioning, your RSE should create an application certificate request as described in Step 13.1: Request RSE Application Certificate and send it to the RA API as documented in RA - Request Application Certificate Provisioning. Your RSE will get a response from the RA with an *URL* and a *download time*.

   ii. Once your RSE's clock reaches *download time*, your RSE can download the application certificate at *URL* following the process in Step 13.3: Download RSE Application Certificate using the RA API as documented in RA - Download Application Certificate.

c. OBE Identification Certificate:

   i. Following the process in Use Case 19: OBE Identification Certificate Provisioning, your OBE should create an identification certificate request as described in Use Case 19: OBE Identification Certificate Provisioning and send it to the RA API as documented in RA - Request Identification Certificate Provisioning. Your OBE will get a response from RA with an *URL* and a *download time*.

   ii. Once your OBE's clock reaches *download time*, your OBE can download the identification certificate at *URL* following the process in Step 19.3: Initial Download of OBE Identification Certificates using the RA API as documented in RA - Download Identification Certificate and the .info file using RA's API documented in RA - Download .info File.

9. Depending on the certificate type, the SCMS constantly pre-generates them and your EE can download top-offs like this:

   a. Pseudonym Certificates: Whenever it suits your pseudonym certificate download strategy at a point of time that is after the time given in the .info file, follow the process described in Step 3.5: Top-off Pseudonym Certificates using RA's API documented in RA - Download Pseudonym Certificate Batch to download additional pseudonym certificates.

   b. Identification Certificate: Whenever it suits your identification certificate download strategy at a point of time that is after the time given in the .info file, follow the process described in Step 19.5: Top-off OBE Identification Certificates using RA's API documented in RA - Download Identification Certificate to download the next identification certificate.

10. Your EE should download the latest CRL as often as possible but no later than once a week using the process described in Use Case 6: CRL Download using the API documented in MA - Download CRL.

11. Your EE must verify incoming messages. Part of the verification is to check if the senders certificate was revoked following the process described in Step 8.4: OBE CRL Check, respectively Step 16.4: RSE CRL Check, as well as if a CA certificate in their certificate chain was revoked.
12. Report misbehavior: This is still TBD and will be supported with SCMS Release 2
13. Re-enroll: This is still TBD and will be supported with SCMS Release 2

4 Environments Documentation

The SCMS POC software is operated in three different environments (locations) for three different purposes. All environments have their own, independent Root CA.

4.1 SCMS Proof-of-Concept Connected Vehicle Pilot Environments Overview

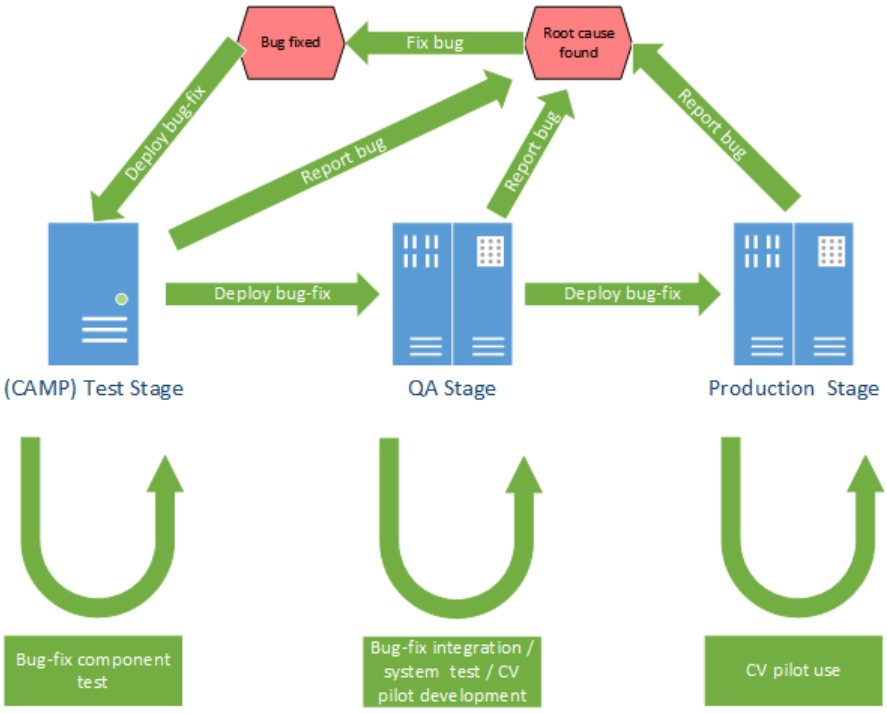


Figure 1 The Three Environments of the SCMS POC Software

The picture above shows these three environments and how they relate to each other:

1. (CAMP) Test Stage (TEST): This environment is internal to CAMP and is not available to any outside stakeholders and is used for SCMS development and testing purposes.
2. QA Stage (QA): This environment is publicly available via Internet IPv6 and IPv4 connections. It is used to evaluate new SCMS software versions, as well as bug fixes and enhancements. The environment provides device developers with a working system that they can use to develop and test their devices. The level of security, as well as the security requirements for devices using certificates, is lower than the Production stage.
3. Production Stage (PROD): This environment has the highest level of security, uses a production grade offline Root CA (including storing the CA's certificate in an HSM) and is strictly used for production devices only. These production devices are more specifically US DOT approved CV Pilot participants. Approved Devices that

handle certificates issued by this system must implement all security requirements as outlined in Use Case 2: OBE Bootstrapping (Manual), Secure Environment for Device Enrollment and Hardware, Software and OS Security Requirements.

If any bugs are detected (in any of the stages) the SCMS software team will analyze the error, respectively create a new version of the SCMS POC software and then apply the following deployment cycle:

1. The new version is deployed to TEST and tested internally at CAMP.
2. After successful testing and assured stability, the software will be deployed to QA. This wiki's blog will be used to provide advanced notice.
3. Following a few of weeks of monitoring the new software in the QA stage, and considering any feedback from the development community, the new version will eventually be deployed to PROD. US DOT will approve this deployment and advanced notice will be given using this wiki's blog.

4.2 SCMS Proof-of-Concept Connected Vehicle Pilot QA Environment

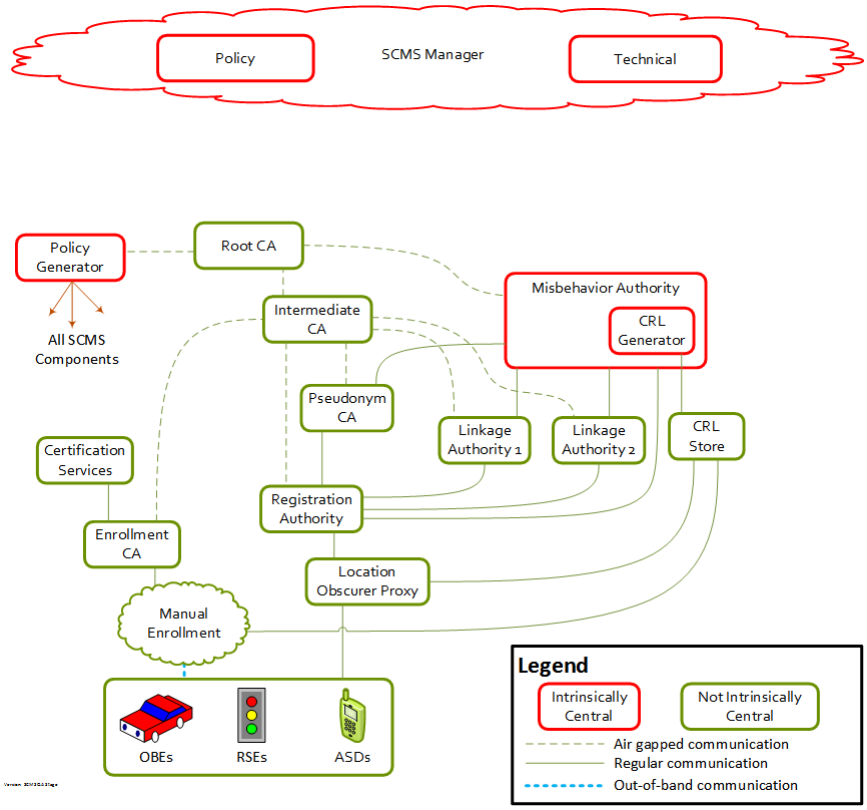


Figure 2 SCMS POC Connected Vehicle Pilot QA Environment

The QA environment has the capability to revoke certificates, however only manual revocation is supported. Bootstrapping is implemented with a manual enrollment as documented in Use Case 2: OBE Bootstrapping (Manual).

Features to be added at a later:

- Global Misbehavior Detection will be implemented to provide an (semi-)automatic way of revoking certificates based on misbehavior reports
- Automatic enrollment for selected device suppliers / operators
- Re-enrollment as documented in Use Case 20: EE Re-Enrollment
- Electors as documented in Elector-based Root Management

4.3 SCMS Proof-of-Concept Connected Vehicle Pilot PROD Environment

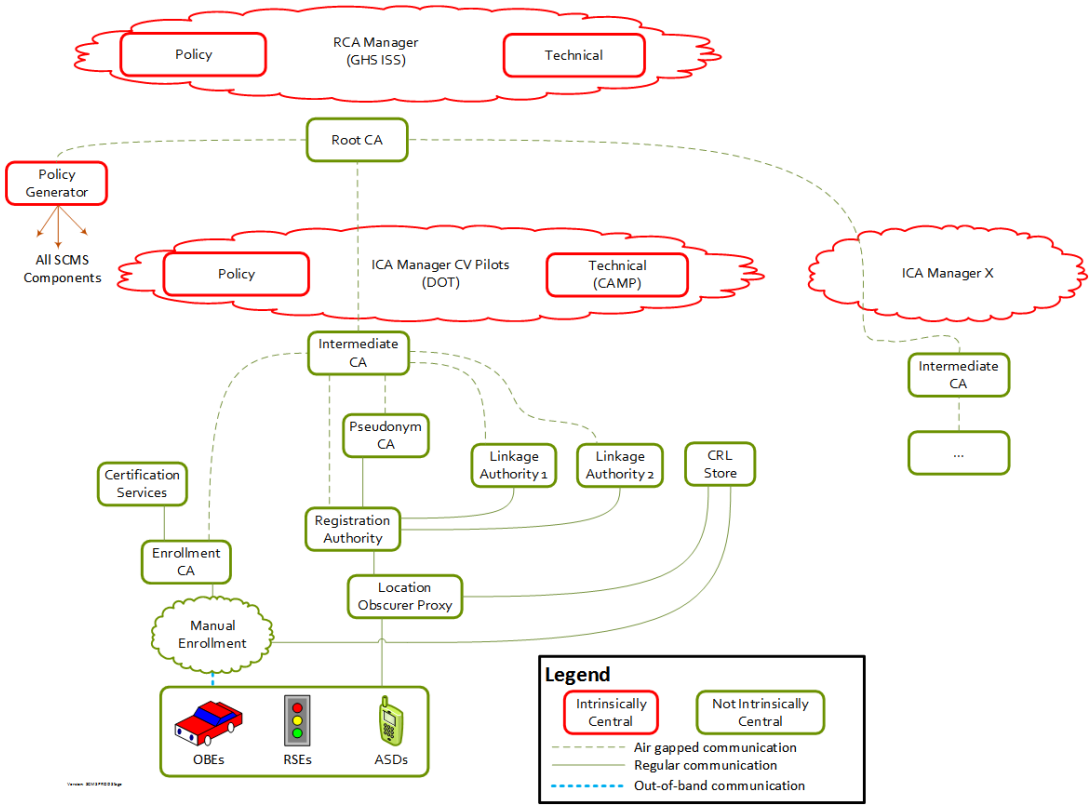


Figure 3 SCMS POC Connected Vehicle Pilot PROD Environment

Initially the PROD environment will not have a MA, and therefore will not have the capability to receive or handle misbehavior reports. To achieve the expected security levels, the PROD stage uses a commercially available Root CA. The overall SCMS system has multiple levels of management as seen in the SCMS PKI hierarchy:

- As a governance body there is a Root CA Manager that sits above the system and is seen as the policy and technical arm. It is responsible to run and protect the Root CA and issue a PG, a CRLG and ICA certificates. Stakeholders that get an ICA must follow the Root CA policies, e.g., the Certificate Policy.
- In the SCMS PKI hierarchy below the Root CA Manager there can be multiple ICA Managers. The USDOT is considered an ICA Manager and will manage an ICA with the help of its policy and technical arm. The SCMS design can support many ICA Managers.

Given a single shared Root CA it's important to note that for certain SCMS features to work all of the ICA Managers have to cooperate with the Root CA Manager.

5 Requirements and Specifications

The following pages contain requirements and specifications of the SCMS PoC protocols and components.

- Common Requirements
- Requirements by Use Case

5.1 Common Requirements

The requirements in this section apply to all use cases, whereas the requirements in the section Requirements by Use Case are specific to the respective use case.

5.1.1 SCMS PoC Supported V2X Applications

This is the list of supported V2X Applications for PoC and Pilot Deployment.
See CAMP PSID Transfer Process for a description of how the "CV Pilot Application X" PSIDs assigned to CAMP may be transferred to a different owner who will develop the application specification, which has to be done before the SCMS PROD stage will issue any certificate with the PSID.

Table 1 Supported V2X Applications

	Application	Application Category	PSID (Hex value) (Decimal value)	Organization/ Documentation	SSP Notes	Comments	SSP Value to Appear in End Entity Certificates for CV Pilots	CVPD Sites That Use It (to be completed)	EE Type	Certificate Type
1	Basic Safety Message (BSM)	BSM inputs (BSM PSID)	0p20 (0x20) (32)	SAE J2735 (data structure) / SAE J945/1 (application specification)		Support multiple V2V safety applications	SSP: absent (default permissions)	NYC THEA Wyoming	OBE	Pseudonym Certificate
2	Vehicle Turning Right in Front of Bus Warning	BSM inputs (BSM PSID)	0p20 (0x20) (32)	SAE J2735 (data structure) / SAE J945/1 (application specification)		Assumes specific application in bus to analyze the received BSMs and determine if a warning should be provided to the bus driver	SSP: absent (default permissions)		OBE	Pseudonym Certificate
3	Intelligent Traffic Signal System (I-SIG) In-Vehicle Information Potential	Current assumption is BSM inputs only (BSM PSID)	0p20 (0x20) (32)	SAE J2735 (data structure) / SAE J945/1 (application specification)	Difficult to know the SSP requirements until the application design is more complete	Difficult to know if there are other application messaging requirements until the application design is more complete	SSP: absent (default permissions)			Pseudonym Certificate

	Application	Application Category	PSID (Hex value) (Decimal value)	Organization/ Documentation	SSP Notes	Comments	SSP Value to Appear in End Entity Certificates for CV Pilots	CVPD Sites That Use It (to be completed)	EE Type	Certificate Type
4	Forward Collision Warning (FCW)	BSM inputs (BSM PSID)	0p20 (0x20) (32)	SAE J2735 (data structure) / SAE J945/1 (application specification)			SSP: absent (default permissions)		OBE	Pseudonym Certificate
5	Emergency Electronic Brake Light (EEBL)	BSM inputs (BSM PSID)	0p20 (0x20) (32)	SAE J2735 (data structure) / SAE J945/1 (application specification)			SSP: absent (default permissions)		OBE	Pseudonym Certificate
6	Blind Spot Warning (BSW)	BSM inputs (BSM PSID)	0p20 (0x20) (32)	SAE J2735 (data structure) / SAE J945/1 (application specification)			SSP: absent (default permissions)		OBE	Pseudonym Certificate
7	Lane Change Warning/Assist (LCA)	BSM inputs (BSM PSID)	0p20 (0x20) (32)	SAE J2735 (data structure) / SAE J945/1 (application specification)			SSP: absent (default permissions)		OBE	Pseudonym Certificate
8	Intersection Movement Assist	BSM inputs (BSM PSID)	0p20 (0x20) (32)	SAE J2735 (data structure) / SAE J945/1 (application specification)			SSP: absent (default permissions)		OBE	Pseudonym Certificate

	Application	Application Category	PSID (Hex value) (Decimal value)	Organization/ Documentation	SSP Notes	Comments	SSP Value to Appear in End Entity Certificates for CV Pilots	CVPD Sites That Use It (to be completed)	EE Type	Certificate Type
9	Stationary Vehicle Ahead (SVA)	BSM inputs (BSM PSID)	0p20 (0x20) (32)	SAE J2735 (data structure) / SAE J945/1 (application specification)			SSP: absent (default permissions)		OBE	Pseudonym Certificate
10	Do Not Pass Warning	BSM inputs (BSM PSID)	0p20 (0x20) (32)	SAE J2735 (data structure) / SAE J945/1 (application specification)			SSP: absent (default permissions)		OBE	Pseudonym Certificate
11	Probe Enabled Traffic Monitoring	BSM inputs (BSM PSID)	0p20 (0x20) (32)	SAE J2735	Detailed application description not available.	Either RSE just collects BSMs or RSE sends WSA with probe request and then vehicle uses IP service to send requested information or establish two-way communications. In the case of probe request it isn't clear whether the probe request PSID	SSP: absent (default permissions)		OBE	Pseudonym Certificate

	Application	Application Category	PSID (Hex value) (Decimal value)	Organization/ Documentation	SSP Notes	Comments	SSP Value to Appear in End Entity Certificates for CV Pilots	CVPD Sites That Use It (to be completed)	EE Type	Certificate Type
						needs to appear in a certificate.				
12	WAVE security management	Support	0p23 (0x23) (35)	IEEE 1609.2			SSP: absent (default permissions)			
13	Misbehavior Reporting for Common Applications	Support	0p26 (0x26) (38)	Crash Avoidance Metrics Partners LLC	Detailed application description not available.	NOTE: This PSID is also used for event data recording in NYC, because it already appears in the BSM certificate and because event data reporting is very similar to misbehavior reporting. But this is a bit of a hack.	SSP: absent (default permissions)		OBE	Pseudonym Certificate
14	Vulnerable Road Users Safety Application	Vulnerable Road Users Safety PSID	0p27 (0x27) (39)	SAE J2735 (data structure) / SAE J945/9 (application specification – draft)	Detailed application description not available.					Application Certificate

	Application	Application Category	PSID (Hex value) (Decimal value)	Organization/ Documentation	SSP Notes	Comments	SSP Value to Appear in End Entity Certificates for CV Pilots	CVPD Sites That Use It (to be completed)	EE Type	Certificate Type
15	Differential GPS Corrections, Uncompressed	Support	0p80-00 (0x80) (128)	SAE J2735 (data structure)	Detailed application description not available				TMC App	Application Certificate
16	Differential GPS Corrections, Compressed	Support	0p80-01 (0x81) (129)	SAE J2735 (data structure)	Detailed application description not available					Application Certificate
17	Red Light Violation Warning / RSE	3 - Signal Violation Warning (Intersection Safety and Awareness PSID. SPaT & MAP use message ID to distinguish message type)	0p80-02 (0x82) (130)	SAE J2735 (data structure) SAE J2945/2 (SSP framework) SAE J2945/10 (application specification, in progress) RSU requirements document (partial application specification)	Detailed application description not available. SAE subgroup has been tasked with developing SSP specification for SPAT; draft available.				RSE	Application Certificate

	Application	Application Category	PSID (Hex value) (Decimal value)	Organization/ Documentation	SSP Notes	Comments	SSP Value to Appear in End Entity Certificates for CV Pilots	CVPD Sites That Use It (to be completed)	EE Type	Certificate Type
18	Pedestrian in Signalized Crosswalk Warning / RSE	16 - Pedestrian Warnings (Intersection Safety and Awareness PSID. SPaT & MAP use message ID to distinguish message type)	0p80-02 (0x82) (130)	SAE J2735 (data structure) SAE J2945/2 (SSP framework) SAE J2945/10 (application specification, in progress) RSU requirements document (partial application specification)	SAE subgroup has been tasked with developing SSP specification for SPAT; draft available May require SSP field to indicate that RSU is equipped with ability to detect pedestrians.				RSE	Application Certificate
19	Mobile Accessible Pedestrian Signal System (PED-SIG)	SRM	SRM – which PSID?	SAE J2735 (Data structure) SAE J2945/11 (Application specification, in progress)	Detailed application description being developed within Pilot Deployment projects. No SSP definition currently known.					Application Certificate

	Application	Application Category	PSID (Hex value) (Decimal value)	Organization/ Documentation	SSP Notes	Comments	SSP Value to Appear in End Entity Certificates for CV Pilots	CVPD Sites That Use It (to be completed)	EE Type	Certificate Type
20	Transit Signal Priority/ Special Vehicles	1 - Signal Pre-emption/Priority (SignalRequest Message)	SRM – which PSID?	SAE J2735 (Data structure) SAE J2945/11 (Application specification, in progress)	Detailed application description being developed within Pilot Deployment projects. No SSP definition currently known.					Identification Certificate
21	Modified Eco-Speed Harmonization / RSE	2 - Speed Harmonization (Traveler Information and Roadside Signage PSID)	0p80-03 (0x83) (131)	SAE J2735 (Data Structure) SAE J2945/4 (Application specification, in progress) CVPD site-specific documents	SAE subgroup has been tasked with developing SSP specification for TIM. Draft available.	Not clear that this message will ever be signed by RSE; NYC and Wyoming approaches assume all TIMs are signed by TMC			TMC App or RSU	Application Certificate
22	Modified Eco-Speed Harmonization / TMC	2 - Speed Harmonization (Traveler Information and	0p80-03 (0x83) (131)	SAE J2735 (Data Structure) SAE J2945/4 (Application	SAE subgroup has been tasked with developing SSP specification for TIM. Draft available. SSP may	NYC and Wyoming approaches assume all TIMs are signed by TMC			TMC App or RSU	Application Certificate

	Application	Application Category	PSID (Hex value) (Decimal value)	Organization/ Documentation	SSP Notes	Comments	SSP Value to Appear in End Entity Certificates for CV Pilots	CVPD Sites That Use It (to be completed)	EE Type	Certificate Type
		Roadside Signage PSID)		specification, in progress) CVPD site-specific documents	differentiate between different speed harmonization categories (e.g., eco-, light vehicles, freight, transit)					
23	Curve Speed Warning	8 - Curve Speed Warning (Traveler Information and Roadside Signage PSID)	0p80-03 (0x83) (131)	SAE J2735 (Data Structure) SAE J2945/4 (Application specification, in progress) CVPD site-specific documents	SAE subgroup has been tasked with developing SSP specification for TIM. Draft available.				TMC App or RSU	Application Certificate
24	Reduced Speed / Work Zone Warning / RSE	9 - Temporary Situation Warning (Traveler Information and	0p80-03 (0x83) (131)	SAE J2735 (Data Structure) SAE J2945/4 (Application specification, in progress)	SAE subgroup has been tasked with developing SSP specification for TIM. Draft available.	NYC is assuming that TIMs are signed by the TMC, even for situations like this where they contain local information.			TMC App or RSU	Application Certificate

	Application	Application Category	PSID (Hex value) (Decimal value)	Organization/ Documentation	SSP Notes	Comments	SSP Value to Appear in End Entity Certificates for CV Pilots	CVPD Sites That Use It (to be completed)	EE Type	Certificate Type
		Roadside Signage PSID)		CVPD site-specific documents						
25	Reduced Speed / Work Zone Warning / TMC	9 - Temporary Situation Warning (Traveler Information and Roadside Signage PSID)	0p80-03 (0x83) (131)	SAE J2735 (Data Structure) SAE J2945/4 (Application specification, in progress) CVPD site-specific documents	SAE subgroup has been tasked with developing SSP specification for TIM. Draft available.	NYC is assuming that TIMs are signed by the TMC, even for situations like this where they contain local information.			TMC App or RSU	Application Certificate
26	Spot Specific Weather Warnings / RSE	9 - Temporary Situation Warning (Traveler Information and Roadside Signage PSID)	0p80-03 (0x83) (131)	SAE J2735 (Data Structure) SAE J2945/4 (Application specification, in progress) CVPD site-specific documents	SAE subgroup has been tasked with developing SSP specification for TIM. Draft available.	NYC is assuming that TIMs are signed by the TMC, even for situations like this where they contain local information.			TMC App or RSU	Application Certificate

	Application	Application Category	PSID (Hex value) (Decimal value)	Organization/ Documentation	SSP Notes	Comments	SSP Value to Appear in End Entity Certificates for CV Pilots	CVPD Sites That Use It (to be completed)	EE Type	Certificate Type
27	Spot Specific Weather Warnings / TMC	9 - Temporary Situation Warning (Traveler Information and Roadside Signage PSID)	0p80-03 (0x83) (131)	SAE J2735 (Data Structure) SAE J2945/4 (Application specification, in progress) CVPD site-specific documents	SAE subgroup has been tasked with developing SSP specification for TIM. Draft available.	NYC is assuming that TIMs are signed by the TMC, even for situations like this where they contain local information.			TMC App or RSU	Application Certificate
28	Variable Speed Limits / RSE	10 - Speed Zone (Traveler Information and Roadside Signage PSID)	0p80-03 (0x83) (131)	SAE J2735 (Data Structure) SAE J2945/4 (Application specification, in progress) CVPD site-specific documents	SAE subgroup has been tasked with developing SSP specification for TIM. Draft available.	NYC is assuming that TIMs are signed by the TMC.			TMC App or RSU	Application Certificate
29	Variable Speed Limits / TMC	10 - Speed Zone (Traveler Information and	0p80-03 (0x83) (131)	SAE J2735 (Data Structure) SAE J2945/4 (Application	SAE subgroup has been tasked with developing SSP specification	NYC is assuming that TIMs are signed by the TMC.			TMC App or RSU	Application Certificate

	Application	Application Category	PSID (Hex value) (Decimal value)	Organization/ Documentation	SSP Notes	Comments	SSP Value to Appear in End Entity Certificates for CV Pilots	CVPD Sites That Use It (to be completed)	EE Type	Certificate Type
		Roadside Signage PSID)		specification, in progress) CVPD site-specific documents	for TIM. Draft available.					
30	Speed Harmonization / RSE	2 - Speed Harmonization	0p80-03 (0x83) (131)	SAE J2735 (Data Structure) SAE J2945/4 (Application specification, in progress) CVPD site-specific documents	SAE subgroup has been tasked with developing SSP specification for TIM. Draft available.	NYC is assuming that TIMs are signed by the TMC.			TMC App or RSU	Application Certificate
31	Speed Harmonization / TMC	2 - Speed Harmonization (Traveler Information and Roadside Signage PSID)	0p80-03 (0x83) (131)	SAE J2735 (Data Structure) SAE J2945/4 (Application specification, in progress) CVPD site-specific documents	SAE subgroup has been tasked with developing SSP specification for TIM. Draft available.	NYC is assuming that TIMs are signed by the TMC.			TMC App or RSU	Application Certificate

	Application	Application Category	PSID (Hex value) (Decimal value)	Organization/ Documentation	SSP Notes	Comments	SSP Value to Appear in End Entity Certificates for CV Pilots	CVPD Sites That Use It (to be completed)	EE Type	Certificate Type
32	Work Zone Alerts / RSE	9 - Temporary Situation Warning (Traveler Information and Roadside Signage PSID)	0p80-03 (0x83) (131)	SAE J2735 (Data Structure) SAE J2945/4 (Application specification, in progress) CVPD site-specific documents	SAE subgroup has been tasked with developing SSP specification for TIM. Draft available.	NYC is assuming that TIMs are signed by the TMC.			TMC App or RSU	Application Certificate
33	Work Zone Alerts / TMC	9 - Temporary Situation Warning (Traveler Information and Roadside Signage PSID)	0p80-03 (0x83) (131)	SAE J2735 (Data Structure) SAE J2945/4 (Application specification, in progress) CVPD site-specific documents	SAE subgroup has been tasked with developing SSP specification for TIM. Draft available.	NYC is assuming that TIMs are signed by the TMC.			TMC App or RSU	Application Certificate
34	Truck Restrictions / RSE	11 - Special Vehicle Warning (Traveler Information and	0p80-03 (0x83) (131)	SAE J2735 (Data Structure) SAE J2945/4 (Application	SAE subgroup has been tasked with developing SSP specification	NYC is assuming that TIMs are signed by the TMC.			TMC App or RSU	Application Certificate

	Application	Application Category	PSID (Hex value) (Decimal value)	Organization/ Documentation	SSP Notes	Comments	SSP Value to Appear in End Entity Certificates for CV Pilots	CVPD Sites That Use It (to be completed)	EE Type	Certificate Type
		Roadside Signage PSID)		specification, in progress) CVPD site-specific documents	for TIM. Draft available.					
35	Truck Restrictions / TMC	11 - Special Vehicle Warning (Traveler Information and Roadside Signage PSID)	0p80-03 (0x83) (131)	SAE J2735 (Data Structure) SAE J2945/4 (Application specification, in progress) CVPD site-specific documents	SAE subgroup has been tasked with developing SSP specification for TIM. Draft available.	NYC is assuming that TIMs are signed by the TMC.			TMC App or RSU	Application Certificate
36	Automatic Alerts for First Responders	11 - Special Vehicle Warning (Traveler Information and Roadside Signage PSID)	0p80-03 (0x83) (131)	SAE J2735 (Data Structure) SAE J2945/4 (Application specification, in progress) CVPD site-specific documents	SAE subgroup has been tasked with developing SSP specification for TIM. Draft available. Specific SSPs may need to be designated for	NYC is assuming that TIMs are signed by the TMC.			TMC App or RSU	Application Certificate

	Application	Application Category	PSID (Hex value) (Decimal value)	Organization/ Documentation	SSP Notes	Comments	SSP Value to Appear in End Entity Certificates for CV Pilots	CVPD Sites That Use It (to be completed)	EE Type	Certificate Type
					messages to special vehicles					
37	CV-enabled Weather-Responsive Variable Speed Limits	9 - Temporary Situation Warning (Traveler Information and Roadside Signage PSID)	0p80-03 (0x83) (131)	SAE J2735 (Data Structure) SAE J2945/4 (Application specification, in progress) CVPD site-specific documents	SAE subgroup has been tasked with developing SSP specification for TIM. Draft available.	NYC is assuming that TIMs are signed by the TMC.			TMC App or RSU	Application Certificate
38	Road Weather Advisories for Trucks and Vehicles	9 - Temporary Situation Warning (Traveler Information and Roadside Signage PSID)	0p80-03 (0x83) (131)	SAE J2735 (Data Structure) SAE J2945/4 (Application specification, in progress) CVPD site-specific documents	SAE subgroup has been tasked with developing SSP specification for TIM. Draft available. Different SSPs may be needed to differentiate messages for	NYC is assuming that TIMs are signed by the TMC.			TMC App or RSU	Application Certificate

	Application	Application Category	PSID (Hex value) (Decimal value)	Organization/ Documentation	SSP Notes	Comments	SSP Value to Appear in End Entity Certificates for CV Pilots	CVPD Sites That Use It (to be completed)	EE Type	Certificate Type
					different categories of vehicles					
39	Emergency Communications and Evacuation (EVAC)	9 - Temporary Situation Warning (Traveler Information and Roadside Signage PSID)	0p80-03 (0x83) (131)	SAE J2735 (Data Structure) SAE J2945/4 (Application specification, in progress) CVPD site-specific documents	SAE subgroup has been tasked with developing SSP specification for TIM. Draft available.	NYC is assuming that TIMs are signed by the TMC.			TMC App or RSU	Application Certificate
40	Probe Data Collection	BSM and alert event data collection for researchers Regional extension of PDM / PVD Alternatively: IPv6	0p80-04 (0x84) (132)	SAE J2735 (data structures) SAE J2945/12 (application specification) CVPD site-specific documents		Not clear that this appears in certificates – may appear only in WSAs?	SSP: absent (default permissions)			

	Application	Application Category	PSID (Hex value) (Decimal value)	Organization/ Documentation	SSP Notes	Comments	SSP Value to Appear in End Entity Certificates for CV Pilots	CVPD Sites That Use It (to be completed)	EE Type	Certificate Type
41	WAVE Service Advertisement	Support	0p80-07 (0x87) (135)	IEEE 1609.3			SSP: absent (default permissions)			
42	Peer-to-peer distribution of Security Management Information	Peer-to-peer Certificate Distribution Psid	0p80-08 (0x88) (136)	Crash Avoidance Metrics Partners LLC		Doesn't appear in certificates				
43	Certificate Revocation List Application	Support	0p80-80 (0x100) (256)	IEEE 1609.2 (Data structures / SSP) / CAMP (application specification)		Only appears in appPermissions of the CRLG	SSP: specific to CRL as specified in 1609.2 CRL ASN.1 module			
44	Vehicle initiated distress notification		0pC0-00-02 (0x40-82) (16,514)	Wyoming DOT	UPER-encoded J2945/2 DSRC-SSP containing a SSPentry. Version is set to 1, allowedSSPs is a SEQUENCE containing exactly		SSP (DSRC-SSP UPER encoded in hex): 00 80 01 F0 40 Entire 1609.2 PsidSsp structure as	Wyoming		Identification Certificate

	Application	Application Category	PSID (Hex value) (Decimal value)	Organization/ Documentation	SSP Notes	Comments	SSP Value to Appear in End Entity Certificates for CV Pilots	CVPD Sites That Use It (to be completed)	EE Type	Certificate Type

					one SSPentry field, as follows:
					`SSPentry ::= SEQUENCE { index INTEGER(msg-travelerInformation), -- 31`
					`constraint (SSPconstraintAll) -- Boolean: True }`
							an OPAQUE OCTET STRING in COER: 80 02 40 82 80 05 00 80 01 F0 40			

45	Transcore software update	Support	0pE0-00-00-03 (0x20-40-83) (2,113,667)	Transcore, Inc						Application Certificate
46	Over-the-air File Broadcast	Support	0pE0-00-00-08 (0x20-40-88) (2,113,672)	Siemens Industry, Inc.						Application Certificate

	Application	Application Category	PSID (Hex value) (Decimal value)	Organization/ Documentation	SSP Notes	Comments	SSP Value to Appear in End Entity Certificates for CV Pilots	CVPD Sites That Use It (to be completed)	EE Type	Certificate Type
47	Data Log Transfer	Support	0pE0-00-00-09 (0x20-40-89) (2,113,673)	Siemens Industry, Inc.						Application Certificate
48	CV Pilot Application 3		0pE0-00-00-0A (0x20-40-8A) (2,113,674)	Crash Avoidance Metrics Partners LLC						
49	CV Pilot Application 4		0pE0-00-00-0B (0x20-40-8B) (2,113,675)	Crash Avoidance Metrics Partners LLC						
50	CV Pilot Application 5		0pE0-00-00-0C (0x20-40-8C) (2,113,676)	Crash Avoidance Metrics Partners LLC						
51	CV Pilot Application 6		0pE0-00-00-0D (0x20-40-8D) (2,113,677)	Crash Avoidance Metrics Partners LLC						
52	CV Pilot Application 7		0pE0-00-00-0E (0x20-40-8E) (2,113,678)	Crash Avoidance Metrics Partners LLC						

	Application	Application Category	PSID (Hex value) (Decimal value)	Organization/ Documentation	SSP Notes	Comments	SSP Value to Appear in End Entity Certificates for CV Pilots	CVPD Sites That Use It (to be completed)	EE Type	Certificate Type
53	CV Pilot Application 8		0pE0-00-00-0F (0x20-40-8F) (2,113,679)	Crash Avoidance Metrics Partners LLC						
54	CV Pilot Application 9		0pE0-00-00-10 (0x20-40-90) (2,113,680)	Crash Avoidance Metrics Partners LLC						
55	CV Pilot Application 10		0pE0-00-00-11 (0x20-40-91) (2,113,681)	Crash Avoidance Metrics Partners LLC						
56	CV Pilot Application 11		0pE0-00-00-12 (0x20-40-92) (2,113,682)	Crash Avoidance Metrics Partners LLC						
57	CV Pilot Application 12		0pE0-00-00-13 (0x20-40-93) (2,113,683)	Crash Avoidance Metrics Partners LLC						
58	CV Pilot Application 13		0pE0-00-00-14 (0x20-40-94) (2,113,684)	Crash Avoidance Metrics Partners LLC						

	Application	Application Category	PSID (Hex value) (Decimal value)	Organization/ Documentation	SSP Notes	Comments	SSP Value to Appear in End Entity Certificates for CV Pilots	CVPD Sites That Use It (to be completed)	EE Type	Certificate Type
59	CV Pilot traffic signal priority status	SSM	0pE0-00-00-15 (0x20-40-95) (2,113,685)	US Department of Transportation					RSU	Application Certificate
60	CV Pilot traffic signal request	SRM	0pE0-00-00-16 (0x20-40-96) (2,113,686)	US Department of Transportation					OBE	Identification Certificate
61	CV Pilot MAP distribution	MAP	0pE0-00-00-17 (0x20-40-97) (2,113,687)	US Department of Transportation						Application Certificate

UPER-encoded DSRC-SSP containing the SSPentry.

5.1.1.1 CAMP PSID Transfer Process

Crash Avoidance Metric Partners LLC has registered 16 PSIDs with IEEE 1609.2 and IEEE RA and included them in the PROD ICA certificate. Before requesting certificates with one of those PSIDs, the PSID has to be re-assigned following this process, otherwise your request will be rejected:

1. The requesting organization mails their request to psid-request@campllc.org, with a copy also sent to ieee-registration-authority@ieee.org. The mail should include:
    a. A specific note that this is a request for a transfer of one of the CAMP CV Pilot Application PSIDs
    b. The standard PSID request form from http://standards.ieee.org/develop/regauth/psid/psid_application.pdf, filled out in full
    c. An explanation of how the PSID will be used in the Pilot Deployments so that CAMP can determine whether the use case warrants the use of one of the CAMP PSIDs.
2. If CAMP is not satisfied that there is a compelling reason to transfer, CAMP engages in correspondence with the requester to understand why it is necessary to use one of the CAMP PSIDs.
3. Once CAMP is satisfied that the transfer is necessary, CAMP mails a response back to the requester and ieee-registration-authority@ieee.org. CAMP also sends copies of its response to kevin.s.smith@cox.net and wwhyte@onboardsecurity.com. This mail includes a soft copy of a letter on CAMP letterhead stating that the transfer is requested by CAMP subject to review by the PSID allocation subgroup in 1609. The mail instructs the requester to fill out the IEEE-RA Change of Information form, http://standards.ieee.org/develop/regauth/psid/infocx.html.
4. The requesting organization fills out an IEEE-RA Change of Information form. In that form, the requester must provide the email address of a contact at CAMP who can approve the transfer (psid-request@campllc.org), as well as the email address of the organization's contact.
5. The IEEE RA does their vetting:
    a. RA requires formal documentation from the entity, including the name of the application, etc. The RA may require other formal documentation from the entity as they see fit.
    b. RA passes the request to the 1609 PSID allocation subgroup for review.
6. The request is put on the agenda of the monthly PSID allocation meeting (first Wednesday of every month) for 1609 review.
7. If the request is approved, the 1609 subgroup contacts CAMP (scroll-bookmark-51psid-request@campllc.org), the IEEE-RA (ieee-registration-authority@ieee.org), and the original requester to inform them that the request has been approved.

8. IEEE-RA carries out any further necessary due diligence, updates the online list of assigned PSIDs, and notifies the requesting organization, the 1609 subgroup, and CAMP that the transfer is complete.

Once step 7 of the process is successfully completed, CAMP will update SCMS PoC Supported V2X Applications and inform the USDOT and their contractors to start accepting enrollment requests with the transferred PSID for eligible devices.

5.1.2 Certificate Types

The V2X system uses several types of certificates. SCMS components generate these and in many cases can also revoke them. All certificate lifetimes and renewal periods are listed separately for PoC and CV Pilot Test, QA, and Prod stages. All the EE certificates are of **implicit** type to save storage space and over-the-air bytes. All the SCMS component certificates are of **explicit** type.

5.1.2.1 On-Board Equipment (OBE)

5.1.2.1.1 OBE Enrollment

An enrollment certificate is like a passport for the OBE in that it uses the enrollment certificate to request other certificates: pseudonym and identification certificates. It does not have an encryption key. It is provided to the OBE during its **bootstrap** process. Each enrollment certificate has at least one PSID; however, an OBE cannot have more than one enrollment certificate associated with a particular (PSID, SSP) combination. In cases where an enrollment certificate has more than one PSID, the corresponding apps are expected to be similar in nature. Such groupings of PSIDs in an enrollment certificate are likely to be related to policy decisions made by the SCMS Manager. Enrollment certificates have a validity period expected **not** to cover the OBE's full operational lifetime. Therefore, re-establishment is a required feature. Revocation of an enrollment certificate is done through an **internal blacklist** at the RA.

5.1.2.1.2 Pseudonym

Pseudonym certificates are used by an OBE primarily for BSM authentication and misbehavior reporting and do not have encryption keys.

Main features of this certificate and the provisioning process are: **pseudonymity**, **location privacy** via LOP, **butterfly keys**, **shuffling of requests** at RA, **linkage values** from pair of LAs, and revocation using **CRLs**. For privacy reasons, an OBE is given multiple certificates that are valid simultaneously, so that it can change them as often as necessary and possible. For further details about pseudonym certificates and their provisioning process, see the SCMS design. There is a one-to-one mapping of (PSID, SSP) combination from enrollment certificates to pseudonym certificates.

Note: If additional applications besides V2V-Safety are required, additional sets of privacy-preserving certificates may be required. The level of privacy and linkability might depend on the level of privilege provided to the certificate holder. This is a policy decision to be made by the SCMS Manager.

5.1.2.1.3 Identification

Identification certificates are used by an OBE primarily for authorization in V2I applications. None of the current V2I applications require encryption by the OBE at the application level; however, there might be a need in the future. OBE identification certificates may use an encryption key that is determined by the butterfly key mechanism. The provisioning process of identification certificates is very similar to that of pseudonym certificates, except for different PSIDs and other parameters, such as the number of certificates and their validity duration. As there are no pseudonymity constraints for identification certificates, an OBE has **only one** identification certificate valid at a time for a given application. While pseudonymity and tracking is no concern, identity certificates still protect the privacy of a user and do not contain any privacy sensitive information such as VIN or owner's name. Certificates for consecutive time periods might overlap. Just like pseudonym certificates, **butterfly keys** are used to facilitate automatic pre-generation of identification certificates by the RA. Revocation of identification certificates is done through **CRLs**. There is a one-to-one mapping of the (PSID, SSP) combination from enrollment certificates to identification certificates.

5.1.2.2 Road-Side Equipment (RSE)

5.1.2.2.1 RSE Enrollment

An enrollment certificate is like a passport for the RSE in that it uses the enrollment certificate to request application certificates. It does not have an encryption key. It is provided to the RSE during its **bootstrap** process. Each enrollment certificate has at least one PSID; however, an RSE cannot have more than one enrollment certificate associated with a particular (PSID, SSP) combination. In cases where an enrollment certificate has more than one PSID, the corresponding apps are expected to be similar in nature. Such groupings of PSIDs in an enrollment certificate are likely to be related to policy decisions to be made by the SCMS Manager. Enrollment certificates have a validity period expected **not** to cover the RSE's full operational lifetime. Therefore, re-establishment is a required feature. The certification process needs to include geographic limits, application classes, etc. Revocation of an enrollment certificate is done through an **internal blacklist** at the RA.

5.1.2.2.2 Application

Application certificates are used by an RSE for authentication and encryption; therefore, they might have **encryption keys**. As there are no privacy constraints for RSEs, an RSE has **only one** application certificate valid at a time for a given application. Moreover for continuity reasons, an RSE may be given up to one extra application certificate that is valid for the next time period (i.e., say the validity period is one day, then an RSE will have only one certificate valid for today and up to one certificate valid for tomorrow). Revocation of application certificates are dependent on their validity periods:

1. **Short validity periods** (e.g., daily, hourly) require frequent certificate renewal, and hence, **no CRL** except under exceptional circumstances

2. **Long validity periods** (e.g., monthly, annually) require **CRLs**.

Note that for PoC, only option #1 will be used and implemented since RSEs are assumed to have a regular online connection to renew certificates.

5.1.2.3 SCMS Component

The elector, root CA, PCA, and ICA certificates are of explicit type to support P2P distribution, and while all other certificates can be of implicit type, they have been kept explicit to remove any confusion. There are no privacy constraints for any of the SCMS component certificates. A SCMS component may be given extra certificates that are valid for the next time period and overlap with the current certificate due to continuity reasons in operations. Revocation of these certificates is done through **CRLs** issued by CRL Generator.

5.1.2.3.1 Electors

Elector certificates are not part of the PKI hierarchy of the SCMS, i.e., verifying a certificate chain in the system does not involve verifying elector certificates. They are used primarily for root CA certificate management, including adding and removing a root CA. They will probably use cryptographic algorithms different from the rest of the system, preferably quantum-safe algorithms, to provide a recovery option in case quantum computers become a reality. The signature on the elector certificate does not have any cryptographic value as the signature is by the elector itself, and, therefore, the trust in an elector certificate is established through out-of-band means. Elector certificates do not have an encryption key as electors are mostly offline and do not accept any incoming messages, whether encrypted or not. Elector certificates must be made available to everyone in the system. As elector certificates are self-signed, the integrity of the initial set of electors must be ensured by other means, other than the cryptography used in generating the certificate itself, such as tamper-proof hardware and software validation of elector messages. For the same reason, the initial provisioning of elector certificates is done through out-of-band means in a secure environment during enrollment. Subsequent updating of elector certificates can be done in-band through e.g., revocation and adding by using the elector model as explained in Elector-based Root Management.

5.1.2.3.2 Root CA

The root CA certificate is different from all other types of certificates in many ways:

1. It is the end of trust chain, i.e., verification of any certificate in the system ends at verifying this certificate
2. The signature on the root CA certificate does not have any cryptographic value as the signature is by the root CA itself, and, therefore, the trust in a root CA certificate is established through out-of-band means
3. Usually the root CA certificate has a long lifetime, as changing a root CA certificate is a time consuming, and potentially expensive operation

4. Only a quorum of electors can issue root management messages and add them to a CRL to revoke a root CA certificate

A root CA certificate does not have an encryption key as the root CA is mostly offline and does not accept any incoming messages, whether encrypted or not. The root CA certificate needs to be made available to everyone in the system. Also, for the reason explained in (2) above, integrity of a root CA certificate must be ensured by other means, other than the cryptography used in generating the certificate itself, such as tamper-proof hardware and software validation of elector messages. For the same reason, the initial provisioning of the root CA certificate is done through out-of-band means in a secure environment during enrollment. Subsequent updating of root CA certificates can be done in-band through e.g., revocation or adding by using the elector model as explained in Elector-based Root Management.

5.1.2.3.3 ICA

ICA certificates can be used to only issue certificates to other SCMS components and nothing else. Only the root CA or the ICA can issue, or authorize someone to issue, a CRL to revoke an ICA certificate.

5.1.2.3.4 ECA

As mentioned above, ECA certificates are of **explicit** type as they do not need to be distributed through P2P distribution. ECA certificates can be used to only issue certificates to end-entities including OBEs and RSEs. These certificates have an encryption key. Revocation of ECA certificate is done through **CRLs** issued by the CRL Generator.

5.1.2.3.5 PCA

PCA certificates can be used to only issue certificates to end-entities including OBEs and RSEs. PCA certificates need to have validity periods that are at least as long as the longest validity certificates issued using them. These certificates have an encryption key. Revocation of PCA certificate is done through **CRLs** issued by CRL generator.

5.1.2.3.6 CRL Generator

CRL generator certificates are issued by the root CA and can be used only to sign CRLs, and nothing else. As revocation of CRL generator certificates is difficult (i.e., can be done by either root CA or ICA), the validity period of the CRL generator certificates is kept as low as possible. For a given CRACA and CRL series, there is **only one** valid CRL generator certificate at any time, except for a short overlap time as defined in PoC Certificate Expiration Timelines and CV Pilot PROD Certificate Expiration Timelines.

5.1.2.3.7 Policy Generator

Policy generator certificates are issued by the root CA and can be used only to sign the global policy configuration files that are distributed to SCMS components. The policies around validity are the same as for CRL generator certificates.

5.1.2.3.8 Other

These include LA, MA, and RA certificates. These certificates **cannot** be used to issue certificates. They are described are as follows:

5.1.2.3.8.1 LA Certificates

Can be short as LAs do not interact with end-entities. These certificates do not have encryption keys. To receive encrypted messages, the owner of these certificates can include an ephemeral response encryption key in the request messages.

5.1.2.3.8.2 RA Certificates

Must be long enough so that end-entities can successfully make a certificate provisioning request after being bootstrapped. These certificates have an encryption key.

5.1.2.3.8.3 MA Certificates

Needs to be long so that end-entities do not need to retrieve these certificates very often. These certificates have an encryption key.

5.1.2.4 EE Certificate Type Features

The following table provides an overview of the EE certificate types. 'X' describes mandatory features, and '(x)' describes optional features. The table provides a comprehensive overview. The following are assumptions for the POC:

- All RSEs have regular connectivity. Hence, case 5.b is not implemented
- The response by the PCA is not encrypted for case 3 and case 5

Table 2 Certificate Type Features

	OBE Enrollment Certificate	OBE Pseudonym Certificate	OBE Identification Certificate	RSE Enrollment Certificate	RSE Application Certificate	
					RSE with Connectivity	**RSE without Connectivity**
Provisioning	1 per EE per PSID category	20 per week, up to 3 years, top-up refresh using butterfly keys	1 per time period, only issue very small number of certificates at a time, top-up refresh using butterfly keys	1 per EE per PSID category	1 per time period, only issue for short time periods, require frequent renewal. RSE generates public/private key pair and provides	1 per time period, issue longer time periods. RSE generates public/private key pair and provides public-key to RA

	OBE Enrollment Certificate	OBE Pseudonym Certificate	OBE Identification Certificate	RSE Enrollment Certificate	RSE Application Certificate	
					public-key to RA	
Revocation	RA blacklist	leverage linkage values	add certificate digests of all issued certificates (can be more than one)	RA blacklist	Cannot renew certificates, due to RA blacklist of enrollment certificate	Add certificate digest of all issued certificates (can be more than one)
Response is Encrypted by PCA		X	X		X	X
Shuffle in RA		X				
CRL for End-entity Devices (Certificates of this type can be listed on CRL)		X	X			X
Simultaneous Validity for given PSID		X	only allow minimal overlap to account for critical events			
Linkage Values		X				
Butterfly Keys		X	X			
Continued Generation		X	X			
Issuing Certificates for Multiple Time Periods		X	X			
Pseudonymity	X	X				
Misbehavior Reporting		X	X		X	X

	OBE Enrollment Certificate	OBE Pseudonym Certificate	OBE Identification Certificate	RSE Enrollment Certificate	RSE Application Certificate	
Non-Traceability		X				
Encryption Key			(X) (determined using butterfly key mechanism)		X	

5.1.2.5 Requirements

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-1311	CLOSED	Issue only one OBE identification certificate valid at a time	PCA shall only issue one OBE identification certificate to an OBE that is valid at a time for a given application.	There is no need for privacy (by definition).		PCA
SCMS-1312	CLOSED	Issue RSE application certificates with optional encryption key	PCA shall issue RSE application certificates with optional encryption key.	The encryption key is optional.	RSE application certificates always have a signature key and optionally an encryption key.	PCA
SCMS-1313	CLOSED	Issue only one RSE application certificate valid at a time	PCA shall only issue one RSE application certificate to an RSE valid at a time for a given application, except for the allowed overlap period.	There is no need for privacy.		PCA
SCMS-1314	MANUAL PROCESS	SCMS component certificate types (implicit vs. explicit)	The SCMS component shall have a certificate of explicit type.	Implicit: OBE Enrollment, RSE Enrollment, Pseudonym,	Details discussed in certificate types	CRL Store, CRLG, DCM, IBLM, ICA, LA, PCA, PG, RA, RCA

Key	Status	Summary	Description	Justification	Notes	Component/s
				Application, Identification Explicit (Self Signed): RootCA, Elector Explicit: Everything else PCA, ICA, Root CA, and elector certificates need to be of explicit type in order to support P2P distribution. All the EE certificates are of implicit type to save storage space and over-the-air bytes, and all the SCMS Component certificates are of explicit type.		
SCMS-1315	MANUAL PROCESS	Only 1 certificate valid at a time	Each SCMS component shall have only 1 valid and in-use certificate at a time.	There are no privacy concerns for SCMS components that would justify more than one certificate valid at a given time. At the same time, it is desirable to keep complexity		CRL Store, CRLG, DCM, ECA, IBLM, ICA, LA, PCA, PG, RA

Key	Status	Summary	Description	Justification	Notes	Component/s
				low and have maximum control over components, hence allowing exactly one certificate at a given time.		
SCMS-1316	SCMS POC OUT OF SC OPE	Additional SCMS component certificate for the next time period	Each SCMS component shall be allowed to request and receive a certificate that is valid for the next time period at a time defined by the certificate policy given by the SCMS Manager.	To allow continuity of secure communication between SCMS components.	The additional certificate is likely requested by the SCMS component towards the end of the current time period.	CRL Store, CRLG, DCM, ECA, IBLM, ICA, LA, PCA, PG, RA

6 issues

5.1.2.6 PoC Certificate Expiration Timelines

5.1.2.6.1 Goals

1. Establish a reasonable root certificate expiration period by shortening the EE Enrollment certificate expiration period from previous 30 years as mentioned in the Vehicle Safety Communications Security Studies Project (VSCS)
2. Allow EE to use their existing enrollment certificate for authentication when requesting a rollover enrollment (Re-enrollment) certificate
3. Minimize the number of root certificates that are valid at any time

5.1.2.6.2 Assumptions

1. Vehicles have an estimated life of up to 30 years
2. EEs may only have connectivity once every three years
3. Initial EE enrollment certificates and rollover certificates are issued by the ECA
4. Only one enrollment certificate for an EE shall be valid at a time
5. EE must request and download the rollover certificate before the current certificate expires

6. Re-enrollment certificates will not be generated or available for download until three years before the expiration of the current enrollment certificate

5.1.2.6.3 Factors Influencing Certificate Lifetimes

Certificate lifetimes affect the security of PKI infrastructures. The longer a public/private key pair is in use, the greater the chances are that the keys can be compromised. As computing power increases and technologies improve over time, cryptanalysis becomes a risk. For these reasons, excessively long-lived CA certificate lifetimes are undesirable.

The below diagram illustrates the calculation of the minimum lifetime of a typical CA certificate.

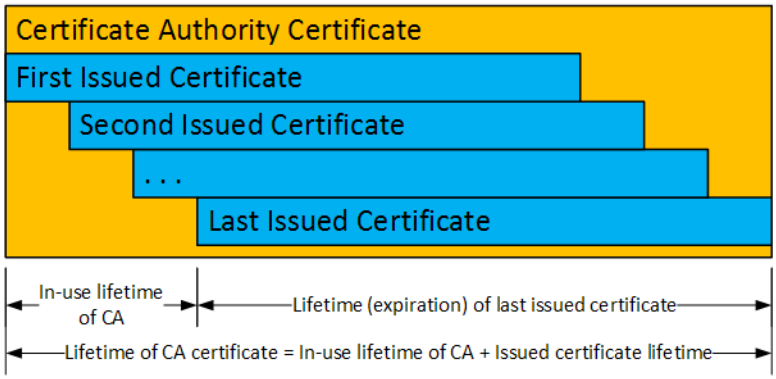


Figure 4 Calculating In-use Lifetime of a Certificate Authority

Some certificate authorities may issue certificates that are not valid until a significant time in the future. Examples of this within the SCMS are pseudonym certificates and rollover enrollment certificates. As a recommendation, the validity lag for these certificates can be up to 3 years. For example, a pseudonym certificate generated (issued) today may have a "Valid from" date that is up to 3 years from now. The below diagram illustrates the impact of the validity lag on the lifetime of the issuing CA certificate.

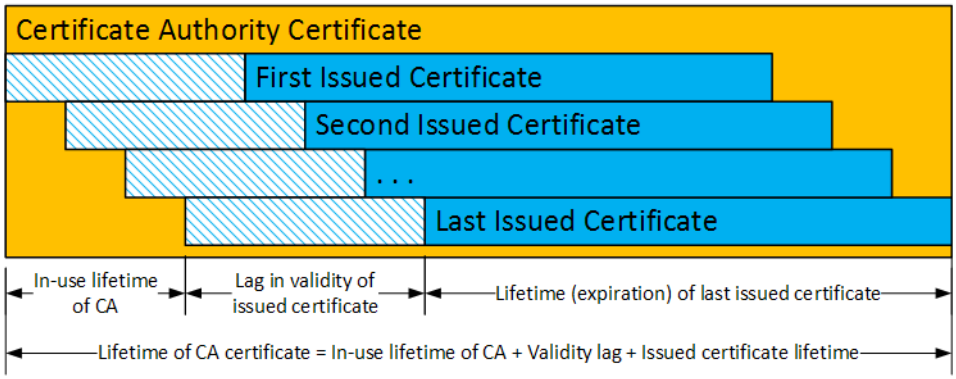


Figure 5 Impact of Lag in Validity of Issued Certificates

As additional layers are added to the certificate hierarchy, this process is repeated up to the root CA. When operational factors and the requirement to have the ability to issue new certificates at any time are considered, the required lifetime of each CA certificate in the trust chain is further increased.

It will be necessary to renew the enrollment certificate multiple times for an estimated vehicle lifetime of 30 years. An enrollment certificate lifetime of 6 years greatly reduces security concerns due to certificate longevity, but it requires an automatic renewal mechanism that can accommodate the EEs with infrequent network connectivity. As better and more frequent network connectivity becomes available to the EEs, it may be possible to further reduce these lifetimes.

The below diagram illustrates the impact of issued certificate lifetime, certificate validity lag and operational factors on the PKI hierarchy.

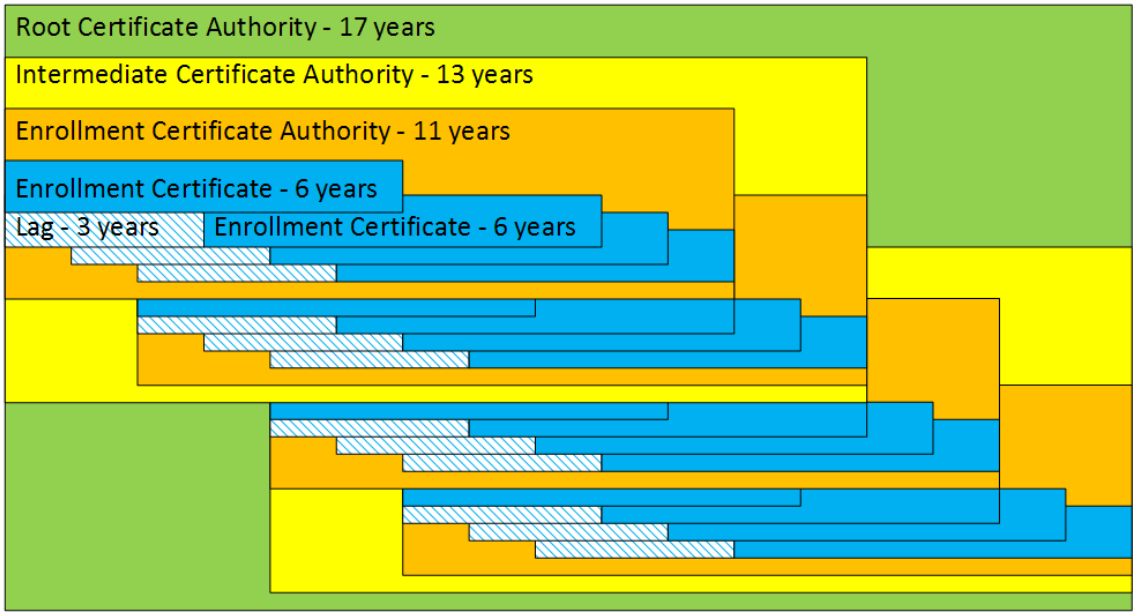


Figure 6 Relationship Between Enrollment and CA Certificate Lifetimes

Establishing a fixed schedule for the expiration of elector certificates, root CA certificate(s), intermediate CA certificates and enrollment CA certificates is recommended to reduce operational complexities. For offline CAs, this procedure increases security by minimizing the frequency of required access. Certificates issued in the middle of this fixed schedule, due to revocation or new instances, will expire according to the defined schedule and will have a reduced overall lifetime due to a shorter in-use lifetime.

The following guidelines shall be followed when component certificates are issued mid-sequence:

- This concept is mandatory for all certificates issued by the root CA and intermediate CA
- The certificate's in-use and expiration shall be reduced by the same amount

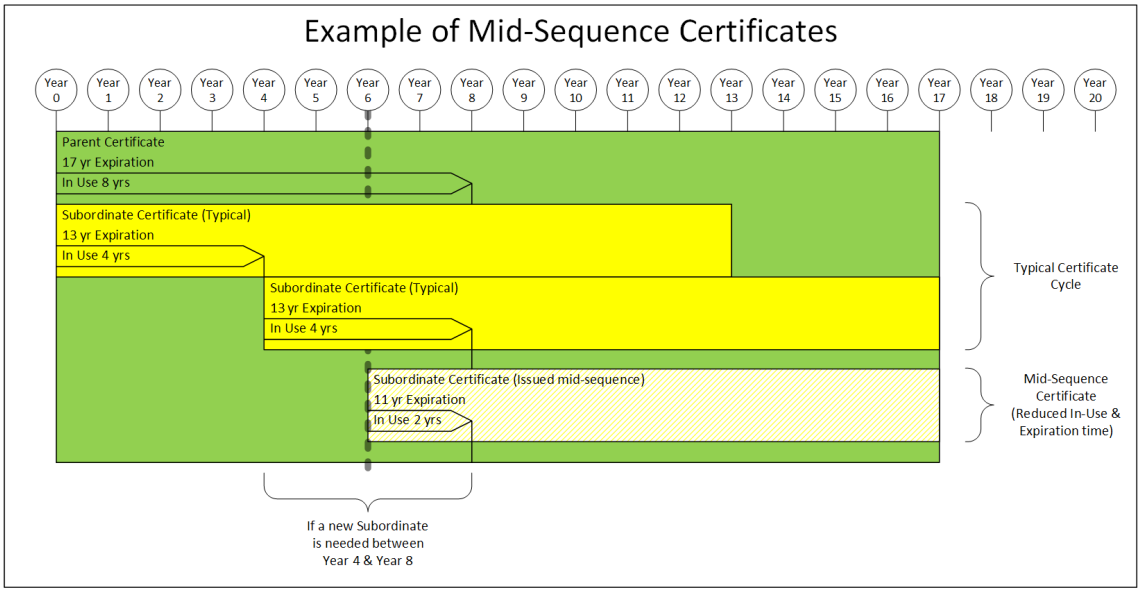


Figure 7 Example of Mid-Sequence Certificates

To ensure the overall integrity of the SCMS, the minimum and maximum lifetime of each certificate type will be defined and enforced by the SCMS manager policy. Operators will have some amount of flexibility in defining the actual certificate lifetimes.

5.1.2.6.4 Certificate Lifetime Overview

The following table provides the certificate expiration and renewal periods to be used in a SCMS that supports EE enrollment certificate rollover.

Table 3 PoC Certificate Expiration Timelines - Certificate Expiration and Renewal

Certificate Type	Issuing CA	Expiration	In Use	Request for Renewal	Start of Validity for Renewal	Number of Concurrently Valid Certificates (In-Use [+ Legacy])	Example Size in Bytes (Certs are Not Fixed Size)	Notes
OBE Enrollment	ECA	6 years	6 years	Anytime (see notes)	6 years	1	87	Rollover certificate will be available no more than 3 years before start of validity.
OBE Pseudonym	PCA	1 week + 1 hour	1 week	Anytime	1 week	20 + 20 (for just 1 hour)	86	
OBE Identification	PCA	1 month + 1 hour	1 month	Anytime	1 month	1 + 1 (for just 1 hour)	89	
RSE Enrollment	ECA	6 years	6 years	Anytime (see notes)	6 years	1	87	Rollover certificate will be available no more than 3 years before start of validity.
RSE Application	PCA	1 week + 1 hour	1 week	Anytime	1 week	1 + 1 (for just 1 hour)	89	
DCM	ICA	3 years + 1 week	3 years	3 months before end of In-Use	3 years	1 + 1 (for just 1 week)	219	
ECA	ICA	11 years	2 years	3 months before end of In-Use	2 years	1 + 5	150	

Certificate Type	Issuing CA	Expiration	In Use	Request for Renewal	Start of Validity for Renewal	Number of Concurrently Valid Certificates (In-Use [+ Legacy])	Example Size in Bytes (Certs are Not Fixed Size)	Notes
RA	ICA	3 years + 1 week	3 years	3 months before end of In-Use	3 years	1 + 1 (for just 1 week)	217	
LA	ICA	3 years + 1 week	3 years	3 months before end of In-Use	3 years	1 + 1 (for just 1 week)	205	
PCA	ICA	4 years	1 year	3 months before end of In-Use	1 year	1 + 3	216	
ICA	Root CA	13 years	4 years	3 months before end of In-Use	4 years	1 + 3	195	
MA	Root CA	4 years + 1 week	4 years	3 months before end of In-Use	4 years	1 + 1 (for just 1 week)	205	
CRLG	Root CA	4 years + 1 week	4 years	3 months before end of In-Use	4 years	1 + 1 (for just 1 week)	190	
Policy Generator (PG)	Root CA	4 years + 1 week	4 years	3 months before end of In-Use	4 years	1 + 1 (for just 1 week)	172	

Certificate Type	Issuing CA	Expiration	In Use	Request for Renewal	Start of Validity for Renewal	Number of Concurrently Valid Certificates (In-Use [+ Legacy])	Example Size in Bytes (Certs are Not Fixed Size)	Notes
Root CA (RCA)	Self	17 years	8 years	3 months before end of In-Use	8 years	1 + 2	211	
Elector	Self	12 years	12 years	3 months before end of In-Use	12 years	3	166	The initial elector certificates have an expiration and "in use" time of 4, 8 and 12 years, respectively.

5.1.2.6.5 Expiration, In-use, and Overlap Requirements

Table 4 Expiration, In-use, and Overlap Requirements

Key	Summary	Description	Justification	Notes	Component/s
SCMS-1412	Destroy certificate's private key	The certificate's private key shall be destroyed at the end of the "In-use" life of a certificate. The in-use lifetime of certificates shall be defined either by SCMS policy and/or based on the expiration and In-use lifetime of subordinate certificates.	To prevent the usage of certificates that have reached the end of defined In-use lifetime.	Out of scope as this needs to be implemented as operational policy.	CRL Store, CRLG, DCM, ECA, ICA, LA, MA, PCA, PG, RA
SCMS-1725	Component certificate FQDN match	The SCMS component shall have a certificate with a certificateId field that matches the FQDN of the component.	FQDN of each component must match the official ID of the component.		CRLG, DCM, ECA, LA, MA, PCA, PG, RA

Key	Summary	Description	Justification	Notes	Component/s
SCMS-1581	Component certificate in-use period	The SCMS component shall use its certificate for an in-use period of 3 years.	Use 3 years for standard SCMS components	Out of scope as this needs to be implemented as operational policy. This is for POC & CV-Pilot only.	CRLG, DCM, LA, MA, PG, RA
SCMS-1319	Component certificate expiration	The component shall request a certificate with a validity of 3 years and 1 week.	Use 3 years for standard SCMS components	This is for POC & CV-Pilot only.	CRLG, DCM, LA, MA, PG, RA
SCMS-1591	ECA certificate validity	ECA shall request an ECA certificate with a validity of 11 years.	To support issuing of subordinate certificates.	This is for POC only.	ECA
SCMS-1307	Enrollment certificate lifetime	ECA shall issue Enrollment Certificates with a lifetime of 6 years.	For PoC, enrollment certificates use a life span of 6 years	This is for PoC only	ECA
SCMS-1809	Elector certificate validity	Elector certificates validity period shall be set to 12 years.	Elector certificates must have an expiration date.	Certificate types and expiration periods are defined in the Certificate Types common requirements section. This is for PoC and CV-Pilot only.	Elector
SCMS-1590	Elector Certificate In-Use period	The Elector certificate In-Use period shall be the same as the Expiration period.	Out of scope as this needs to be implemented as operational policy. To maintain a fixed number of valid Elector at all times.		Elector

Key	Summary	Description	Justification	Notes	Component/s
SCMS-1423	Elector Certificate Expiration	The Technical Component of the SCMS Manager (TCotSCMSM) shall issue Elector certificates with an expiration of 12 years.	Component 1609 certificates shall have a defined expiration.	In the case of the certificate being revoked, the new certificate may have a different expiration to align with predefined replacement schedules (if any exist). For the initial system deployment, 1 of the 3 Electors shall have a certificate expiration of 4 years, another one a certificate expiration of 8 years, to prevent multiple elector certificates from expiring at the same time. These durations are for the SCMS PoC and CV-Pilot only. For other SCMS instances, this duration should be reevaluated.	Elector
SCMS-1597	ICA certificate in-use period	ICA shall use its ICA certificate for an in-use period of 4 years.	The in-use period shall be short to minimize impact, if revocation is required.	Out of scope as this needs to be implemented as operational policy. This is for POC only.	ICA
SCMS-1596	ICA certificate validity	ICA shall request an ICA certificate with a validity of 13 years.	To support issuing of subordinate certificates.	This is for POC only.	ICA

Key	Summary	Description	Justification	Notes	Component/s
SCMS-1595	PCA certificate in-use period	PCA shall use its certificate for an in-use period of 1 years.	The In-use period shall be short to minimize impact if revocation is required.	Out of scope as this needs to be implemented as operational policy. This is for POC & CV-Pilot only.	PCA
SCMS-1594	PCA certificate expiration	PCA shall request a certificate with a validity of 4 years.	The expiration must be sufficiently long to issue pseudonym certificates for 3 years in the future.	This is for POC only.	PCA
SCMS-1416	Certificate Overlap: OBE Identification Certificates	RA shall request PCA to generate OBE identification certificates with an overlap $t_{overlap}$ of one hour.	This is in line with pseudonym certificates. $t_{overlap}$ of 1 hour (60 minutes) reduces the risk of a vehicle operating without a valid certificate.	This is for POC & CV-Pilot only.	RA
SCMS-1415	Certificate Validity: OBE Pseudonym Certificates	RA shall request PCA to generate OBE pseudonym certificates with validity period $t_{validity}$.	This allows flexible certificate handling.	Validity period $t_{validity}$ is currently set to 1 week + 1 hour for POC & CV-Pilot.	RA
SCMS-1370	Certificate Validity: OBE Identification Certificates	RA shall request PCA to generate OBE identification certificates with validity period $t_{validity}$.	This is in line with pseudonym certificates. It allows revocation by not renewing certificates, and does not require a permanent but only regular online connection to renew certificates.	Validity period $t_{validity}$ is currently set to 1 month + 1 hour for POC & CV-Pilot.	RA

Key	Summary	Description	Justification	Notes	Component/s
SCMS-1213	Certificate Validity: RSE Application Certificates	RA shall request PCA to generate RSE application certificates with validity period $t_{validity}$ as defined in rse_application_cert_validity.	As per communications with USDOT, RSEs will have frequent connectivity. Therefore, a short validity period is justified for RSE application certificates.	Validity period $t_{validity}$ is currently set to 1 week for POC & CV-Pilot.	RA
SCMS-1212	Certificate Overlap: RSE Application Certificates	RA shall request PCA to generate RSE application certificates with an overlap $t_{overlap}$ as defined in rse_application_cert_overlap	$t_{overlap}$ of e.g. 1 hour (60 minutes) reduces the risk of a vehicle having to verify another RSE certificate during a critical time period.	This is for POC & CV-Pilot only.	RA
SCMS-526	Certificate Overlap: OBE Pseudonym Certificates	RA shall request PCA to generate OBE pseudonym certificates with an overlap $t_{overlap}$ of one hour.	The original value for $t_{overlap}$ was 1 minute but there are safety concerns with such a small overlap. For example, a device could be in an alert state for more than 1 minute. Extending $t_{overlap}$ to 1 hour (60 minutes) reduces the risk of a vehicle operating without a valid certificate.	This is for POC & CV-Pilot only.	RA
SCMS-1332	Root CA certificate overlap	Root CA certificates shall have an overlap of 9 years (an in-use period of 8 years).	The overlap is necessary to allow rollover.	This is for POC & CV-Pilot only.	RCA
SCMS-1318	Root CA certificate validity	The root CA certificate validity period shall be set to 17 years.	Root CA certificates must have an expiration date. The root CA certificate must be valid	Certificate types and expiration periods are defined in the Certificate Types common	RCA

Key	Summary	Description	Justification	Notes	Component/s
			at least as long as the longest issued enrollment certificate.	requirements section. This is for PoC only.	

21 issues

5.1.2.6.6 Overview Diagrams

The following diagrams illustrate the expiration period of various certificate types. The diagrams show the specific duration of the certificate (valid from and to dates) only and do not account for setup time (request generation, signing ceremony, distribution, etc.). Each section shows the life of a single instance of a component under typical (non-compromised) conditions. If multiple instances exist, they would follow a similar pattern but the specific dates may be shifted within the validity period.

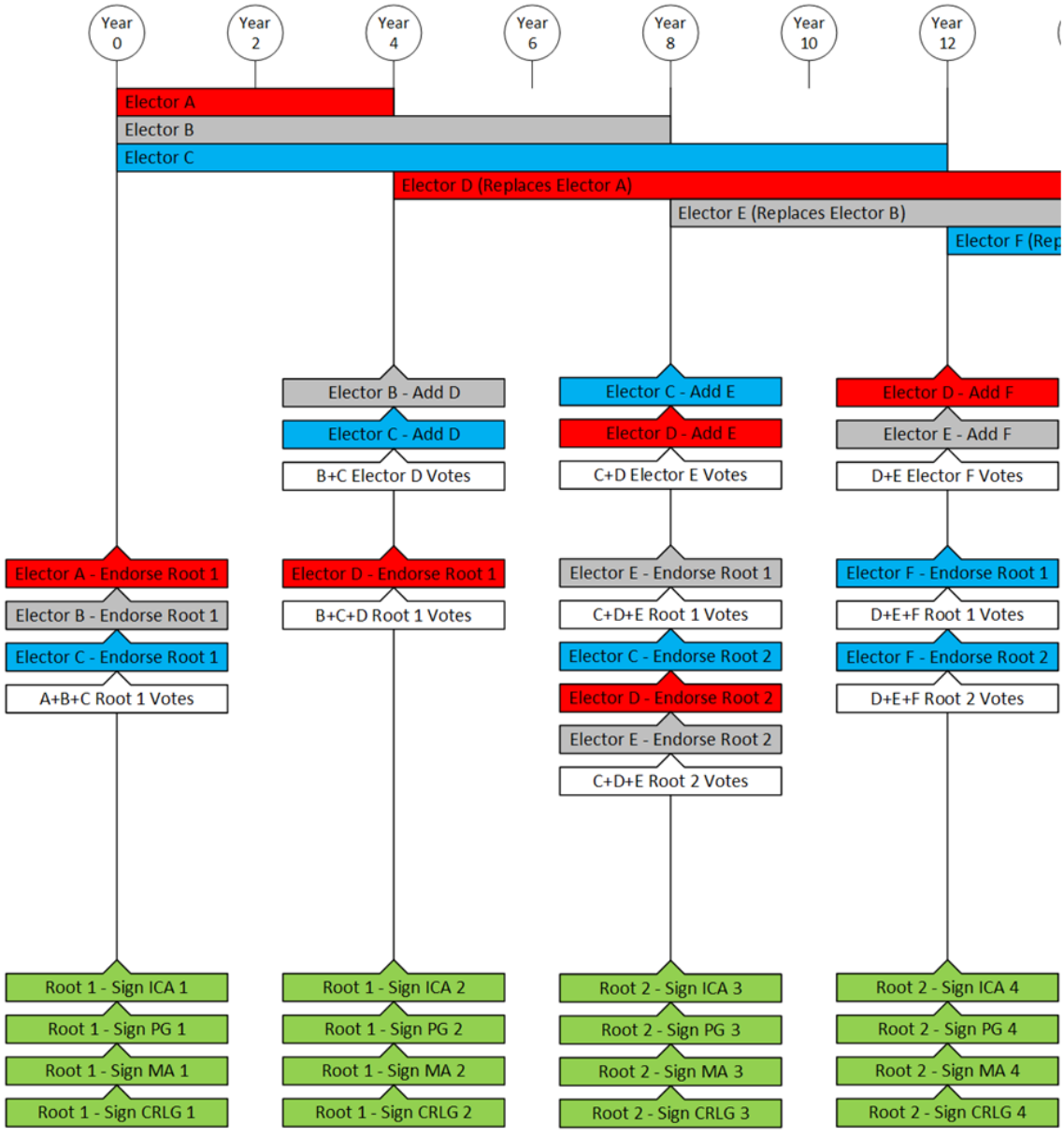


Figure 8 Summary of Elector and Root CA Activities, 1 of 2

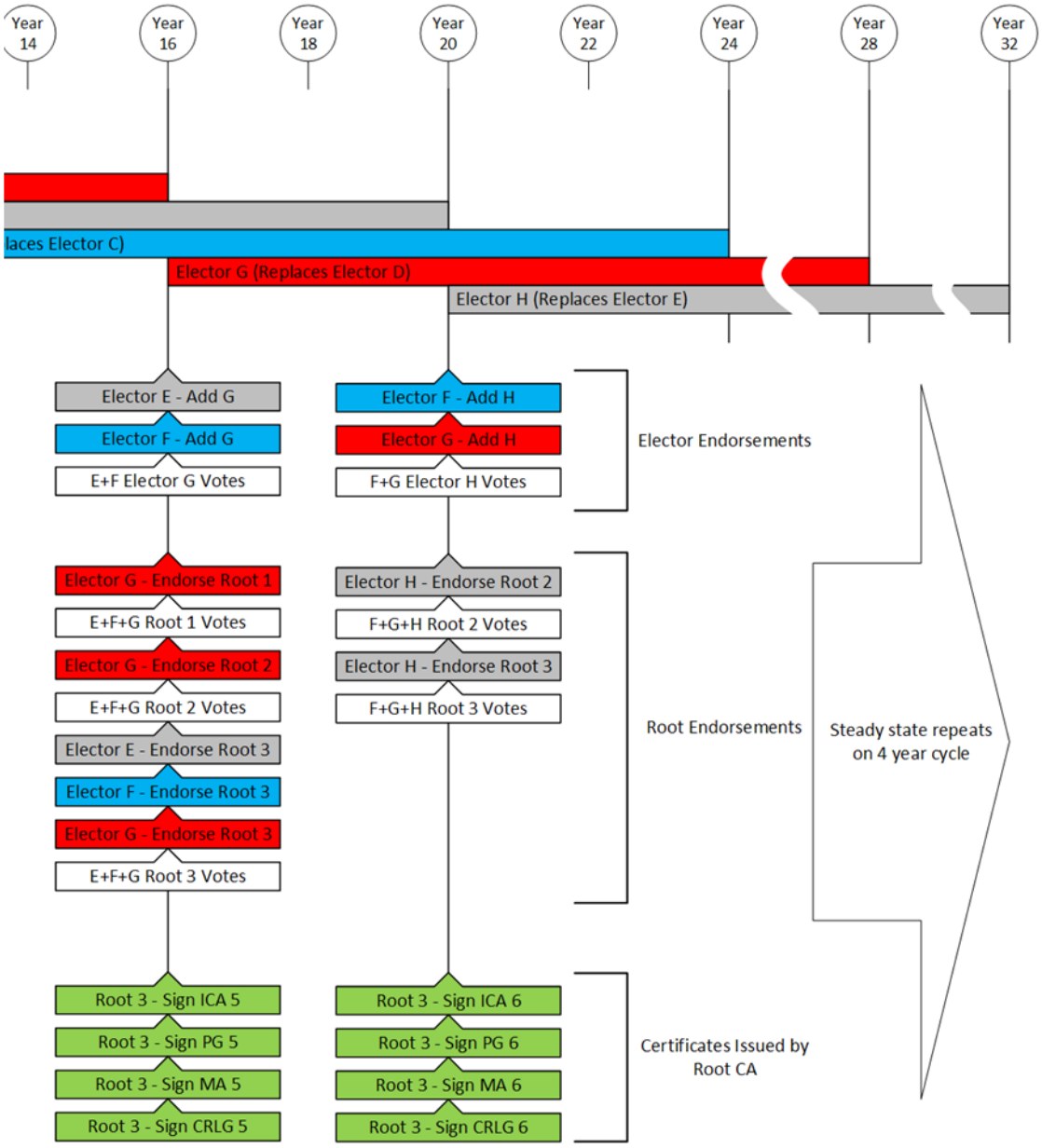


Figure 9 Summary of Elector and Root CA Activities, 2 of 2

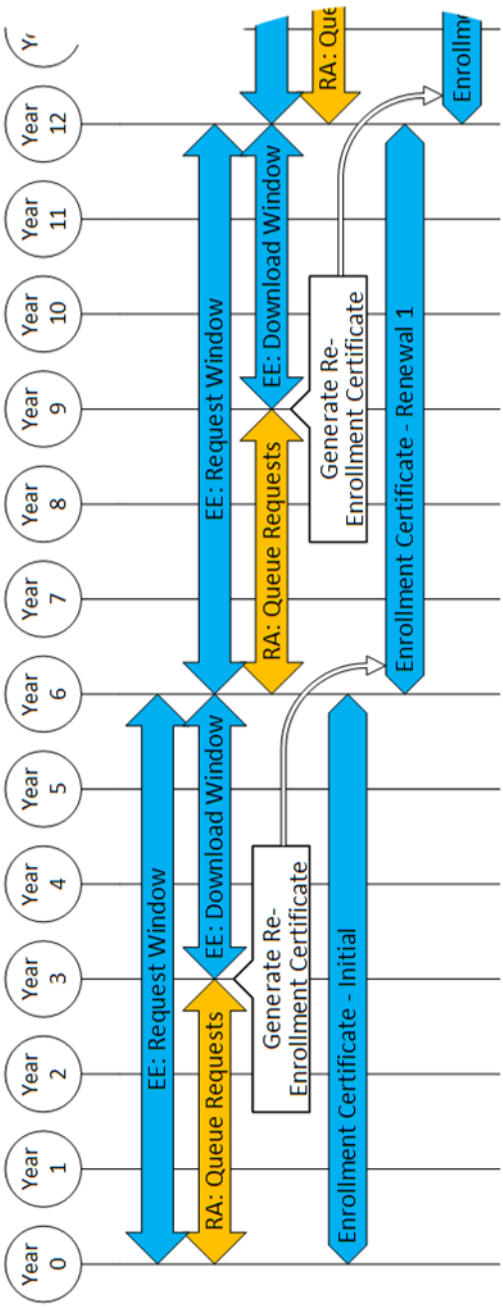


Figure 10 EE Enrollment Rollover Timeline

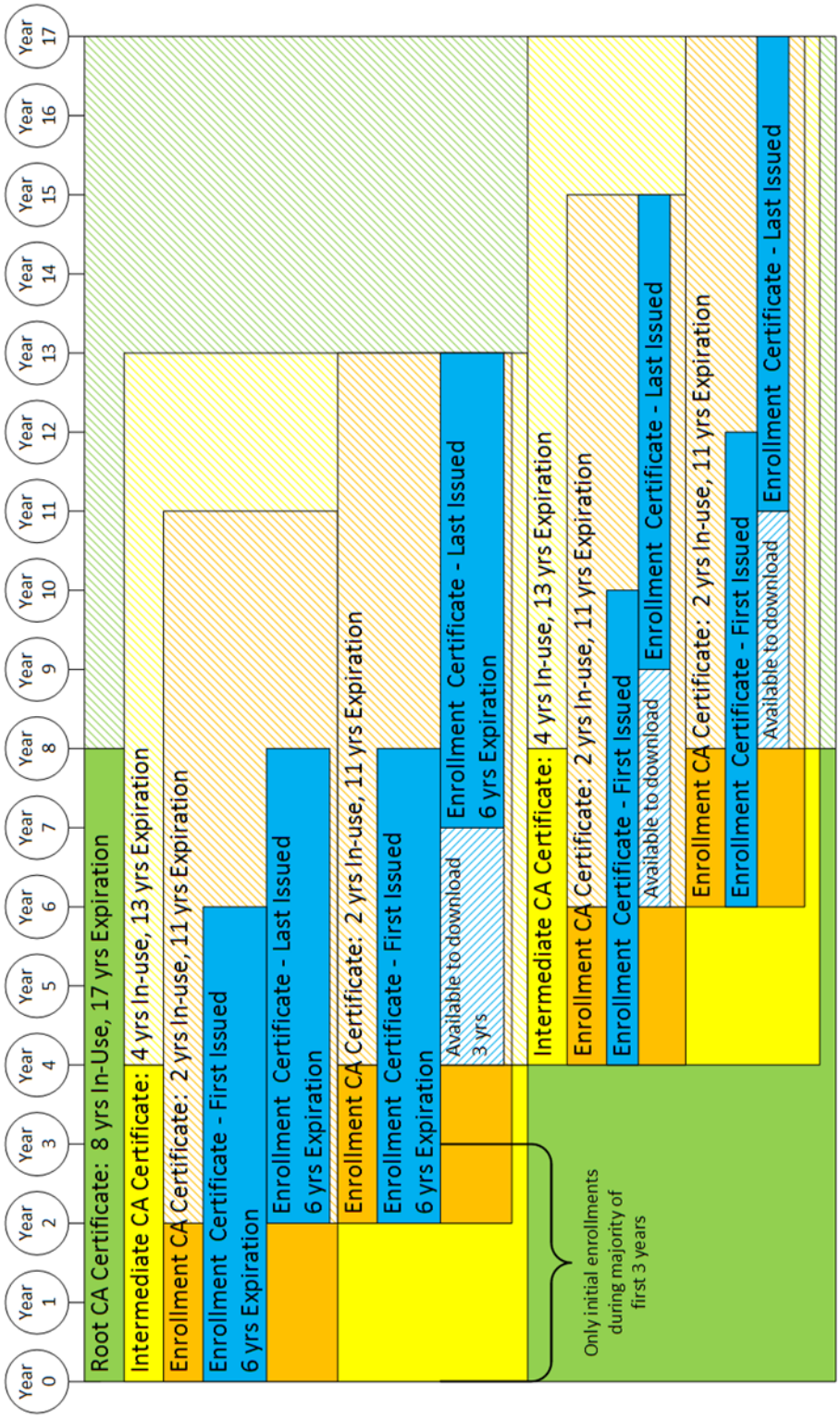


Figure 11 PoC Certificate Expiration Timelines - Overview Diagram, 1 of 3

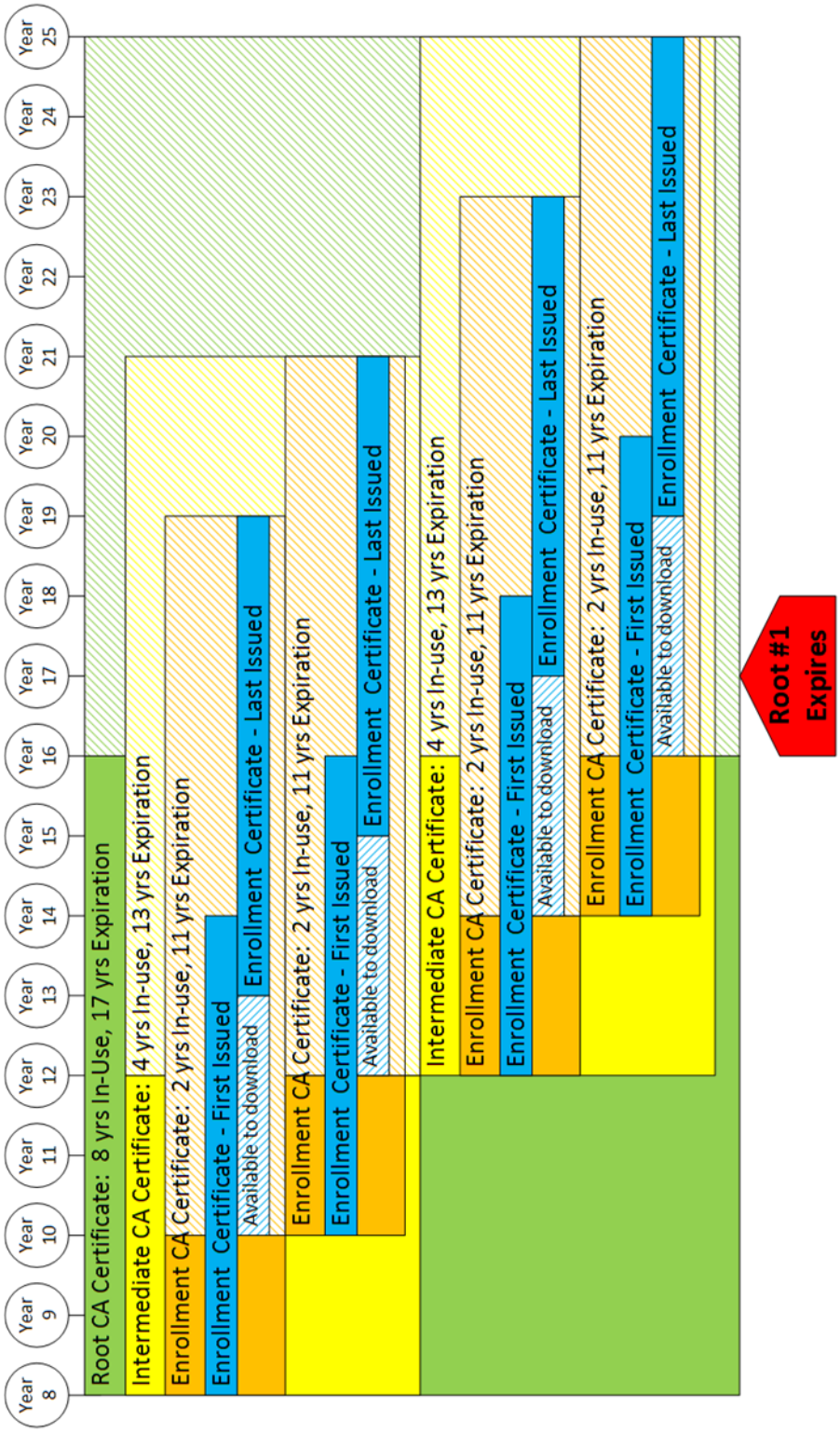


Figure 12 PoC Certificate Expiration Timelines - Overview Diagram, 2 of 3

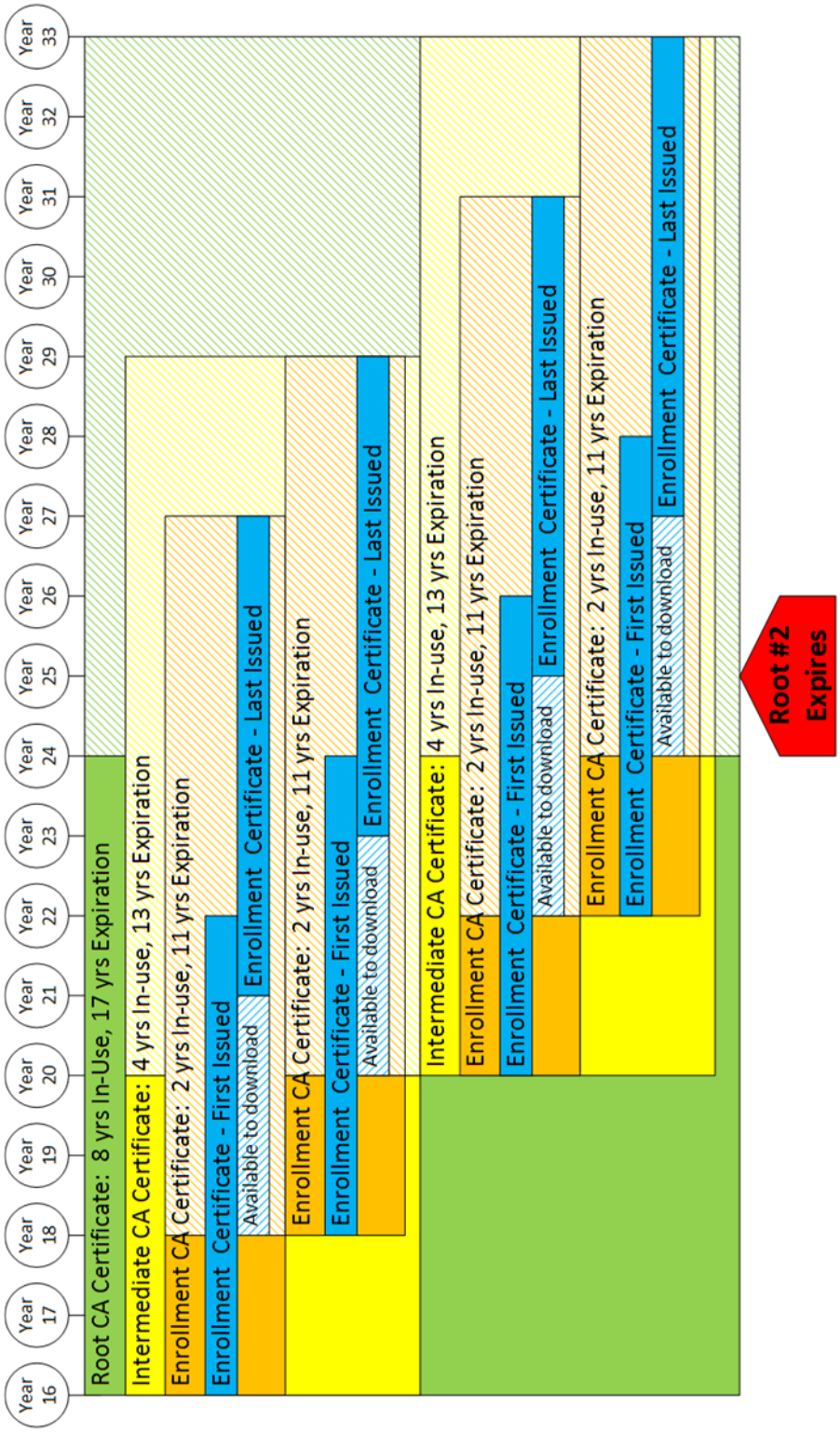


Figure 13 PoC Certificate Expiration Timelines - Overview Diagram, 3 of 3

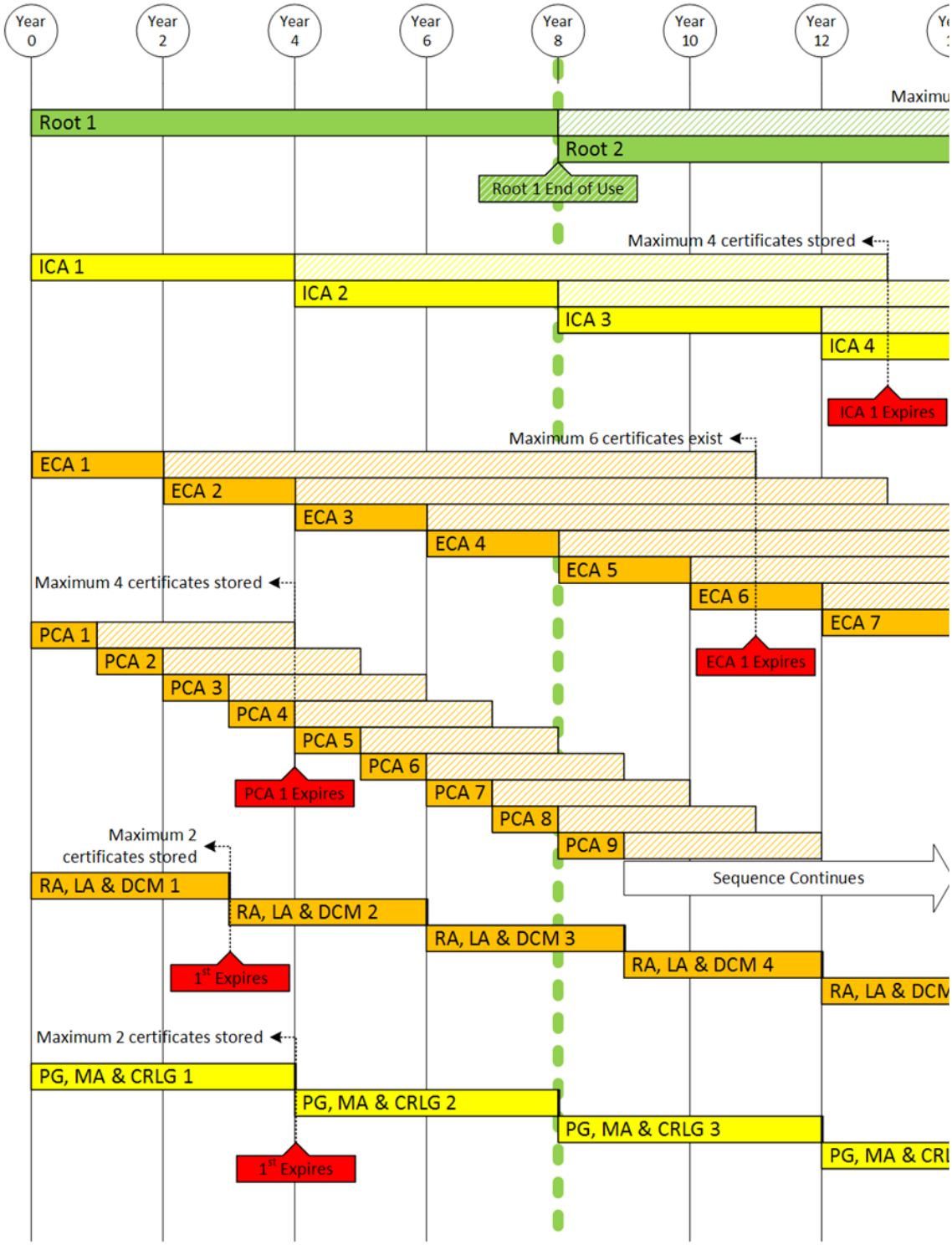


Figure 14 PoC Certificate Expiration Timelines - Stackup, 1 of 3

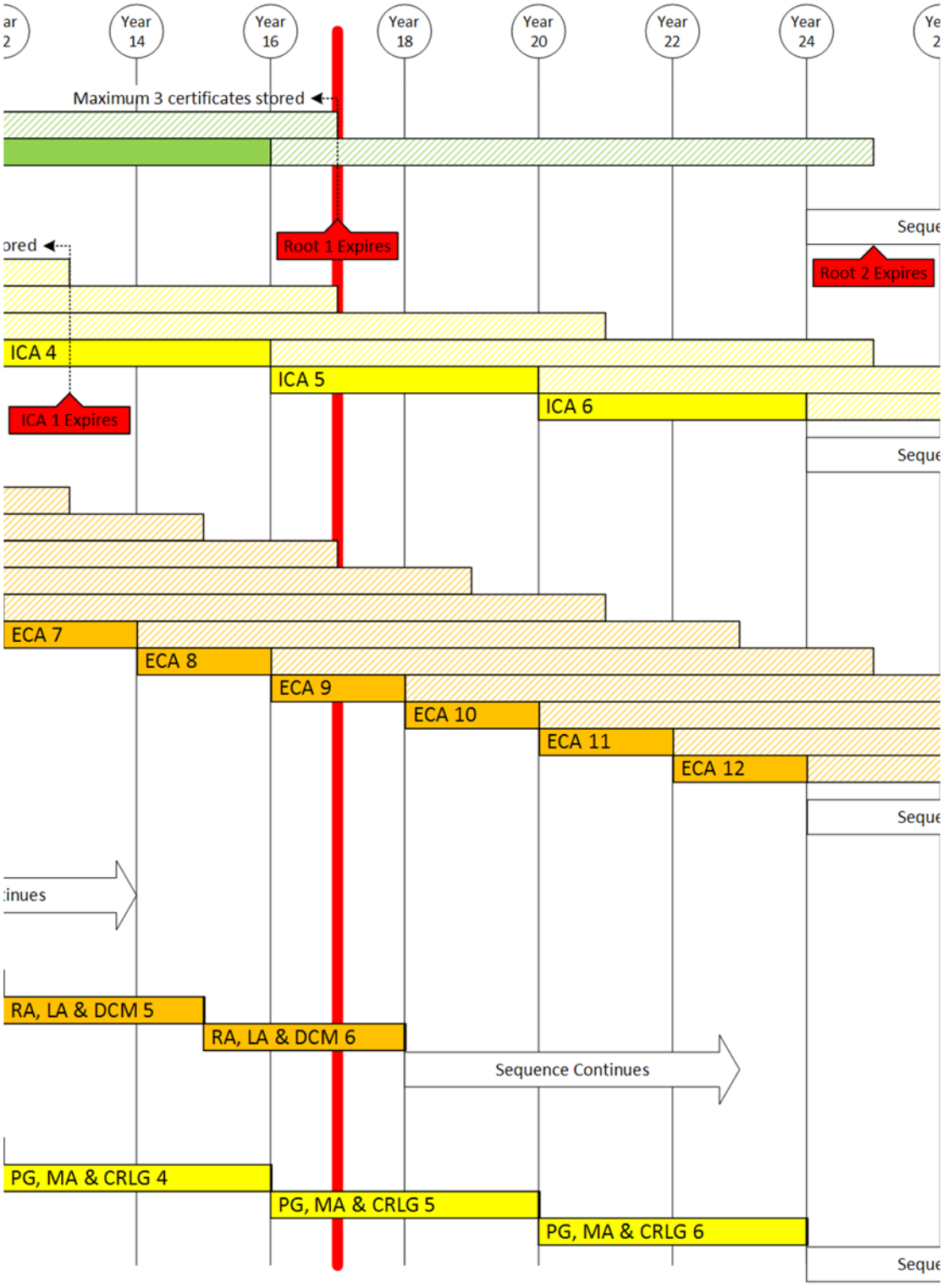


Figure 15 PoC Certificate Expiration Timelines - Stackup, 2 of 3

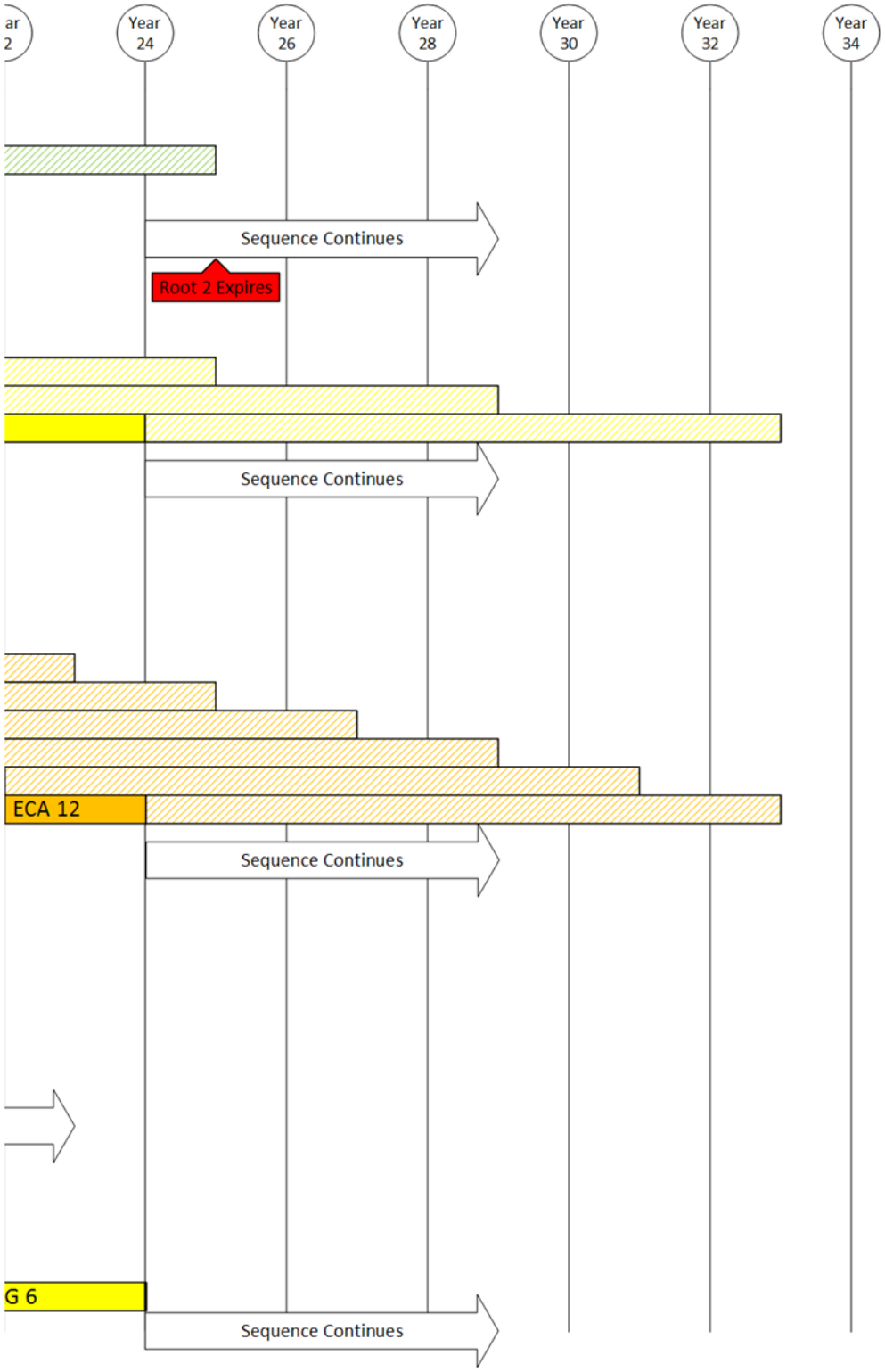


Figure 16 PoC Certificate Expiration Timelines - Stackup, 3 of 3

5.1.2.7 CV Pilot PROD Certificate Expiration Timelines

5.1.2.7.1 Assumptions

- The SCMS instance created for the CV Pilots shall be separate from the SCMS PoC instance
- The ICA and subordinate certificates shall expire on or before 12:00:00 UTC January 3, 2025
    - Estimated project expiration of 00:00:00 UTC January 1, 2025 + 60 hours (due to 1609.2 time unit restrictions)
- No component certificates shall have a starting date after the end of the estimated project duration
- The private keys of all component certificates subordinate to the root shall be destroyed at the end of the estimated project duration
- The root certificate shall have an expiration of 70 years and an in-use lifetime of 20 years to support possible future activities
- All components subordinate to the ICA have an in-use lifetime that is sufficiently short and requires at least one rollover (renewal) event during the estimated project duration
- PKI hierarchy:
    - The ICA, policy generator, CRL generator and MA certificates shall be issued directly by the Root CA
    - The subtree below ICA is identical to that of the POC, i.e., it has one instance of all components: ECA, PCA, DCM, RA, and LA
- Leap seconds declared after 00:00:00 UTC 1/1/2017 are not considered

5.1.2.7.2 Certificate Lifetime Overview

Definitions of available 1609.2 units of time used by certificates can be found in IEEE Std 1609.2-2016, Sections 6.4.14, 6.4.15 and 6.4.16. Note that the "years" duration is defined as a specific number of seconds.

The following tables provide the certificate expiration and renewal periods to be used for the CV pilot, Production instance deployment.

Table 5 CV Pilot Certificate Expiration Timelines - Certificate Expiration

Certificate Generation	**Start** (1609.2 Time32)	**Duration** (1609.2 units)		**Duration** (TAI seconds)	**Expiration** (1609.2 Time32)	**Start** (UTC)	**Expiration** (UTC)	Notes
Root CA Certificate								
	385,689,600	70	years	2,208,986,640	2,594,676,240	23:59:55 March 21, 2016 (Monday)	23:23:55 March 21, 2086 (Thursday)	ISS - Reference only
ICA Certificate								
	410,313,605	1169	sixtyHours	252,504,000	662,817,605	00:00:00 January 1, 2017 (Sunday)	12:00:00 January 1, 2025 (Wednesday)	
ECA Certificates								
1	428,630,405	1084	sixtyHours	234,144,000	662,774,405	00:00:00 August 1, 2017 (Tuesday)	00:00:00 January 1, 2025 (Wednesday)	
2	523,324,805	38736	hours	139,449,600	662,774,405	00:00:00 August 1, 2020 (Saturday)	00:00:00 January 1, 2025 (Wednesday)	Reduced Lifetime
PCA Certificates								
1	428,662,805	35281	hours	127,011,600	555,674,405	09:00:00 August 1, 2017 (Tuesday)	10:00:00 August 10, 2021 (Tuesday)	
2	460,112,405	35113	hours	126,406,800	586,519,205	09:00:00 July 31, 2018 (Tuesday)	10:00:00 August 2, 2022 (Tuesday)	
3	491,562,005	35113	hours	126,406,800	617,968,805	09:00:00 July 30, 2019 (Tuesday)	10:00:00 August 1, 2023 (Tuesday)	

Certificate Generation	Start (1609.2 Time32)	Duration (1609.2 units)		Duration (TAI seconds)	Expiration (1609.2 Time32)	Start (UTC)	Expiration (UTC)	Notes
4	523,011,605	35113	hours	126,406,800	649,418,405	09:00:00 July 28, 2020 (Tuesday)	10:00:00 July 30, 2024 (Tuesday)	
5	554,461,205	30099	hours	108,356,400	662,817,605	09:00:00 July 27, 2021 (Tuesday)	12:00:00 January 1, 2025 (Wednesday)	Reduced Lifetime
6	585,910,805	21363	hours	76,906,800	662,817,605	09:00:00 July 26, 2022 (Tuesday)	12:00:00 January 1, 2025 (Wednesday)	Reduced Lifetime
7	617,965,205	12459	hours	44,852,400	662,817,605	09:00:00 August 1, 2023 (Tuesday)	12:00:00 January 1, 2025 (Wednesday)	Reduced Lifetime
8	649,414,805	3723	hours	13,402,800	662,817,605	09:00:00 July 30, 2024 (Tuesday)	12:00:00 January 1, 2025 (Wednesday)	Reduced Lifetime
RA, LA, DCM Certificates								
1	428,630,405	26472	hours	95,299,200	523,929,605	00:00:00 August 1, 2017 (Tuesday)	00:00:00 August 8, 2020 (Saturday)	Leap Day
2	523,324,805	26448	hours	95,212,800	618,537,605	00:00:00 August 1, 2020 (Saturday)	00:00:00 August 8, 2023 (Tuesday)	
3	617,932,805	12456	hours	44,841,600	662,774,405	00:00:00 August 1, 2023 (Tuesday)	00:00:00 January 1, 2025 (Wednesday)	Reduced Lifetime

Table 6 CV Pilot Certificate Expiration Timelines - Certificate Expiration and Renewal Guidelines

Certificate Type	Issuing CA	Expiration	In Use	Request for Renewal	Start of Validity for Renewal	Number of Concurrently Valid Certificates (In-Use [+ Legacy])	Example Size in Bytes (Certs are Not Fixed Size)	Notes
OBE Enrollment	ECA	Variable	Same as expiration	N/A	N/A	1	87	All OBE enrollment certificates shall be issued with an expiration on or before 12:00:00 UTC January 3, 2025 regardless of the date they are issued
OBE Pseudonym	PCA	1 week + 1 hour	1 week	Anytime	1 week	20 + 20 (for just 1 hour)	91	
OBE Identification	PCA	1 month + 1 hour	1 month	Anytime	1 month	1 + 1 (for just 1 hour)	89	
RSE Enrollment	ECA	Variable	Same as expiration	N/A	N/A	1	109	All RSE enrollment certificates shall be issued with an expiration on or before 12:00:00 UTC January 3, 2025 regardless of the date they are issued
RSE Application	PCA	1 week + 1 hour	1 week	Anytime	1 week	1 + 1 (for just 1 hour)		
Elector	Self	12 years	12 years	3 months before end of In-use	12 years	3 (1 per elector)	166	The initial elector certificates have an expiration and "in use" time of 4, 8 and 12 years, respectively

5.1.2.7.3 Renewal/Rollover Requirements

Table 7 Renewal/Rollover Requirements

Key	Summary	Description	Justification	Notes	Component/s
SCMS-1422	Renewal of component certificate	A SCMS component shall request rollover IEEE 1609.2 certificates no sooner than 3 months prior to the end of the In-use life of the current certificate. A SCMS component shall not issue rollover IEEE 1609.2 certificates prior 3 months to the end of the In-use life of the current certificate.	To prevent the existence of certificates that are not valid until a significant time in the future.	Does not apply to component compromise/revoked situations. For the PoC & CV-Pilot, 3 months is being used. This should be re-evaluated for other deployments.	CRL Store, CRLG, DCM, ECA, ICA, LA, MA, PCA, PG, RA, RCA

1 issue

5.1.2.7.4 Expiration, In-use, and Overlap Requirements

Table 8 Expiration, In-use, and Overlap Requirements

Key	Summary	Description	Justification	Notes	Component/s
SCMS-1412	Destroy certificate's private key	The certificate's private key shall be destroyed at the end of the "In-use" life of a certificate. The in-use lifetime of certificates shall be defined either by SCMS policy and/or based on the expiration and In-use lifetime of subordinate certificates.	To prevent the usage of certificates that have reached the end of defined In-use lifetime.	Out of scope as this needs to be implemented as operational policy.	CRL Store, CRLG, DCM, ECA, ICA, LA, MA, PCA, PG, RA
SCMS-2842	Estimated project expiration	Certificates shall expire on or before 12:00:00 UTC January 3, 2025.	To ensure no certificates are valid beyond the defined project period.	Due to the 1609.2 sixtyHours unit of time, the actual certificate expiration may be up to 60 hours after the estimated project expiration	CRLG, DCM, ICA, LA, MA, PG, RA

Key	Summary	Description	Justification	Notes	Component/s
				of 00:00:00 UTC January 1, 2025. This is for CV-Pilot only.	
SCMS-1725	Component certificate FQDN match	The SCMS component shall have a certificate with a certificateId field that matches the FQDN of the component.	FQDN of each component must match the official ID of the component.		CRLG, DCM, ECA, LA, MA, PCA, PG, RA
SCMS-1581	Component certificate in-use period	The SCMS component shall use its certificate for an in-use period of 3 years.	Use 3 years for standard SCMS components	Out of scope as this needs to be implemented as operational policy. This is for POC & CV-Pilot only.	CRLG, DCM, LA, MA, PG, RA
SCMS-1319	Component certificate expiration	The component shall request a certificate with a validity of 3 years and 1 week.	Use 3 years for standard SCMS components	This is for POC & CV-Pilot only.	CRLG, DCM, LA, MA, PG, RA
SCMS-1605	ECA certificate validity	ECA shall request an ECA certificate with a maximum validity of 8 years +/- 1 week.	To support issuing of subordinate certificates.	1st generation: Start = 428,630,405, Duration = 1,084 sixtyHours This is for CV-Pilot only.	ECA
SCMS-1602	ECA certificate in-use period	ECA shall use its ECA certificate for an in-use period of 3 years.	Use 3 years for Enrollment SCMS components	Out of scope as this needs to be implemented as operational policy. This is for CV-Pilot only.	ECA

Key	Summary	Description	Justification	Notes	Component/s
SCMS-1600	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-1809	Elector certificate validity	Elector certificates validity period shall be set to 12 years.	Elector certificates must have an expiration date.	Certificate types and expiration periods are defined in the Certificate Types common requirements section. This is for PoC and CV-Pilot only.	Elector
SCMS-1590	Elector Certificate In-Use period	The Elector certificate In-Use period shall be the same as the Expiration period.	Out of scope as this needs to be implemented as operational policy. To maintain a fixed number of valid Elector at all times.		Elector
SCMS-1423	Elector Certificate Expiration	The Technical Component of the SCMS Manager (TCotSCMSM) shall issue Elector certificates with an expiration of 12 years.	Component 1609 certificates shall have a defined expiration.	In the case of the certificate being revoked, the new certificate may have a different expiration to align with predefined replacement schedules (if any exist). For the initial system deployment, 1 of the 3 Electors shall have a certificate expiration of 4 years, another one a certificate expiration of 8	Elector

Key	Summary	Description	Justification	Notes	Component/s
				years, to prevent multiple elector certificates from expiring at the same time. These durations are for the SCMS PoC and CV-Pilot only. For other SCMS instances, this duration should be reevaluated.	
SCMS-1604	ICA certificate in-use period	ICA shall use its ICA certificate for the entire validity period of the certificate.	The In-use period shall be short to minimize impact if revocation is required.	Out of scope as this needs to be implemented as operational policy. This is for CV-Pilot only.	ICA
SCMS-1603	ICA certificate validity	ICA shall request an ICA certificate with a maximum validity of 8 years +/- 1 week.	To support issuing of subordinate certificates.	Start = 410,313,605 Duration = 1,169 sixtyHours This is for CV-Pilot only.	ICA
SCMS-2843	PCA certificate expiration	PCA shall request a certificate with a maximum validity of 4 years +/- 2 weeks.	The expiration must be sufficiently long to issue pseudonym certificates for 3 years in the future.	1st generation: Start = 428,630,405, Duration = 1,084 sixtyHours This is for CV-Pilot only.	PCA
SCMS-1595	PCA certificate in-use period	PCA shall use its certificate for an in-use period of 1 years.	The In-use period shall be short to minimize impact if revocation is required.	Out of scope as this needs to be implemented as operational policy. This is for POC & CV-Pilot only.	PCA

Key	Summary	Description	Justification	Notes	Component/s
SCMS-1416	Certificate Overlap: OBE Identification Certificates	RA shall request PCA to generate OBE identification certificates with an overlap $t_{overlap}$ of one hour.	This is in line with pseudonym certificates. $t_{overlap}$ of 1 hour (60 minutes) reduces the risk of a vehicle operating without a valid certificate.	This is for POC & CV-Pilot only.	RA
SCMS-1415	Certificate Validity: OBE Pseudonym Certificates	RA shall request PCA to generate OBE pseudonym certificates with validity period $t_{validity}$.	This allows flexible certificate handling.	Validity period $t_{validity}$ is currently set to 1 week + 1 hour for POC & CV-Pilot.	RA
SCMS-1370	Certificate Validity: OBE Identification Certificates	RA shall request PCA to generate OBE identification certificates with validity period $t_{validity}$.	This is in line with pseudonym certificates. It allows revocation by not renewing certificates, and does not require a permanent but only regular online connection to renew certificates.	Validity period $t_{validity}$ is currently set to 1 month + 1 hour for POC & CV-Pilot.	RA
SCMS-1213	Certificate Validity: RSE Application Certificates	RA shall request PCA to generate RSE application certificates with validity period $t_{validity}$ as defined in rse_application_cert_validity.	As per communications with USDOT, RSEs will have frequent connectivity. Therefore, a short validity period is justified for RSE application certificates.	Validity period $t_{validity}$ is currently set to 1 week for POC & CV-Pilot.	RA
SCMS-1212	Certificate Overlap: RSE Application Certificates	RA shall request PCA to generate RSE application certificates with an overlap $t_{overlap}$ as defined in rse_application_cert_overlap	$t_{overlap}$ of e.g. 1 hour (60 minutes) reduces the risk of a vehicle having to verify another RSE certificate during a critical time period.	This is for POC & CV-Pilot only.	RA

Key	Summary	Description	Justification	Notes	Component/s
SCMS-526	Certificate Overlap: OBE Pseudonym Certificates	RA shall request PCA to generate OBE pseudonym certificates with an overlap $t_{overlap}$ of one hour.	The original value for $t_{overlap}$ was 1 minute but there are safety concerns with such a small overlap. For example, a device could be in an alert state for more than 1 minute. Extending $t_{overlap}$ to 1 hour (60 minutes) reduces the risk of a vehicle operating without a valid certificate.	This is for POC & CV-Pilot only.	RA
SCMS-1332	Root CA certificate overlap	Root CA certificates shall have an overlap of 9 years (an in-use period of 8 years).	The overlap is necessary to allow rollover.	This is for POC & CV-Pilot only.	RCA

22 issues

5.1.2.7.5 Overview Diagrams

The following diagrams illustrate the expiration period of various certificate types. The diagrams show the specific duration of the certificate (valid from and to dates) only and do not account for setup time (request generation, signing ceremony, distribution, etc.). Each section shows the life of a single instance of a component under typical (non-compromised) conditions. If multiple instances exist, they would follow a similar pattern but the specific dates may be shifted within the validity period. Lifetimes may be adjusted in the future to account for leap seconds, rounding requirements or operational requirements.

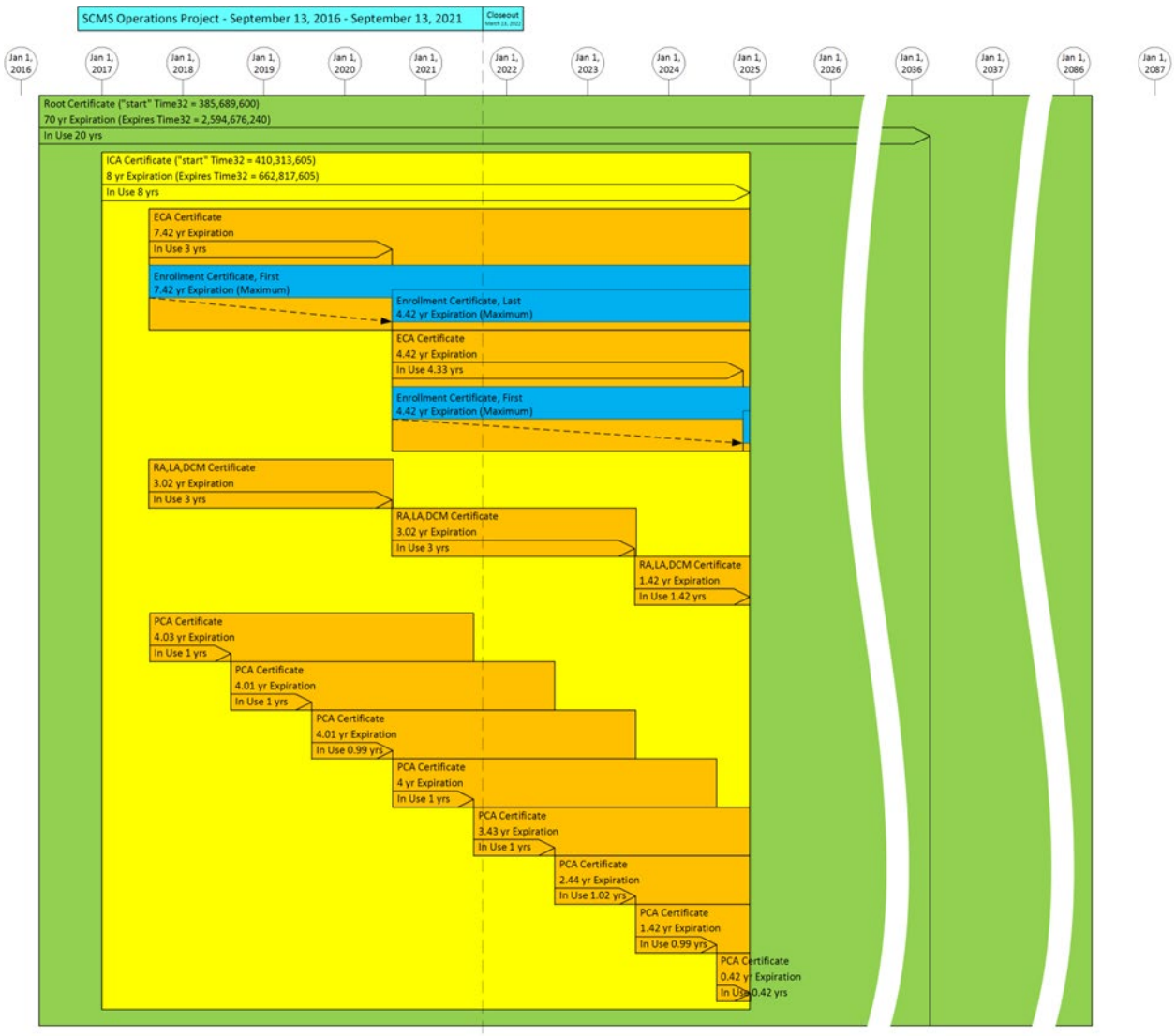


Figure 17 Illustration of the Expiration Period of Various Certificate Types

5.1.2.8 CV Pilot QA+Test Certificate Expiration Timelines

5.1.2.8.1 Assumptions

- The SCMS instance created for the CV Pilots shall be separate from the SCMS PoC instance
- The estimated duration of the CV Pilot project shall be seven years
- All EE-specific CV Pilot certificates shall expire by the end of the estimated project duration
- No component certificates shall have a starting date after the end of the estimated project duration
- The private keys of all component certificates subordinate to the root shall be destroyed at the end of the estimated project duration
- All components subordinate to the ICA have an in-use lifetime that is sufficiently short and requires at least one rollover (renewal) event during the estimated project duration
- PKI hierarchy:
    - The ICA, policy generator, CRL generator and MA certificates shall be issued directly by the Root CA
    - The subtree below ICA is similar to that of the POC, i.e., it has one instance of all components: ECA, PCA, RA, and LA, but no DCM. There might be a DCM introduced at a later stage.

5.1.2.8.2 Certificate Lifetime Overview

The following table provides the certificate expiration and renewal periods to be used for CV pilot deployments.

NOTE for certificate example sizes: FQDN range was 14-23 bytes, and at most 2 PSID's (4 bytes each) were used where applicable.

Table 9 CV Pilot Certificate Expiration Timelines - Certificate Expiration and Renewal

Certificate Type	Issuing CA	Expiration	In Use	Request for Renewal	Start of Validity for Renewal	Number of Concurrently Valid Certificates (In-Use [+ Legacy])	Example Size in Bytes (Certs are Not Fixed Size)	Notes
OBE Enrollment	ECA	6 months	6 months	anytime	variable, max 6 months	1	87	
OBE Pseudonym	PCA	1 week + 1 hour	1 week	Anytime	1 week	20 + 20 (for just 1 hour)	91	Limit pseudo cert load to 6 months (520 certs)
OBE Identification	PCA	1 month + 1 hour	1 month	Anytime	1 month	1 + 1 (for just 1 hour)	89	
RSE Enrollment	ECA	1 year	1 year	anytime	variable, max 1 yr	1	109	
RSE Application	PCA	1 week + 1 hour	1 week	Anytime	1 week	1 + 1 (for just 1 hour)		
DCM	ICA	2 years + 1 week	2 years	3 months before end of In-use	2 years	1 + 1 (for just 1 week)	219	
ECA	ICA	3 years	2 years	3 months before end of In-use	2 years	1 + 1	150	
RA	ICA	2 years + 1 week	2 years	3 months before end of In-use	2 years	1 + 1 (for just 1 week)	217	

Certificate Type	Issuing CA	Expiration	In Use	Request for Renewal	Start of Validity for Renewal	Number of Concurrently Valid Certificates (In-Use [+ Legacy])	Example Size in Bytes (Certs are Not Fixed Size)	Notes
LA	ICA	2 years + 1 week	2 years	3 months before end of In-use	2 years	1 + 1 (for just 1 week)	205	
PCA	ICA	1.5 years	1 year	3 months before end of In-use	1 year	1 + 1 (for 6 months)	216	
ICA	Root CA	5 years	4 years	3 months before end of In-use	4 years	1 + 1 (for 1 yr)	195	
MA	Root CA	2 years + 1 week	2 years	3 months before end of In-use	2 years	1 + 1 (for just 1 week)	205	
CRLG	Root CA	2 years + 1 week	2 years	3 months before end of In-use	2 years	1 + 1 (for just 1 week)	190	
Policy Generator	Root CA	2 years + 1 week	2 years	3 months before end of In-use	2 years	1 + 1 (for just 1 week)	172	
Root CA	Self	9 years	8 years	3 months before end of In-use	8 years	1 + 1 (for 1 yr)	211	

Certificate Type	Issuing CA	Expiration	In Use	Request for Renewal	Start of Validity for Renewal	Number of Concurrently Valid Certificates (In-Use [+ Legacy])	Example Size in Bytes (Certs are Not Fixed Size)	Notes
Elector	Self	6 years	6 years	3 months before end of In-use	6 years	3 (1 per elector)	166	At start, electors are staggered, so first expiration's are 2, 4, 6 yrs - The initial elector certificates have an expiration and "in use" time of 2, 4 and 6 years, respectively; and thereafter 6 years with their renewals.

5.1.3 Hardware, Software and OS Security Requirements

5.1.3.1 Overview and Goals

This document describes hardware, software, and operating system security for systems that run DSRC applications and use cryptographic private keys and certificates in the format specified by IEEE Standard 1609.2-2016 and that are issued by the Security Credentials Management System (SCMS).

The security requirements apply to two logically distinct sets of functional blocks:

- **Privileged applications**: These applications run autonomously (i.e., do not require human intervention to start running) and either send or receive signed messages. They run on the **host processor**.
- **Cryptographic operations**: These operations use secret keys from symmetric cryptographic algorithms, or private keys from asymmetric cryptographic algorithms. They run on the **Hardware Security Module (HSM)**.

The goals of these requirements are:

1. Different privileged applications can have different sets of keys such that:
    a. A privileged application is able to sign with its own keys
    b. A privileged application is not able to sign with keys reserved for use by a different privileged application
    c. Non-privileged applications do not have any access to keys that are reserved for use by privileged applications
2. No application has read access to key material – all key material is execute- or write-only
3. Keys used for verification are protected against unauthorized replacement
4. The system supports software/firmware update in such a way that the above properties continue to hold

This document does not address processes for certifying that systems meet the requirements. Its purpose is simply to state the requirements.

5.1.3.2 Architecture

The requirements below cover three architectures.

- **Integrated architecture**: The host processor and the HSM are the same processor
- **Connected architecture**: The host processor and the HSM are different, but they are physically connected using a connector that connects only those two processors. The only way to read or write data flowing between the two processors is by physically tapping into that connector.
- **Networked architecture**: The host processor and the HSM are different and connected over a network or bus that has other processors connected to it

The document provides requirements for the host processor and the HSM separately and then provides architecture-specific requirements for the different architectures.

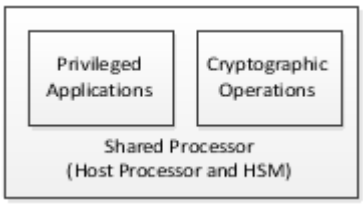


Figure 18 Integrated Architecture

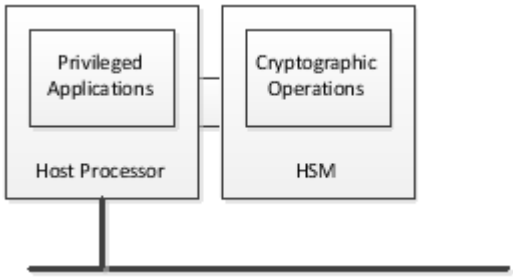


Figure 19 Connected Architecture

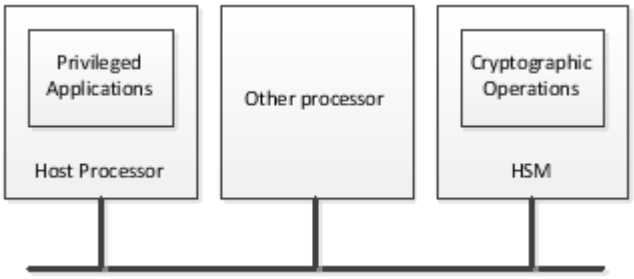


Figure 20 Networked Architecture

5.1.3.3 Host Processor

5.1.3.3.1 Manufacturing and Operational States

The host processor and its software shall be delivered in an *operational state* that implements all the protections below.

The host processor may be initialized while in a *manufacturing state* that does not implement all the protections.

A device may be designed so it can return from the operational state to the manufacturing state. If this functionality is provided, the transition shall wipe all privileged applications from the host processor and all keys from the HSM. The device

may allow a user to perform a reset to a manufacturing state without any authentication if the mechanism for a reset guarantees that the user is physically present.

5.1.3.3.2 Secure Boot

The host processor shall perform integrity checks on boot to ensure that it is in a known good software state. The integrity checks shall require the use of a hardware-protected value such that the integrity cannot be successfully compromised unless the hardware-protected value is modified. Examples of these integrity checks include signing the software such that the verification key is protected by hardware, or storing hashes via the Platform Configuration Registry (PCR) mechanism of the Trusted Computing Group's (TCG) Trusted Platform Module (TPM).
The host processor integrity check shall verify the software and firmware configuration of the host processor such that:

- The host processor shall not allow any privileged application to sign until the integrity checks have passed
- If the host processor fails the integrity checks, it shall not grant access for any process to private keys
- If the host processor fails the integrity checks, it shall not allow any privileged application to operate

The host processor integrity check shall carry out a check that stored root CA certificates have not been modified since they were last accessed.

- If this integrity check fails, the device shall reject all incoming signed messages that chain back to those root CA certificates as invalid.

5.1.3.3.3 Operating System

The host processor operating system shall meet the following requirements (derived from FIPS 140-2 section 4.6.1):

- The operating system shall support roles, which are used as specified below. Each privileged application shall map to a role.
- The discretionary access control mechanisms of the operating system shall be configured to:
    - Specify the set of roles that has execute permissions on each private key stored within the HSM
    - Specify the set of roles that can modify (i.e., write, replace, and delete) programs and plaintext data stored at specific locations within the host processor boundary
    - Specify the set of roles that can read data stored within the host processor boundary and what data can be read by those roles

    - Specify the set of roles that can enter cryptographic keys (It is permissible for the host to require that all keys are generated on the device and that keys cannot be entered directly)
- The OS shall allow the following roles to operate without explicit authentication by a user:
    - Processes that correspond to privileged applications, i.e., applications that are intended to run without user initiation or intervention, and that have execute access to private keys
    - Processes that update private key material to the HSM, i.e., to implement the butterfly key process specified within the SCMS documentation
- The OS may allow the following roles to operate without explicit authentication or may require authentication:
    - Processes that install new software or firmware if that software or firmware is signed
    - Processes that write private key material to the HSM (It is permissible for the host to require that all keys are generated on the device and that keys cannot be entered directly)
- The OS may support the following roles and, if it supports them, shall require explicit authentication:
    - Processes that modify or inspect executing processes
- The OS shall not allow the following roles to exist:
    - Processes that read private cryptographic key material from the HSM (NOTE: The HSM as well must not provide this functionality)

5.1.3.3.4 Secure Updates

The host processor shall use the following mechanisms to ensure that its software and firmware can be securely updated:

- The host processor requires that all software installed be signed. When requested to install software, the host processor OS ensures that the software is signed by an authority with appropriate permissions before proceeding with the installation and rejects the installation if the signature or any of the validity checks on the software or its signing certificate fail.
    - If this approach is taken, the integrity of the verification key shall be protected by local hardware, either by directly storing the key in local hardware, or by creating a chain of trust from the key to a hardware-protected key. The hardware protection shall be equivalent to FIPS 140-2 at the level appropriate to the device as a whole.
- In addition, the host processor may require that only an authenticated user can install software.

The update mechanism shall include mechanisms to prevent updates being rolled back.

5.1.3.4 HSM

The HSM shall meet the requirements for an operating system given in FIPS 140-2 Level 2 except for the audit requirements and certain additional exceptions. The baseline requirements are the following:

- All cryptographic software and firmware shall be developed and installed in a form that protects the software and firmware source and executable code from unauthorized disclosure and modification
- A cryptographic mechanism using an approved integrity technique (e.g., an approved message authentication code or digital signature algorithm) shall be applied to all cryptographic software and firmware components within the HSM
    - The message authentication code may be used in the following circumstances only:
        - If the HSM itself calculates the MAC when the software is installed using a secret key known only to the HSM and uses this secret key to verify the software on boot
        - If the software or firmware provider has a unique shared key with each distinct device and uses this to authenticate the software

A Message Authentication Code (MAC) may not be used to protect the software unless the MAC key is unique to the HSM.

- All cryptographic software and firmware, cryptographic keys, and control and status information shall be under the control of an operating system that meets the functional requirements specified in the protection profiles listed in FIPS 140-2 Annex B and is capable of evaluation at the CC evaluation assurance level EAL2, or an equivalent trusted operating system
- To protect plaintext data, cryptographic software and firmware, cryptographic keys, and authentication data, the discretionary access control mechanisms of the operating system shall be configured to:
    - Specify the set of roles that can execute stored cryptographic software and firmware
    - Specify the set of roles that can modify (i.e., write, replace, and delete) the following cryptographic module software or firmware components stored within the cryptographic boundary: cryptographic programs, cryptographic data (e.g., cryptographic keys and audit data), and plaintext data
    - Specify the set of roles that can read the following cryptographic software components stored within the cryptographic boundary: cryptographic data (e.g., cryptographic keys and audit data), and plaintext data
    - Specify the set of roles that can enter cryptographic keys

- The discretionary access control mechanisms may allow a role without explicit authorization to create a new cryptographic key by combining an existing key with new input if the device follows the Integrated or Connected Architectures. The discretionary access control mechanisms shall require explicit authorization to create a new cryptographic key by combining an existing key with new input if the device follows the Networked Architecture.
- The discretionary access control mechanisms may allow a role without explicit authorization to execute stored cryptographic software and firmware if the device follows the Integrated or Connected Architectures. The discretionary access control mechanisms shall require explicit authorization to execute stored cryptographic software and firmware if the device follows the Networked Architecture.
- The discretionary access control mechanisms of the OS may allow automated software and firmware update if that update is carried out by a process that includes cryptographic checks to ensure the validity of the update prior to installation.
- The operating system shall prevent all operators and executing processes from modifying executing cryptographic processes (i.e., loaded and executing cryptographic program images). In this case, executing processes refer to all non-operating system processes (i.e., operator-initiated), cryptographic or not.
- The operating system shall prevent operators and executing processes from reading cryptographic software stored within the cryptographic boundary.

5.1.3.4.1 Hardware Protection

A HSM that requires low confidentiality and medium integrity shall store keys in tamper-evident hardware equivalent to FIPS 140-2 level 2.

A HSM that requires medium confidentiality and medium integrity shall store keys in tamper-evident hardware equivalent to FIPS 140-2 level 3.

5.1.3.4.2 Random Number Generator

An HSM shall use a random number generator from the list of approved random number generators in FIPS 140-2 Annex C.

5.1.3.5 Architecture-specific Requirements

5.1.3.5.1 Integrated Architecture

An integrated processor has no additional requirements beyond the ones identified above.

5.1.3.5.2 Connected Architecture

A connected processor has no additional requirements beyond the ones identified above.

5.1.3.5.3 Networked Architecture

In addition to the requirements identified above, the host processor must authenticate itself to the HSM with an authentication mechanism based in hardware with the same physical security level as the HSM itself.

5.1.3.6 Secure Environment for Device Enrollment

5.1.3.6.1 Overview and Goals

All End Entities (EEs) that participate in the SCMS must be enrolled. The enrollment process is the point where an initial trust relationship is established between a new EE (either an OBE or RSE) and the rest of the SCMS infrastructure. The integrity of the system requires that only authorized devices are allowed to enroll and that each EE receives the correct credentials to operate with the infrastructure. Therefore, the enrollment process must be performed in a secure environment using an approved process and equipment.

This guidance applies to the equipment and procedures used in the bootstrapping procedures defined in Use Case 2, respectively Use Case 12.

5.1.3.6.2 Architecture

The secure environment used for device enrollment requires the following elements:

1. A documented procedure for performing the enrollment process
2. A physically secure location where the enrollment will take place
3. One or more authorized devices (computers) for managing the enrollment process
4. An activity log or recording of the enrollment operations that were performed

5.1.3.6.2.1 Documented Procedure

The procedure used to enroll devices shall be documented and followed consistently. It is recommended that a checklist or automated procedure be used to ensure consistency and compliance. The procedure shall include the following cases:

1. List of Authorized Operators and Equipment
    a. Each facility must maintain a list of authorized personnel and equipment that may participate in the enrollment and provisioning process
    b. The means of identifying individuals and systems shall be specified
    c. The procedures for adding and removing personnel and equipment from the authorized list shall be part of the documented procedure
    d. The list of authorized personnel shall include a list of auditors (and procedures for adding and removing auditors) who can observe the process
2. Acceptance of a New EE
    a. Authorized operators (or an automated process) must be able to validate that the new EE, that is to be enrolled, is an authentic device. For example,

this may be done by checking the device serial number against a manifest or by inspecting key features of the devices.

b. If the EE employs tamper evident packaging, operators must inspect the tamper seals to ensure that they have not been compromised

c. The software or firmware installed in the EE must be checked to confirm that it is running an allowed version. It is recommended that a secure hash of the installed software be checked against a trusted reference to validate that it has not been modified.

d. If the EE has the capacity to run a self-test to confirm correct operation, the successful result of this test shall be confirmed

e. Refer to PCI HSM Security Requirements version 3.0 (June 2016), Section I (Device Security Requirements During Manufacturing) for additional guidance on validating the EE to be provisioned

3. Connection to the EE

a. During the bootstrapping process, certain information must be transferred with high integrity. The procedure must describe how an operator (or automated process) can validate that a trusted connection has been established to the new EE. For example, a physical cable connection that can be visually inspected is acceptable.

b. If a wireless connection is to be used, the procedures must describe how the connection to the EE will be secured. This connection must provide authenticity and secrecy and it must prevent against replay of old, valid messages. Standard protocols may be used, if their authentication and encryption mechanisms meet these requirements.

4. Key Generation or Injection

a. The enrollment process requires that each EE generate or receive a private key and the corresponding public key. This procedure must be initiated and completed in a secure environment and follow the 'level 2' requirements defined in FIPS PUB 140-2 Section 4.7 for key generation and secure key management.

b. The association of the device public key to the EE must be securely established. It is recommended that the Certificate CSR be generated on the target EE and exported using the secure connection established in #3. Alternative approaches must define a procedure to ensure that the private key used to generate the CSR is correctly associated with the EE.

5. Enrollment Certificate and Parameter Installation

a. The enrollment process requires the installation of one or more root CA certificate and elector certificates into the EE's secure storage. This must be performed in a secure environment using the high-integrity communications channel established in #3.

6. Creation of an Activity Log
    a. The documented procedure shall describe the steps that shall be taken to log or record the enrollment process. Note that the log may not include any private keys or seeding material used to initialize any device.
7. Exceptions and Changes
    a. The procedures shall define what steps are to be taken in case of an error or failure. This should include guidelines for repair or secure decommissioning of failed equipment.
    b. Changes or exceptions to the enrollment procedure shall be recorded.

5.1.3.6.2.2 Secure Environment

The enrollment process shall take place within a physically secure location with restricted access control. Alternatively, the procedures may be carried out in an open area with active monitoring or surveillance to ensure that only authorized individuals and equipment are involved. Refer to the PCI Physical Security Requirements version 2 (Nov 2016) Section 3 for guidelines for establishing a physically secure area for secure provisioning.

- Only authorized personnel shall be able to initiate the enrollment process or have access to the equipment used for enrollment
- Only authorized equipment shall be connected (wired or wireless) to any network, system, or OBE involved in the enrollment process
- The access control mechanism (or area monitoring) must keep a log of who is present in the area at any time when the enrollment process is active

5.1.3.6.2.3 Authorized Equipment

Only specific, authorized equipment shall be used in the enrollment process. This equipment may include one or more general-purpose computers.

- The equipment shall not be used for any purpose other than EE enrollment or related logging, testing, or quality control procedures
- This equipment shall operate on a network segment that is protected from other general-purpose systems used for any other purpose
- Only authorized personnel may access the equipment or install software, updates, or patches to the equipment. All approved and validated security patches shall be applied to all authorized systems.
- The operating system and application software shall be specified in the section Documented Procedures

5.1.3.6.2.4 Audit and Activity Log

The ability for independent auditors to observe a secure process in real-time as well as logs that can be used to reconcile events or audit procedures later are both required to

ensure accountability and to recover from newly emerging threats. The secure environment shall support process oversight in the following ways:

1. Each enrollment location shall maintain a log that records the results of the steps defined in the section Documented Procedures. It must be possible to reconcile enrollment activity against a list of authorized, operational EEs along with any securely scraped or in-repair units to account for the final destination of all successfully enrolled device identities.
2. Authorized and identified independent auditors shall have access to the secure environment in order to periodically supervise and inspect the ongoing procedures. Auditors shall not directly view or record any secret information such as private keys or random number seed values.

5.1.3.7 Storage Considerations

5.1.3.7.1 High Availability and Standard Availability Storage

Our understanding is that there are at least the following grades of data storage medium for automotive electronics systems.

- ROM stores code for use by ECUs and is written only once
- EEPROM stores code for use by ECUs and may be overwritten a limited number of times
- Flash stores code and persistent data for use by ECUs and may be overwritten a (relatively) large number of times. It is more expensive than ROM or EEPROM
- There may also be other grades of storage. Our understanding is that there is a spectrum of storage media from highly reliable and highly expensive (which are referred to as “automotive grade”) to less reliable but cheaper storage (which are referred to as “standard grade”). For example, infotainment systems may use less-reliable, cheaper storage to allow more storage to be provided.

The following are assumptions:

1. Automotive-grade storage is so expensive that less than 1 MB will be available
2. Standard-grade storage will also be available and that it will be sufficiently cheap to be provided in larger volumes, 100 MB or more
3. Executable security and security management codes can be provided in a form that does not use the automotive-grade flash

5.1.3.7.2 Secure Storage

- The OBE needs to store the following in the highly available memory (encrypted):
    - Local private keys for signing
    - Local CSR signing key

    - Any symmetric keys used for certificate management, i.e. for expanding the butterfly keys
    - Seed butterfly key
- If the OBE does not encrypt its certificates, there may be an attack that allows them to be read from storage, which in turn allows the OBE to be tracked. However, an attacker with this level of access to the OBE can probably carry out other attacks. There is no requirement for certificates to be encrypted in place as long as they are integrity-checked.
- The OBE needs to provide integrity checks on the encrypted stored values noted above and also on the following:
    - Root certificates
    - Its own local certificates (if not encrypted)
    - Any certificates used for validating software updates
- It is assumed that an arbitrary amount of automotive-grade storage can be converted to secure storage by using a hardware security module that stores a content encryption and authentication key.
    - Integrity checks can be provided on a block wise basis rather than per data element. This reduces the storage overhead for integrity checks but increases the cost to check an integrity check (the entire block must be checked) and requires that the integrity check for the entire block is recalculated if any single element is changed.
    - The content encryption key should be protected by TPM-like mechanisms so it can only be accessed if the software platform is in a known good state

5.1.4 Elector-based Root Management

After a root CA certificate's validity period ends or a revocation was necessary and a new root CA certificate has been established for replacement, how can an EE start trusting this new root CA certificate? The trust in an initial root CA certificate is implicit, as it is installed in a secure environment with out-of-band communication during bootstrapping of the device. One option would be to get the device back to that secure environment and use out-of-band communication to install the new root CA certificate. However, this is suboptimal due to the required effort and will render the overall V2X system partly out-of-order until all devices have installed the new certificate.

To manage the root CA certificate over time and gain resilience against compromises on any level, the SCMS needs the ability to heal itself, which means to bring itself into a state where it can endure another single compromise or end of the validity period of a Root CA. This recovery should occur while keeping the devices operational whenever possible, that is, capable of sending, receiving and validating BSMs, and be able to restore the system hierarchy without requiring physical access to devices. Elector-

based Root Management is the solution that provides those means by installing a distributed management schema on top of the SCMS Root CAs.

5.1.4.1 Distributed Management & Electors

A distributed management scheme, like a democracy, contains within itself the power to replace an established hierarchy and does not succumb to a single failure. The concept of ***Electors***, which together have the power to change and manage the trust relationships of the system, adds such a scheme to the SCMS design. Within a system like the SCMS, the number of electors should be 2n+1, where n is the number of simultaneous elector expiration/compromises that the SCMS can tolerate.

Like in a democracy the Elector-based Root Management introduces a ***Ballot*** with ***Endorsements***. The electors cast ***Votes*** by signing an endorsement of a given root CA or elector certificate. A ballot aggregates all these endorsements. When a quorum of valid elector endorsements is on the ballot, any component in the system can trust the ballot.

The electors are not part of the PKI hierarchy, and therefore they can use a different crypto-system than the SCMS PKI. In fact, each of them can use a different one. This raises the probability that in case of a root CA or elector certificate compromise due to a broken cryptography, the system is still able to heal itself.

The resulting system may have multiple, self-signed root CA certificates, each of which operates at the top of their trust chain. Each root CA's certificate is endorsed by a ballot with at least a quorum of votes from non-revoked electors. Devices need to verify the trust chain up to a root CA certificate, at which point they must verify that a quorum of non-revoked electors has endorsed that root CA certificate.

5.1.4.2 Ballots & Endorsements

Electors operate by signing endorsements. A ballot can include the following basic types of endorsements:

- Add root CA certificate
- Add elector certificate
- Revoke root CA certificate
- Revoke elector certificate

Each ballot contains only one type of endorsement. SCMS components, including devices, receive ballots adding a certificate via a certificate chain file distributed by the PG. They receive ballots removing a certificate via the CRL distributed by the CRL store.

All components know the quorum and the certificates of the initial set of electors and therefore can validate the endorsements contained in the ballot. Once the ballot is validated, the component can follow the endorsed action to add or remove the ballot’s certificate from its trust store.

The SCMS Manager will coordinate the production of the ballot messages.

5.1.4.2.1 Structure of Ballots

The ballot which aggregates all independent elector endorsements is an ASN.1 structure. This structure contains the following elements:

1. The certificate of the root CA or elector to be endorsed
2. A sequence of endorsements, each containing:
    a. The type of endorsement
    b. The hash id of the certificate to be endorsed
    c. The generation time of the endorsement
    d. A signature of the elector.

Note that the validity period of a ballot is implicitly given by the validity period of the endorsed certificate.

5.1.4.2.2 Revocation/Endorsement Impact on Devices

A key consideration in the design of the root management system is to maintain secure operation of devices without requiring recall or manual re-enrollment of individual devices. The following table outlines the status of devices through the addition or revocation of Electors and Root CAs.

Table 10 EE Status through Addition/Revocation of Electors and Root CAs

Operation	Elector Model Implementation
Revoking an Elector	As long as there are at least three electors with a quorum of two, then one elector may be removed without impacting operation: The remaining electors are still a quorum and their endorsements of the root CA certificate would still be valid. A single revoked elector would not stop operations of any device. A replacement elector may then be added back to the system to return to a state with three valid electors. A larger number of electors may be used to improve the system's resilience to compromise or failure of these top-level trust anchors.
Revoking a Root CA	Revoking a root CA certificate would stop operations of devices that possess certificates chaining up to the revoked root CA certificate. Those devices would need to re-enroll and be re-provisioned with a different root CA before they could be trusted by other devices.
Adding an Elector	A new self-signed elector certificate that is endorsed by a quorum of valid electors can be trusted by devices and other SCMS components without the need of returning them to a secure environment. In addition, this new elector can endorse existing root CA certificates without the need for any updates of the existing valid certificates, including the device's pseudonym certificates.
Adding a Root CA	A new, self-signed root CA certificate that is endorsed by a quorum of valid electors can be trusted by devices and other SCMS components without the need

Operation	Elector Model Implementation
	of returning them to a secure environment. Devices can immediately begin to trust messages that chain up to the new root CA.

5.1.4.2.3 Effect of Voting Schemes on the GCCF

The Global Certificate Chain File (GCCF) contains all the trust chains needed by the SCMS (including EEs), including the Root CA certificates. With the elector model, the Root CA certificates are also accompanied with elector endorsements. The Root CA certificates in the GCCF will be supplied in the form of the "Add Root CA" ballots. The trust chain for certificates under a Root CA will be recorded in the GCCF as a list of IEEE 1609.2 certificates.

5.1.4.2.4 Structure of the Trust Hierarchy

The diagram below shows how the SCMS-specific implementation of the elector-based scheme (shown in green) can be implemented in parallel with a standard PKI hierarchy, which supports all SCMS components and EEs. Note that all of the structures shown here can be implemented with standard IEEE 1609.2 certificates without modification. A significant advantage of the elector-based scheme is that, as new Electors are added at level 0, an existing root CA can receive new endorsements from an elector without having to change their certificates.

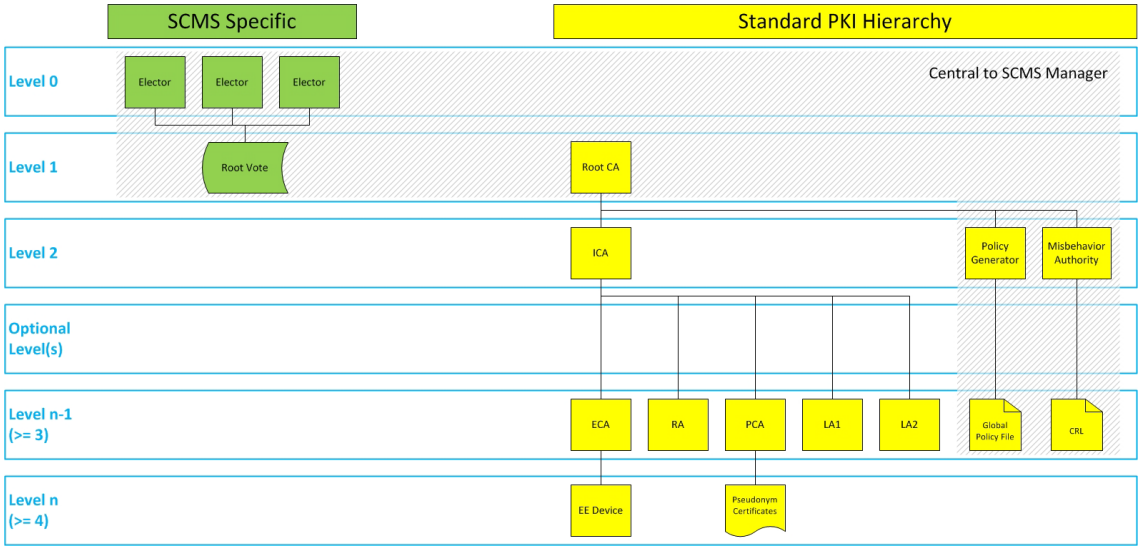


Figure 21 Endorsement Method Details

5.1.4.3 Impact on EE Storage

The implementation of the elector scheme will affect how EE storage is used.

1. An EE must be able to store securely a number of elector IEEE 1609.2 self-signed certificates. In the PoC, three electors will be operational. Storage for four electors and elector endorsements must be available. In deployment, perhaps nine will be operational, and storage for ten is assumed.
2. An EE must be able to store securely a number of Root CA self-signed certificates. In the PoC, there will be at most two (to allow for testing of Root replacement). In deployment, storage for ten is assumed. If the EE will check the votes on these Root CA self-signed certificates each time, then these need not be stored in the secure trust store.
3. EEs must have secure software used to update the trust store through the correct processing of ballots. This also involves protection for basic parameters under which votes are acted upon, the *quorum*, which is an assumed number less than ten.

Note that all EEs (and other SCMS components) must have a secure method for storing and recovering Root CA certificates. Developers of EE hardware and software may choose from a variety of methods for managing secure storage, but their chosen approach must be approved through an EE certification process. To demonstrate some of the various options that are available, three methods are suggested and described in the following diagram:

- Suggestion 1: Store the Root CA certificate directly in tamper-evident storage. This approach allows the EE to quickly access the Root CA certificate with no further validation (EE must validate it only once before it is placed in secure storage).
- Suggestion 2: The EE may store the endorsement message signed by the electors in secure storage to support peer-to-peer certificate learning of root CA certificates.
- Suggestion 3: The EE may validate the root CA certificate once and then store a hash of the certificate in tamper evident storage. Note that this is effectively the same as Suggestion 2 since the endorsement itself will contain a hash of the root CA certificate, but the EE may choose to use a different hashing algorithm to optimize for speed or to reduce storage.

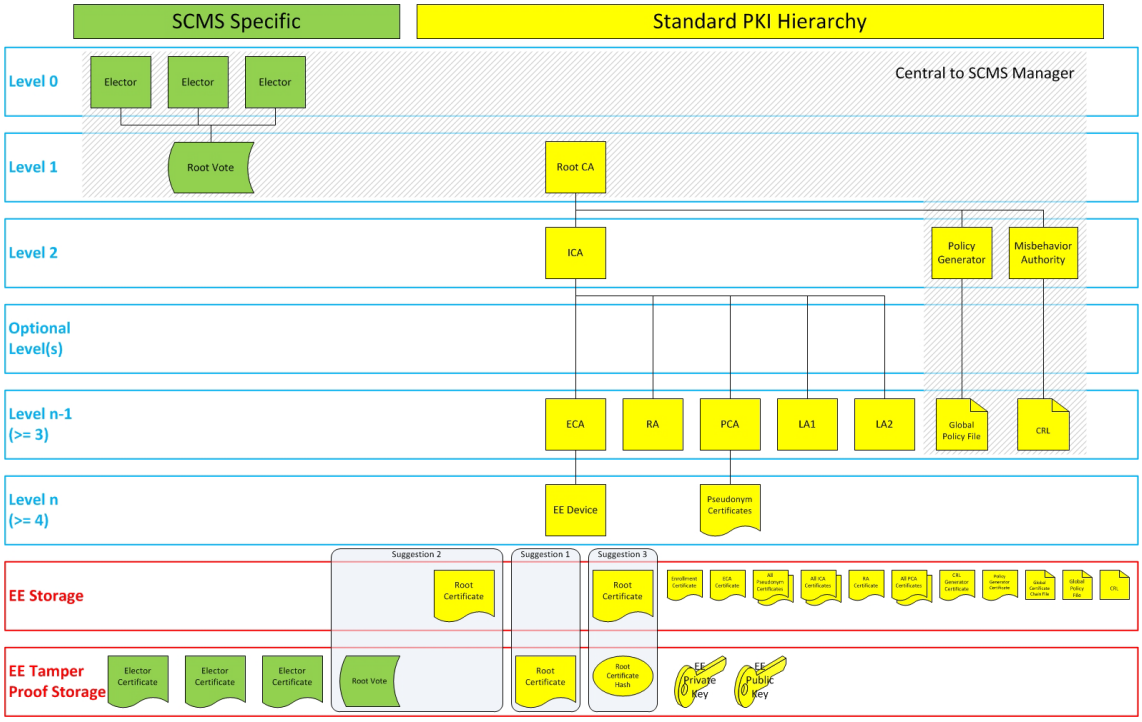


Figure 22 EE Storage Requirements

5.1.4.4 Root Management and Disaster Recovery in Action

This section aims to show root management and disaster recovery in action. As a result, the revocation and replacement of an elector is described below:

- Day 1: Typical SCMS Operations
- Day 2: Revoking an Elector
- Day 3: SCMS Operating with 2 Electors Only
- Day 4: Replacing a Elector
- Day 5: SCMS Returning to Typical Operation

The diagrams given below (and in sections above) are high-level summaries only, and do not contain all requirements for the SCMS components or the EEs.

Day 1: Typical SCMS Operations

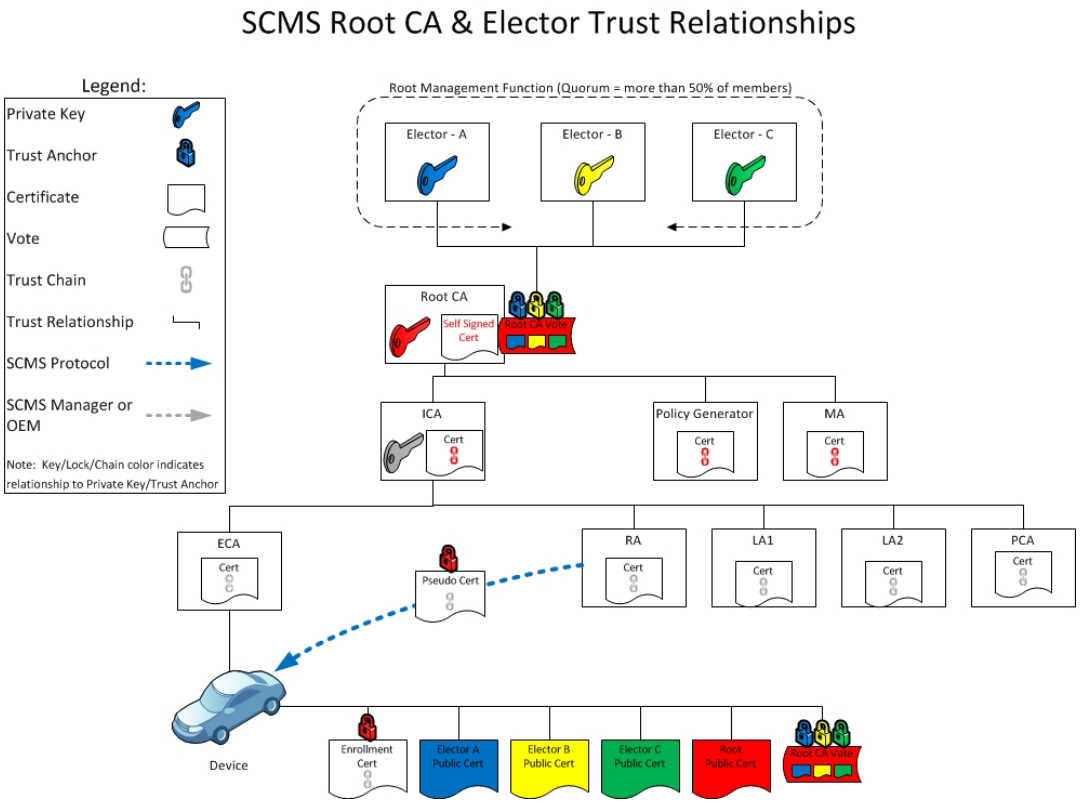


Figure 23 Day 1: Typical SCMS Operations

Day 2: Revoking an Elector

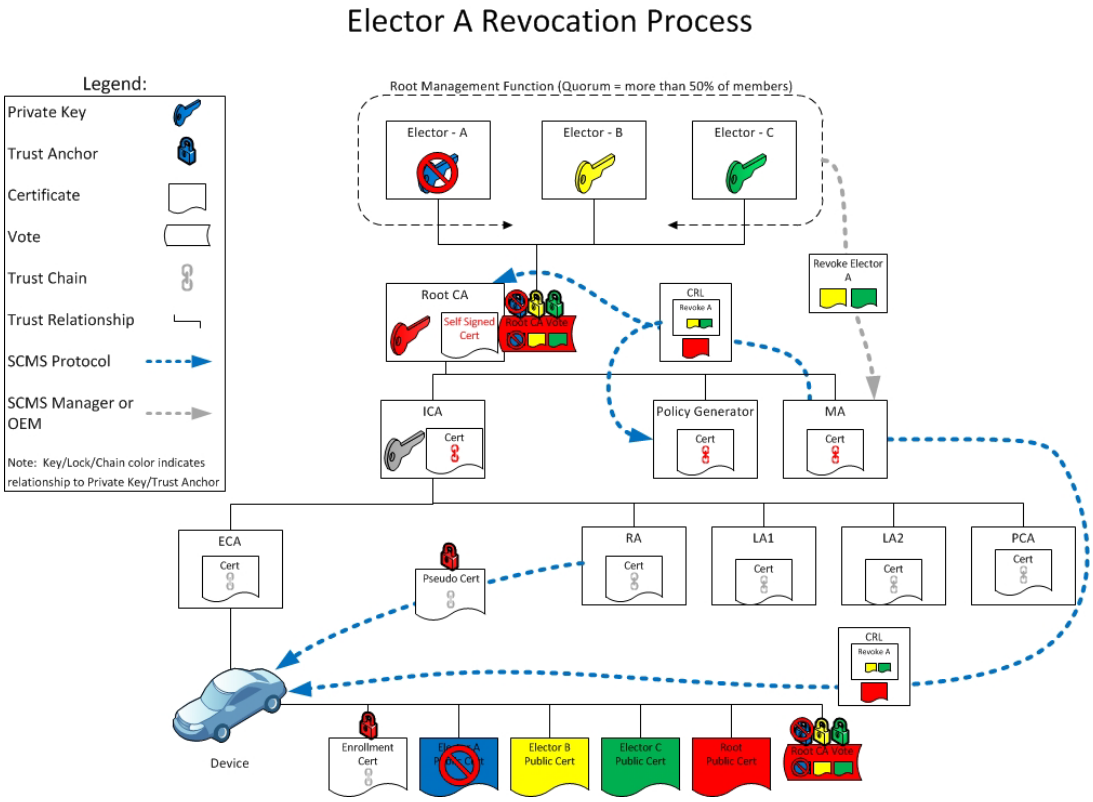


Figure 24 Day 2: Revoking an Elector

At Day 2, an elector has been revoked by votes from *m* electors (here *m*=2). These votes are included in the CRL. The CRL is distributed to all SCMS components and EEs. The SCMS is still operational.

Day 3: SCMS operating with two electors only

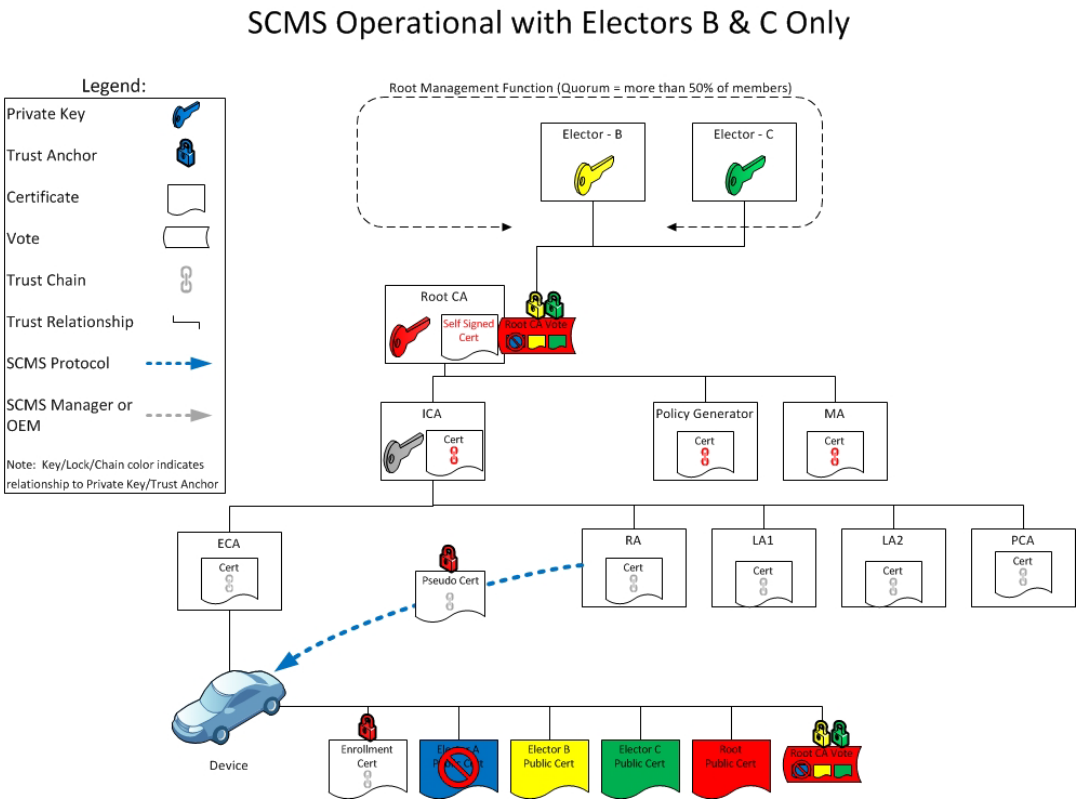


Figure 25 Day 3: SCMS Operating with Two Electors Only

In Day 3, the SCMS is operational with only two, non-revoked electors. Pseudonym certificates continue to validate and EEs to operate.

Day 4: Replacing an Elector

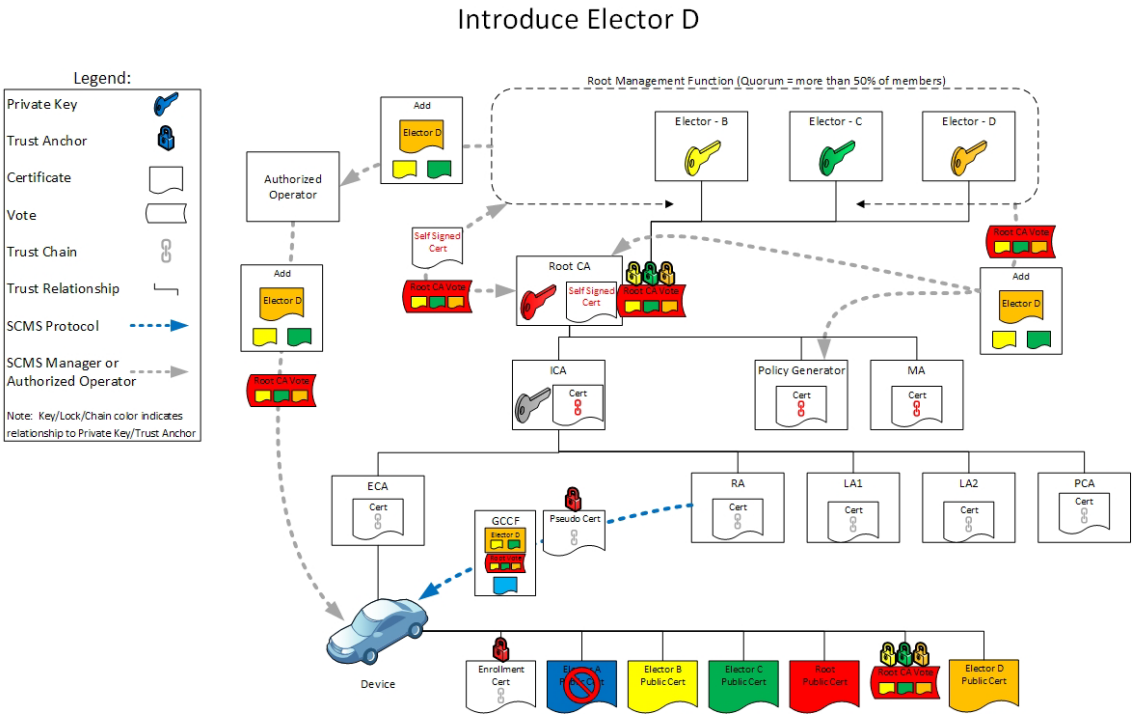


Figure 26 Day 4: Replacing an Elector

In Day 4, the SCMS Manager introduces a new elector through votes endorsing the new elector obtained from the two, remaining, non-revoked electors. Existing devices that do not recognize the new elector continue to operate. The SCMS Manager adds a new elector through a *Ballot* inserted into the Global Certificate Chain File (GCCF), which it then provides through the Policy Generator to RAs. The root management message includes votes from the electors, which the SCMS components and EEs will need to validated before performing the root management operation (adding the elector to the trust store). The SCMS Manager provides a new vote from the new elector for the existing root CA certificate and adds it to the GCCF as well. Even with the addition of the new elector, pseudonym certificates continue to validate and EEs to operate.

Day 5: SCMS Returning to Typical Operation

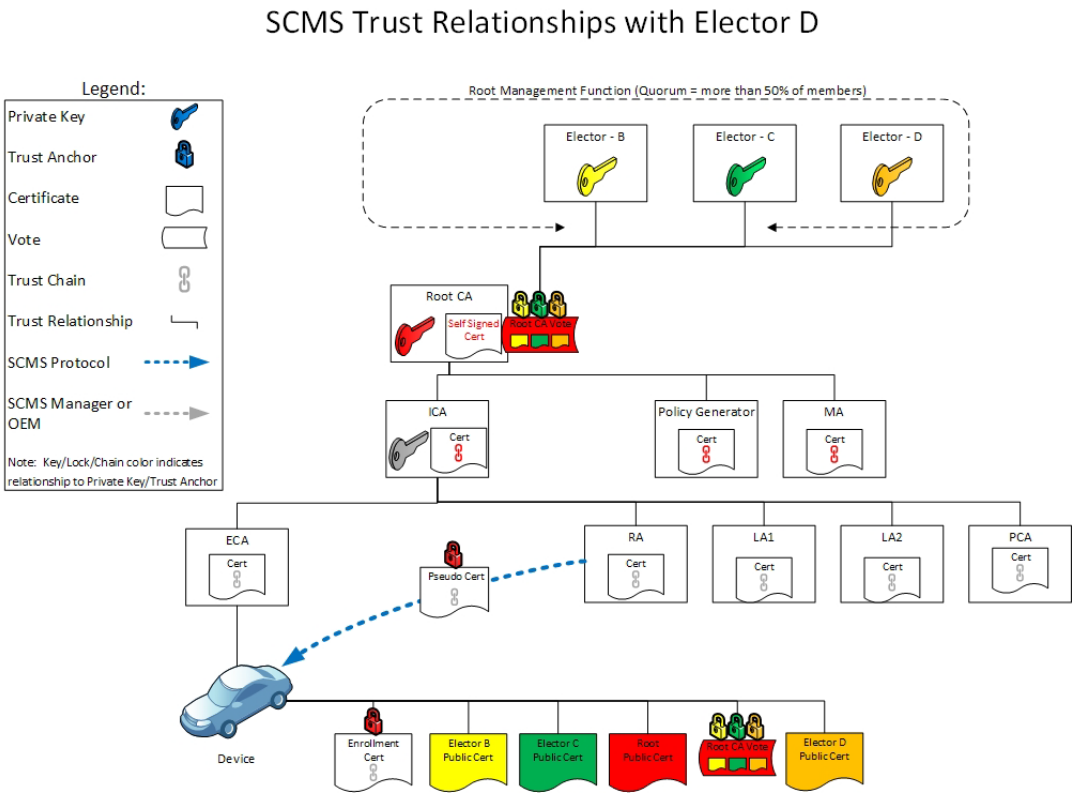


Figure 27 Day 5: SCMS Returning to Typical Operation

In Day 5, the SCMS has been returned to an equivalent of the Initial State of Day 1 with a replacement elector.

The following describes the revocation and replacement of a root CA certificate:

- Day 1: Typical SCMS operations
- Day 2: Standing up a new root CA certificate
- Day 3: Putting the SCMS backend trust relationships in place for the new root CA certificate
- Day 4: Revoking the existing and adding the new root CA certificate
- Day 5: Revoked root CA certificate, system non-functional
- Day 6: System functionality restored

Day 1: Typical SCMS operations

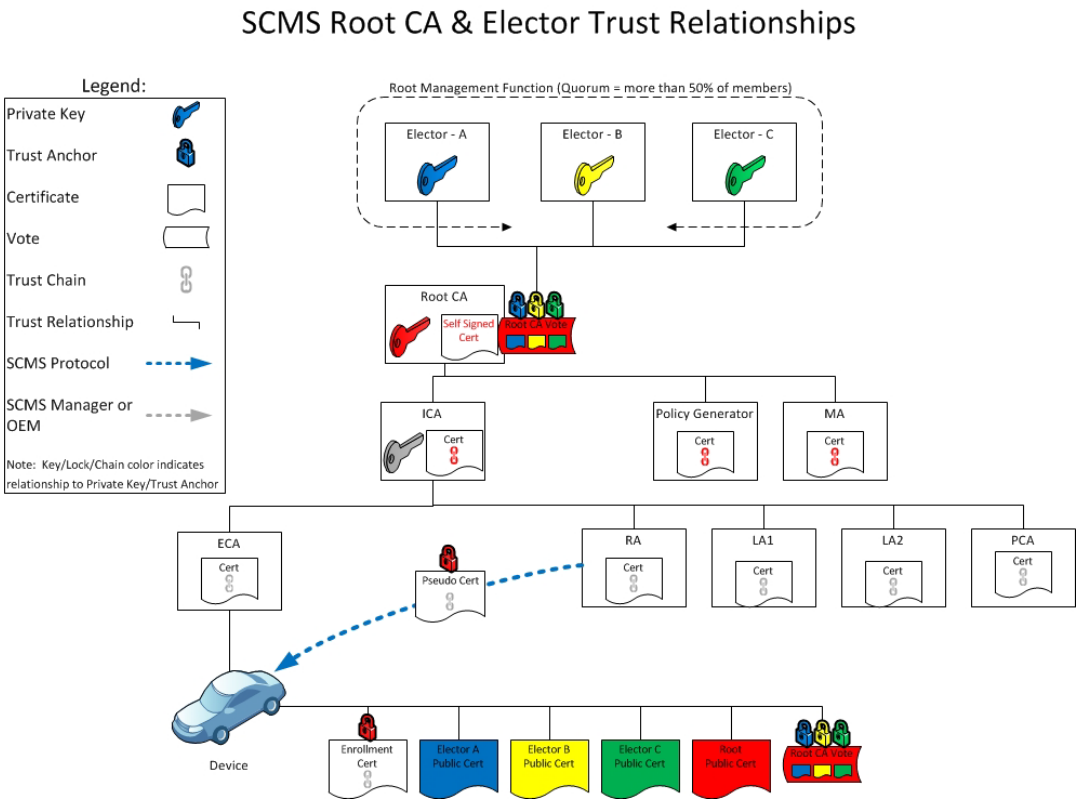


Figure 28 Day 1: Typical SCMS Operations

Day 2: Standing up a new root CA certificate

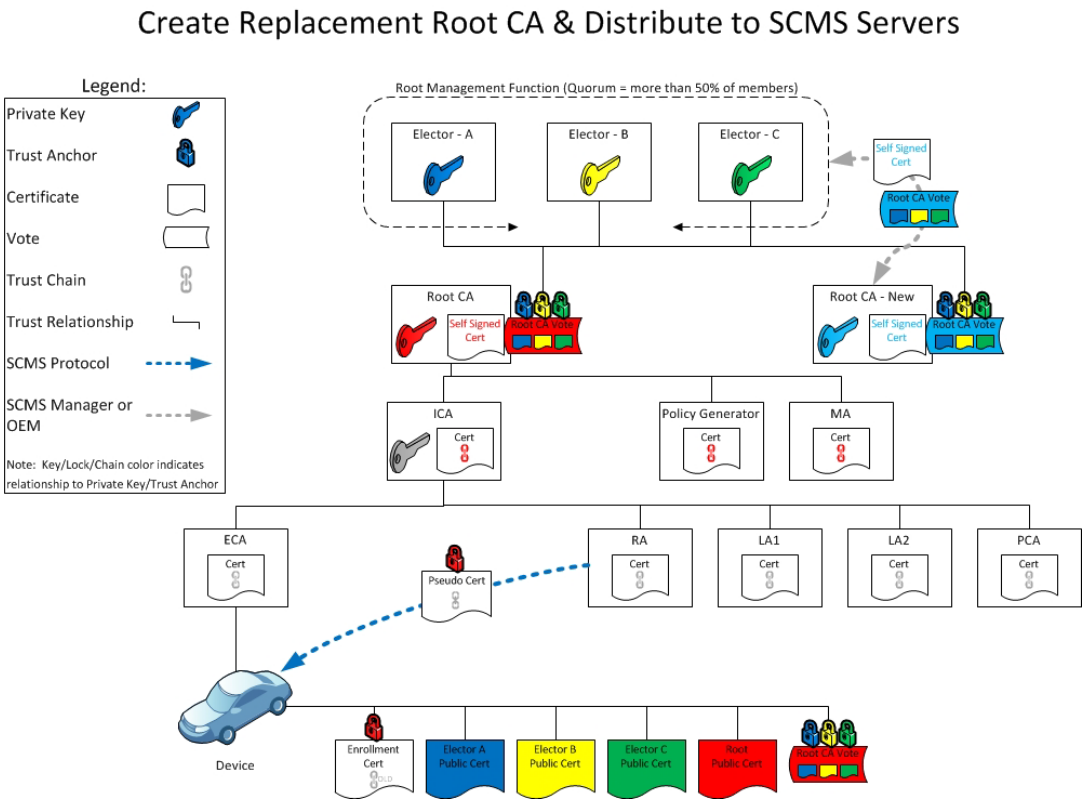


Figure 29 Day 2: Standing Up a New Root CA Certificate

In Day 2, the new root CA certificate is established and endorsed but is not used by the SCMS.

Day 3: Putting the SCMS backend trust relationships in place for the new root CA certificate

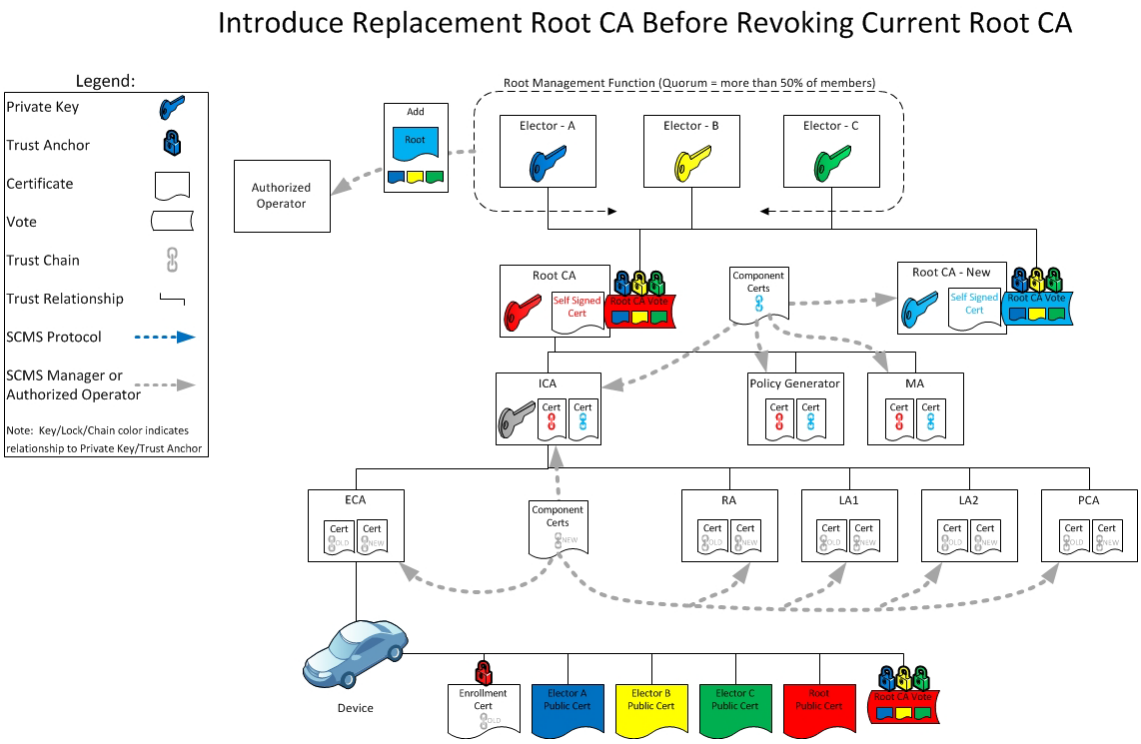


Figure 30 Day 3: Putting the SCMS Backend Trust Relationships in Place for the New Root CA Certificate

On Day 3, all of the background tasks of generating new certificates for SCMS components is performed, but these are not made active. The new root management operation, "Add Root CA," is distributed to all the authorized operators to prepare them for distribution.

Day 4: Revoking the existing and adding the new root CA certificate

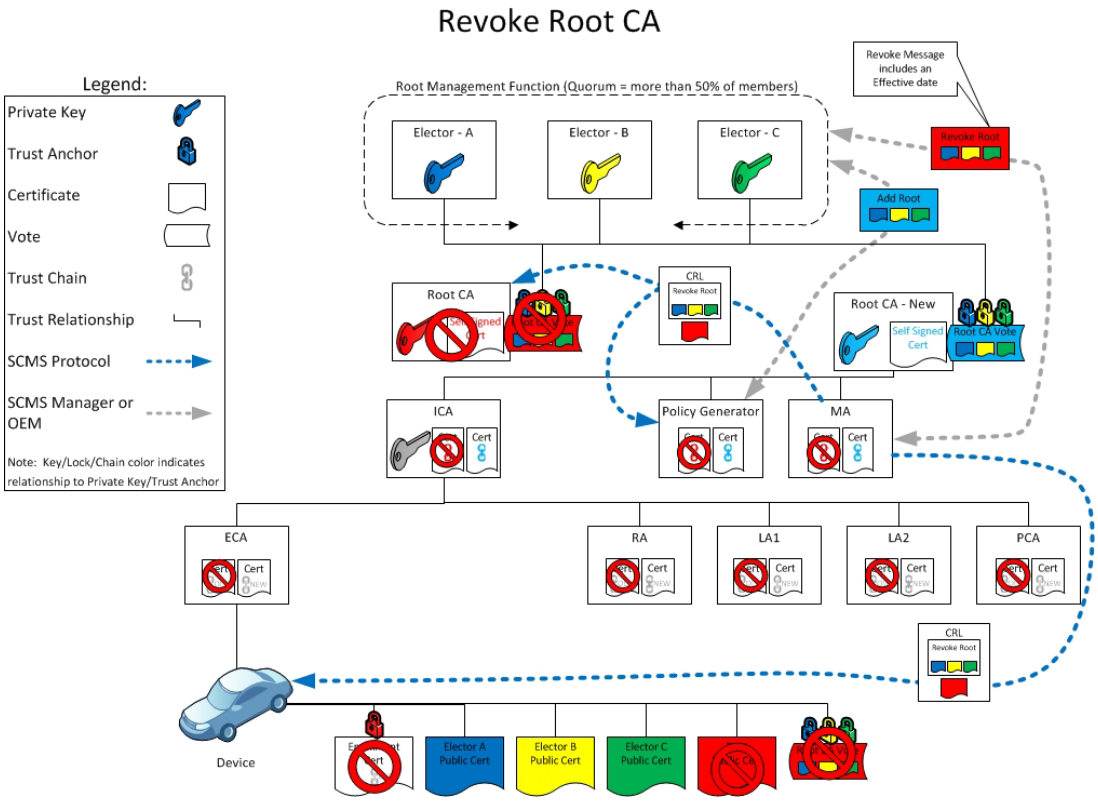


Figure 31 Day 4: Revoking the Existing and Adding the New Root CA Certificate

On Day 4, the old root CA is revoked and the new root CA is added simultaneously to all SCMS components (not EEs). The EEs only receive the revoke message. The GCCF needs to be reset with the new trust structure, which was created on Day 3. All the SCMS components start using the certificates, which chain to the new root CA certificate.

Day 5: Revoked root CA certificate, system non-functional

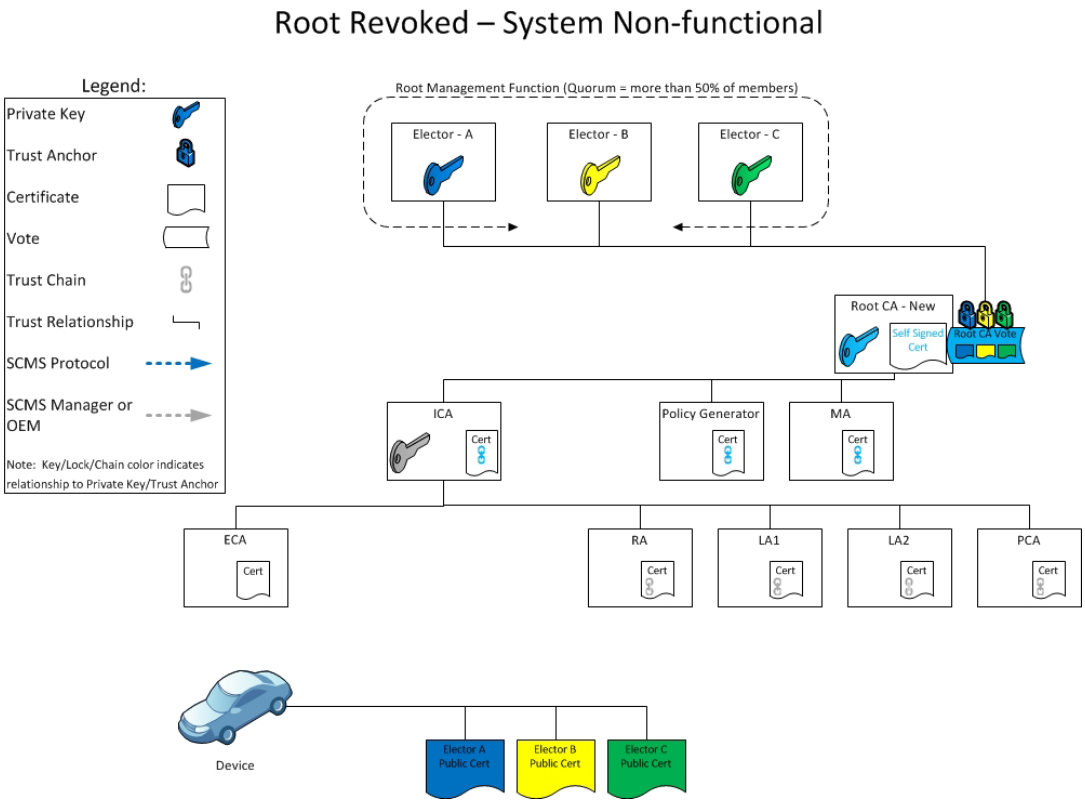


Figure 32 Day 5: Revoked Root CA, System Non-Functional

On Day 5, all of the existing pseudonym and enrollment certificates are no longer valid. This means that from an EE point of view, the SCMS is not functioning. The CRL also needs to be reset: any certificate without linkage values can be removed. The handling of the linkage values on the CRL will depend on if the linkage values are continued. Those that are continued will need to remain on the CRL.

Day 6: System functionality restored

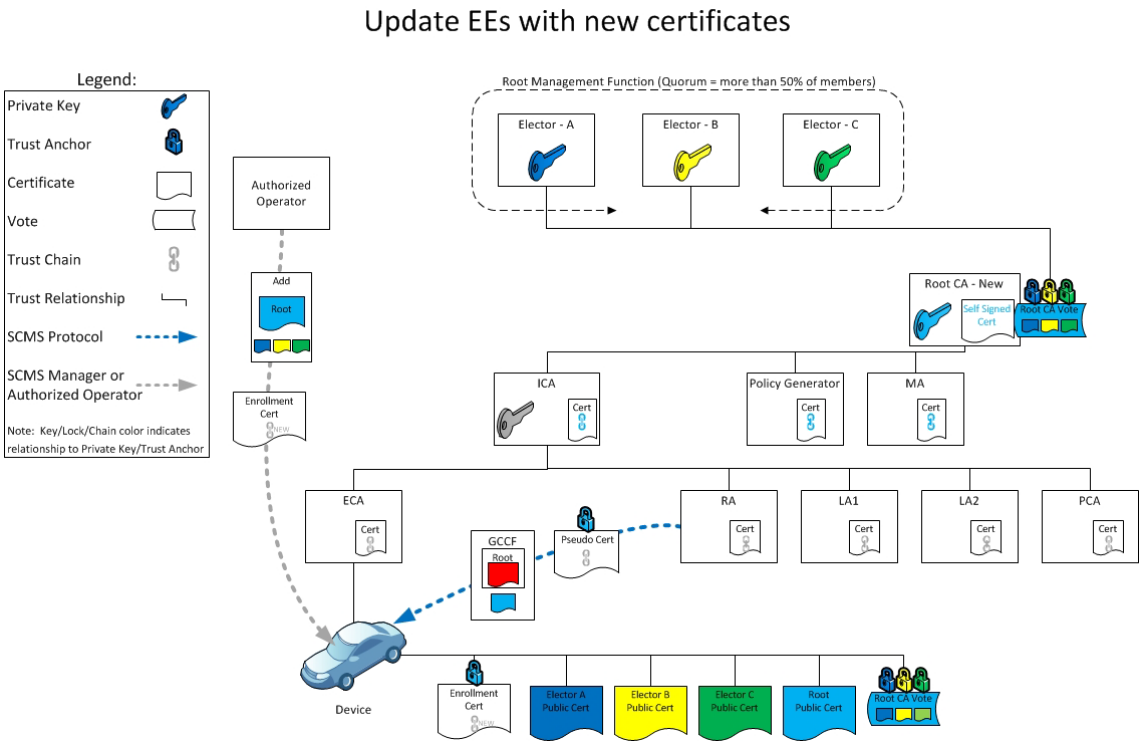


Figure 33 Day 6: System Functionality Restored

On Day 6, the authorized operators will issue new enrollment certificates to the EEs. All EE certificates, including pseudonym certificates, are generated. The EEs require new enrollment certificates to authenticate themselves to their RA. The SCMS does not yet specify the mechanism used to provide new enrollment certificates to EEs; a later release will support this. Once an EE receives its new enrollment certificate, it can download the policy file, the GCCF, and new pseudonym Certificates. The EEs now become operational again.

5.1.5 Cryptography

5.1.5.1 Approved Cryptographic Algorithms

The following algorithms are approved for use as specified in IEEE 1609.2-2016:

- **Signing:** ECDSA over NIST P-256
- **Public key encryption:** ECIES over NIST P-256
- **Hash:** SHA-256
- **Symmetric Encryption:** AES-CCM with 128-bit keys

See IEEE 1609.2 for normative references to the definitions of the algorithms.

5.1.5.2 Approved Random Number Generators

This is a non-exhaustive list of recommended software random number generators. Generally, hardware random number generators are preferred. Both types should follow the requirements specified in CB2: Types of Cryptographic Algorithms.

Based on java documentation, a random number can be generated using SecureRandom. This class provides a cryptographically strong random number generator (RNG).

```
public class SecureRandom extends Random
/*
A cryptographically strong random number minimally complies with the
statistical random number generator
tests specified in FIPS 140-2, Security Requirements for Cryptographic
Modules.  SecureRandom must produce
non-deterministic output. SecureRandom is acceptable only if
seeding/entropy source is provable sufficiently secure
*/

public static void main(String[] args) t..... {
    SecureRandom ranGen = new SecureRandom();
}
```

Implementation

- A software based RNG solution shall be sufficient through CV pilot until hardware based solutions are identified and accepted.
- Java SecureRandom running on a virtual machine is only acceptable if the host machine entropy is accessible and used by the VM. This can be accomplished by employing utilities such as virtio-rng. Please check your desired VM implementation for support of such a feature.

Testing

- The used RNG shall be tested using the NIST SP800-22b statistical test suite "sts-2.1.1". A description of the test suite (NIST Special Publication 800-22rev1a, dated April 2010) and the NIST statistical test suite software sts-2.1.1 are available at http://csrc.nist.gov/groups/ST/toolkit/rng/documentation_software.html.
- The NIST test suite allows testing an input file of RNG output with various tests. The following tests shall be performed. All tests shall use sufficiently sized input files to the NIST test suite.
    a. *Test Randomness*: Generate random output of SecureRandom on the VM and run *all* tests of the NIST test suite.
    b. *Test Seeding*: Generate random output o_1 of SecureRandom on the VM at time t (relative to start-up time). Restart the VM and generate random output o_2 of SecureRandom on the VM at time t (relative to start-up time). Combine o_1 and o_2 in a single file, and run the full NIST test suite.

c. *Test nonce and reconstruction values*: While an SCMS component operates normally, store the output of SecureRandom in a file and run the full NIST test suite.

- A third party description of proper RNG testing can be found at http://www.st.com/web/en/resource/technical/document/application_note/DM00073853.pdf (cp. sections 2 and 3).

5.1.5.3 Cryptography Background

5.1.5.3.1 CB1: Cryptographic Services

5.1.5.3.1.1 Standard Services: Confidentiality, Integrity, Authenticity

The standard cryptographic services are confidentiality, integrity, and authenticity. They are provided by the cryptographic mechanisms of encryption and authentication. Two fictional people, Alice and Bob, are used in the following descriptions to help simplify the explanations.

Confidentiality means that when Alice sends a message to Bob, she knows that no one can learn anything (except its length) about the message in transit. Confidentiality is provided by *encryption*.

Integrity means that when Alice sends a message to Bob, she knows that if the message is altered in transit, Bob will be able to detect that the message has been modified; this provides a deterrent to an attacker who may want to modify the message.

Authenticity means that when Alice sends a message to Bob, she knows that Bob can be certain that the message actually came from her.

Authenticity and *integrity* are typically provided together (authenticity is of little use without integrity) by *authentication*.

Cryptographic mechanisms allow Alice and Bob to leverage a small amount of secure information into a large amount of secure data. This small amount of information is a key. For confidentiality, Alice uses a key to encrypt the data and Bob uses a related key to decrypt the data. For authentication, Alice uses a key to apply an authentication code to the data, and Bob uses a related key to check that the code is valid. Although a great deal of attention is paid to particular encryption algorithms (such as the algorithm by Rivest, Shamir, and Adleman (RSA), the advanced encryption standard (AES), and so on), real-life key management is a much more difficult problem than choosing a cryptographic algorithm, and many more weaknesses are caused in systems by poor key management than by a poor choice of cryptographic algorithm.

5.1.5.3.1.2 Privacy

A main goal of the SCMS is to protect the privacy of drivers. This means that it should provide the following services:

- Anonymity: A message should contain no information that explicitly identifies the driver, the passengers, or the vehicle.

- Unlinkability: It should be difficult for an eavesdropper to track a driver or vehicle by recording its BSM transmissions.

Unlinkability is not a binary property of the system. For example, an eavesdropper who is able to record all messages sent by a vehicle will be able to track that vehicle by constructing the path indicated by that vehicle's BSMs. However, it is a design goal that the V2V communications system does not increase the risk that an individual may be tracked.

For purposes of this report, the requirement is that if a vehicle's messages contain data that is unique to the vehicle, the data should change frequently such that it is extremely difficult for an eavesdropper to track that vehicle. This in turn means that:

- Any application identifiers should change frequently. This is supported in the TemporaryID field in the BSM.
- Any network identifiers, such as source Media Access Control (MAC) addresses, should change frequently. This is permitted by IEEE Standard 802.11 and actively supported by service primitives in IEEE Standard 1609.4.
- Any cryptographic information unique to the vehicle should change frequently. As discussed below, messages in the system are authenticated by signing them with digital certificates, which are issued by a certificate authority (CA). To meet the requirement, a device must either have multiple digital certificates, or share its certificate with other vehicles. Previous research has concluded that shared certificates are not viable (cf. e.g., Jason J. Haas, Yih-Chun Hu, and Kenneth P. Laberteaux. The Impact of Key Assignment on VANET Privacy. Security and Communication Networks. 3(2):233-249, John Wiley & Sons, Ltd., March 2010). Only the case where each device has multiple certificates is considered in this system.
- All identifier changes should be synchronized: if one identifier does not change between observations, the attacker can link even if all other identifiers change.
- The vehicle's privacy should be preserved even if the attacker has inside information from one of the SCMS components.

However, in addition to supporting privacy, the system design has to support identification of misbehaving devices in order to remove them from the system. These two goals are fundamentally in contradiction. This SCMS design allows identification of devices for misbehavior detection purposes only through a series of defined interactions between SCMS components. No individual SCMS component can identify a device, and the information revealed to any SCMS component can be controlled.

The Vehicle Infrastructure Integration Consortium (VIIC) provides a full discussion of the policy requirements arising from this high-level requirement for privacy-by-design.

5.1.5.3.2 CB2: Types of Cryptographic Algorithms

There are two different types of keyed cryptographic algorithms, which use very different types of key management. This section discusses those keyed algorithms and also two other important cryptographic primitives, hash functions and random number.

5.1.5.3.2.1 Symmetric Algorithms

In a symmetric algorithm, the sender and receiver use the same key (or keys that are related to each other in some trivial-to-derive way). Alice uses k1 to encrypt; Bob uses k1 to decrypt. Alice uses k2 to authenticate; Bob uses k2 to validate. Symmetric algorithms have two significant properties:

- They are fast (which translates into implementations being low cost). For example, AES, a symmetric encryption algorithm, can encrypt 81 MB per second on a 2 GHz processor, or generate authentication codes on 1,000,000 messages per second with a size of 100 bytes per message.
- They require *secure, private key exchange*. Before Alice and Bob can use a key k to communicate, they must securely agree on k in such a way that no other party (except perhaps a trusted center) knows k. This means that Alice and Bob must have some kind of pre-existing relationship to use symmetric cryptography.
    - NOTE: In a vehicular setting, vehicles are often encountering each other for the first time and do not have a pre-existing relationship. This is one of the main reasons why symmetric key cryptography is not being considered for use in authenticating V2V safety messages.

5.1.5.3.2.2 Public Key Algorithms

In an *asymmetric or public key algorithm*, the encryption and decryption, or authentication and validation, keys come as a pair, *Pub and Priv*, with the property that they are related but that it is very expensive (in terms of computer time) for someone who only knows *Pub* to work out *Priv*. *Pub* is called the public key. *Priv* is called the private key. The private key is not widely shared and usually known only to the key owner; the public key can be distributed widely. They are used this way:

- For confidentiality: Alice uses Bob's (note, not Alice's) public key to encrypt the message. Only Bob knows his own private key, so only Bob can decrypt the message.
- For authentication: Alice uses her own private key to generate the authentication code – for a public key algorithm, this is called *signing*. Bob uses Alice's (note, not Bob's) public key to validate the authentication code – for a public key algorithm, the authentication code is called a *signature* and the validation is called *verification*. If the signature verifies with Alice's public key, then the signature was generated with Alice's private key and the message was not modified. Because only Alice knows her own private key, that means that Alice generated the signature and so that the message came from Alice. For performance reasons, an actual implementation would perform the signature operation on a checksum of the message only.

Public-key algorithms have two significant properties:

- They are *relatively slow* compared to symmetric algorithms (which translates into implementations being more expensive in terms of processing compared to symmetric algorithms). For example, ECDSA-256, the public key algorithm that is used in the CAMP VSC3 design, can generate about 1500 signatures per second on a 2 GHz processor and can verify only about 300 signatures per second.
- They require *authenticated key exchange*, but the key exchange can be *public*. If Alice has some assurance that a public key belongs to Bob, she can use that key to verify Bob's signed messages or encrypt messages to him even if many other people know the public key as well. Alice knows that a public key belongs to Bob usually because the CA attests to it by signing Bob's public key. Bob's public key is signed by the CA and is referred to as Bob's certificate. So long as Alice and Bob trust the CA and have access to the CA's public key, they can trust that keys signed by the CA are genuine. This makes public key cryptography ideal for settings where two parties encounter each other briefly and need to trust each other's communications, even if they do not have access to an *online* key service. This is the relevant setting for V2V communications, which is why CAMP VSC3 and IEEE 1609.2 use public key cryptography.

5.1.5.3.2.3 Hash Functions

There is a third useful type of cryptographic algorithm, known as the hash function. A hash function produces a cryptographically strong, fixed-length checksum of a message. The output from the hash function, often called a hash or a digest, is cryptographically strong in the following senses:

- The output looks random: small changes to the input message result in significant changes to the hash
- It is computationally infeasible to find a message that hashes to a particular hash value. (Hash functions are non-invertible, or have pre-image resistance.)
- It is computationally infeasible to find two messages that hash to the same value. (Hash functions have collision resistance.)
- Hashes are fast, comparable to or faster than symmetric algorithms. In the CAMP VSC3 SCMS, hashes are used for a number of purposes:
    - A truncated hash of a certificate can be used as an identifier in messages signed by that certificate, so that the sender does not have to send the full certificate with every message
    - Messages are hashed before signing them: the (private-key) signature operation is actually applied to the hash of the message but not to the message itself. This has both security and efficiency benefits and is standard practice in cryptographic systems outside the CAMP VSC3 system.
    - Hashes are used to generate linkage values as described in SCP2: Linkage Values

5.1.5.3.2.4 Random Number Generators

Random number generators are used to generate keys and other random data within a system that uses cryptography. Since the security of a system depends on private and secret keys being unobtainable through unauthorized exposure, it is important that the random number generators used to generate them are good. In this context, “good” means a number of things:

- An attacker must not be able to determine the next output from the random number generator, no matter how much previous output the attacker has seen. This means that the output must be statistically random and contain no bias. If the random number generator is used to generate an integer modulo some modulus *n*, all numbers between 0 and *n-1* must be equally probable with no bias towards particular values.
- If the random number generator uses an internal state, an attacker must not be able to guess the internal state of the random number generator and use this to predict output. This means that:
    - The internal state must be large enough to be infeasible to guess by brute force
    - The initialization process that initialized the internal state must be infeasible to reproduce
- If the random number generator uses some hardware-produced randomness source, the output from this source must be infeasible to reproduce

As well as secret and private keys, random number generators are used for other purposes within the SCMS:

- When signing with Elliptic Curve Digital Signature Algorithm (ECDSA), a fresh entirely random number must be generated for each signature with the same key. Repeated random numbers, random numbers with a bias, or random numbers with a known relationship to each other will reveal the private key.
- Random numbers are used by the PCA when creating implicit certificates or when expanding a butterfly signing key (see SCP1: Butterfly Keys). If these random numbers are not good, it can result in the Registration Authority (RA) being able to track a device, or even the PCA’s private key being revealed.
- Random numbers are used to generate Linkage Seeds (LSs) for linkage chains (see CB3: Public Key Infrastructure, SCP2: Linkage Values). If these random numbers are not good, it can result in a device being trackable by a Linkage Authority (LA) or the PCA.

All SCMS components, as well as EEs, must be equipped with industrial quality random number generators, e.g., one of the Approved Random Number Generators.

5.1.5.3.3 CB3: Public Key Infrastructure

In a symmetric key system, each sender and receiver pair needs to share a secret key, thus resulting in a significant amount of shared keys. The great advantage of public key

cryptography is that it makes it feasible for parties to communicate securely with each other, even if they have never encountered each other before and do not have access to an online service.

Alice sends a signed message to Bob. Bob can trust this message without having previously seen Alice's certificate if both of these statements are true:

- Alice signed the message, and the signature verifies using Alice's public key from her certificate
- Alice's certificate is signed by the private key, which corresponds to the public key from a CA certificate. Bob already knows the CA certificate and is able to verify Alice's certificate using the CA certificate's public key.

This may be extended. Bob does not need to know the CA certificate that issued Alice's certificate. This CA certificate, call it Certificate (CA1), could have been issued by another CA, call it CA2. If Bob knows Certificate (CA2), and receives both Certificate (Alice) and Certificate (CA1) in the signed message, he can still trust Alice's message by verifying that Alice signed the message, that her certificate was issued by CA1 and that CA1's certificate was issued by CA2. This can obviously be extended any number of times until the certificate chain reaches a root certificate. A root certificate is a certificate that was signed by its own private key. The root key is the key to trusting the entire PKI. The root public key has to be distributed securely so that recipients do not receive the wrong key and so trust the wrong certificates. The root private key also must be protected very carefully – anyone who had access to the private key would in principle be able to set up an entire CA hierarchy made of compromised CAs, which would be trusted by everyone who knew the public key. For this reason in real-world PKI deployments, the root key is used as infrequently as possible and is kept and used on a machine that cannot be accessed from an external network.

The CAMP SCMS design features a CA hierarchy, with:

- A root CA that issues certificates for other CAs but not for vehicles or other end-entities
- Optionally, intermediate CAs (ICAs), which obtain their certificates from other CAs above them and also issue certificates for other CAs rather than end-entities. The advantage of using intermediate CAs is that if an intermediate CA is compromised, it is less catastrophic than if the root CA is compromised, so this gives the system more flexibility to introduce new CAs without running the risks incurred by using the root CA key. It is possible to use intermediate CAs in a cascade, so an intermediate CA is either validated by the root CA or the intermediate CA above it.
- Enrollment authorities that issue enrollment certificates (long-term certificate signing requests) for the end-entities. These enrollment certificates are used only to communicate with the SCMS, not with other vehicles or end-entities. Note: the lifetime of the certificate is currently assumed to be the lifetime of a car (e.g., 30 years). However, this still needs discussion as it influences the size of the internal blacklist and is hence a cost issue. Note: the certificate lifetime and the lifetime of the actual CA do not have to be equal.

- Pseudonym CAs that issue certificates for the applications on the cars

The CAMP SCMS also distinguishes between the CA, which actually signs the certificate and the RA, which approves certificate requests. This results in a system diagram that appears complicated at first glance. In fact, this aspect of the CAMP approach is fully in line with standard PKIs used elsewhere in government and industry. This complexity of the abstract architecture allows for flexibility and robustness in introducing new CAs, retiring old ones, and allowing different organizations to take responsibility for authorizing activities that they properly have jurisdiction over. The initial deployment may not require all the boxes on the diagram to be filled immediately; however, it is important for the initial system to support migration to the full CAMP SCMS architecture, even if this migration happens slowly.

5.1.5.3.3.1 Certificates

A certificate links its holder's public key to a statement about the holder, such as an identity or a list of permissions. The statement is trusted because it is attested to by a CA. A receiver checks that the statement is true about a particular signed message by first using the public key of the CA to verify the certificate and subsequently the sender's public key to verify the signature on the message. If the receiver trusts the CA, and the signature on the message verifies, then the receiver knows that the public key owner signed the message and therefore the statement (identity, permissions, etc.) can be trusted as true about the message sender.

The standard way of creating and trusting a certificate is:

- The certificate contains the public key
- The CA signs the certificate
- The receiver verifies the CA signature on the certificate and the public key holder's signature on the message

This requires two verifications on the receiver's side and further requires (with recommended cryptographic algorithm choices) 64 bytes on each certificate to contain the CA signature.

5.1.5.3.3.2 Implicit Certificates

Implicit certificates are a different way of creating and trusting a certificate. With implicit certificates, the certificate requester and the CA cooperate to derive a final public key from the seed public key that the requester submits with the request. Instead of including a signature in the certificate, the CA includes a reconstruction value. A message recipient can combine the reconstruction value with the CA's public key and the rest of the contents of the certificate to recover the certificate holder's public key. This public key is only correct if the reconstruction value was created by the CA. Therefore, the CA's approval of the holder's public key is implicit, which means the public key only works if the CA was involved in creating it. This is different to an explicit approval as in standard certificates, where the public key's validity is explicitly confirmed by the CA signature.

The information flow for implicit certificates is:

- Certificate Creation
    - The certificate requester creates a seed public key
    - The CA calculates a mathematical transformation using the CA private key, the contents of the certificate, and the seed public key, to create:
        - A new public key for the certificate requester, the certified public key
        - A transformation that the certificate requester can use on the seed private key
        - A reconstruction value
    - The CA sends the certificate contents, the reconstruction value and the private key transformation back to the certificate requester
    - The certificate requester applies the private key transformation to the seed private key to obtain the certified private key
    - The certificate requester checks that the certified private key corresponds to the certified public key
- Certificate Use
    - The certificate holder (who was the certificate requester in the previous step) signs a message with the certified private key and attaches the certificate (contents + reconstruction value)
    - The receiver uses the certificate contents, reconstruction value and CA public key to recover the certified public key
    - The receiver verifies the signature on the message with the certified public key

Implicit certificates have the following advantages over standard (explicit) certificates:

- An explicit certificate contains a public key (which is an elliptic curve point) and a signature, while an implicit certificate contains only a reconstruction value (which is an elliptic curve point). An implicit certificate is therefore smaller by the size of the signature, which in this case is 64 bytes. (The private key transformation adds 32 bytes to the certificate response compared to a response for an explicit certificate, but this is less than the signature size and is only included in the certificate response, not in signed messages). It is important to note that more details on this topic can be found in Standards for Efficient Cryptography Group, “SEC 4: Elliptic Curve Qu-Vanstone Implicit Certificate Scheme (ECQV)”, Working Draft Version 0.97, March 2011, available from http://www.secg.org.
- The public key recovery operation and the signature verification can be combined into a single operation that takes approximately the same amount of time as required for a single verification. This is an advantage over explicit certificates, which require two verifications when assuming that the chain of trust ends at the authority issuing the certificate. However, this advantage applies only if a receiver

verifies very occasionally. If the receiver verifies multiple messages signed by the same certificate, it is more efficient overall to recover the public key once and cache it. In this case, implicit and explicit certificate verification takes about the same time. A significant population of devices that verify only occasional messages and verify in software is anticipated and for these devices the performance advantages of implicit certificates are very important.

Implicit certificates are covered by patents owned by Certicom Corp. of Mississauga, Ontario, which is currently a wholly-owned subsidiary of BlackBerry Ltd. At the time of this document, there has been an agreement reached between Certicom and the Institute of Electrical and Electronics Engineers (IEEE) concerning the use of the associated patents. OEM lawyers should review this agreement carefully to determine whether it is acceptable and understand what alternatives might exist.

5.1.5.3.3.3 Detailed Comparison of Explicit and Implicit Certificate Calculations

There are two cases to consider: verifying the certificate chain and message signature and the case where only the message signature is being verified.

5.1.5.3.3.3.1 Explicit Certificates

Let us first focus on the case of verifying the certificate chain and message signature. In this case, one needs to verify the message signature and the signature on each of the certificates. Verifying requires to perform a “double multiply and add,” i.e., calculating aX + bY, where X and Y are elliptic curve points and a and b are integers. Let us denote the cost for one double multiply and add by V. The cost for full certificate chain verification is V * n, where n is the length of the chain.

Once the full chain is verified, the following information is cached:

[Cert ID, public key, “successfully verified”]

This means that any time a message signed by that certificate is received, only one verification step needs to be performed: a lookup of the certificate establishes that it already has been verified. The cached public key is used to verify the message. The computational cost of this reads V.

Summarizing, the total cost for verifying a certificate chain using explicit certificates reads V * n for the first verify and V for the subsequent ones.

5.1.5.3.3.3.2 Implicit Certificates

Verifying a message signed with an implicit certificate can be done in two steps: extracting the public key from the certificate and verifying the message. To extract the public key from a certificate, the public key from the issuer’s certificate is required. The public key extraction operation is also a double-multiply-and-add. Thus, verifying an implicit certificate chain can be done using V * (n + 1) operations: V for extracting the public key, and V * n for verifying the certificate chain. At the end of the operation,

[Cert ID, public key, “successfully verified”]

is cached. Subsequent messages signed by that certificate can be verified at a cost of V.

Summarizing, the total cost for verifying reads V * (n + 1) for the first verify, and V for the subsequent ones. This is slightly higher than for the explicit certificates case, but it should be observed that the same hardware as for the explicit case can be used. Recall that implicit certificates have an advantage in terms of size (64 byte in the considered case).

Finally, there is a way to improve the computational performance. Consider the case of a signed message with a certificate chain of length 2, i.e.,

[message, end-entity (implicit) certificate, known trusted (explicit) CA cert].

One can combine public key extraction and verification into a single operation, a "triple" multiply and add operation with cost approximately 1.16 * V. So the first verification comes at a cost of approximately 1.16 * V instead of 2 * V. However, combining operations in this way does not output the public key, so all subsequent operations (e.g., verifying subsequent messages signed with the same certificate) also come at a cost of 1.16 * V.

5.1.5.3.3.3.3 Hardware Support

There are two types of double-multiply-and-add that may be supported by hardware:

- Generic double-multiply-and-add, aX + bY
- Double-multiply-and-add where one point is the base, aX + bG. This second type is easier to accelerate because G is known, so various values can be pre-computed.

Verifying a signature only requires the second type of operation. Implicit certificate key extraction needs the first type. More precisely, it needs a subset of the first type, aX + Y. As a consequence, an accelerator for signature verification can only be applied partially for key extraction: it would be used to calculate aX, and Y would have to be added in software.

Adding Y in software would slow things down, but only marginally as a single point add takes less than 1/50 the time for a full multiply. This would add less than one msec to total latency on a 400 MHz processor. However, it is a slowdown compared to explicit certificates.

In conclusion, hardware that supports signature verification may support implicit certificate key extraction with no performance cost (if generic double multiply-and-add is supported), or it may require additional software processing to support implicit certificate key extraction. The software processing is non-zero time, but given that key extraction happens only when a certificate is first seen, if software processing is needed, its impact is very low.

5.1.5.3.3.3.4 Conclusions

In the following, certificate chains of reasonable length are assumed. Assuming one verifies signatures only occasionally (verify-on-demand), implicit certificates allow for an improvement in terms of size and computational effort, as there is no need to extract the public key from the implicit certificate. If every message is verified, it makes sense to extract the public key from the implicit certificate. In this case, implicit

certificates allow only for improvements in terms of size which comes at the cost of one additional double-multiply-and-add operation at the first verify. As extraction of the public key needs to be performed on the first verify only, the first type of double-multiply-and-add does not necessarily have to be implemented in hardware.

5.1.5.4 Special Cryptographic Primitives in SCMS

The CAMP SCMS uses some cryptographic techniques that are not in widespread use in other PKIs. This section provides relevant cryptographic background. In the subsection Crypto Primitives affecting End-Entity, we point out the primitives that also affect EEs.

5.1.5.4.1 Notation

To understand the special cryptographic constructions in this section, it is necessary to understand some of the underlying mathematics first. In the Elliptic Curve Cryptography system, the objects of interest are “elliptic curve points” which have the form (x, y) where (x, y) are all the points that are solutions of a particular cubic equation. A point P can be scalar-multiplied by an integer, a (a-times repeated addition of P by itself), to get a new point Q = aP. (Upper-case letters are used to indicate points, lower-case to indicate integers). In this coherence, multiplication of a point by an integer is defined so that it follows typical mathematical rules and always generates another point on the curve. The Elliptic Curve Discrete Logarithm Problem is basically the statement:

Given P and Q = aP, but not a, it is very difficult to work out the value of a.

In the following, for a, an element of {0, 1} and an integer b, a^b denotes a b-bit string of a's (e.g., 0^{64} is a 64-bit string of 0's); for bit strings c and d, c XOR d denotes their exclusive-OR; for bit strings x and y, x || y denotes their concatenation; and for a bit string Z and an integer n, $[Z]_n$ denotes n most significant bits of Z. For a key k and message m, AES(k, m) means AES encryption of m with k in ECB mode. In addition, unless otherwise noted, l is the order of the elliptic curve, la_id1 and la_id2 are 16-bit identifiers of linkage authorities LA1 and LA2, respectively, i, j, and k are 32-bit strings, and for brevity (i, j) are sometimes denoted by ι (Greek letter iota).

5.1.5.4.2 Time Periods

1. Cryptographic primitives explained in the sub-pages including SCP1: Butterfly Keys and SCP2: Linkage Values generate a sequence of cryptographic values. In other words, both techniques use functions that map from a known sequence (such as 1, 2, 3, …) to a sequence whose entries are *a priori* unknown and unpredictable. The cryptographic details of the functions do not depend on the exact form of the input sequence, so one natural way they could be defined would be for the input sequence to be a single counter *i* = {0, 1, 2, 3, …}. In practice, in this document, two different approaches to define the techniques are employed. When defining the techniques for purposes of explaining the core concept, the techniques are written as if they take an input defined by a single counter ι. This is the Greek letter *iota*.

2. For purposes of implementation, the input will be defined by two values, *i* and *j*. These are related to the pseudonym certificate provisioning model described in Use Case 3: OBE Pseudonym Certificates Provisioning. This use case utilizes a coarse time period with a counter *i* and a more granular counter *j*, which is reset to 0 at the start of each *i*-period.

Note that *i* and *j* uniquely define ι, an exemplary bijective. The term bijective is a mathematical term describing the characteristics of a function. A bijective function is both injective and surjective and implies a unique one-to-one relationship between the inputs and outputs of the function. When *i* and *j* are used for the input sequence, it is assumed that all devices and all SCMS components use the same value of *i* to denote the same time slot. In other words, *i* is a globally assigned variable, not a variable that individual OBEs or RAs have the ability to choose at will.

Pseudonym Certificate Validity

The length of the i-period should be the number of minutes in a week, 10080. We need to express it in minutes (as opposed to seconds) because the encoding in 1609.2 lets us use quantities of up to 2^{16} units and there are more than 2^{16} seconds in a week. The lifetime of the certificate is the i-period plus an overlap period. In the old design, the overlap period is one minute, but there are safety concerns with such a small overlap period, so we are extending the overlap period to one hour. This will enable vehicles to postpone certificate change if they are in an alert state that lasts more than a minute. With this extended overlap period, the lifetime of a pseudonym certificate is **10140 minutes**.

The start validity time of a pseudonym certificate is given in seconds since the 1609.2 epoch of 00:00:00 UTC, January 1, 2004.

If leap seconds happen, we may choose to adjust the start validity time of the certificates so it is not always 60*10080 seconds after the start of the previous batch but instead always lines up with the top of the hour. This concern is out of scope for POC and will be addressed later.

5.1.5.4.3 Clock Time Corresponding to global i=0

For the Safety Pilot, the clock time corresponding to i=0 was defined to be 00:00 UTC January 1, 2010. However, a lot has changed since, and in particular, the meanings of i and j have changed significantly in the old design. An important consideration for selecting the new clock time corresponding to i=0 is that changing i should cause minimum disruption to safety. According to http://www.forbes.com/2009/01/21/car-accident-times-forbeslife-cx_he_0121driving.html, the fewest deaths by crash happened between 4 and 5 am on Tuesday. With the highest population density on the East Coast, 4:00 am Eastern Standard Time makes most sense as during Daylight Saving Time, it will move to 5:00 am, which is still consistent with the above article. Considering all these, i=0 corresponds to: **4:00 am Eastern Standard Time on Tuesday, January 6, 2015** (i.e., in TAI 4023 days, 9 hours plus 3 leap seconds or **347,619,603 TAI seconds** since 1609.2 epoch).

5.1.5.4.4 Encryption of Pre-linkage Values by LA for PCA

In the old design, when LA sends pre-linkage values to RA for pseudonym certificate provisioning, it encrypts them for PCA using symmetric encryption. The secret key used for encryption is shared between LA and PCA through an out-of-band means. This has an impact on privacy (though only minor) from a malicious PCA, if RA uses more than one pair of LAs for a given PCA, as PCA can easily tell which pair of LAs were used in any given request sent by RA to PCA. This privacy impact can easily be mitigated if LA were to use public-key encryption for encrypting pre-linkage values for PCA, as a ciphertext generated using public-key encryption, does not need to contain any sender-related (in this case, LA) information. However, the team realized that using public-key encryption will add a significant amount of computational overhead on both LA and PCA, and decided to stick with symmetric encryption, **with a recommendation for RA to keep the number of pairs of LAs per PCA as low as possible, ideally one**.

5.1.5.4.5 Misbehavior Investigation: PCA Returns Encrypted Pre-linkage Values to MA

In the old design, during misbehavior investigation, PCA returns pre-linkage values to MA, which MA would then forward to LA. However, there is no need for MA to learn the pre-linkage values; PCA only needs to be able to point to a pre-linkage value that LA can then find information about. The design change is as follows: PCA returns an encrypted pre-linkage value to MA. The encrypted pre-linkage value matches the encrypted pre-linkage value that LA originally provided to PCA as part of the pseudonym certificate provisioning process.

The new design is described in Step 8.2: Misbehavior Investigation.

5.1.5.4.6 Crypto Primitives Affecting End-Entity

All of the changes mentioned below affect end-entities, and therefore they need to be informed to the V2V-SE team.

- SCP1: Butterfly Keys
- SCP2: Linkage Values
- Clock Time corresponding to i=0
- Pseudonym Certificate Validity

5.1.5.4.7 SCP1: Butterfly Keys

5.1.5.4.7.1 Summary

Butterfly Keys are a novel cryptographic construction that allow a device to request an arbitrary number of certificates, each with different signing keys and each encrypted with a different encryption key, using a request that contains only one verification public key "seed" and one encryption public key "seed" and two “expansion functions.” The expansion functions allow a second party to calculate an arbitrarily long sequence of statistically uncorrelated (as far as an outside observer is concerned) public keys such that only the original device knows the corresponding private keys. Without butterfly

keys, the device would have to send a unique verification key and a unique encryption key for each certificate. Butterfly keys reduce upload size, allowing requests to be made when there is only spotty connectivity, reduce the work to be done by the requester to calculate the keys, and smoothen peak requests.

A core principle of PKI implementations is that all private keys should be generated on the device that is going to use them. If private keys are generated off the device (and then installed on it), and if the device appears to misbehave, the device owner can claim that the misbehavior was actually carried out by whoever generated the keys. However, in the original CAMP design, a single device had over 100,000 certificates per year. Generating 100,000 distinct certificate requests would be a significant computational burden, and arguably an unnecessary one given that most vehicles are only in operation for about 5% of the time. Additionally, 100,000 distinct certificate requests would take a long time to upload and, if connections from the onboard equipment (device) to the CA are unreliable, there is a risk that certificate requests would not complete successfully within a single communication session.

The CAMP design thus updated its approach to use butterfly keys to address both these concerns. In the butterfly key approach, the certificate requester only needs to generate a single key pair and include the public key in a single certificate request. The difference from the standard approach is that the requester also creates an expansion function that allows a single public key to be expanded into multiple public keys and a single private key to be expanded into multiple private keys, while ensuring that only someone who knows the original private key will know the expanded private keys (i.e., the device). This reduces the computational burden on the device (it only has to generate one key) and also the size of the upload (reduced to less than 1K bytes). The cost is that the download of certificate responses increases in size.

5.1.5.4.7.2 Preliminaries

5.1.5.4.7.2.1 i and j Values

1. For **pseudonym** certificates, the i value used in any certificate is the *global* i value.
    a. The clock time corresponding to the global i=0 shall be as per Special Cryptographic Primitives in SCMS.
    b. The increment period for the global i value shall be fixed at 1 week, i.e., 7*24 hours, where *hours* is the field defined under the type Duration in IEEE 1609.2, see https://github.com/wwhyte-si/1609dot2-asn/blob/master/1609dot2-base-types.asn.
    c. The j value shall range from 0 to j_{max}-1. For POC and CV Pilots, j_{max} for all devices is fixed at 20.
2. For **identification** certificates, the i value used in any certificate is the *local* i value corresponding to the *enrollment* certificate used for requesting that identification certificate.
    a. The clock time corresponding to that local i=0 shall be the value of *toBeSigned.validityPeriod.start* field of the *enrollment* certificate.

b. The increment period for that local i value shall be the value of *toBeSigned.validityPeriod.duration* field (minus the overlap period, see PoC Certificate Expiration Timelines, CV Pilot PROD Certificate Expiration Timelines) of the *identification* certificate.

c. For POC and CV Pilots, the j value for all devices is fixed at 0.

5.1.5.4.7.3 Description

Butterfly keys make use of ECDLP as follows. There is an agreed "base point" called G (this is standard practice for elliptic curve cryptography). The device generates two ECC key-pairs (a, A = aG) (seed for the signing keys) and (p, P = pG) (seed for keys used for encrypting the certificates, i.e., encryption keys), and descriptions of two expansion functions f1 (for signing keys) and f2 (for encryption keys). The expansion functions map an integer ı to another integer in a range from 0 to l, the order of the elliptic curve. Functions f1 and f2 are designed to be cryptographically secure, which roughly means that the output looks random so that given two values of {f1(ı), ı} (or, {f2(ı), ı}), a third party cannot tell whether the two values were generated by the same version of f1 (or, f2), or by different versions. The vehicle stores a, p, and descriptions of f1 and f2, and sends A, P, and description of f1 and f2 encrypted to the SCMS. In the CAMP design, the expansion functions are defined as:

1. $f1(k, ı) = f1^{int}(k, ı) \bmod l$, where
    a. $f1^{int}(k, ı)$ is the big-endian integer representation of (AES(k, x+1) XOR (x+1)) || (AES(k, x+2) XOR (x+2)) || (AES(k, x+3) XOR (x+3)),
    b. x+1, x+2, and x+3 are obtained by simply incrementing x by 1 each time, e.g., if x = 01 … 00, then x+1 = 01 … 01, x+2 = 01 … 10, x+3 = 01 … 11,
    c. 128-bit input x for AES is derived from time period ı = (i, j) as: (0^{32} || i || j || 0^{32}).
2. f2(k, ı) is defined in an identical way as f1(k, ı), **except** x is derived as: **(1^{32} || i || j || 0^{32})**.

The "description" of f1 and f2 are simply the AES keys ck (for signing keys) and ek (for encryption keys): to generate f1 and f2 the device simply generates 2 AES keys ck and ek, and to send the description of f1 and f2 the device sends ck and ek.

Now the SCMS has the ability to generate an extremely large number of derived points: it can generate

- $B_ı = A + f1(ck, ı) * G$, with A = aG (signing keys)
- $Q_ı = P + f2(ek, ı) * G$, with P = pG (encryption keys)

The corresponding private keys will be

- $b_ı = a + f1(ck, ı)$ (signing keys)
- $q_ı = p + f2(ek, ı)$ (encryption keys)

Since the SCMS doesn't know the original value of a (or, p), it cannot know any of the $b_ı$ (or, $q_ı$) values, so it can generate an arbitrary number of public keys for which only

the vehicle knows the corresponding private keys. Additionally, because the expansion functions are cryptographically secure, anyone who doesn't know the description of f1 cannot tell whether two different signing public keys belong to the same series $\{B_i\}$ or to different series. This means that the RA, described in detail later, can safely use f1 to create an expanded list of signing public keys to send to the CA, and the CA will not be able to tell that the keys belong to the same vehicle.

In the CAMP SCMS, this underlying approach is used as follows. Note: There are a couple of minor technical differences between this description and the CAMP approach – explained after this description, which focuses on the core butterfly key operations and omits optimizations that might obscure the explanation:

- Device generates two 128-bit AES keys ck and ek, for expansion functions of signing keys and encryption keys, respectively, and two "caterpillar" key pairs:
    - (a, A = aG) used for signing, i.e., A to be placed in the certificate
    - (p, P = pG) used for encryption of the certificate

Device sends {ck, ek, A, P} to the RA. Note: ck will define the expansion function for the signing keys and ek will define the expansion function for the encryption keys.

- RA uses ck to generate $\{B_i\}$, the series of "cocoon" signing public keys for the certificate requests, and ek to generate $\{Q_i\}$, the series of cocoon encryption public keys for encrypting the certificate response, pairs each B_i with the corresponding Q_i, and sends the pairs $\{B_i, Q_i\}$ to the CA.
- CA does not know which public keys have come from the same device, but RA knows which public keys are in the requests, so CA must further randomize the public keys to hide them from RA. For each request, CA generates a unique random integer c and sets the public key in each certificate to the "butterfly" value $(B_i + cG)$. CA then uses Q_i to encrypt the response, which contains:
    - Certificate containing the public key $(B_i + cG)$
    - CA's contribution to the private key, c
- RA sends the encrypted message to the device along with the corresponding ı.
- Device uses ek, p, ı to calculate q_i. It uses q_i to decrypt the response and recover the certificate containing the public key $(B_i + cG)$ and CA's contribution to the private key, c. It then uses ck, a, ı to calculate b_i. The private key for the certificate is then:
    - Butterfly private key = b_i (calculated above) + c (provided by CA)

Device should at this point check that the recovered private key corresponds to the public key certified by the certificate to ensure that it has been sent the correct certificate.

This means that the device has obtained a set of certificates such that:

- Only the device knows the private keys

- RA does not know the public keys in the certificates
- CA cannot tell from the requests alone which requests have come from the same device

Notes:

1. In the CAMP design, there are a couple of differences. First, implicit certificates are used by a device, so the CA's contribution to the private key is calculated slightly differently; however, the principle is the same, namely that the CA modifies the public key and sends information to the vehicle that allows it to make the corresponding modification to the private key. Moreover, in the table below, butterfly keys process has been summarized for both explicit and implicit certificates. Second, the CA additionally signs (using its private key) the encrypted implicit certificate to prevent a man-in-the-middle (MITM) attack by the RA. To launch the MITM attack, the RA can simply use a different public key of its choice (for which it knows the corresponding private key) in the request to the CA, so that it can decrypt the encrypted response by the CA, view the underlying certificate, and then while responding to the vehicle encrypt the certificate with the right public key.
2. Since the RA knows the public encryption key J_i, it could in principle create a fake response to the vehicle. This would allow the RA to give a set of known certificates to a target vehicle, allowing the RA to track. However, any fake response will not have been created with the CA private key and so the vehicle can detect this attack and discard the resulting keys.
3. The per-certificate value *c* generated by the CA is vital in hiding the final certified public key from the RA. If *c* were a constant, all the certificates would be related to their requests in some known way, and the RA could work out the set of certificates corresponding to a set of certificate requests and track the vehicle. Likewise, if the CA generates *c* with bad randomness, or with randomness that is known to the RA, then the RA may be able to work out which certificate belongs to which vehicle. (see Random Number Generators under CB2: Types of Cryptographic Algorithms and Approved Random Number Generators for further details on "good randomness.").
4. Test vectors for butterfly expansion function are available at http://stash.campllc.org/projects/SCMS/repos/crypto-test-vectors/browse/bfkeyexp.txt

Table 11 Butterfly Key

	Device	RA	PCA
Explicit Certs	1) Generate: a) AES key ck for expansion function of **signing** keys	3) For each ı, compute: a) "Cocoon" signing public keys for certificate requests, $B_ı = A + f1(ck, ı) * G$	5) Generate an ECC key pair (c, C = cG) for hiding the signing public key from RA, and compute the "butterfly" public key ($B_ı$+ C)

	Device	RA	PCA
	b) AES key ek for expansion function of **encryption** keys c) ECC key pair (a, A = aG) for **signing**, i.e., “caterpillar” signing key pair d) ECC key pair (p, P = pG) for **encryption of the certificate**, i.e., "caterpillar" encryption key pair 2) Send (ck, ek, A, P) to RA	b) "Cocoon" encryption public keys for encrypting the certificate response, $Q_ı$ = P + f2(ek, ı) * G 4) For each ı, send ($B_ı$, $Q_ı$) individually to PCA	6) Generate an explicit certificate on butterfly public key ($B_ı$+ C), encrypt (certificate, c) with $Q_ı$, sign the ciphertext again, and send the signed ciphertext to RA
		7) Collate all the signed ciphertexts along with the corresponding ı value for a device and send them to device	
	8) For each ı, compute: a) Cocoon signing private keys, $b_ı$ = a + f1(ck, ı) (mod l) b) Cocoon decryption keys for decrypting the certificate response, $q_ı$ = p + f2(ek, ı) (mod l) 9) For each ı, verify PCA’s signature on the ciphertext: a) If verification succeeds, decrypt the ciphertext using $q_ı$ to obtain (certificate, c). Compute the “butterfly” private key corresponding to the public key in the certificate: ($b_ı$ + c) (mod l) b) If verification fails, abort and report to MA.		
Implicit Certs	1) Generate: a) AES key ck for expansion function of **signing** keys	3) For each ı, compute: a) “Cocoon” signing public keys for certificate requests, $B_ı$ = A + f1(ck, ı) * G	5) Generate an implicit certificate on $B_ı$, let the private and public reconstruction values be r and R, respectively

	Device	RA	PCA
	b) AES key ek for expansion function of **encryption** keys c) ECC key pair (a, A = aG) for **signing**, i.e., “caterpillar” signing key pair d) ECC key pair (p, P = pG) for **encryption of the certificate**, i.e., "caterpillar" encryption key pair 2) Send (ck, ek, A, P) to RA	b) "Cocoon" encryption public keys for encrypting the certificate response, $Q_ı$ = P + f2(ek, ı) * G 4) For each ı, send ($B_ı$, $Q_ı$) individually to PCA	6) Encrypt (r, R) with $Q_ı$, sign the ciphertext again, and send the signed ciphertext to RA
		7) Collate all the signed ciphertexts along with the corresponding ı value for a device and send them to device	
	8) For each ı, compute: a) Cocoon signing private keys, $b_ı$ = a + f1(ck, ı) (mod l) b) Cocoon decryption keys for decrypting the certificate response, $q_ı$ = p + f2(ek, ı) (mod l) 9) For each ı, verify PCA’s signature on the ciphertext: a) If verification succeeds, decrypt the ciphertext using $q_ı$ to obtain (r, R). Reconstruct the “butterfly” private key corresponding to the certificate using $b_ı$ and r. b) If verification fails, abort and report to MA.		

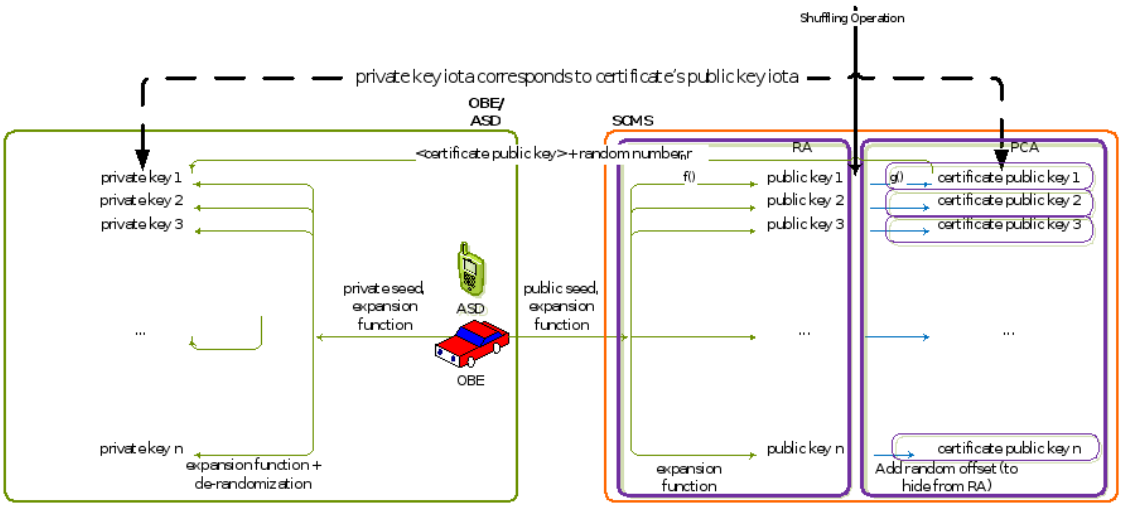


Figure 34 Butterfly Key Mechanism

5.1.5.4.8 SCP2: Linkage Values

5.1.5.4.8.1 Summary

To support efficient revocation, end-entity certificates contain a linkage value (LV), which is derived from (cryptographic) linkage seed material. Publication of the seed is sufficient to revoke all certificates belonging to the revoked device, but without the seed an eavesdropper cannot tell which certificates belong to a particular device. Note: The revocation process is designed such that it does not give up backward privacy. For protection against insider attacks by the SCMS, the LV is the combination of two pre-linkage values (PLVs) produced by two independent LAs; this ensures that no single SCMS entity knows all the information belonging to a single device. An extension to the linkage values approach allows for group revocation, so that if all devices of a particular type have a flaw they can be revoked with a single entry on the revocation list, while keeping group membership secret until the relevant group seed is revealed. Group revocation is currently not implemented as no practical real-world use case been identified so far.

LVs and LAs are used to enable the SCMS to help achieve the following preliminary design requirements, which were developed by the research team to ensure appropriate privacy protections and efficiency:

1. There is an efficient way of revoking all the certificates within a device
2. Certificates are not linkable by an eavesdropper unless the owner has been revoked
3. A vehicle is trackable only after its credentials are revoked but not before it was revoked.

4. No single entity within the system is able to determine that two certificates belong to the same device. An exception to this rule is the Misbehavior Authority (MA).
5. No single entity within the SCMS is able to track a vehicle. Once a single LA is introduced, this requirement is not fulfilled any longer. For that reason, two LAs are used and the information which allows for tracking is split between them.

5.1.5.4.8.2 Description

The basic concept of LVs uses the well-known cryptographic construction known as a hash chain. As described above, a hash algorithm is like a cryptographic checksum; if the hash of 'a' is computed as H(a) = b, it is very hard for someone who sees only b to derive the input a, but given a and b it is trivial to determine that a hashes to b. Hence, it is desirable to have a series of identifiers in each certificate such that if a secret is revealed, the identifiers can be linked.

First a description of the revocation of individual nodes is provided. For simplicity, a system with a single LA that generates LVs is initially described. This system meets requirements 1), 2), and 3) discussed, above. It does not meet requirement 4), because the LA can link certificates. The following describes the basic process for a single series of certificates. A more detailed description will be provided below. For a complete description of the process see Section 4.2.2.

- LA starts with an initial linkage seed (ILS), ls(0). (This will be different for each vehicle.)
- For each time period i > 0, LA sets the LS ls(i) = H(ls(i-1)), for some hash function H (SHA-256, a National Institute for Standards and Technology (NIST)-approved standardized hash algorithm that is used throughout IEEE 1609.2 is employed)
- The certificate for each time period i contains the linkage value lv(i) = AES(ls(i), 0)
- To revoke a vehicle from time period i onwards, the revocation authority publishes ls(i)
- To check revocation at time period i' > i, the recipient of a signed message:
    - Hashes ls(i), and then hashes the output of the hash, repeated (i'-i) times to obtain ls(i')
    - Calculates lv(i') = AES(ls(i'), 0)
    - Checks whether the certificate that signed the message contains the LV lv(i'). If it does, the certificate is considered revoked and the message is rejected

This achieves requirements 1), 2), and 3) as follows:

- Efficient revocation: Only one value needs be published to revoke all the certificates on a vehicle. The cost of maintaining the revocation data on the receiver side is one hash per revoked vehicle per time period. Hashing is very efficient, so this maintenance is inexpensive in terms of processing.

- Unlinkability against eavesdroppers: To tell if two certificates belong to the same vehicle, an eavesdropper would have to determine the two LSs ls1, ls2 that encrypt 0 to the PLVs plv1, plv2 in the certificates. Since AES is assumed to be a secure block cipher, this is not possible.
- Retrospective unlinkability: The hash chain can be run forward from the revocation value ls(i), but not backwards to recover previous values of ls(i). (This is a result of the non-invertibility of hash functions.)

However, the system has the problem that the LVs are generated centrally and the entity that generates the LVs knows the complete set of values that belong to a vehicle. To overcome this problem, the CAMP SCMS uses two LAs: LA1 and LA2.

In the description above, there is a single chain of LSs and LVs. In the CAMP SCMS, each of the LAs generates a chain of PLVs. These PLVs are individually encrypted and passed to the PCA; the PCA then XORs them together to obtain the LV that is put in the certificate. Now neither of the LAs knows the XORed linkage values that appear in the final certificate, because neither knows the values produced by the other LA. To revoke, the MA publishes the LSs from both LAs, and the recipient reconstructs both chains of PLVs and carries out the XORing to obtain the LVs for revoked certificates. The following describes the generation process in more detail:

- LA1 starts with a random ILS, ls1(0)
- LA2 starts with a random ILS, ls2(0)
- For each time period i > 0:
    - LA1 sets its LS ls1(i) = H(ls1(i-1)), and LA2 sets its LS ls2(i) = H(ls2(i-1))
    - LA1 sets its PLV, defined as plv1(i) = AES(ls1(i), 0) and LA2 sets its plv2(i) = AES(ls2(i), 0)
    - The CA sets the LV lv(i) = plv1(i) XOR plv2(i) and puts it in the certificate for time period i
- To revoke a vehicle from time period i onward, the revocation authority publishes the linkage seeds ls1(i) and ls2(i)
- To check revocation at time period i' > i, the recipient of a signed message:
    - Iteratively hashes ls1(i) (i'-i) times to obtain ls1(i'); does the same for ls2(i)
    - Calculates PLVs plv1(i') = AES(ls1(i'), 0) and plv2(i') = AES(ls2(i'), 0)
    - Checks whether the certificate that signed the message contains the LV lv(i') = plv1(i') XOR plv2(i'). If it does, the certificate is considered revoked and the message is rejected.

Four additional refinements in the CAMP SCMS are:

1. Instead of using a single time period counter i, time periods are denoted (i, j), where i counts up larger time periods (e.g., a day, a week, etc.) and j can be used in one of (at least) two ways: (a) for non-overlapping certificates, it can count up smaller

time intervals within the larger time periods (e.g., 5-minute intervals); (b) for overlapping certificates, it can specify the number of certificates that are valid in a given time period i (e.g., fixing the range of j as 1-20 would imply that 20 certificates are valid simultaneously). The LSs ls1(i) and ls2(i) are calculated as described above, but the PLVs plv1(i, j) and plv2(i, j) are calculated as AES(ls1(i), j) and AES(ls2(i), j) , respectively. The reason for this is to save time for vehicles that have been offline for some time. If a vehicle has been turned off for 1 year, without this refinement, at key-on the vehicle will have to carry out 52 * 20 hashes for each revocation entry to bring its revocation information up to date (assuming that a vehicle is issued 20 simultaneously-valid certificates per week). With this refinement, the vehicle only has to perform one hash per week for each revocation entry. If revocation lists get large, this efficiency gain may be very useful.

2. To reduce the chance of collisions in the PLVs between two LAs, their identities are also employed during the computation of LSs and PLVs: la_id1 and la_id2 are unique 16-bit identity strings associated with LA1 and LA2, respectively. The LSs are calculated as: ls1(i) = H(la_id1 || ls1(i-1)), ls2(i) = H(la_id2 || ls2(i-1)). The PLVs are calculated as: plv1(i,j) = AES(ls1(i), la_id1 || j), plv2(i,j) = AES(ls2(i), la_id2 || j). This means that even if two LAs produce the same LS for a given time period, they will produce different sets of PLVs (because of the use of the identifier to produce the PLV from the LS), and their LSs will be different in the next time period (because of the use of the identifier to create the next seed from the current seed).
3. To reduce the size of certificate revocation list (CRL), which contains the LSs of the revoked vehicles, the LSs are truncated to 16 bytes.
4. Instead of plain AES, AES is used in the Davies-Meyer mode as a derivation function, which is basically XORing the output of AES with the input. In particular, for a key k and message m, instead of $AES_k(m)$, ($AES_k(m)$ XOR m) is returned for every invocation of AES.

The table below summarizes the linkage value generation and the figure below visualizes the described scheme. Test vectors for Linkage Values are available at http://stash.campllc.org/projects/SCMS/repos/crypto-test-vectors/browse/lv.txt

Table 12 Linkage Values

LA1	LA2	RA	PCA
1. Generate initial linkage seed, ls1(0) (128-bit string chosen at random for every device).	1. Generate initial linkage seed, ls2(0) (128-bit string chosen at random for every device).	5. Include encrypted plv1(i, j) and plv2(i, j) in the certificate request.	6. Decrypt the packet from RA to obtain plv1(i, j) and plv2(i, j).
2. Compute linkage seed for i^{th} period through an iterative process defined as: ls1(i) = $[SHA\text{-}256(la\_id1 \| ls1(i\text{-}1) \| 0^{112})]_{128}$.	2. Compute linkage seed for i^{th} period through an iterative process defined as: ls2(i) = $[SHA\text{-}256(la\_id2 \| ls2(i\text{-}1) \| 0^{112})]_{128}$.		7. Compute linkage value, lv(i, j) = plv1(i, j) XOR plv2(i, j)

LA1	LA2	RA	PCA
3. Compute pre-linkage value, plv1(i, j) = [(AES(ls1(i), la_id1 || j || 0^{80})) XOR (la_id1 || j || 0^{80})]$_{72}$. 4. Encrypt plv1(i, j) for PCA, and send it to RA.	3. Compute pre-linkage value, plv2(i, j) = [(AES(ls2(i), la_id2 || j || 0^{80})) XOR (la_id2 || j || 0^{80})]$_{72}$. 4. Encrypt plv2(i, j) for PCA, and send it to RA.		

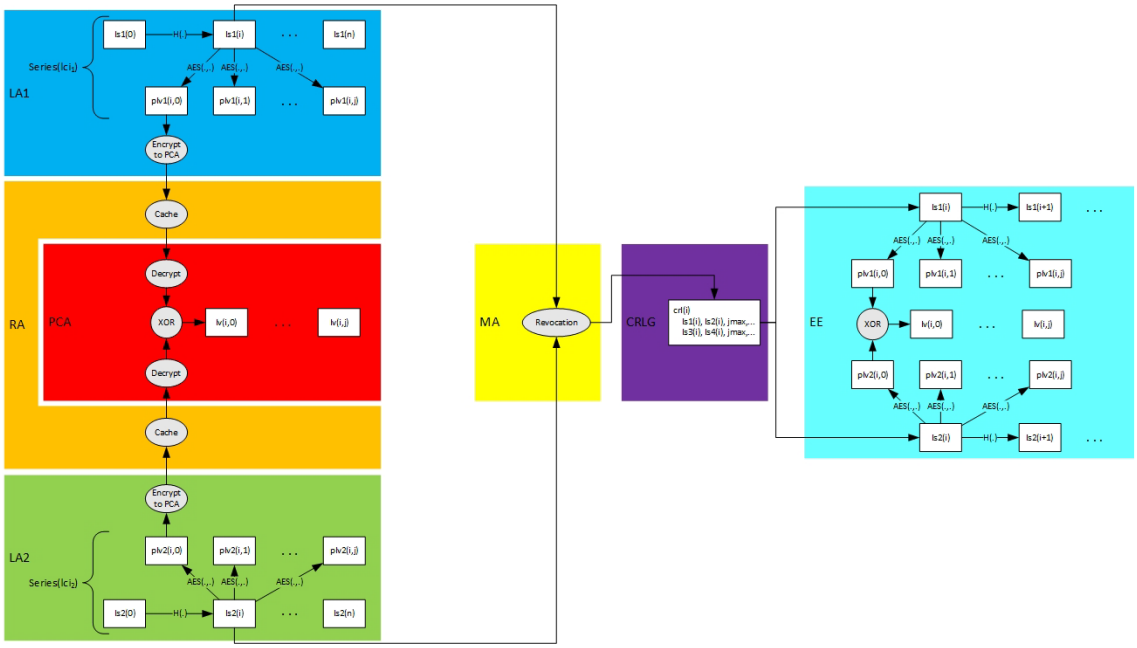


Figure 35 Creation of Individual Linkage Values and Revocation of Individual Device

5.1.6 CRL Series Diagram

This is the CRL series diagram for POC / Pilot Deployments.

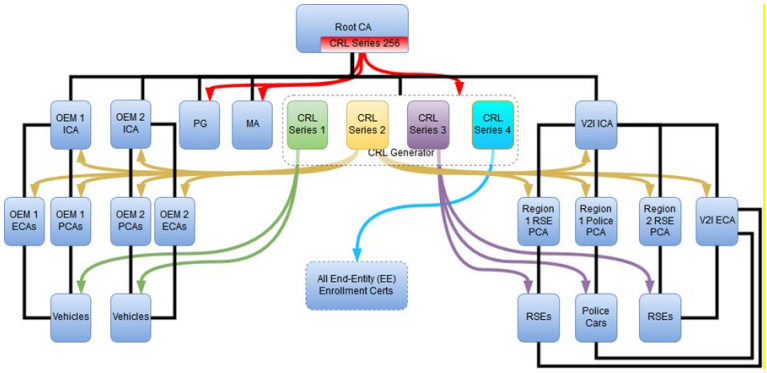


Figure 36 CRL Series Diagram

5.1.7 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.

5.1.7.1 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.

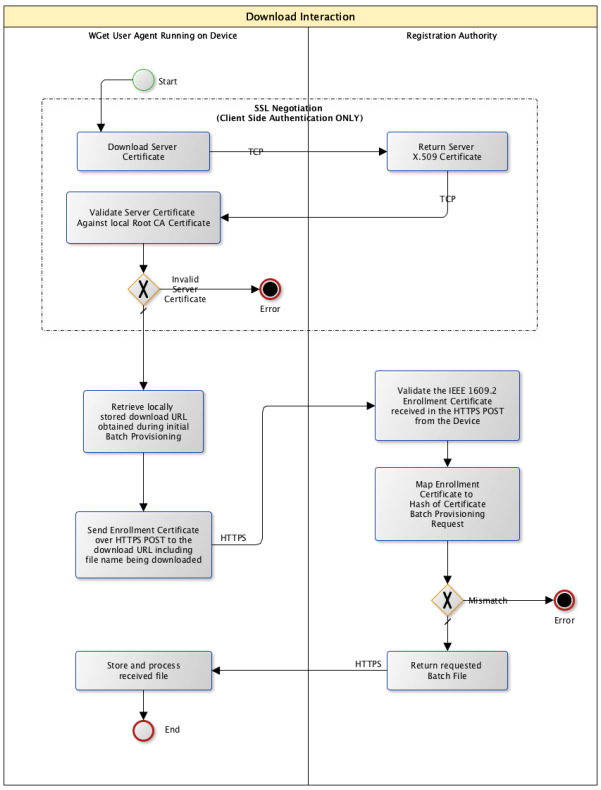


Figure 37 EE-RA Download Interaction

5.1.7.2 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.

5.1.7.3 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.

5.1.7.4 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.

5.1.7.5 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.

5.1.8 EE-SCMS Core Communication Requirements

5.1.8.1 Goals

- The goal of the EE-SCMS Core Communication Requirements section is to define all requirements that an EE must follow whenever establishing a connection to the SCMS.
- Individual requirements shall be labeled with their respective use case(s).
- In cases where a specific use case has a conflicting requirement, that use case shall define the new requirement and reference which core requirement is being overridden.

5.1.8.2 Background and Strategic Fit

5.1.8.2.1 IP Address Translation

- Prevent SCMS component (RA, CRL Store, etc.) from learning location information based on the IP address of the EE.
- LOP & SCMS Component must have adequate separation.

5.1.8.2.2 TLS Connection

- Provide a means to verify the identity of the SCMS component by using x.509 1-way authentication.
- Encryption is an added privacy preserving enhancement but not a core requirement.

5.1.8.2.3 IEEE 1609.2 Encrypting and/or Signing

- Provides application layer security and privacy.

5.1.8.3 Diagrams of Communications Methods

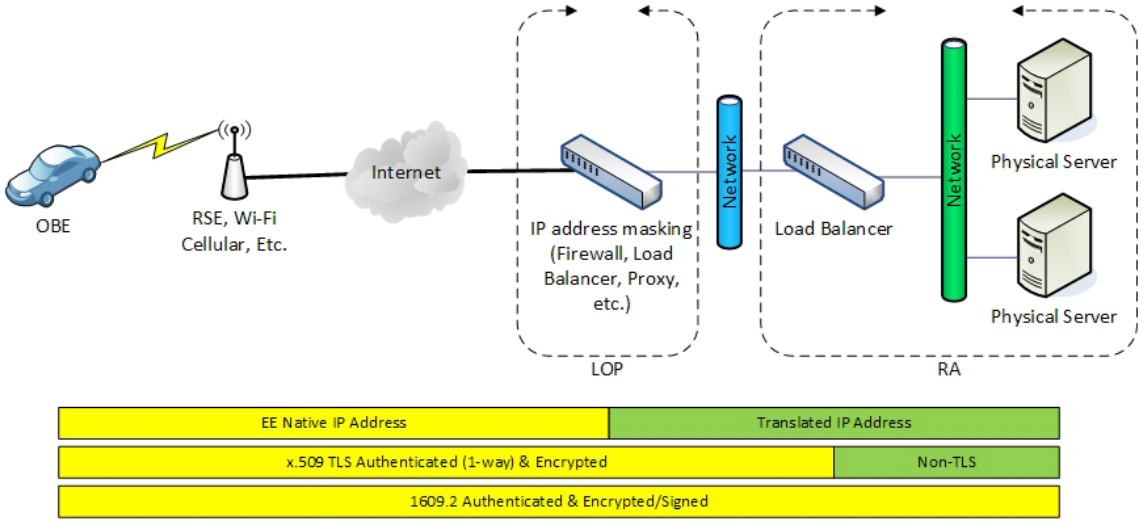


Figure 38 Overview of Methods

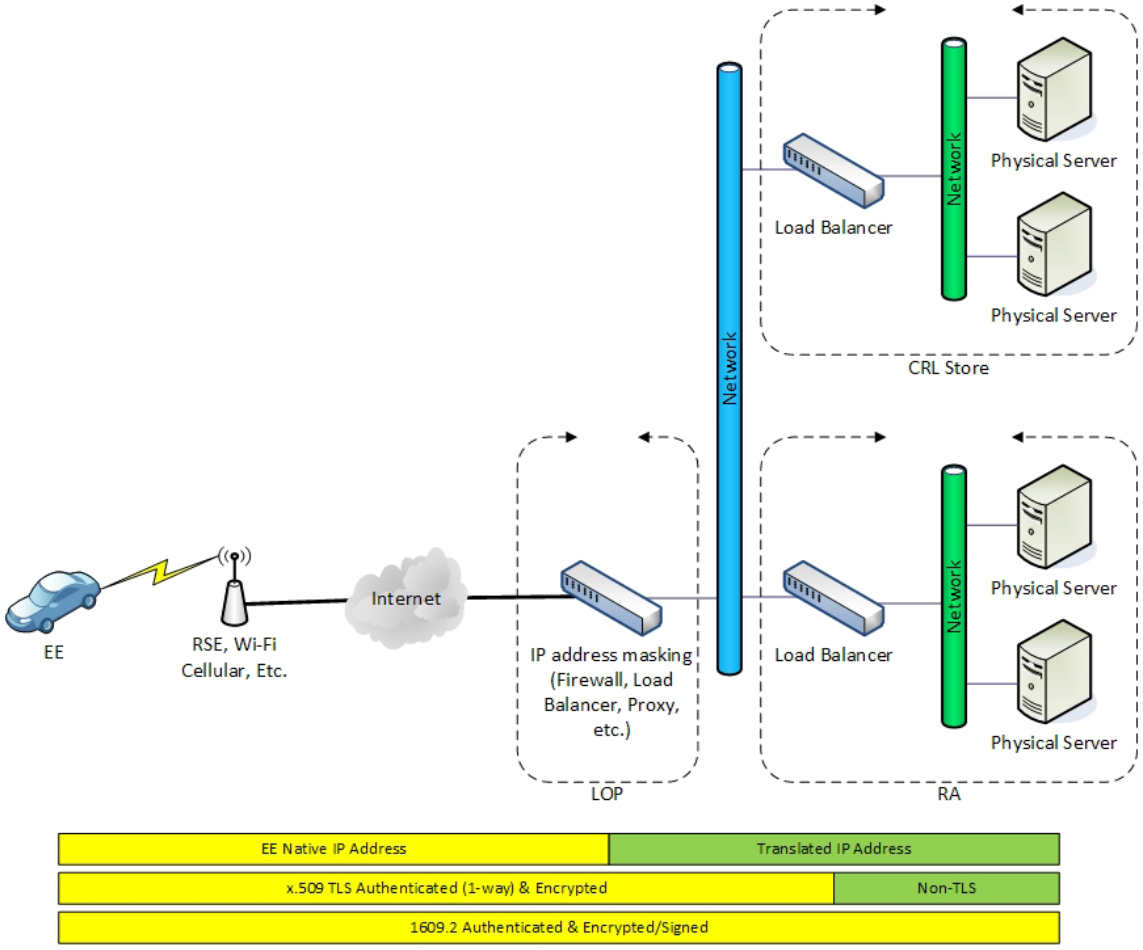


Figure 39 Overview of Multiple SCMS Components Served by Single LOP

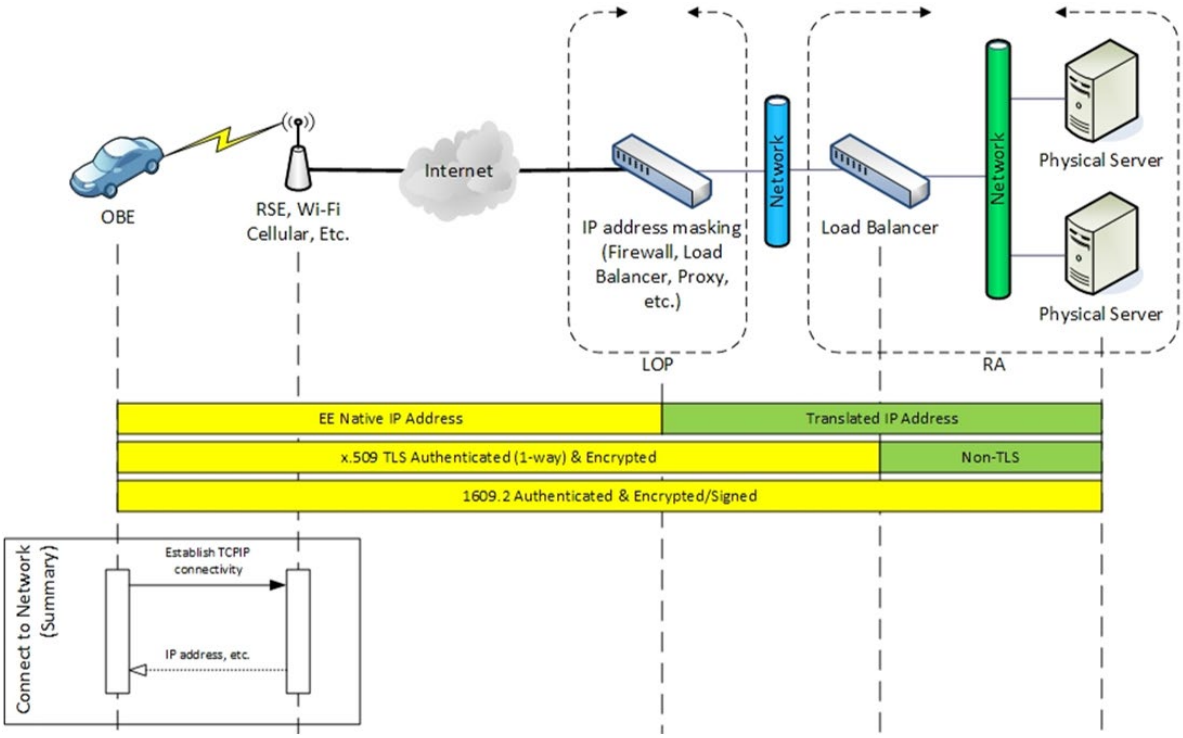


Figure 40 Universal SCMS Handshake Processes, 1 of 5

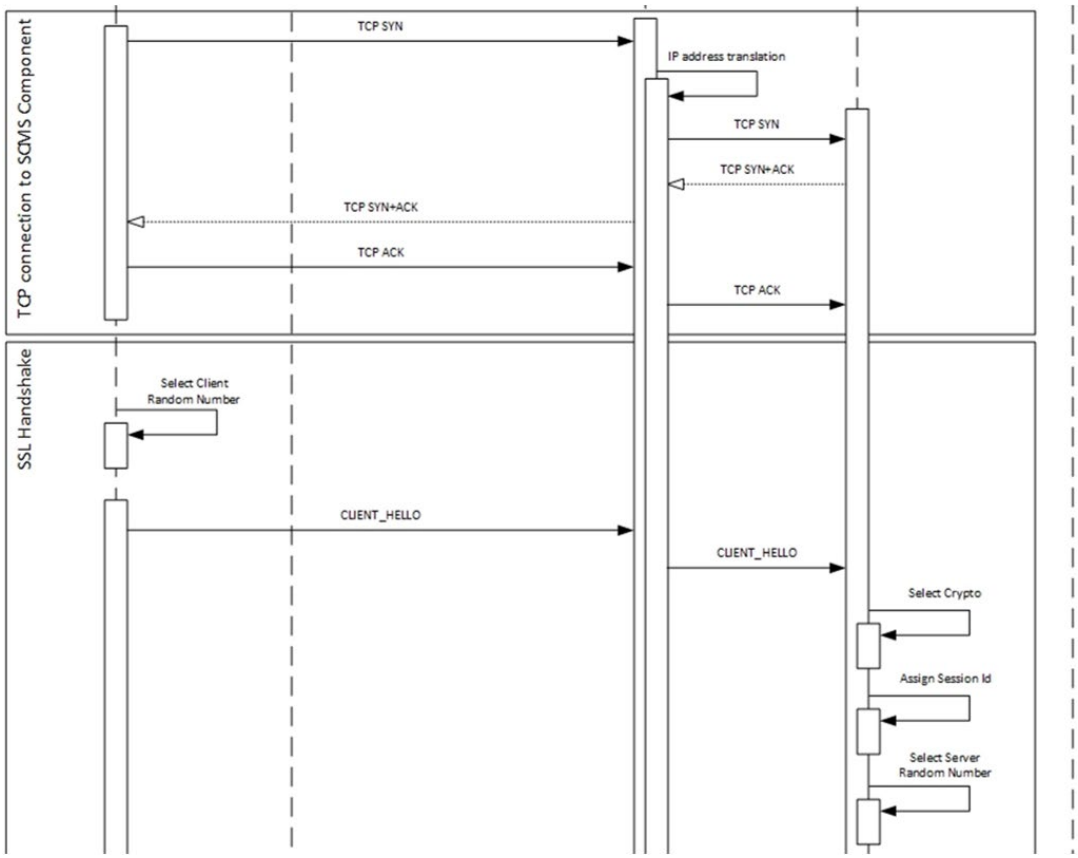


Figure 41 Universal SCMS Handshake Processes, 2 of 5

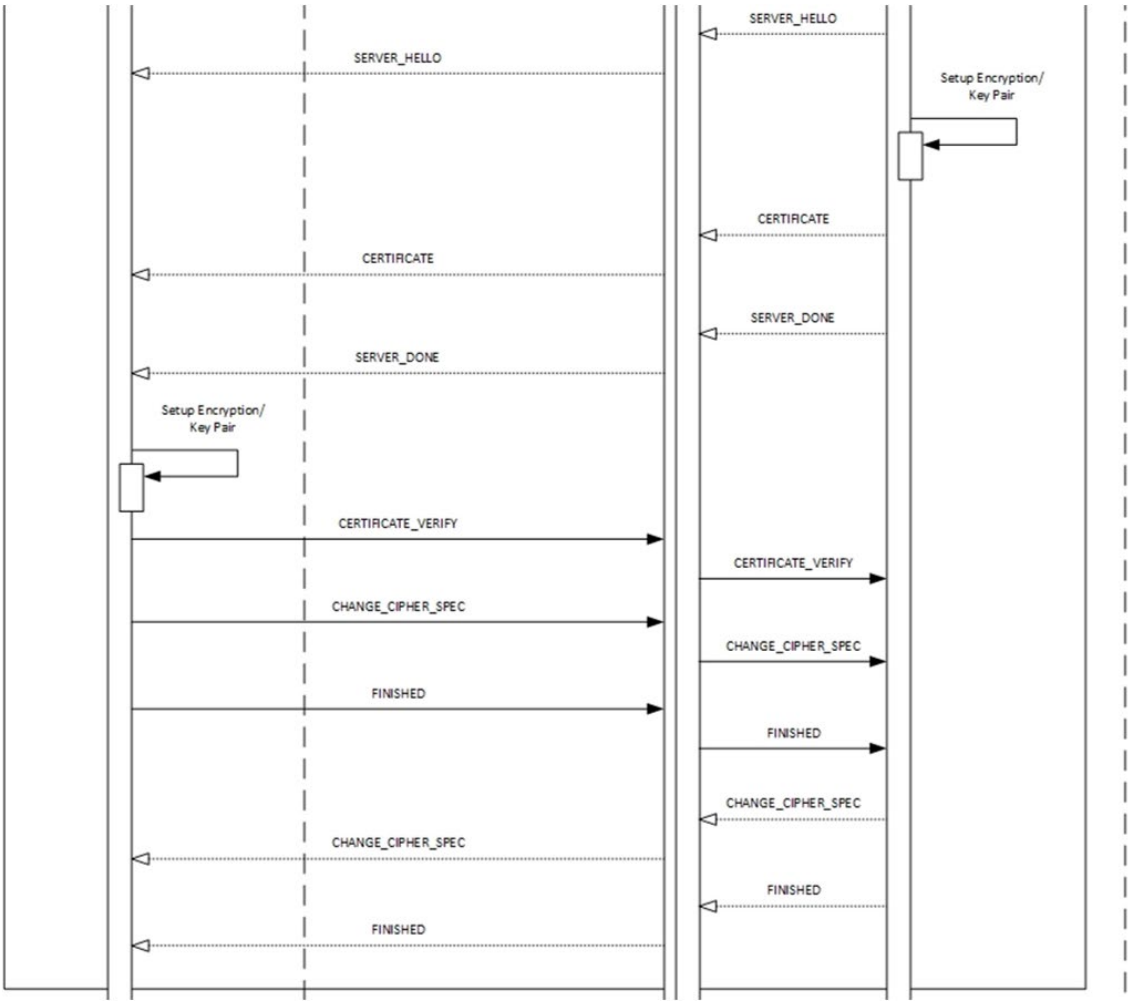


Figure 42 Universal SCMS Handshake Processes, 3 of 5

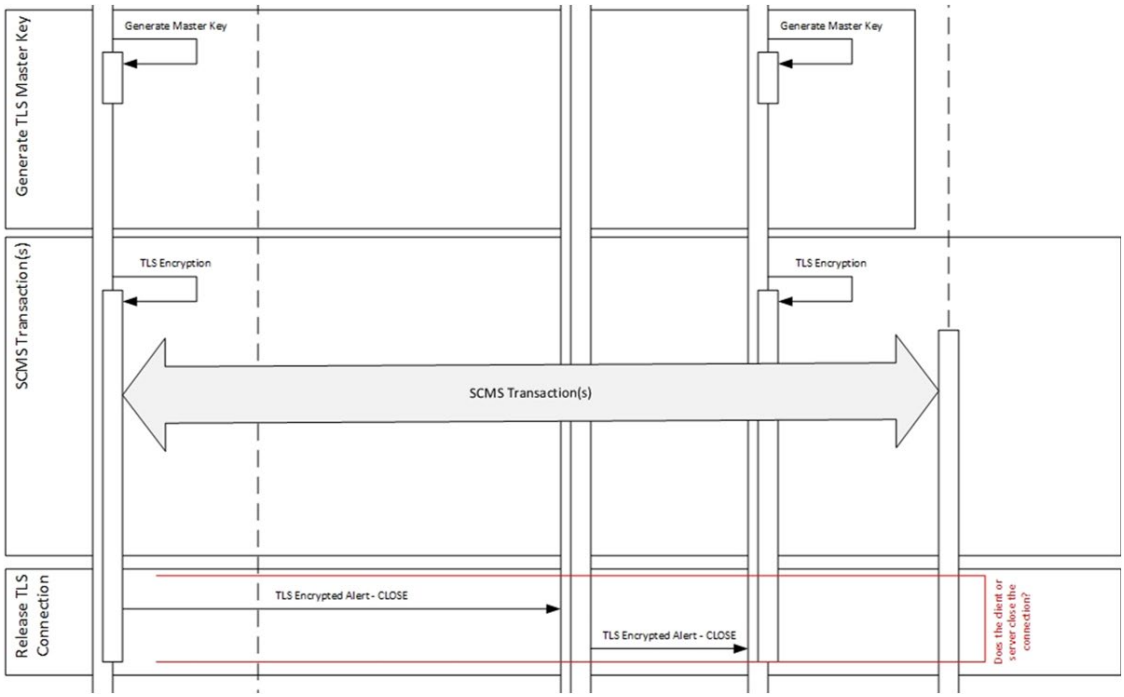


Figure 43 Universal SCMS Handshake Processes, 4 of 5

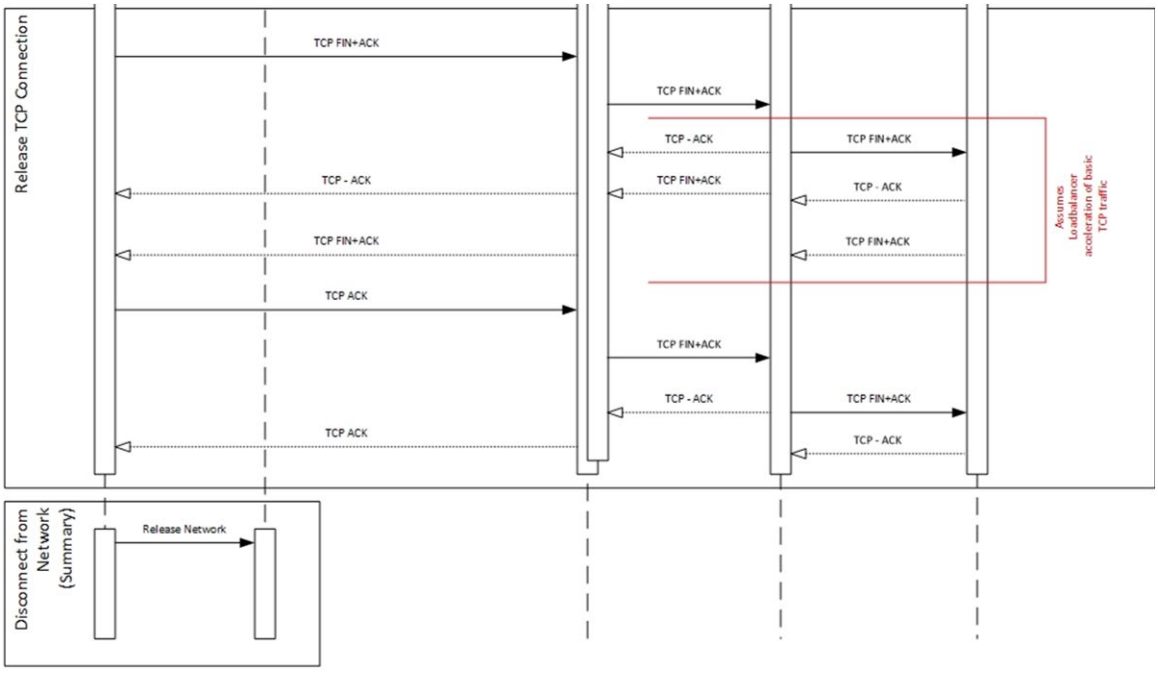


Figure 44 Universal SCMS Handshake Processes, 5 of 5

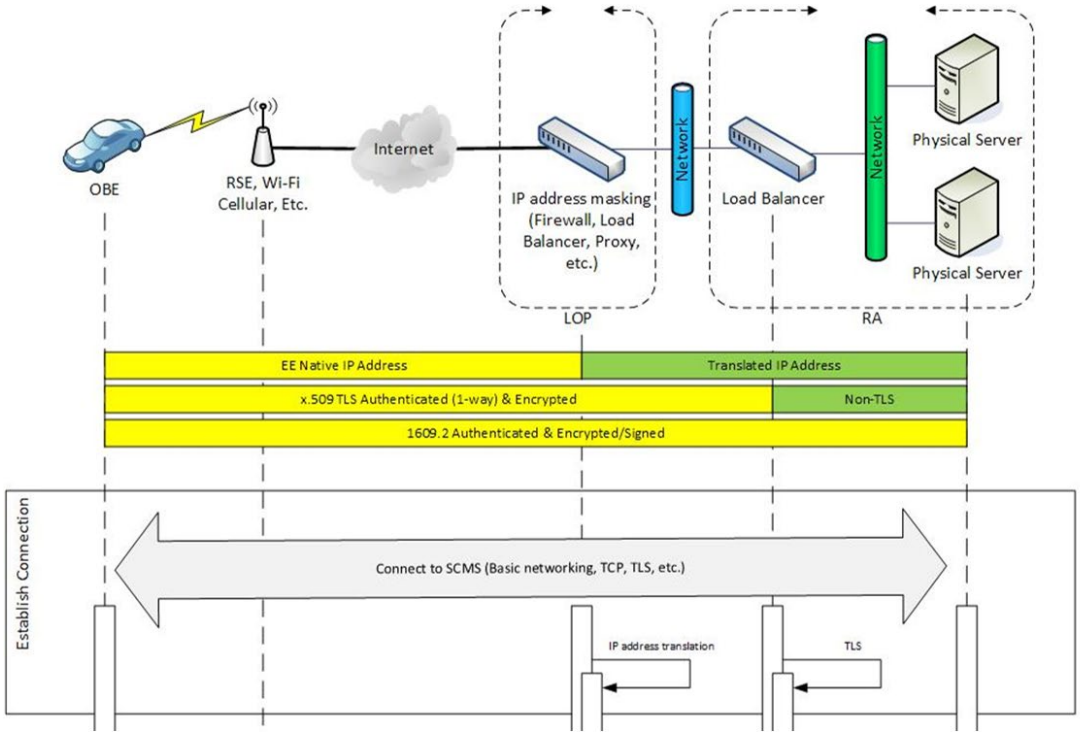


Figure 45 Common Process for File Download Operations, 1 of 3

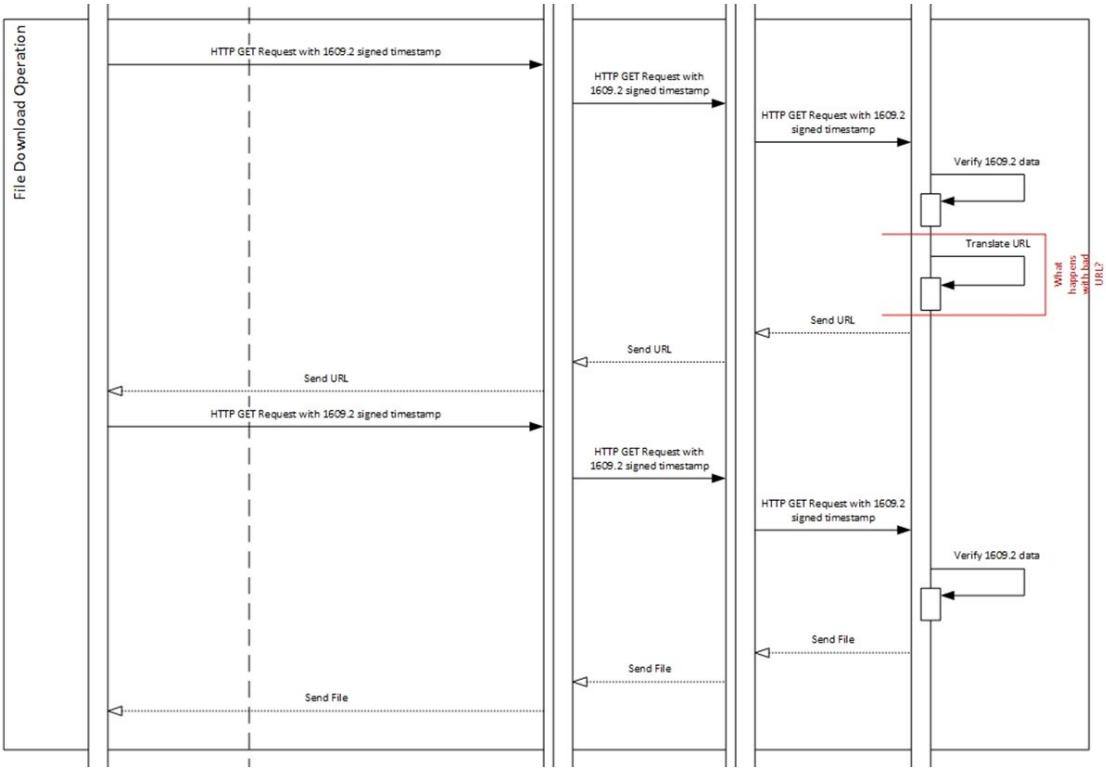


Figure 46 Common Process for File Download Operations, 2 of 3

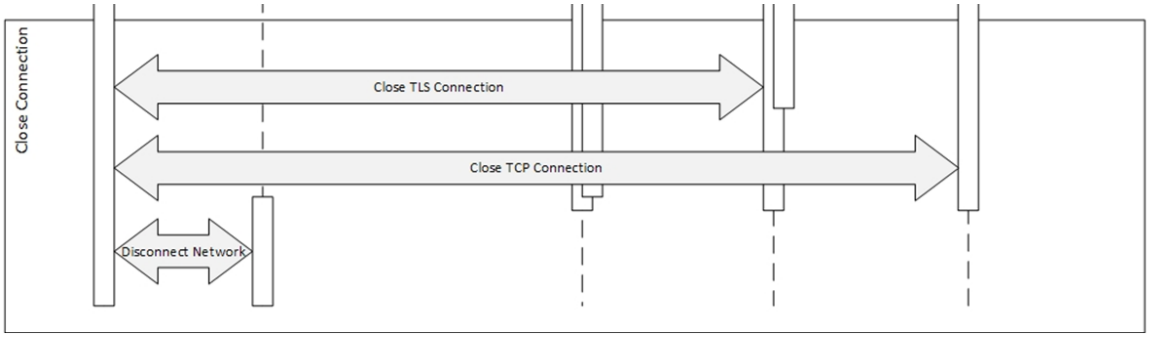


Figure 47 Common Process for File Download Operations, 3 of 3

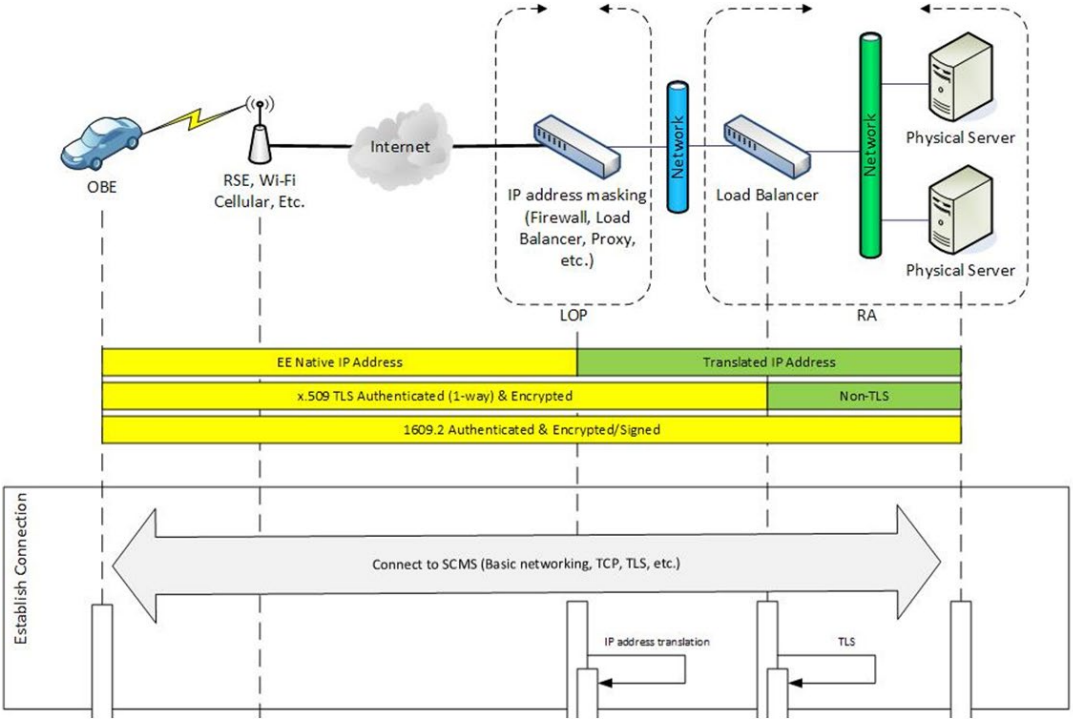


Figure 48 Common Process for Sending SCMS Messages, 1 of 2

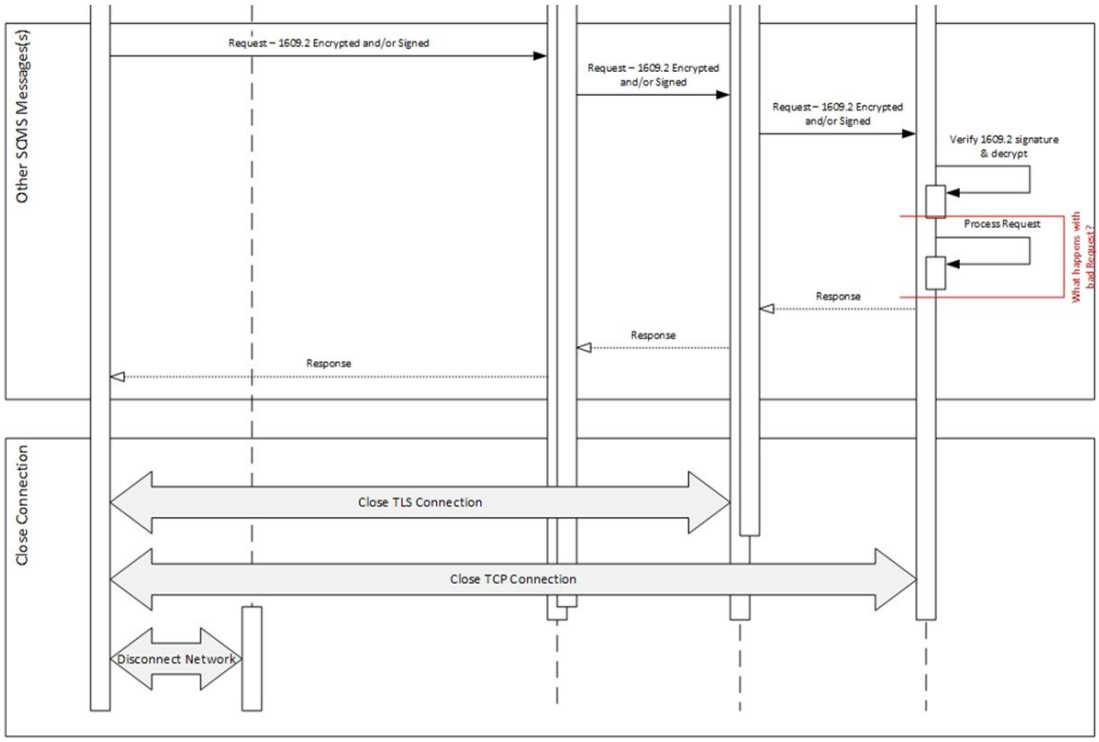


Figure 49 Common Process for Sending SCMS Messages, 2 of 2

5.1.9 Overview of Used Error Codes

This section summarizes error codes used in SCMS interfaces across all use cases.

- RA-EE Errors
- SCMS Errors
- SCMS Error Log Values
- Standard HTTP Error Codes

5.1.9.1 RA-EE Errors

This table contains all RA-EE interface errors. A production stage RA always returns a HTTP status code 500 (HTTP Status Code PROD) to an EE if an error occurs and it is able to respond. A QA stage RA will return more detailed HTTP status codes (HTTP Status Code QA) and SCMS specific HTTP headers with detailed error information (SCMS-POC-Error resp. SCMS-POC-Error-Message).

Table 13 RA-EE Errors

Key	Summary	EE / SCMS	HTTP Status Code	SCMS-Error-Code	Error Message	Additional information
SCMS-964	Error code: raNoCertFileAvailable	SCMS	500	5065	Requested certificate file is not available for download	
SCMS-976	Error code: raInvalidURL	SCMS	500	5072	Invalid URL sent in download request	
SCMS-978	Error code: raAuthenticationFailed	SCMS	500	5067	EE authentication failed	Any of the 1609.2 data layers cannot be validated. It can be caused by failed signature verification, untrusted certificates, or bad encryption. Please see EE-RA Communications - General Guidance and the respective RA - Services View documentation
SCMS-981	Error code: raNoPcaCertificateChainFileAvailable	SCMS	500	5068	Requested certificate chain file not available for download	
SCMS-983	Error code: raNoInfoFileAvailable	SCMS	500	5069	Requested .info file is not available for download	
SCMS-987	Error code: raWrongParameters	SCMS	500	5070	EE request contained invalid parameter values	
SCMS-990	Error code: raMoreThanAllowedTries	SCMS	500	5071	EE exceeded retry limit	
SCMS-1065	Error code: raBlacklisted	SCMS	500	5055	Enrollment certificate blacklisted	
SCMS-1068	Error code: raRequestForMultipleCerts	SCMS	500	5056	Multiple application certificates	

Key	Summary	EE / SCMS	HTTP Status Code	SCMS-Error-Code	Error Message	Additional information
					requests for same PSID/SSP	
SCMS-1070	Error code: raDuplicateRequestReceived	SCMS	500	5057	Duplicate request received	
SCMS-1082	Error code: raInvalidSignature	SCMS	500	5058	Invalid signature or signature missing	
SCMS-1083	Error code: raRequestNotEncrypted	SCMS	500	5059	Request not encrypted	
SCMS-1084	Error code: raInvalidCredentials	SCMS	500	5060	EE used invalid credentials (blacklisted, expired, unauthorized)	
SCMS-1085	Error code: raUnauthorizedRequest	SCMS	500	5061	Unauthorized request (invalid permissions)	
SCMS-1087	Error code: raMismatch	SCMS	500	5063	EE attempted to contact an RA that does not have it on the white list	
SCMS-1088	Error code: raInvalidTimeReceived	SCMS	500	5064	Invalid timestamp sent	

5.1.9.2 SCMS Errors

This table contains SCMS interface errors that are sent among SCMS components.

Table 14 SCMS Errors

Key	Summary	EE / SCMS	HTTP Status Code	SCMS-Error-Code	Error Message
SCMS-789	Error code: InternalTimeout	SCMS	500	5001	Internal timeout. Request could not be processed in time.
SCMS-792	Error code: noMaAuthorizationSignature	SCMS	401	5002	MA signature missing

Key	Summary	EE / SCMS	HTTP Status Code	SCMS-Error-Code	Error Message
SCMS-793	Error code: pcaInvalidMaAuthorizationSignature	SCMS	401	5003	Signature invalid
SCMS-795	Error code: pcaInvalidInputValueFormat	SCMS	400	5004	Request values improperly formatted
SCMS-796	Error code: pcaInvalidLinkageValue	SCMS	400	5005	Invalid linkage value send
SCMS-804	Error code: pcaNumberOfLinkageValuesExceeded	SCMS	400	5006	Number of linkage values above threshold
SCMS-812	Error code: raInvalidHashRequest	SCMS	400	5007	Invalid RA-PCA request hash send
SCMS-820	Error code: raNumberOfRequestsExceeded	SCMS	400	5008	Number of linkage values above threshold
SCMS-829	Error code: raInvalidLinkageValue	SCMS	400	5009	Invalid linkage value send
SCMS-844	Error code: laInvalidLinkageValue	SCMS	400	5010	Invalid LCI value send
SCMS-851	Error code: laNumberOfLciValuesExceeded	SCMS	400	5011	Number of LCI values above threshold
SCMS-875	Error code: pcaInvalidInputValueFormat	SCMS	400	5012	Request values improperly formatted
SCMS-876	Error code: pcaInvalidLinkageValue	SCMS	400	5013	Invalid linkage value send
SCMS-884	Error code: pcaNumberOfLinkageValuesExceeded	SCMS	400	5014	Number of linkage values above threshold
SCMS-892	Error code: laInvalidInputValueFormat	SCMS	400	5015	Request values improperly formatted
SCMS-893	Error code: laInvalidPrelinkageValuePresented	SCMS	400	5016	Invalid encrypted pre-linkage value send

Key	Summary	EE / SCMS	HTTP Status Code	SCMS-Error-Code	Error Message
SCMS-900	Error code: laNumberOfLinkageValuesExceeded	SCMS	400	5017	Number of linkage values above threshold
SCMS-910	Error code: raInvalidInputValueFormat	SCMS	400	5018	Request values improperly formatted
SCMS-917	Error code: raCertificateAlreadyBlacklisted	SCMS	400	5020	Enrollment certificate already blacklisted
SCMS-929	Error code: raInvalidRIFValue	SCMS	400	5022	Invalid RIF value send
SCMS-936	Error code: raNumberOfRequestsExceeded	SCMS	400	5023	Number of RIF values above threshold
SCMS-1041	Error Code: pcaAuthFailure	SCMS	401	5044	PCA could not authenticate LA
SCMS-1043	Error code: raAuthFailure	SCMS	401	5046	RA could not authenticate LA
SCMS-1045	Error code: maAuthFailure	SCMS	401	5048	MA failed to authenticate LA
SCMS-1277	Error code: pcaCertificateEncryptionFailed	SCMS	500	5066	PCA unable to encrypt certificate

5.1.9.3 SCMS Error Log Values

This table contains SCMS error conditions that are added to a local error log but not returned or communicated directly to another component. In most cases, a log entry is the end of processing for an error condition. In other words, once one of these values is captured in a log, there are no other programmatic steps performed by the system. These log values are created for debugging or administrative purposes. In the future, automated monitoring may use these values to take corrective action or alert system managers, but for now they are just saved in a log.

Table 15 SCMS Error Log Values

Key	Summary	EE / SCMS	Error Message
SCMS-988	Error code: raRetries	SCMS	The value is saved to the log, no error is returned.

Key	Summary	EE / SCMS	Error Message
SCMS-1014	Error code: maDecryptionFailed	SCMS	MA unable to decrypt misbehavior report
SCMS-1026	Error code: authCAAuthenticationFailed	SCMS	The value is saved to the log, no error is returned.
SCMS-1031	Error code: tcComponentAddressingInfoInvalid	SCMS	The value is saved to the log, no error is returned.
SCMS-1032	Error code: tcComponentUnreachable	SCMS	The value is saved to the log, no error is returned.
SCMS-1033	Error Code: issuedCertInvalid	SCMS	The value is saved to the log, no error is returned.
SCMS-1042	Error code: laEncFailure	SCMS	The value is saved to the log, no error is returned.
SCMS-1044	Error code: laEncFailure	SCMS	LA could not establish TLS link with RA
SCMS-1046	Error code: laEncFailure	SCMS	LA could not establish TLS link with MA
SCMS-1047	Error code: tcNotifyDCMListFailure	SCMS	The value is saved to the log, no error is returned.
SCMS-1048	Error code: tcNotifyDCMAuthenticationFailure	SCMS	The value is saved to the log, no error is returned.
SCMS-1056	Error code: crlNotAvailable	SCMS	The value is saved to the log, no error is returned.

5.1.9.4 Standard HTTP Error Codes

This table contains a list of standard HTTP error codes for reference. The source of this information including description is Wikipedia as of September 30, 2016.

Table 16 Standard HTTP Error Codes

HTTP Error Code Number	Summary	Description
		Client Error Responses
400	Bad Request	The server cannot or will not process the request due to an apparent client error. (e.g., malformed request syntax, invalid request message framing, or deceptive request routing)
401	Unauthorized	Similar to 403 Forbidden, but specifically for use when authentication is required and has failed or has not yet been provided. The response must include a WWW-Authenticate header field containing a challenge applicable to the requested resource.
402	Payment Required	Reserved for future use. The original intention was that this code might be used as part of some form of digital cash or micro-payment scheme, but that has not happened and this code is not usually used.
403	Forbidden	The request was a valid request, but the server is refusing to respond to it. 403 error semantically means "unauthorized," i.e., the user does not have the necessary permissions for the resource.
404	Not Found	The requested resource could not be found but may be available in the future. Subsequent requests by the client are permissible.
405	Method Not Allowed	A request method is not supported for the requested resource; for example, a GET request on a form which requires data to be presented via POST, or a PUT request on a read-only resource.
406	Not Acceptable	The requested resource is capable of generating only content not acceptable according to the Accept headers sent in the request.
407	Proxy Authentication Required	The client must first authenticate itself with the proxy.
408	Request Timeout	The server timed out waiting for the request. According to HTTP specifications: "The client did not produce a request within the time that the server was prepared to wait." The client MAY repeat the request without modifications at any later time.

HTTP Error Code Number	Summary	Description
409	Conflict	Indicates that the request could not be processed because of conflict in the request, such as an edit conflict between multiple simultaneous updates.
410	Gone	Indicates that the resource requested is no longer available and will not be available again. This should be used when a resource has been intentionally removed and the resource should be purged. Upon receiving a 410 status code, the client should not request the resource in the future. Clients such as search engines should remove the resource from their indices.
411	Length Required	The request did not specify the length of its content, which is required by the requested resource
412	Precondition Failed	The server does not meet one of the preconditions that the requester put on the request
413	Payload Too Large	The request is larger than the server is willing or able to process. Previously called "Request Entity Too Large."
414	URI Too Long	The URI provided was too long for the server to process. Often the result of too much data being encoded as a query-string of a GET request, in which case it should be converted to a POST request.
415	Unsupported Media Type	The request entity has a media type which the server or resource does not support. For example, the client uploads an image as image/svg+xml, but the server requires that images use a different format.
416	Requested Range Not Satisfiable	The client has asked for a portion of the file (byte serving), but the server cannot supply that portion. For example, if the client asked for a part of the file that lies beyond the end of the file.
417	Expectation Failed	The server cannot meet the requirements of the Expect request-header field
418	I'm a teapot	This code was defined in 1998 as one of the traditional IETF April Fools' jokes, in RFC 2324
421	Misdirected Request	The request was directed at a server that is not able to produce a response
426	Upgrade Required	The client should switch to a different protocol such as TLS/1.0, given in the Upgrade header field
428	Precondition Required	The origin server requires the request to be conditional. Intended to prevent "the 'lost update' problem, where a client GETs a resource's state, modifies it, and PUTs it back to the server, while

HTTP Error Code Number	Summary	Description
		meanwhile a third party has modified the state on the server, leading to a conflict."
429	Too Many Requests	The user has sent too many requests in a given amount of time. Intended for use with rate limiting schemes
431	Request Header Fields Too Large	The server is unwilling to process the request because either an individual header field, or all the header fields collectively, are too large
Server Error Responses		
500	Internal Server Error	A generic error message, given when an unexpected condition was encountered and no more specific message is suitable
501	Not Implemented	The server either does not recognize the request method, or it lacks the ability to fulfill the request
502	Bad Gateway	The server was acting as a gateway or proxy and received an invalid response from the upstream server
503	Service Unavailable	The server is currently unavailable (because it is overloaded or down for maintenance). Generally, this is a temporary state.
504	Gateway Timeout	The server was acting as a gateway or proxy and did not receive a timely response from the upstream server
505	HTTP Version Not Supported	The server does not support the HTTP protocol version used in the request
506	Variant Also Negotiates	Transparent content negotiation for the request results in a circular reference
507	Insufficient Storage	The server is unable to store the representation needed to complete the request
511	Network Authentication Required	The client needs to authenticate to gain network access. Intended for use by intercepting proxies used to control access to the network

5.1.10 Re-enrollment

In order to avoid confusion around the terms used for enrollment after revocation, we will use terms as follows:

- **Re-instantiation:**An EE is reinstated if the original enrollment certificate is reinstated. This means that: (1) the enrollment certificate is removed from RA's blacklist by either directly removing it or by removing a CA certificate on the path to

the root CA from the CRL and (2) that the EE keeps using the original enrollment certificate to request certificates from the SCMS. The already issued pseudonym/identification/application certificates can be used as before, or new certificates can be requested and issued.

- **Re-bootstrapping:**An EE is re-bootstrapped if the EE's storage is completely erased (including all certificates and cryptographic credentials) and the bootstrap mechanism is executed. A new enrollment certificate is issued and there is no link between the original enrollment certificate and the new enrollment certificate. The re-bootstrapped EE cannot be distinguished to a factory-new EE.
- **Re-issuance:**An EE enrollment certificate may be re-issued if the public-key of the enrollment certificate stays and an ECA issues a new enrollment certificate based on that same public key. The EE keeps all pseudonym certificates and keeps using the same butterfly key parameters.
- **Re-establishment:**An EE is re-established if the integrity of the EE can be verified remotely, and the EE generates a new key pair and receives a new enrollment certificate that contains the newly generated public key.
- **Re-enrollment**: A device is re-enrolled if either re-instantiation, re-bootstrap, a re-issue, or re-establishment is performed.

SCMS PoC for CV Pilots will initially only support re-bootstrapping in the first year of operation. Other forms of re-enrollment will be added at a later point. The SCMS will not support re-issuance.

5.2 Requirements by Use Case

The following pages are a hierarchy of requirements sorted by SCMS use cases. A use case contains all requirements that must be implemented from an end entities (EE) perspective to fulfill a major feature of the SCMS. A use case might comprehend multiple steps from a system's architecture perspective that can be run without interference with each other to return a partial result of the overall use case. In general, steps need to be executed in the given order to fulfill the use case. For example, Use Case 3: OBE Pseudonym Certificates Provisioning describes all necessary processes to equip an OBE with pseudonym certificates. It comprehends five steps that are coherent but self-contained:

- Step 3.1: Request for Pseudonym Certificates
- Step 3.2: Pseudonym Certificate Generation
- Step 3.3: Initial Download of Pseudonym Certificates
- Step 3.4: Schedule Generation of Subsequent Batch of Pseudonym Certificates
- Step 3.5: Top-off Pseudonym Certificates

This format supports end-to-end implementation as well as testing better than a pure listing of requirements.

5.2.1 On-board Equipment (OBE) Use Cases

The following chapters are about OBE requirements. These are the main use cases for OBEs, but there are requirements throughout all chapters for OBEs. For example, in 11. Backend Management are requirements about what an OBE needs to do if a root CA is revoked or a new root CA is introduced to the system.

- Use Case 2: OBE Bootstrapping (Manual)
- Use Case 3: OBE Pseudonym Certificates Provisioning
- Use Case 8: Global Misbehavior Detection and Revocation
- Use Case 19: OBE Identification Certificate Provisioning

5.2.2 Road-side Equipment (RSE) Use Cases

The following chapters are about RSE requirements. These are the main use cases for RSEs, but there are requirements throughout all chapters for RSEs. For example, in 11. Backend Management are requirements about what an RSE needs to do if a root CA is revoked or a new root CA is introduced to the system.

- Use Case 12: RSE Bootstrapping (Manual)
- Use Case 13: RSE Application Certificate Provisioning
- Use Case 16: RSE Application and OBE Identification Certificate Revocation

5.2.3 Common EE Use Cases

Both EE types should implement the following chapters:

- Use Case 5: Misbehavior Reporting
- Use Case 6: CRL Download
- Use Case 11: Backend Management (CA compromise recover strategy)
- Use Case 18: Provide and Enforce Technical Policies
- Use Case 20: EE Re-Enrollment

5.2.4 Backend Use Cases

Features specific only to the SCMS (no relevance to end entities) as well as deployment and management requirements are listed in the following use cases:

- Use Case 1: SCMS Component Setup
- Use Case 7: CRL Broadcast

- Use Case 11: Backend Management

5.2.5 Requirement Status

All requirements are listed with all details including their status of implementation (e.g., SCMS-500 - Firewall whitelist SCMS POC OUT OF SCOPE) and a JIRA link is given for traceability reasons. Statuses given are:

Table 17 Document Header and Status

Status	Description
Review	Requirement is currently under review by the Software Team
In Implementation	Requirement is currently in implementation by the Software Team
Implemented	Software Team finished the implementation as well as the unit tests
Ready for Testing	Test Team created test cases as well as test scripts for this requirement and the requirement is ready to be tested with the next test run
Tests Passed	All tests of the given requirement were successful within the latest test run
Tests Failed	One or more tests of the given requirement failed during the latest test run
Closed	Requirement is implemented and successfully tested
Manual Process	Requirement is meant to be manually executed within the PoC software and will not be implemented in software
SCMS PoC Out Of Scope	Requirement will neither be implemented in the PoC software nor executed manually. This applies especially to EE requirements or SCMS production requirements that are listed but out of scope for implementation during the PoC project.

5.2.6 Use Case 2: OBE Bootstrapping (Manual)

- Background and Goals
- Assumptions and Preconditions
- Process Steps
    - Manual Bootstrapping Process - QA Environment
    - Manual Bootstrapping Process - PROD Environment
        - Enrollment certificate request checks
        - OBE Bootstrap Process Logging Requirement
- Enrollment Certificate Request Example
- Requirements

- Additional Reference Information
- ASN.1 Specification

5.2.6.1 Background and Goals

The bootstrap process enables the OBE to interact with the SCMS.

Bootstrapping is executed at the start of the OBE's lifecycle. At the start of bootstrapping, the OBE has no SCMS certificates and no knowledge of how to contact the SCMS. At the end of bootstrapping the OBE has the following:

- Certificates and information that allows an OBE to trust the SCMS:
    - The required Root CA certificate(s), optional Intermediate CA and Pseudonym CA certificates to allow it to verify received messages. The OBE can learn unknown PCA and ICA certificates in ongoing operation as defined in IEEE 1609.2 P2P CD. At minimum, any EE needs the certificate chain of the PCA that issued certificates to it.
    - The latest CRL (includes the CRL Generator certificate, which in turn includes the FQDN of the CRL store)
    - The MA certificate to encrypt misbehavior reports, before submitting them to the RA
- Credentials and information allowing an OBE to communicate with the SCMS:
    - A correctly issued enrollment certificate, private key reconstruction value, and ECA certificate.
    - The RA certificate (which includes the FQDN of the RA).

Bootstrapping must protect the OBE from getting incorrect information, and the ECA from issuing a certificate to an unauthorized OBE. Any bootstrapping process is acceptable, that results in secure placement of this information on an OBE device.

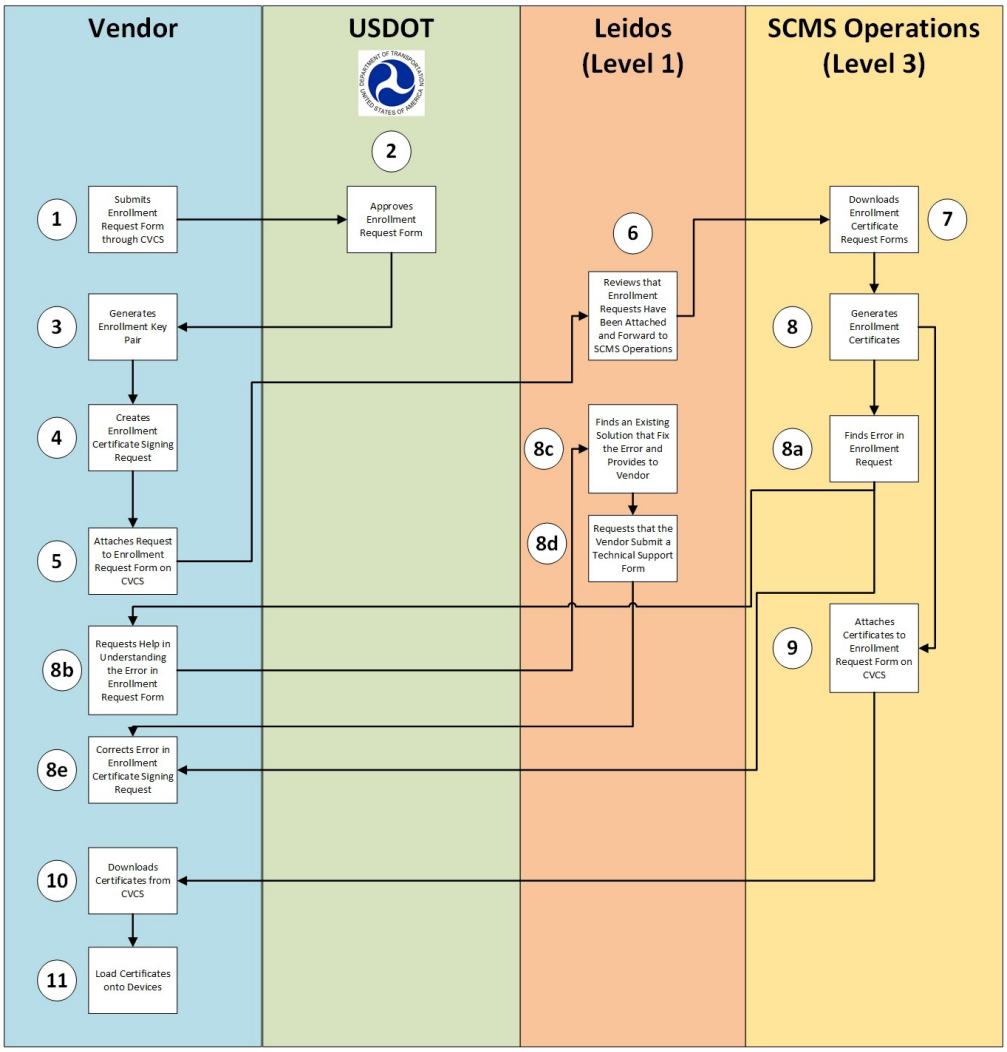
5.2.6.2 Assumptions and Preconditions

- A documented procedure for performing the enrollment process.
- A “secure environment” as defined in Secure Environment for Device Enrollment, ensures that the OBE is under control of the operator running the bootstrapping operation.
- One or more authorized devices (computers) for managing the enrollment process.
- An activity log or recording of the enrollment operations performed.
- A user account at the USDOT workflow tool.

5.2.6.3 Process Steps

5.2.6.3.1 Manual Bootstrapping Process - QA Environment

The CV Pilot will initially use a manual bootstrapping process that combines device initialization and enrollment. The following process applies to the SCMS QA stage. The vendor will initiate this process by requesting device initialization information and enrollment certificate from a **DOT Workflow Approval** tool, as depicted in this process:



Step	Actor	Description	Status	Assignee
1	Vendor	Logs into CVCS Samanage, initiates an enrollment certificate request. There is a dedicated form for that.	**New**	USDOT
2	USDOT	Logs into CVCS Samanage and reviews the enrollment certificate request form. They ensure that: • The vendor is on the list of known vendors for CV device manufacture. • If the request is not correct, USDOT will deny the request, and the vendor will need to correct the request and resubmit through Step 3. USDOT Personnel approve the request, if it meets the above criteria, and USDOT sends the request back to the Vendor for them add the enrollment certificate signing request.	**Awaiting Customer Input**	Leidos
3	Vendor	The vendor **in a secure environment** generates **in each OBE** a verification key pair (see Public Key Algorithms in CB2: Types of Cryptographic Algorithms). The private key is used to sign the enrollment certificate request (CSR) in step 4. The public key is added to the request and used by the ECA subsequently as input to calculating the public value within the implicit certificate, issued at end of this process. **NOTE:** The verification key pair must be generated using an algorithm approved for use (see Approved Cryptographic Algorithms, Approved Random Number Generators). Best practice is to generate the verification key pair inside the EE's HSM and the private key never leaves the EE.	**Awaiting Customer Input**	Leidos
4	Vendor	The vendor **in a secure environment** creates an enrollment certificate signing request **for each device**, a signed structure called SignedEeEnrollmentCertRequest. The CSR includes the verification public key to use to create the public key reconstruction value in the enrollment certificate. The enrollment certificate request permissions (PSIDs, SSPs, Geographic Region) and lifetime are stated in the CSR as well. The vendor signs the CSR with the **device's private key**, and writes the CSR to a file with filename format <enrollment pub hex>.oer in OER encoding. The vendor then collects multiple CSRs, places them in a flat directory and zips the directory. The directory structure within the zip file should look identical to the following example. IMPORTANT: DUE TO AUTOMATED PROCESSING	**Awaiting Customer Input**	Leidos

Step	Actor	Description	Status	Assignee

		OF REQUESTS, DEVIATIONS FROM THIS ZIPFILE AND DIRECTORY STRUCTURE WILL RESULT IN REQUESTS FAILING TO BE PROCESSED.
		`+ 4A2...BC1.oer`
		`+ 61C...E1F.oer`
		`+ ...`
		`+ ...`
		`+ 23B1...5FF.oer`
		Code Block 1 Enrollment Request Zip File Example		

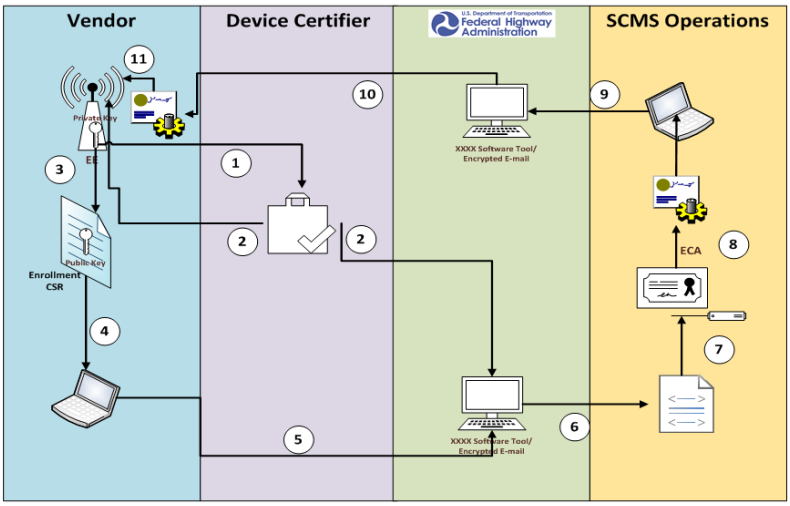
5	Vendor	Vendor logs into CVCS Samanage and attaches the enrollment request zip file to the previous enrollment request form.	**Awaiting Customer Input**	Leidos
6	Leidos	Reviews Enrollment Request Form and ensures files have been attached and manually verifies the following fields: • PSID • Region	**Assigned**	SCMS Operations
7	SCMS Operations	Logs into CVCS Samanage and downloads the enrollment certificate request zip file.	**Work in Progress**	SCMS Operations
8	SCMS Operations	Executes their enrollment requests script to create enrollment certificates. If successful move to Step 9. The ECA generates and returns an enrollment certificate for each individual request. The response is a signed structure called SignedEeEnrollmentCertResponse. The SCMS operator collects all ECA responses, creates a directory structure that includes bootstrapping information as well as one directory per CSR using the filename of the CSR as directory name. Each of those directories contains the RA certificate to be used by the OBE to communicate with the SCMS, the certificate of the ECA that signed the enrollment certificate, as well as the enrollmentCert itself and the privKeyReconstruction. The SCMS operator zips all files into a single zip file. Following the example in step 4, the directory structure within the zip file would look like this (please be aware that the Root CA certificate is explicitly given in the file root.oer):	**Work in Progress**	SCMS Operations

Step	Actor	Description	Status	Assignee
		+ root.oer: IEEE 1609.2 root CA certificate encoded as OER + LCCF.oer: current Local Certificate Chain File including ICA and PCA certificates. + LPF.oer: current Local Policy File + CRL.oer: current Certificate Revocation List + root.tls: TLS (X.509) root certificate RA's TLS cert chains to + 4A2...BC1 (dir) | +RA.oer: RA's 1609.2 certificate | +ECA.oer: ECA's 1609.2 certificate | +enrollment.oer: (EE's enrollment certificate, see enrollmentCert as part of the ECA response SignedEeEnrollmentCertResponse) | +enrollment.s: (EE's Private key reconstruction value, see privKeyReconstruction as part of the ECA response SignedEeEnrollmentCertResponse) + 61C...E1F (dir) | +RA.oer | +ECA.oer | +enrollment.oer | +enrollment.s + ... + ... + 23B1...5FF (dir) | +RA.oer | +ECA.oer | +enrollment.oer | +enrollment.s **Code Block 2 Enrollment Resonse Zip File Example**		
8a	SCMS Operations	If SCMS Operations finds an error within the request, SCMS Operations will send the Error Response to the Vendor through the CVCS enrollment request.	**Awaiting Customer Input**	SCMS Operator
8b	Vendor	Requests help/clarification in understanding the error found in the enrollment certificate signing request as a comment to the Enrollment Request Form.	**Work in Progress**	Leidos
8c	Vendor	Looks for an existing solution that will fix the vendors error. If they find a solution they provide it to the vendor.	**Awaiting Customer Input**	SCMS Operator

Step	Actor	Description	Status	Assignee
8d	Vendor	If an existing solution cannot be found, Leidos requests the vendor submit the Technical Support form and sends the Vendor the link.	**Awaiting Customer Input**	SCMS Operator
8e	Vendor	Corrects the error and reattaches the enrollment certificate signing request to the Enrollment Request Form.	**Awaiting Customer Input**	SCMS Operator
9	SCMS Operator	Logs into the CVCS Samanage and creates an enrollment certificate response for the appropriate vendor and attaches the enrollment response **zip file.**	**Resolved**	Vendor
10	Vendor	Vendor logs into CVCS Samanage and downloads their device enrollment certificates **in their secure environment**.	**Resolved**	Vendor
11	Vendor	The vendor loads the appropriate enrollment certificate onto the appropriate device, **in their secure environment.**	**Resolved**	Vendor

5.2.6.3.2 Manual Bootstrapping Process - PROD Environment

The CV Pilot will initially use a manual Bootstrap Process that combines device initialization and enrollment. The process on the SCMS PROD stage is essentially the same as for QA (see QA process above) with the exception that the vendor must first submit their OBE device to a certification lab for certification before requesting the device enrollment certificate. The complete process is described below:



1. Vendor submits their device to one of the device certification companies for certification. Vendor logs into DOT Workflow Approval tool and creates a device certification request, for a specific model of device, selecting the appropriate device certification company.

2. Device certification company conducts device certification testing. After successful completion of certification, device certification company notifies DOT Workflow Approval tool of certification for the specific device model, and attaches certification documentation. DOT Workflow Approval tool notifies the vendor and USDOT of the approval, and maintains device certification documentation in database of certified devices.
3. to 11. Same step 1-9 in QA

5.2.6.3.2.1 Enrollment certificate request checks

The following checks have to be done in step 6:

- The CSR only contains PSID from SCMS PoC Supported V2X Applications
- The CSR only contains PSIDs the device is eligible to
- The CSR contains the right SSP values for the requested PSID
- The CSR only contains SSP values the device is eligible to
- The CSR only contains Region USA
- The CSR does not contain a public key that was used with a previous enrollment cert request
- The CSR does have a validity period that fits the ECA's validity period
- The CSR contains the correct cracaId
- The CSR contains the correct crlSeries
- The CSR contains a useful CertificateId

5.2.6.3.2.2 OBE Bootstrap Process Logging Requirement

The following bootstrap operation information must be logged and maintained by the organization performing the PROD bootstrapping process, for each unique device, and for each enrollment certificate, if multiple enrollment certificates are requested for a single device.

- OBE serial number or unique unit identifier
- Initial Bootstrap Start Date
- Bootstrap LCCF file version identifier
- Bootstrap LPF file version identifier
- Enrollment cert
- Bootstrap Complete Date

5.2.6.4 Enrollment Certificate Request Example

The following clear text is an example for an enrollment certificate request that we provide in an OER encoded version, as it is supposed to be sent during manual enrollment.

```
value ScmsPDU ::= {
  version 1,
  content eca-ee : eeEcaCertRequest : {
    version 1,
    currentTime 431026272,
    tbsData {
      id name : "obeenr",
      cracaId '000000'H,
      crlSeries 4,
      validityPeriod {
        start 431026272,
        duration hours : 4320
      },
      region identifiedRegion : {
        countryOnly : 124,
        countryOnly : 484,
        countryOnly : 840
      },
      certRequestPermissions {
        {
          subjectPermissions explicit : {
            {
              psid 32,
              sspRange opaque : {}
            },
            {
              psid 38,
              sspRange opaque : {}
            }
          },
          minChainDepth 0,
          chainDepthRange 0,
          eeType {app}
        }
      },
      verifyKeyIndicator verificationKey : ecdsaNistP256 : compressed-y-1
: '8751D2FDC5D7BF8CCE4A7FACE5E5AD7B92FA6B8CA0B202FBC93CBC08412AA934'H
    }
  }
}
```

Code Block 3 Clear Text Before Signing/Encrypting

```
value SecuredScmsPDU ::= {
  protocolVersion 3,
  content signedCertificateRequest :
'00018180000119B0F0604481066F6265656E72000000000419B0F0608410E083010380'H
-- truncated --
}
```

Code Block 4 Textual After Signing/Encrypting (SecuredScmsPDU Layer)

```
038381a500018180000119b0f0604481066f6265656e72000000000419b0f0608410e08301
0380007c8001e480034801018080010280012080010080012680010001008080838751d2fd
c5d7bf8cce4a7face5e5ad7b92fa6b8ca0b202fbc93cbc08412aa934828080301d57f8d01e
98c685428c49328be8164bae24e18d46030048911c5fd4275df73121b89c7919fd75d7ab41
1cfb254a44660997f7b1ae9235f2d0f1949198826
```

Code Block 5 Binary (Hexadecimal) After Signing/Encrypting

```
value SignedCertificateRequest ::= {
  hashId sha256,
  tbsRequest {
    version 1,
    content eca-ee : eeEcaCertRequest : {
      version 1,
      currentTime 431026272,
      tbsData {
        id name : "obeenr",
        cracaId '000000'H,
        crlSeries 4,
        validityPeriod {
          start 431026272,
          duration hours : 4320
        },
        region identifiedRegion : {
          countryOnly : 124,
          countryOnly : 484,
          countryOnly : 840
        },
        certRequestPermissions {
          {
            subjectPermissions explicit : {
              {
                psid 32,
                sspRange opaque : {}
              },
              {
                psid 38,
                sspRange opaque : {}
              }
            },
            minChainDepth 0
          }
        },
        verifyKeyIndicator verificationKey : ecdsaNistP256 : compressed-y-
1 : '8751D2FDC5D7BF8CCE4A7FACE5E5AD7B92FA6B8CA0B202FBC93CBC08412AA934'H
      }
    }
  },
  signer self : NULL,
  signature ecdsaNistP256Signature : {
    r x-only :
'301D57F8D01E98C685428C49328BE8164BAE24E18D46030048911C5FD4275DF7'H,
    s '3121B89C7919FD75D7AB411CFB254A44660997F7B1AE9235F2D0F19491988265'H
  }
}

value ScmsPDU ::= {
  version 1,
  content eca-ee : eeEcaCertRequest : {
    version 1,
    currentTime 431026272,
    tbsData {
      id name : "obeenr",
```

```
        cracaId '000000'H,
        crlSeries 4,
        validityPeriod {
          start 431026272,
          duration hours : 4320
        },
        region identifiedRegion : {
          countryOnly : 124,
          countryOnly : 484,
          countryOnly : 840
        },
        certRequestPermissions {
          {
            subjectPermissions explicit : {
              {
                psid 32,
                sspRange opaque : {}
              },
              {
                psid 38,
                sspRange opaque : {}
              }
            },
            minChainDepth 0
          }
        },
        verifyKeyIndicator verificationKey : ecdsaNistP256 : compressed-y-1
: '8751D2FDC5D7BF8CCE4A7FACE5E5AD7B92FA6B8CA0B202FBC93CBC08412AA934'H
      }
    }
}
```

Code Block 6 Textual After Signing/Encrypting (SignedCertificateRequest Layer)

5.2.6.5 Requirements

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-364	MANUAL PROCESS	DCM Configuration of EEs After Component Revocation	DCM shall not configure new EEs with credentials of revoked SCMS component.	The SCMS Manager will manage the transition of devices after the revocation of a component.	In the PoC this will occur by a manual process. The DCM will provision EEs with valid certificates for SCMS components including one or more ICA and one or more RA. When the DCM learns that any component is revoked, it shall no longer provision new EEs with that revoked certificate.	DCM
SCMS-486	MANUAL PROCESS	DCM shall acquire the current CRL	The DCM shall acquire the current CRL from the CRL Store.	The DCM will provide the latest CRL to newly provisioned EEs. This saves the EE from having to get the CRL right away.	The DCM will request these from the CRL Store and will provide these to the EE.	DCM
SCMS-557	EE REQUIREMENT	Secure chain of custody	EE shall get firmware, enrollment certificates, etc. injected within a secure chain of custody.	Documented and audited processes are crucial to the security of EEs.	See Secure Environment for Device Enrollment for guidelines on physical security for device provisioning. Not software testable, procedural	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-562	CLOSED	RA certificate and FQDN	DCM shall provide the EE with the RA certificate and the FQDN for the RA.	The EE will need to communicate securely with the RA (e.g., to request new certificates).		DCM
SCMS-563	CLOSED	ECA certificate and FQDN	DCM shall provide the EE with the ECA certificate and the FQDN for the ECA.	The EE will need to communicate securely with the ECA.		DCM
SCMS-564	CLOSED	MA certificate and FQDN	DCM shall provide the EE with the MA certificate.	The EE will need to communicate securely with the MA (e.g., in order to download CRLs)		DCM
SCMS-565	CLOSED	ICA certificates	DCM shall provide the EE with its own ICA certificate. Optionally, include other existing ICA certificates.	The EE needs its ICA certificate, e.g., to provide this to other EE in peer-to-peer certificate updates.		DCM
SCMS-566	CLOSED	PCA certificates	DCM shall provide the EE with its own PCA certificate. Optionally, include other existing PCA certificates.	The EE needs its PCA certificate, e.g., to provide this to other EE in peer-to-peer certificate updates.		DCM
SCMS-567	CLOSED	CRL	DCM shall provide the EE with the latest CRL and contact information for the	The EE will be provided with the current CRL so as to reject		DCM

Key	Status	Summary	Description	Justification	Notes	Component/s
			CRL (CRACA certificate is part of the CRL).	communication from invalidated devices.		
SCMS-568	CLOSED	X.509 certificate	DCM shall provide the EE with the Root X.509 TLS certificate.	The EE will need to communicate securely, at the TLS level, with the RA (e.g., in order to download certificates) and the MA (to upload misbehavior reports).	Revocation status shall be available online, e.g., via OCSP.	DCM
SCMS-570	SCMS POC OUT OF SCOPE	Certification Services	Certification Services shall utilize a secure connection to provide attestation to the ECA that the EE is of a type it certified	So that valid EEs are certified and uncertified EEs cannot get enrollment certificates.	Does not apply to POC. For PoC every EE requesting an enrollment certificate is assumed to be certified.	Certification Service
SCMS-573	EE REQUIREMENT	Secure Key Injection	EE shall generate the private key for the enrollment certificate or the DCM shall use a secure key injection mechanism to provide it to the EE.	To maintain confidentiality of private keys	Does not apply to POC	DCM, On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-946	CLOSED	Root CA certificates	DCM shall provide the EE with all Root CA certificates.	The Root CA will have signed the current ICA certificate as well as the centralized components, the Policy Generator and		DCM

Key	Status	Summary	Description	Justification	Notes	Component/s
				the Misbehavior Authority.		
SCMS-948	CLOSED	Bootstrap: Local Certificate Chain File	DCM shall provide the EE with the latest Local Certificate Chain File.	The EE will use this in the verification process of SCMS certificates.		DCM
SCMS-949	EE REQUIREMENT	Error code: eeInitCertProvFailed	EE shall log this error code, if the Initialization process fails at completing a certificate provisioning of any of the certificates	The EE must signal an error, if any, in the provisioning of any of the certificates.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-950	EE REQUIREMENT	Error code: eeInitCRLProvError	EE shall log this error code, if the Initialization process fails at completing the CRL provisioning.	The EE must signal an error, if any, in the provisioning of the CRL.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1095	CLOSED	RSE Enrollment	RSE enrollment shall be the same as OBE enrollment as specified in Step 2.2: Enrollment (Bootstrapping)	RSE enrollment is the same in terms of process and the resulting certificate.		ECA
SCMS-1160	EE REQUIREMENT	EE securely stores Root CA certificates	EE shall store all root CA certificates in tamper-resistant (or equivalent) storage.	Root CA certificates must be protected against manipulation. It is public and no read protection is required, however, it must be stored in secure storage so that it can only	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
				be updated when the proper root (elector) Management authentication mechanisms have been satisfied.		
SCMS-1174	EE REQUIREMENT	EE stores the Policy Generator certificate	EE shall store the Policy Generator certificate.	The EE requires this to validate the signature on Policy Files.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1176	EE REQUIREMENT	EE stores the CRLG certificate	EE shall store the Certificate Revocation List Generator certificate.	The EE requires this to validate the signature on the CRL.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1205	CLOSED	Policy Generator certificate	DCM shall provide the EE with the Policy Generator certificate.	The EE requires this to validate the signature on Policy Files.		DCM
SCMS-1206	CLOSED	Certificate Revocation List Generator certificate	DCM shall provide the OBE with the Certificate Revocation List Generator (CRLG) certificate.	The OBE requires this to validate the signature on the CRL.		DCM
SCMS-1207	EE REQUIREMENT	EE securely stores Certificate Revocation List	EE shall store the Certificate Revocation List in tamper-resistant (or equivalent) storage.	The EE will be provided with the current CRL so as to reject communication from invalidated devices.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-1208	EE REQUIREMENT	EE securely stores X.509 root certificate	EE shall store the X.509 root certificate in tamper-resistant (or equivalent) storage.	The EE will need to communicate securely, at the TLS level, with the RA (e.g., in order to download pseudonym certificates) and the MA (to upload misbehavior reports).	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1209	EE REQUIREMENT	EE securely stores Local Certificate Chain File	EE shall store the Local Certificate Chain File in tamper-resistant (or equivalent) storage.	EE will use Local Certificate Chain File during verification of SCMS certificates	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1210	EE REQUIREMENT	EE Secure Key Storing	EE shall store the following keys in tamper-resistant (or equivalent) storage: • Private enrollment key • Butterfly key parameters (seed + expansion function parameter) • All private keys (e.g., of OBE application certificates and private keys calculated from the Butterfly key parameters)	To avoid extraction of private keys via software-based attacks.	This is out of scope since it defines EE's behavior. It is highly recommended to protect the content encryption key by a TPM-like mechanism that offers secure boot and that protects the keys against software-based attacks. Additional details are listed in Hardware, Software and OS Security	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-1305	CLOSED	PSID in enrollment certificate	ECA shall assign each Enrollment Certificate at least one PSID.	Each enrollment certificate is associated with a particular application that is represented by a PSID/SSP combination. Enrollment certificates cannot have an empty PSID field.		ECA
SCMS-1306	REVIEW	ECA: Not more than one enrollment certificate with same PSID/SSP combination	ECA shall not issue more than one enrollment certificate per requested public key.	A clear mapping is required for proper administration.	In cases where an enrollment certificate has more than one PSID, the corresponding apps are expected to be similar in nature. Such groupings of PSIDs in an enrollment certificate are likely to be related to policy decisions to be made by the SCMS Manager.	ECA
SCMS-1411	SCMS POC OUT OF SCOPE	CV pilots: DCM keep track of generated enrollment certificates	The Single Point of Contact (SPOC) of the DCMs shall keep track of all issued enrollment certificates for the CV pilot deployment.	To be able to revoke all devices from a supplier that was not able to securely handle his enrollment certificates/part of the enrollment process.	This is out of scope for PoC as it defines a manual process for CV pilot operations that is not part of the SCMS PoC project.	DCM

Key	Status	Summary	Description	Justification	Notes	Component/s
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-1441	SCMS POC OUT OF SCOPE	DCM: Not more than one enrollment certificate per PSID/SSP	DCM shall not allow that a single EE requests more than one enrollment certificate associated with the same PSID/SSP values.	To avoid that an EE can receive multiple sets of certificates via different enrollment certificates for a single application (PSID/SSP).	This is enforced by policy mechanisms (e.g., audit). There are no technical means for ECA to validate that an EE didn't request several enrollment certificates for the same PSID/SSP.	DCM
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	This is necessary because otherwise the device won't be able to use the enrollment		DCM, On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
			correctly verifies, including building a chain back to the root CA.	certificate for requesting pseudonym/identification/ application certificates.		
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)

35 issues

5.2.6.6 Additional Reference Information

- CB2: Types of Cryptographic Algorithms
- Approved Cryptographic Algorithms
- Approved Random Number Generators

5.2.6.7 ASN.1 Specification

- scms-protocol.asn
- eca-ee.asnhttps://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/dcm-ee.asn
- scms-policy.asnhttps://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/dcm-ee-errors.asn

5.2.7 Use Case 3: OBE Pseudonym Certificates Provisioning

5.2.7.1 Goals

The goal is to provide a freshly bootstrapped OBE with the very first batch of pseudonym certificates that it can use in applications like Basic Safety Message (BSM).

5.2.7.2 Background and Strategic Fit

The initial provisioning of pseudonym certificates is the process by which an OBE receives its very first batch of pseudonym certificates. This use case also acts as a trigger for subsequent provisioning of pseudonym certificates. The OBE does not need to make any more requests, the RA automatically does everything necessary (such as doing the butterfly key expansion, getting pre-linkage values from the LAs, making individual certificate requests to the PCA, etc.) for the next batches of certificates.

Due to the time constraints imposed by the OEMs, shuffling requirements for the initial provisioning may be relaxed.

This use case involves the following SCMS components:

- Linkage Authorities (LAs)
- Location Obscurer Proxy (LOP)
- Pseudonym Certificate Authority (PCA)
- Registration Authority (RA)

At the start of this use case, the OBE has no pseudonym certificates. At the end of this use case, the OBE has three years worth of pseudonym certificates, and the RA has everything it needs from the OBE for generating and providing subsequent pseudonym certificate batches for the OBE.

5.2.7.3 Assumptions

In order to facilitate the certificate request process, an OBE must meet the following prerequisites:

- OBE has a valid enrollment certificate
- OBE has Root CA, RA and PCA certificates installed
- OBE knows the FQDN of the RA

5.2.7.4 Requirements

Table 18 Use Case 3 - Requirements

Key	Status	Summary	Description	Justification	Notes	Component/s
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 (comparehttps://jira.campllc.org/browse/SCMS-859~~SCMS-859~~, SCMS-504) and the X.509 CRL (https://jira.campllc.org/browse/SCMS-405~~SCMS-405~~).	RA
SCMS-510	CLOSED	Keep interactions as independent as possible	RA shall keep the interactions with the device, the LAs, and the PCA as independent as possible	so that organizational separation is maintained	Not software testable, but should be checked in code review. RA should simply follow the protocol.	RA

2 issues

5.2.7.5 Design

The following flow chart documents the general flow of steps an OBE needs to carry out in the given order to obtain Pseudonym certificates. It is not a 100% accurate description of the process. Please refer to the use case's steps and their requirements in the following subsections for a complete description of the process.

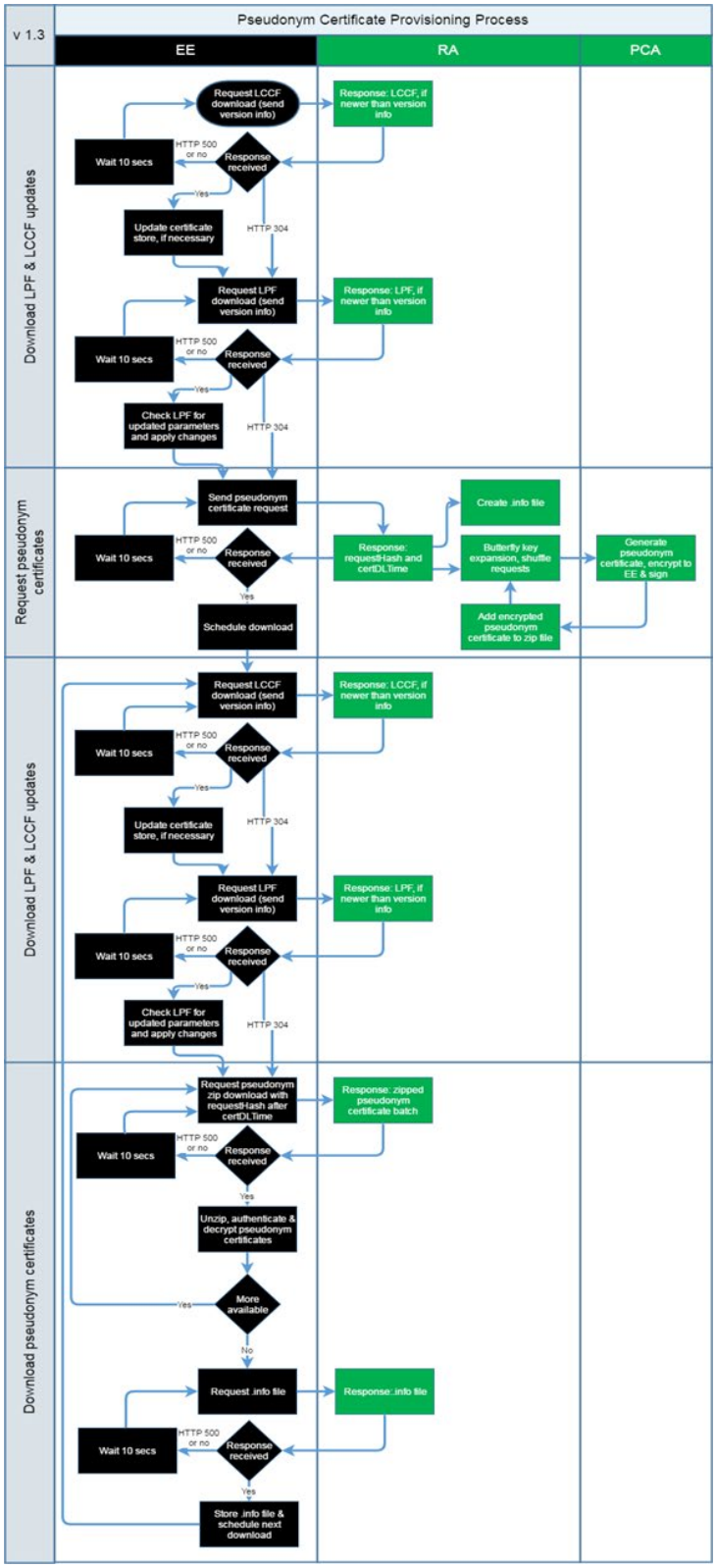


Figure 50 Pseudonym Certificate Provisioning Process

At a high level, three steps are relevant towards an OBE:

1. Request for Pseudonym Certificates
2. Initial Download of Pseudonym Certificates
3. Top-off Pseudonym Certificates

Having determined which RA to submit the request to, the OBE creates a request, signs it with the enrollment certificate, encrypts the signed request for the RA and sends it to the LOP/RA. The LOP strips any IP information that could be used to determine the OBE's location and forwards it to the RA. The RA checks to make sure that the certificate request is correct and authorized and sends back a download location (*requestHash*) and time (*certDLTime*). The RA performs butterfly key expansion on the request to create a batch of public keys to be certified. The RA then merges the certificate request information with linkage information from the LAs to create a series of individual certificate requests. RA then sends those requests to the PCA, mixing the certificate requests with certificate requests generated for other OBEs to provide privacy against insiders at the PCA. The PCA signs the pseudonym certificates, encrypts them for the OBE, signs the encrypted version of the certificate, and returns the encrypted and signed pseudonym certificates to the RA. The RA does not remove any of the named signatures or encryptions, adds them to a zip file and stores them for download by the OBE. The OBE starts downloading the zip files at *certDLTime.*

5.2.7.6 Step 3.1: Request for Pseudonym Certificates

5.2.7.6.1 Goals

The goal of this use case is to define the messages and actions which allow a device to request new pseudonym certificates from the RA. An initial request is for 3,000 (3,120 to be exact) certificates and is assumed to be the default for a batch request. (20 pseudonym certificates per week x 52 weeks per year x 3 years). Note: 20 pseudonym certificates is minimum number of certificates per week. Each OEM can decide to have more certificates per week. The number of requested certificates per week changes the number of request towards PCA and, therefore, requires more computational and storage capacity at the PCA.

5.2.7.6.2 Background and Strategic Fit

Whenever the SCMS Manager decides to change technical policies for the SCMS, all participating devices must be updated. Therefore, the RA provides a Local Policy File (LPF) based on the Global Policy File (GPF) generated and signed by the Policy Generator. The Policy Generator as well signs the LPF. The OBE must download the LPF and Local Certificate Chain File (LCCF) before sending any subsequent request or any certificate download every time it connects to the RA.

The OBE must request pseudonym certificates from its RA within the overall policy set by the SCMS Manager in the LPF. The OBE will be preconfigured during Use Case 2:

OBE Bootstrapping (Manual) with the FQDN of the RA to which it submits the certificate batch request.

5.2.7.6.3 Assumptions

OBE has successfully completed Use Case 2: OBE Bootstrapping (Manual).

5.2.7.6.4 Process Steps

The OBE should follow the steps outlined below to request pseudonym certificates. Neither order nor fulfillment of all steps is enforced, but highly recommended.

1. The OBE downloads the Local Policy File (LPF) and the Local Certificate Chain File (LCCF) using the API documented in RA - Download local policy file and RA - Download Local Certificate Chain File
    a. The OBE applies all changes to its trust-store (necessary for PCA Certificate Validations) if there is an updated LCCF
    b. The OBE applies those changes if there is an updated LPF
2. The OBE creates the request, signs it with the enrollment certificate, encrypts the signed request to the RA and sends it via LOP to the RA using the API documented in RA - Request Pseudonym Certificate Batch Provisioning
3. The LOP strips any information that could be used to determine the OBE's location and forwards it to the RA
4. The RA ensures that the certificate batch request is correct and authorized before it starts Step 3.2: Pseudonym Certificate Generation

5.2.7.6.5 Error Handling

1. The OBE will abandon further interactions with the RA after a certain number of failed communication attempts resulted in errors
2. The OBE will not attempt to execute the certificate provisioning process if it finds itself on the latest CRL (assumes that a willful violator has not compromised the device). The OBE will need to execute the certification/bootstrap process again to exit a revoked state.

5.2.7.6.6 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>
</table>

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-411	EE REQUIREMENT	EE Authentication to RA for Request	The EE shall authenticate its requests with its enrollment certificate and signed timestamp to avoid replay attacks on the RA.	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.	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.	On-board Equipment (OBE), Road-side Equipment (RSE)
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	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
					component certificate validation.	
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 (comparehttps://jira.campllc.org/browse/SCMS-859~~SCMS-859~~, SCMS-504) and the X.509 CRL (https://jira.campllc.org/browse/SCMS-405~~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

Key	Status	Summary	Description	Justification	Notes	Component/s
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 (https://jira.campllc.org/browse/SCMS-537~~SCMS-537~~) and RA-EE authentication (https://jira.campllc.org/browse/SCMS-539~~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	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
					Communications - General Guidance	
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-520	EE REQUIREMENT	Request only initial set	OBE shall make a certificate provisioning request only for the initial set of pseudonym and application certificates or when the certificate parameters change	Because top-up certificates are generated automatically by the RA.	This is out of scope as it defines OBE behavior.	On-board Equipment (OBE)
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	PoC will only store 3 years	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
				based on historical trends for vehicle ownership. For example, collector vehicles that are kept on the road for longer than typical vehicles.		
SCMS-534	CLOSED	Certificate Batch	RA shall store certificates to be downloaded by EE in the folder provided in the ack message to the provisioning request.	Certificate batch is the basis for receiving pseudonym certificates. The use-case objective is to transfer certificate batches from RA to EE.		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	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
				Communications - General Guidance		
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-544	CLOSED	Download resume	RA shall support byte-wise resume of certificate batch, certificate file, or policy file, downloads, even if EE switches the IP address.	To improve reliability of the download protocol.		RA
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	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)

Key	Status	Summary	Description	Justification	Notes	Component/s
				18: Provide and Enforce Technical Policies.		
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		RA

Key	Status	Summary	Description	Justification	Notes	Component/s
				number in the download request to RA and the response will include a newer LCCF if available.		
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-954	EE REQUIREMENT	Error code: eePolicyVerificationFailed	EE shall log this error code in EE's error log file, if EE is not able to verify the digital signature of the local policy file.	To enable EE side diagnostics.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-956	EE REQUIREMENT	Error code: eePolicyFileParsingFailed	EE shall log this error code in EE's error log file, if EE is not able to parse the successfully downloaded local policy file (e.g., because 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 read 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-958	EE REQUIREMENT	Error code: eeConnectionFailed	EE shall log this error code, if it cannot connect to RA because there is a connection timeout.	To enable EE side diagnostics.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-976	CLOSED	Error code: raInvalidURL	RA shall log "Error code: raInvalidURL", if EE requests invalid URL.	To enable server side diagnostics and to avoid giving potential attackers relevant information	This is not in ASN.1 but http 404	RA
SCMS-977	CLOSED	TLS error codes	RA shall return standard TLS error codes if TLS errors occur.	In order to enable client side error handling.		RA
SCMS-978	CLOSED	Error code: raAuthenticationFailed	RA shall log "Error code: raAuthenticationFailed", if EE-to-RA authentication fails.	To enable server side diagnostics and to avoid giving potential		RA

Key	Status	Summary	Description	Justification	Notes	Component/s
				attackers relevant information.		
SCMS-979	EE REQUIREMENT	Error code: eeAuthenticationFailed	EE shall log "Error code: eeAuthenticationFailed", if RA-to-EE authentication fails.	To enable EE side diagnostics.	This is out of scope since it defines EE's behavior. This is part of TLS handshake. OEM defines EE error handling.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-981	CLOSED	Error code: raNoPcaCertificateChainFileAvailable	RA shall return status code HTTP 500, if Local Certificate Chain File is not available and log "Error code: raNoPcaCertificateChainFileAvailable".	To enable client side error handling.		RA
SCMS-987	TESTS FAILED	Error code: raWrongParameters	RA shall log "Error code: raWrongParameters", if a device sends request with wrong parameters.	To enable server side diagnostics and to avoid giving potential attackers relevant information		RA
SCMS-988	TESTS FAILED	Error code: raRetries	RA shall log "Error code: raRetries", if the EE retries within the time specified in SCMS-522.	To enable server side diagnostics and to avoid giving potential attackers relevant information. Retry not allowed within 2 seconds.		RA

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-990	TESTS FAILED	Error code: raMoreThanAllowedTries	RA shall return status code HTTP 500, if the EE violates SCMS-523, and log "Error code: raMoreThanAllowedTries".	To avoid DoS attacks		RA
SCMS-1065	CLOSED	Error code: raBlacklisted	RA shall log "Error code: raBlacklisted" if the requesting EE has been blacklisted.	Error's produced by an EE should always be logged for diagnostic purposes and never returned to the EE to avoid giving a potential attacker sensitive information.	RA response to EE shall follow SCMS-1397	RA
SCMS-1070	CLOSED	Error code: raDuplicateRequestReceived	The RA shall log "Error code: raDuplicateRequestReceived" as well as identifying information of the EE, if EE sent a duplicate request.	This error code catches duplicate requests.	Consider this for MA integration at a later stage.	RA
SCMS-1076	EE REQUIREMENT	Error code: eePolicyVerificationFailed	EE shall log this error code, if EE is not able to verify the digital signature of the local policy file.	As the local policy file contains security relevant configuration, it is essential to verify if a recently downloaded version of that file is coming from a trustworthy source.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1082	CLOSED	Error code: raInvalidSignature	The RA shall log "Error code: raInvalidSignature", if the EE does not sign the certificate request with its enrollment certificate or if the signature is invalid.	To enable server side diagnostics and to avoid giving potential	An unsigned request might be an indication for misbehavior.	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
				attackers relevant information		
SCMS-1083	CLOSED	Error code: raRequestNotEncrypted	The RA shall log "Error code: raRequestNotEncrypted", if the EE does not encrypt the certificate request using the RA's 1609 certificate.	To enable server side diagnostics and to avoid giving potential attackers relevant information	An unencrypted certificate request might be an indication for misbehavior.	RA
SCMS-1084	CLOSED	Error code: raInvalidCredentials	The RA shall log "Error code: raInvalidCredentials", if the EE has invalid credentials (blacklisted, expired, unauthorized)	To enable server side diagnostics and to avoid giving potential attackers relevant information	A request with invalid credentials might be an indication for misbehavior.	RA
SCMS-1085	TESTS FAILED	Error code: raUnauthorizedRequest	RA shall log "Error code: raUnauthorizedRequest", if an EE makes an unauthorized request (invalid permissions)	To enable server side diagnostics and to avoid giving potential attackers relevant information	An unauthorized request might be an indication for misbehavior.	RA
SCMS-1086	TESTS FAILED	Error code: raMalformedRequest	RA shall log "Error code: raMalformedRequest", if an EE makes a malformed request not captured inhttps://jira.campllc.org/browse/SCMS-1082~~SCMS-1082~~,https://jira.campllc.org/browse/SCMS-1083~~SCMS-1083~~,https://jira.campllc.org/browse/SCMS-1084~~SCMS-1084~~, SCMS-1085.	To enable server side diagnostics and to avoid giving potential attackers relevant information.	A malformed request might be an indication for misbehavior.	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-1087	CLOSED	Error code: raMismatch	The RA shall log "Error code: raMismatch", if this RA does not service the requesting EE.	To enable server side diagnostics and to avoid giving potential attackers relevant information.	A request from an EE that is not serviced by the requested RA might be an indication for misbehavior.	RA
SCMS-1088	CLOSED	Error code: raInvalidTimeReceived	The RA shall return status code HTTP 500, if the EE has send an invalid system time, and log "Error code: raInvalidTimeReceived".	To avoid EEs using the invalid certificates		RA
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	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
					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.	
SCMS-1210	EE REQUIREMENT	EE Secure Key Storing	EE shall store the following keys in tamper-resistant (or equivalent) storage: • Private enrollment key • Butterfly key parameters (seed + expansion function parameter) • All private keys (e.g., of OBE application certificates and private keys calculated from the Butterfly key parameters)	To avoid extraction of private keys via software-based attacks.	This is out of scope since it defines EE's behavior. It is highly recommended to protect the content encryption key by a TPM-like mechanism that offers secure boot and that protects the keys against software-based attacks. Additional details are listed in Hardware, Software and OS Security	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-1263	EE REQUIREMENT	EE download resume	EE shall try byte-wise resume of CRL downloads from the CRL store, certificate batches, certificate files, or policy files from RA in case a previous download failed.	This will improve reliability of the download process and reduce communication cost.		On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1270	EE REQUIREMENT	Network connection	EEs shall use TCP/IP to communicate with the SCMS.	SCMS components (server) are only reachable by standard TCP/IP networking methods.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
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-1356	EE REQUIREMENT	EE uses internal certificate store	The EE shall use its internal certificate store to validate received SCMS certificates and respond to P2P certificate requests.	EEs need to be able to validate received SCMS certificates based on their certificate chain up to the SCMS root CA. EEs need to respond to P2P certificate requests to enable	EE does not need to store all certificate chains, the LCCF provides the minimum set and EEs can learn additional chains via P2P certificate request. This is out of scope as it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
				receiving EEs to validate the certificate chain.		
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-1397	TESTS FAILED	Error reporting to EE	The SCMS Components shall return error code "HTTP 500" to EEs in response to all application level errors at RA.	Specific error codes should be hidden from EEs to prevent useful information from being provided to malicious actors	• Standard TCP (https://jira.campllc.org/browse/SCMS-1090~~SCMS-1090~~) and TLS (https://jira.campllc.org/browse/SCMS-977~~SCMS-977~~) errors shall be reported to EEs • All errors at the HTTP and higher levels shall be HTTP 500 for RA & ECA	CRL Store, RA
SCMS-1404	EE REQUIREMENT	EE send data via HTTP post over TCP/IP	EE shall use HTTP post to send data towards the RA	To allow the SCMS endpoint to serve everything based on HTTP protocol	RA - Services View will document the actual HTTP post details. This is out of scope as it defines EE behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-1405	CLOSED	RA accept authenticated HTTP post requests	RA shall accept HTTP post requests only from authenticated EEs.	To allow the SCMS endpoint to serve everything based on HTTP protocol	RA - Services View will document the actual HTTP post details.	RA
SCMS-1421	EE REQUIREMENT	LCCF validation in EE	The EE shall verify the LCCF and then update the internal certificate store each time it receives a new LCCF.	To have the latest certificate chain update available for validating certificates and answering P2P certificate requests.	This is out of scope as it defines EEs behavior	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1512	EE REQUIREMENT	Generating Butterfly Key seeds and expansion function	The EE shall generate butterfly key seeds and expansion function.	Protect privacy of data during transfer by not extracting the keys.	For OBE pseudonym certificates, OBE will generate Butterfly key parameters for the certificate signature keys and the response encryption key. For OBE identification certificates, OBE will generate Butterfly key parameters for the certificate signature keys, and optionally for certificate encryption keys and response encryption keys.	On-board Equipment (OBE)

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-1625	TESTS FAILED	RA-EE Certificate Request Ack Message	RA-EE Certificate Request Ack Message shall contain the following information: Case: Certificate Provisioning Request Accept • Version • Low order 8-bytes of the SHA-256 hash of the encoded "ToBeSigned" certificate request from the device • Time at which the first certificate batches will be available for download (represented by IEEE 1609.2 Time32) • URL of the certificate repository (common for all devices serviced by a specific RA) Case: Certificate Provisioning Request Reject • HTTP 500 error code	As the EE needs to know, when and where it can go to download certificates.		RA
SCMS-2463	EE REQUIREMENT	EE transactions per TLS session	EE shall perform as many SCMS transactions as possible using a single TLS session.	To minimize the number of separate TLS sessions to the SCMS. This will reduce the resources required and improve throughput.	This is out of scope as it defines EE behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
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-2612	REVIEW	Store butterfly parameters	RA shall store butterfly parameters for each OBE for the estimated functional lifetime of the OBE.	So that the certificate pre-generation and revocation can function 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.		RA

Table 19 Use Case 3.1 - Requirements

62 issues

5.2.7.6.7 Design

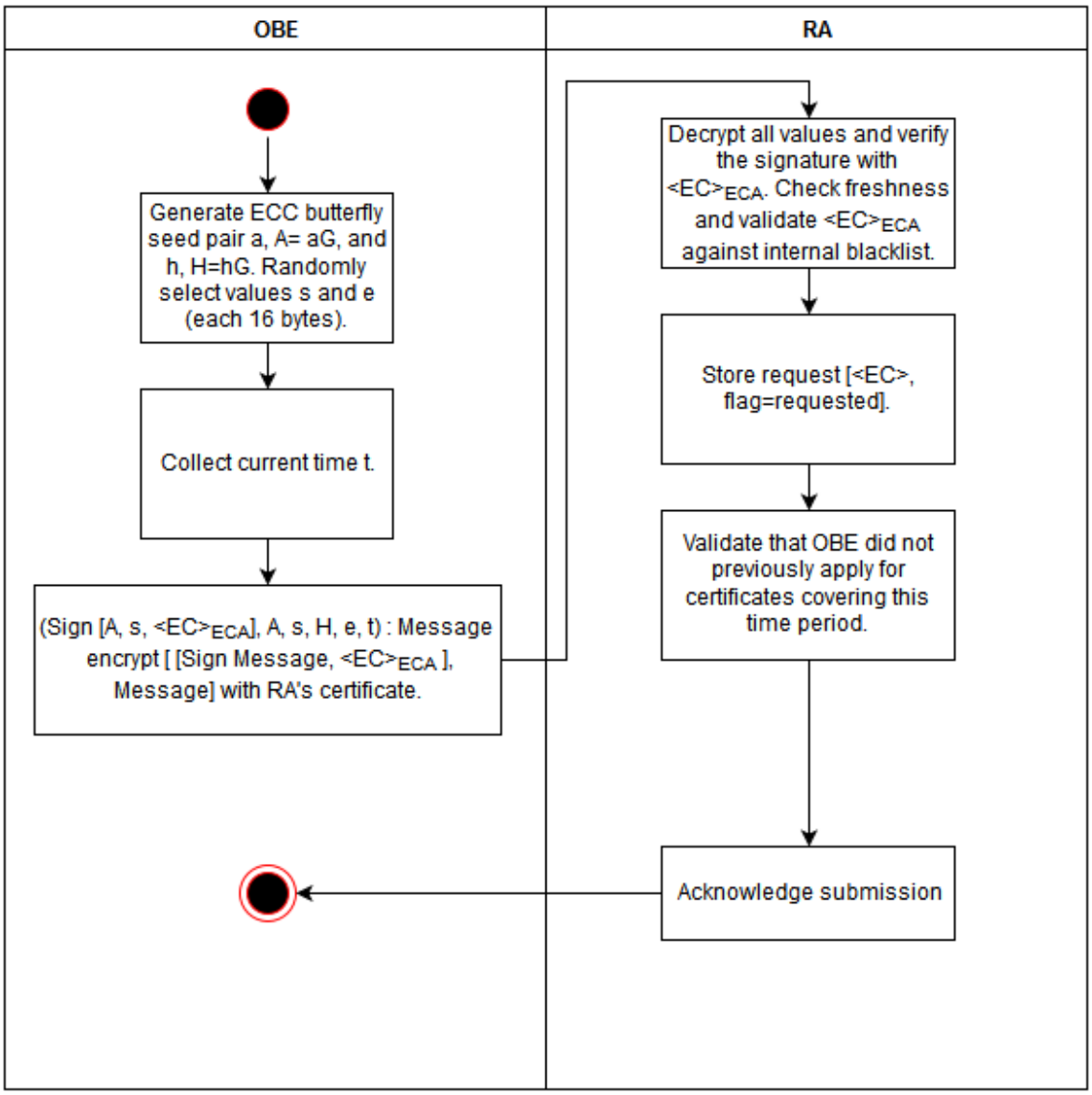


Figure 51 OBE-RA Communication

5.2.7.6.7.1 EE Request

EE initiates the certificate request message to provide the RA with critical information (key parameters, current time, etc.) necessary for certificate batch generation. New devices may experience some delay between the initial request and the time that the first certificate batches are available for download to accommodate provisioning processes such as shuffling, certificate generation, and certificate encryption. The RA will store information from the initial certificate provisioning request message and use it for ongoing certificate pre-generation until:

- The device is blacklisted at the RA due to misbehavior or malfunction

The Certificate Provisioning Request message is sent only once for each unique request and no subsequent Certificate Provisioning Request is necessary to acquire new certificate batches.

5.2.7.6.7.1.1 Security / Privacy

The Certificate Provisioning Request message uses signing and encryption to ensure:

- The request has not been modified in transit
- The RA can verify the message came from EE
- The request is shared confidentially between EE and RA

The EE signs the request with the Enrollment Certificate. The EE also encrypts the request using the RA certificate.

5.2.7.6.7.1.2 Message Contents

The EE uses the ASN.1 defined for creating the Request Certificate message. Details can be found at RA - Request Pseudonym Certificate Batch Provisioning. In order for a request to be validated by the RA, the EE includes the following information in the Certificate Provisioning Request message:

- Version
- EE enrollment certificate
- Butterfly public seed / expansion function (see SCP1: Butterfly Keys for details) parameters for:
    - certificate signing key
    - response encryption key (to encrypt the created certificate towards EE)
- Current device time: 32-bit denoting number of seconds since the Epoch (as defined in 1609.2)
- Requested certificate start time: 32-bit denoting number of seconds since the Epoch (as defined in 1609.2)

5.2.7.6.7.2 RA Response

The RA response to the Certificate Provisioning Request message is either *accept* (indicated by a Request Acknowledgement) or *reject* (indicated by a HTTP 500). Specific error codes will be hidden from EEs in production to avoid providing useful information to malicious actors. RA logs the specific error for future investigation.

5.2.7.6.7.2.1 RA - EE Request Acknowledgement

The Request Acknowledge message is initiated by the RA in response to a Certificate Provisioning Request message successfully received from the EE. If the EE request is received and processed without triggering an error (invalid signature, blacklisted, etc.), the RA processes the certificate request and begins certificate pre-generation. The Request Acknowledge message provides the EE with the URL and the time where and at which the first certificates batches will be available for download.

5.2.7.6.7.3 Security / Privacy

The Request Acknowledge message use signing to ensure:

- The request has not been modified in transit
- The EE can verify the message came from the RA

The RA signs the Request Acknowledge message using the RA certificate.

5.2.7.6.7.3.1 Message Contents

The RA uses the ASN.1 defined for creating the Request Acknowledge message, which can be found at RA - Request Pseudonym Certificate Batch Provisioning.

5.2.7.6.7.4 EE Response

If the RA provides a positive acknowledgement (*accept)* to a Certificate Provisioning Request, the EE moves forward with the certificate batch download process using the provided URL and time both given in the acknowledge message.

If the EE does not receive an acknowledgement from the RA in response to the request within defined time, EE should retry. Several conditions may necessitate the EE sending the request more than once. This may be due to:

- Request lost in transit (no TCP ack)
- RA offline, unavailable or RA network address has changed (EE must query DNS for latest RA network information)
- EE possesses an invalid RA certificate and cannot establish secure communications
- EE received HTTP-500 Error Code

The EE should not attempt to transmit the Request Certificate message without having completed the prerequisites.

5.2.7.6.8 ASN.1 Specification

- ee-ra.asn
- scms-protocol.asn
- scms-base-types.asn
- scms-error.asn
- scms-policy.asn
- scms-common-errors.asn
- 1609dot2-schema.asn
- 1609dot2-base-types.asn

5.2.7.7 Step 3.3: Initial Download of Pseudonym Certificates

5.2.7.7.1 Goals

The goal is to provide a reliable, secure and timely method for certified devices to download credentials, while maintaining a minimum level of privacy that is expected by the end user. The solution should prevent a certified device (that has not been revoked) from running out of credentials required for critical safety systems to operate to the greatest extent possible.

5.2.7.7.2 Background and Strategic Fit

The purpose of this use case is to provide a defined method that a certified OBE can use to download batches of credentials. These credentials will be used to certify the device during transmission of critical safety messages, submission of misbehavior reports, and other critical system functions. The download will include:

1. Files that include batches of certificates (each file holds certificates worth a week)
2. The .info file that includes the time when the next batch of certificates will be available for download
3. A local certificate chain file containing all PCA certificate chains required to validate the pseudonym certificates
4. The local policy file

5.2.7.7.3 Assumptions

1. The OBE has successfully completed Step 3.1: Request for Pseudonym Certificates
2. The RA retrieved from PCA the issued certificates, zipped, and stored them in a folder for OBE to download

5.2.7.7.4 Process Steps

The OBE should follow the following steps to download the initial batch of pseudonym certificates. Neither order nor fulfillment of all steps is enforced, but highly recommended.

1. The OBE downloads the Local Policy File (LPF) and the Local Certificate Chain File (LCCF), as before in Step 3.1: Request for Pseudonym Certificates
    a. The OBE applies all changes to its trust-store (necessary for PCA Certificate Validations) if there is an updated LCCF
    b. The OBE applies those changes if there is an updated LPF
2. The OBE downloads the pseudonym certificate batches using the API documented in RA - Download Pseudonym Certificate Batch
3. The OBE downloads the .info file using the API documented in RA - Download .info File

5.2.7.7.5 Error Handling

1. The OBE will abandon further interactions with the RA after a certain number of failed communication attempts resulted in errors
2. The OBE will not attempt to execute the certificate provisioning process if it finds itself on the latest CRL (assumes that a willful violator has not compromised the device). The OBE will execute the certification/bootstrap process again to exit a revoked state.

5.2.7.7.6 Requirements

Table 20 Use Case 3.3 - Requirements

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-341	EE REQUIREMENT	EE TLS Cipher Suite	The EE shall support at least the following TLS cipher suites for all communications to SCMS components: **Iana Value** / **Description** / **Reference** 0xC0,0x23 / TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 / RFC 5289 0xC0,0x24 / TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 / RFC 5289 0xC0,0x2B / TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 / RFC 5289 0xC0,0x2C / TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 / RFC 5289	This is the requirement for the SSL transport tunnel.	This is out of scope as it defines EE behavior.	On-board Equipme (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
			0xC0,0xAC TLS_ECDHE_ECDSA_WITH_AES_128_CCM RFC 7251 0xC0,0xAD TLS_ECDHE_ECDSA_WITH_AES_256_CCM RFC 7251			
SCMS-411	EE REQUIREMENT	EE Authentication to RA for Request	The EE shall authenticate its requests with its enrollment certificate and signed timestamp to avoid replay attacks on the RA.	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.	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.	On-board Equipme (OBE), Road-side Equipment (RSE)
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	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
					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.	
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	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
					component CRL (comparehttps://jira.campllc.org/browse/SCMS-859~~SCMS-859~~, SCMS-504) and the X.509 CRL (https://jira.campllc.org/browse/SCMS-405~~SCMS-405~~).	
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 (https://jira.campllc.org/browse/SCMS-	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
					537~~SCMS-537~~) and RA-EE authentication (https://jira.campllc.org/browse/SCMS-539~~SCMS-539~~). IEEE 1609.2 certificates within a TLS session will be used for EE-RA authentication (SCMS-538).	
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	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
					Communications - General Guidance	
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 Equipme (OBE), Road-side Equipment (RSE)
SCMS-534	CLOSED	Certificate Batch	RA shall store certificates to be downloaded by EE in the folder provided in the ack message to the provisioning request.	Certificate batch is the basis for receiving pseudonym certificates. The use-case objective is to transfer certificate batches from RA to EE.		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	For pseudonym certificates, this counters a somewhat exotic attack: if an	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
				adversary is able to read PCA-encrypted pseudonym certificates.	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.	
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	This is out of scope since it defines EE's behavior.	On-board Equipme (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
				in EE-RA Communications - General Guidance		
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 Equipme (OBE), Road-side Equipment (RSE)
SCMS-543	CLOSED	Individual certificate downloads	RA shall support individual certificate batch, or certificate file, downloads by EEs.	The design allows download of individual certificate batches, or files, to avoid that an EE needs to download all certificates each time. This also allows easier resume of a download.		RA

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-544	CLOSED	Download resume	RA shall support byte-wise resume of certificate batch, certificate file, or policy file, downloads, even if EE switches the IP address.	To improve reliability of the download protocol.		RA
SCMS-547	CLOSED	Available certificate batches	The number of certificate batches, or certificate files, available for download shall be configurable (e.g. 3 years) as defined by the configuration option max_available_cert_supply in the global policy.	This might change during the lifetime of the SCMS. It might even vary for different EEs.		RA
SCMS-548	CLOSED	X.info file	RA shall provide an .info file for download by EE.	The .info file provides information when new pseudonym certificates, or identification certificates, can be downloaded.	In order for the EE to determine the earliest time which new certificate batches will be available for download, the RA shall maintain a file in each device specific repository. This file will contain a timestamp at which the RA is predicted to update certificate batches in the device repository. The timestamp shall be in the IEEE 1609.2 Time32 format (the	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
					number of (TAI) seconds since 00:00:00 UTC, January 1, 2004). The file shall be named according to the following format: X.info Where X is the lower 8-bytes of the SHA-256 hash of device request in hexadecimal	
SCMS-549	CLOSED	Keep Certificates	The RA shall allow the EE to download certificates that have previously been downloaded, so long as the devices credentials are still valid and the certificates are not expired.	to recover from a loss of certificates at the device level (e.g., disk corruption).		RA
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 Equipme (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
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-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 Equipme (OBE), Road-side Equipment (RSE)
SCMS-954	EE REQUIREMENT	Error code: eePolicyVerificationFailed	EE shall log this error code in EE's error log file, if EE is not able to verify the digital signature of the local policy file.	To enable EE side diagnostics.	This is out of scope since it defines EE's behavior.	On-board Equipme (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-956	EE REQUIREMENT	Error code: eePolicyFileParsingFailed	EE shall log this error code in EE's error log file, if EE is not able to parse the successfully downloaded local policy file (e.g., because 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 read the latest version of that file.	This is out of scope since it defines EE's behavior.	On-board Equipme (OBE), Road-side Equipment (RSE)
SCMS-958	EE REQUIREMENT	Error code: eeConnectionFailed	EE shall log this error code, if it cannot connect to RA because there is a connection timeout.	To enable EE side diagnostics.	This is out of scope since it defines EE's behavior.	On-board Equipme (OBE), Road-side Equipment (RSE)
SCMS-964	CLOSED	Error code: raCertFileUnavailable	RA shall return status code HTTP 500 to EE, if certificate batch is not available and log "Error code: raCertFileUnavailable.	to enable EE side error handling.		RA
SCMS-965	EE REQUIREMENT	Error code: eeCertFileDownloadFailed	If OBE is not able to download pseudonym or identification certificate files (e.g., because there is none or it is corrupted), OBE shall implement OEM defined error handling and store the error code in OBE's error log file.	To enable EE side diagnostics.	This is out of scope since it defines EE's behavior.	On-board Equipme (OBE)
SCMS-967	EE REQUIREMENT	Error code: eeCertFileVerificationFailed	EE shall log this error code, if EE is not able to verify the digital signature of an encrypted certificate.	To enable EE side diagnostics.	This is out of scope since it defines EE behavior. This is for a single-issue certificate that has been encrypted	On-board Equipme (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
					and digitally signed by PCA.	
SCMS-969	EE REQUIREMENT	Error code: eeCertificateFileDecryptionFailed	EE shall log this error code, if EE is not able to decrypt an encrypted certificate.	To enable EE side diagnostics.	This is out of scope since it defines EE's behavior.	On-board Equipme (OBE), Road-side Equipment (RSE)
SCMS-971	EE REQUIREMENT	Error code: eeCertificateVerificationFailed	EE shall log this error code, if EE is not able to verify a certificate.	This is to verify the issued certificate.	This is out of scope since it defines EE's behavior.	On-board Equipme (OBE), Road-side Equipment (RSE)
SCMS-973	EE REQUIREMENT	Error code: eeCertContentFalse	EE shall log this error code, if EE is not able to parse a certificate, or if the certificate has wrong content.	To enable EE side diagnostics.	This is out of scope since it defines EE's behavior.	On-board Equipme (OBE), Road-side Equipment (RSE)
SCMS-976	CLOSED	Error code: raInvalidURL	RA shall log "Error code: raInvalidURL", if EE requests invalid URL.	To enable server side diagnostics and to avoid giving potential attackers relevant information	This is not in ASN.1 but http 404	RA
SCMS-977	CLOSED	TLS error codes	RA shall return standard TLS error codes if TLS errors occur.	In order to enable client side error handling.		RA
SCMS-978	CLOSED	Error code: raAuthenticationFailed	RA shall log "Error code: raAuthenticationFailed", if EE-to-RA authentication fails.	To enable server side diagnostics and to avoid giving potential attackers relevant information.		RA
SCMS-979	EE REQUIREMENT	Error code: eeAuthenticationFailed	EE shall log "Error code: eeAuthenticationFailed", if RA-to-EE authentication fails.	To enable EE side diagnostics.	This is out of scope since it defines EE's behavior.	On-board Equipme (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
					This is part of TLS handshake. OEM defines EE error handling.	
SCMS-981	CLOSED	Error code: raNoPcaCertificateChainFileAvailable	RA shall return status code HTTP 500, if Local Certificate Chain File is not available and log "Error code: raNoPcaCertificateChainFileAvailable".	To enable client side error handling.		RA
SCMS-982	CLOSED	X.info file update period	RA shall update the .info file at least on a weekly basis.	The .info file is updated regularly to provide timely updates to EE		RA
SCMS-984	EE REQUIREMENT	Error code: obeInfoFileDownloadFailed	OBE shall log this error code, if it is not able to download the .info file (e.g. because there is none or it is corrupted).	to enable EE side diagnostics.	This is out of scope since it defines EE behavior.	On-board Equipme (OBE)
SCMS-1065	CLOSED	Error code: raBlacklisted	RA shall log "Error code: raBlacklisted" if the requesting EE has been blacklisted.	Error's produced by an EE should always be logged for diagnostic purposes and never returned to the EE to avoid giving a potential attacker sensitive information.	RA response to EE shall follow SCMS-1397	RA
SCMS-1076	EE REQUIREMENT	Error code: eePolicyVerificationFailed	EE shall log this error code, if EE is not able to verify the digital signature of the local policy file.	As the local policy file contains security relevant configuration, it is essential to verify if a recently downloaded version of that file is coming from a trustworthy source.	This is out of scope since it defines EE's behavior.	On-board Equipme (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-1090	CLOSED	Error code: raTcpErrors	RA shall return standard TCP error codes if TCP errors occur and log "Error code: raTcpErrors" and the encountered TCP error.	in order to enable client side error handling.		RA
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 Equipme (OBE), Road-side Equipment (RSE)
SCMS-1201	EE REQUIREMENT	EE certificate download via HTTPS over TCP/IP	EE shall use HTTPS (TLS) over TCP/IP to download files from the SCMS.	In order to use standard internet technology.	This is out of scope as it defines EE behavior.	On-board Equipme (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	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
					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.	
SCMS-1214	EE REQUIREMENT	OBE downloads .info file	OBE shall download the .info file each time OBE downloaded pseudonym or identification certificates.	EE requires the information to learn when certificates will be available for download.	This is out of scope since it defines EE's behavior.	On-board Equipme (OBE)

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-1215	EE REQUIREMENT	EE contacts RA for certificate download	EE shall try to download certificates any time after the time provided by the time-stamp in the .info file that has been recovered last time EE tried to download, or downloaded, certificates.	To avoid wasting resources by trying to download certificates before they are available.	This is out of scope since it defines EE behavior. The timestamp shall be in the IEEE 1609.2 Time32 format (the number of (TAI) seconds since 00:00:00 UTC, January 1, 2004).	On-board Equipme (OBE), Road-side Equipment (RSE)
SCMS-1263	EE REQUIREMENT	EE download resume	EE shall try byte-wise resume of CRL downloads from the CRL store, certificate batches, certificate files, or policy files from RA in case a previous download failed.	This will improve reliability of the download process and reduce communication cost.		On-board Equipme (OBE), Road-side Equipment (RSE)
SCMS-1270	EE REQUIREMENT	Network connection	EEs shall use TCP/IP to communicate with the SCMS.	SCMS components (server) are only reachable by standard TCP/IP networking methods.	This is out of scope since it defines EE's behavior.	On-board Equipme (OBE), Road-side Equipment (RSE)
SCMS-1279	EE REQUIREMENT	Error code: eeCertificateDecryptionFailed	EE shall log this error if certificate decryption failed at EE.	To allow error reaction and investigation.	Out of scope as it defines EE behavior.	On-board Equipme (OBE), Road-side Equipment (RSE)
SCMS-1280	EE REQUIREMENT	Error code: eeCertificateNotReadable	EE shall log this error if any certificate is not readable.	To enable error reaction and investigation.		On-board Equipme (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-1282	EE REQUIREMENT	Error code: eeDecompressionError	EE shall log "Error code: eeDecompressionError", if it is not able to decompress the received certificate.	To allow error reaction and investigation.	Out of scope as it defines EE behavior.	On-board Equipme (OBE), Road-side Equipment (RSE)
SCMS-1303	EE REQUIREMENT	Verification of certificate validity	EE shall verify the validity of a received certificate against IEEE 1609.2-v3-D12, clause 5.1 and 5.3.	To verify if the certificate is issued by a trustworthy source and therefore messages signed by this certificate can be trusted.	This is for testing that SCMS issued valid and proper certificates. This is out of scope since it defines EE behavior.	On-board Equipme (OBE), Road-side Equipment (RSE)
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 Equipme (OBE), RA, Road-s Equipment (RSE)
SCMS-1356	EE REQUIREMENT	EE uses internal certificate store	The EE shall use its internal certificate store to validate received SCMS certificates and respond to P2P certificate requests.	EEs need to be able to validate received SCMS certificates based on their certificate chain up to the SCMS root CA. EEs need to respond to P2P certificate requests	EE does not need to store all certificate chains, the LCCF provides the minimum set and EEs can learn additional chains via	On-board Equipme (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
				to enable receiving EEs to validate the certificate chain.	P2P certificate request. This is out of scope as it defines EE's behavior.	
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-1397	TESTS FAILED	Error reporting to EE	The SCMS Components shall return error code "HTTP 500" to EEs in response to all application level errors at RA.	Specific error codes should be hidden from EEs to prevent useful information from being provided to malicious actors	• Standard TCP (https://jira.campllc.org/browse/SCMS-1090~~SCMS-1090~~) and TLS (https://jira.campllc.org/browse/SCMS-977~~SCMS-977~~) errors shall be reported to EEs • All errors at the HTTP and higher levels shall be HTTP 500 for RA & ECA	CRL Store, RA

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-1404	EE REQUIREMENT	EE send data via HTTP post over TCP/IP	EE shall use HTTP post to send data towards the RA	To allow the SCMS endpoint to serve everything based on HTTP protocol	RA - Services View will document the actual HTTP post details. This is out of scope as it defines EE behavior.	On-board Equipme (OBE), Road-side Equipment (RSE)
SCMS-1405	CLOSED	RA accept authenticated HTTP post requests	RA shall accept HTTP post requests only from authenticated EEs.	To allow the SCMS endpoint to serve everything based on HTTP protocol	RA - Services View will document the actual HTTP post details.	RA
SCMS-1420	SCMS POC OUT OF SCOPE	Keep track of which authorization (pseudonym, ID, application) certificates are downloaded	The RA shall keep track of how far into the future each device has downloaded its certificates.	This allows revoked devices to be removed from the CRL (or deprioritized for inclusion on the CRL) once they exhaust the set of certificates that they have downloaded.	This is an optimization for CRL handling and therefore out of scope for PoC implementation.	RA
SCMS-1421	EE REQUIREMENT	LCCF validation in EE	The EE shall verify the LCCF and then update the internal certificate store each time it receives a new LCCF.	To have the latest certificate chain update available for validating certificates and answering P2P certificate requests.	This is out of scope as it defines EEs behavior	On-board Equipme (OBE), Road-side Equipment (RSE)
SCMS-1454	CLOSED	Pseudonym certificate batch filename	RA shall name pseudonym certificate batch files according to the following format: • X_Y.zip	File names must be predefined to allow OBEs to make valid download requests.	Example file name: 2AFC55B22CFDBE3E_3C.zip	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
			• Where X is the lower 8-bytes of the SHA-256 hash of device request in hexadecimal in uppercase • Where Y is the i-value in hexadecimal in uppercase • Where the extension is .zip in lowercase			
SCMS-1456	CLOSED	Certificate file content	RA shall organize individual certificates contained within the certificate batch according to the following format: • X_Y • Where X is the i-value in hexadecimal in uppercase • Where Y is a sequence of "j" values from j = 0 to j = j_max-1 in hexadecimal in uppercase • Where there is no extension	File content must be predefined to allow EEs to process the contents.	For example: • 0_0 • 0_1 • … • 0_*<j_max-1>*	*RA*
SCMS-1639	EE REQUIREMENT	Download certificate batches	OBE shall not attempt to download certificate batches for i-value periods more than max_available_cert_supply in the future	To reduce resource usage by not attempting to download certificate batches that do not exist.	• This is out of scope as it defines EE behavior. • This is the OBE counterpart	~~On-board Equipme (OBE)~~

Key	Status	Summary	Description	Justification	Notes	Component/s
					ofhttps://jira.camplic.org/browse/SCMS-547~~SCMS-547~~	
SCMS-2463	EE REQUIREMENT	EE transactions per TLS session	EE shall perform as many SCMS transactions as possible using a single TLS session.	To minimize the number of separate TLS sessions to the SCMS. This will reduce the resources required and improve throughput.	This is out of scope as it defines EE behavior.	On-board Equipme (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 Equipme (OBE), Road-side Equipment (RSE)

67 issues

5.2.7.8 Step 3.5: Top-off Pseudonym Certificates

5.2.7.8.1 Goals

The goal is to provide a reliable, secure and timely method for certified devices to download credentials. The solution should prevent a certified device (that has not been revoked) from running out of credentials required for critical safety systems to operate to the greatest extent possible.

5.2.7.8.2 Background and Strategic Fit

The purpose of this use-case is to provide a defined method that a certified OBE can use to download new batches of credentials. These credentials will be used to certify the device during transmission of critical safety messages, submission of misbehavior reports, and other critical system functions. The download will include:

1. Files that include batches of certificates (each file holds certificates worth a week)
2. The .info file that includes the time when the next batch of certificates will be available for download
3. A local certificate chain file containing all PCA certificate chains required to validate the pseudonym certificates
4. The local policy file

The step at hand is to top-up pseudonym certificates. It is similar to Step 3.3: Initial Download of Pseudonym Certificates and differences are documented in this section. Also, see Step 3.4: Schedule Generation of Subsequent Batch of Pseudonym Certificates for full details of the process to schedule certificate pre-generation.

5.2.7.8.3 Assumptions

- OBE has successfully completed Step 3.1: Request for Pseudonym Certificates
- OBE has successfully completed Step 3.3: Initial Download of Pseudonym Certificates
- RA retrieved the issued certificates from PCA, zipped, and stored them in a folder on RA for OBE to download

5.2.7.8.4 Process Steps

The OBE should follow the following steps to download the initial batch of pseudonym certificates. Neither order nor fulfillment of all steps is enforced, but highly recommended.

1. The OBE checks that, and if necessary waits until, the current time matches or is after the timestamp given in the .info file

2. The OBE downloads the Local Policy File (LPF) and the Local Certificate Chain File (LCCF), as before in Step 3.1: Request for Pseudonym Certificates
    a. If there is an updated LCCF, the OBE applies all changes to its trust-store (necessary for PCA Certificate Validations)
    b. If there is an updated LPF, the OBE applies those changes
3. The OBE downloads pseudonym certificate batches
4. The OBE downloads .info file using the API documented in RA - Download .info File

5.2.7.8.5 Error Handling

1. The OBE will abandon further interactions with the RA after a certain number of failed communication attempts resulted in critical errors
2. The OBE will not attempt to execute the certificate provisioning process if it finds itself on the latest CRL (assumes that a willful violator has not compromised the device). The OBE will need to execute the certification/bootstrap process again to exit a revoked state.
3. The OBE may terminate the certificate batch download process if sufficient storage is not available for subsequent batches

5.2.7.8.6 Requirements

Table 21 Use Case 3.5 - 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</td><td>This is out of scope since it defines EE's behavior.
In the case of re-</td><td>On-board Equipment (OBE), Road-side Equipment (RSE)</td></tr>
</table>

Key	Status	Summary	Description	Justification	Notes	Component/s
				from the EE enables the RA to validate the freshness of EE requests.	enrollment (Use Case 22), the EE must use the current, active enrollment certificate to authenticate to the RA.	
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	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
					component certificate validation.	
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 (comparehttps://jira.campllc.org/browse/SCMS-859~~SCMS-859~~, SCMS-504) and the X.509 CRL (https://jira.campllc.org/browse/SCMS-405~~SCMS-405~~).	RA
SCMS-509	CLOSED	Stop pre-generating pseudonym and OBE identification certificates for revoked device	RA shall stop pre-generating pseudonym and OBE identification certificates for a device that has been revoked by the MA, i.e., for a device that appears on RA's internal blacklist.	so that computing resources are not wasted by generating certificates for revoked devices		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,	Note that LPF might have the same content	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
				and that configuration shall be current.	as the global policy file (GPF).	
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 (https://jira.campllc.org/browse/SCMS-537~~SCMS-537~~) and RA-EE authentication (https://jira.campllc.org/browse/SCMS-539~~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	It is not cost effective to provide OBEs with TLS certificates currently.	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
				requests, download certificates or files.	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	
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)

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-534	CLOSED	Certificate Batch	RA shall store certificates to be downloaded by EE in the folder provided in the ack message to the provisioning request.	Certificate batch is the basis for receiving pseudonym certificates. The use-case objective is to transfer certificate batches from RA to EE.		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

Key	Status	Summary	Description	Justification	Notes	Component/s
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	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
					specified in RFC 6066, Section 8.	
SCMS-543	CLOSED	Individual certificate downloads	RA shall support individual certificate batch, or certificate file, downloads by EEs.	The design allows download of individual certificate batches, or files, to avoid that an EE needs to download all certificates each time. This also allows easier resume of a download.		RA
SCMS-544	CLOSED	Download resume	RA shall support byte-wise resume of certificate batch, certificate file, or policy file, downloads, even if EE switches the IP address.	To improve reliability of the download protocol.		RA
SCMS-547	CLOSED	Available certificate batches	The number of certificate batches, or certificate files, available for download shall be configurable (e.g. 3 years) as defined by the configuration option max_available_cert_supply in the global policy.	This might change during the lifetime of the SCMS. It might even vary for different EEs.		RA
SCMS-548	CLOSED	X.info file	RA shall provide an .info file for download by EE.	The .info file provides information when new pseudonym certificates, or identification certificates, can be downloaded.	In order for the EE to determine the earliest time which new certificate batches will be available for download, the RA shall maintain a file in each device specific repository. This file will contain a	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
					timestamp at which the RA is predicted to update certificate batches in the device repository. The timestamp shall be in the IEEE 1609.2 Time32 format (the number of (TAI) seconds since 00:00:00 UTC, January 1, 2004). The file shall be named according to the following format: X.info Where X is the lower 8-bytes of the SHA-256 hash of device request in hexadecimal	
SCMS-549	CLOSED	Keep Certificates	The RA shall allow the EE to download certificates that have previously been downloaded, so long as the devices credentials are still valid and the certificates are not expired.	to recover from a loss of certificates at the device level (e.g., disk corruption).		RA
SCMS-576	CLOSED	Update .info file	The RA shall update .info files for all EEs even if no new certificate batches are created.	The EE uses the .info file to determine when the the earliest the next download is allowed to happen.	Timestamp in .info file is dynamically calculated based on system load. PoC scope will be to	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
					update .info file for non-revoked EEs only.	
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-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		RA

Key	Status	Summary	Description	Justification	Notes	Component/s
				to RA and the response will include a newer LCCF if available.		
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-954	EE REQUIREMENT	Error code: eePolicyVerificationFailed	EE shall log this error code in EE's error log file, if EE is not able to verify the digital signature of the local policy file.	To enable EE side diagnostics.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-956	EE REQUIREMENT	Error code: eePolicyFileParsingFailed	EE shall log this error code in EE's error log file, if EE is not able to parse the successfully downloaded local policy file (e.g., because 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 read 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)

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-958	EE REQUIREMENT	Error code: eeConnectionFailed	EE shall log this error code, if it cannot connect to RA because there is a connection timeout.	To enable EE side diagnostics.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-964	CLOSED	Error code: raCertFileUnavailable	RA shall return status code HTTP 500 to EE, if certificate batch is not available and log "Error code: raCertFileUnavailable.	to enable EE side error handling.		RA
SCMS-965	EE REQUIREMENT	Error code: eeCertFileDownloadFailed	If OBE is not able to download pseudonym or identification certificate files (e.g., because there is none or it is corrupted), OBE shall implement OEM defined error handling and store the error code in OBE's error log file.	To enable EE side diagnostics.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE)
SCMS-967	EE REQUIREMENT	Error code: eeCertFileVerificationFailed	EE shall log this error code, if EE is not able to verify the digital signature of an encrypted certificate.	To enable EE side diagnostics.	This is out of scope since it defines EE behavior. This is for a single-issue certificate that has been encrypted and digitally signed by PCA.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-969	EE REQUIREMENT	Error code: eeCertificateFileDecryptionFailed	EE shall log this error code, if EE is not able to decrypt an encrypted certificate.	To enable EE side diagnostics.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-971	EE REQUIREMENT	Error code: eeCertificateVerificationFailed	EE shall log this error code, if EE is not able to verify a certificate.	This is to verify the issued certificate.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-973	EE REQUIREMENT	Error code: eeCertContentFalse	EE shall log this error code, if EE is not able to parse a certificate, or if the certificate has wrong content.	To enable EE side diagnostics.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-976	CLOSED	Error code: raInvalidURL	RA shall log "Error code: raInvalidURL", if EE requests invalid URL.	To enable server side diagnostics and to avoid giving potential attackers relevant information	This is not in ASN.1 but http 404	RA
SCMS-977	CLOSED	TLS error codes	RA shall return standard TLS error codes if TLS errors occur.	In order to enable client side error handling.		RA
SCMS-978	CLOSED	Error code: raAuthenticationFailed	RA shall log "Error code: raAuthenticationFailed", if EE-to-RA authentication fails.	To enable server side diagnostics and to avoid giving potential attackers relevant information.		RA
SCMS-979	EE REQUIREMENT	Error code: eeAuthenticationFailed	EE shall log "Error code: eeAuthenticationFailed", if RA-to-EE authentication fails.	To enable EE side diagnostics.	This is out of scope since it defines EE's behavior. This is part of TLS handshake. OEM defines EE error handling.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-981	CLOSED	Error code: raNoPcaCertificateChainFileAvailable	RA shall return status code HTTP 500, if Local Certificate Chain File is not available and log "Error code: raNoPcaCertificateChainFileAvailable".	To enable client side error handling.		RA

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-982	CLOSED	X.info file update period	RA shall update the .info file at least on a weekly basis.	The .info file is updated regularly to provide timely updates to EE		RA
SCMS-984	EE REQUIREMENT	Error code: obeInfoFileDownloadFailed	OBE shall log this error code, if it is not able to download the .info file (e.g. because there is none or it is corrupted).	to enable EE side diagnostics.	This is out of scope since it defines EE behavior.	On-board Equipment (OBE)
SCMS-1065	CLOSED	Error code: raBlacklisted	RA shall log "Error code: raBlacklisted" if the requesting EE has been blacklisted.	Error's produced by an EE should always be logged for diagnostic purposes and never returned to the EE to avoid giving a potential attacker sensitive information.	RA response to EE shall follow SCMS-1397	RA
SCMS-1070	CLOSED	Error code: raDuplicateRequestReceived	The RA shall log "Error code: raDuplicateRequestReceived" as well as identifying information of the EE, if EE sent a duplicate request.	This error code catches duplicate requests.	Consider this for MA integration at a later stage.	RA
SCMS-1076	EE REQUIREMENT	Error code: eePolicyVerificationFailed	EE shall log this error code, if EE is not able to verify the digital signature of the local policy file.	As the local policy file contains security relevant configuration, it is essential to verify if a recently downloaded version of that file is coming from a trustworthy source.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-1090	CLOSED	Error code: raTcpErrors	RA shall return standard TCP error codes if TCP errors occur and log "Error code: raTcpErrors" and the encountered TCP error.	in order to enable client side error handling.		RA
SCMS-1164	EE REQUIREMENT	OBE next download timing	OBE shall use the stored .info file to schedule the next download attempt.	The .info file contains the timestamp when the next batch of certificates (pseudonym or identification) will be available for download. This timestamp is the earliest the OBE is allowed to connect to the RA for the next download. The timestamp shall be in the IEEE 1609.2 Time32 format (the number of (TAI) seconds since 00:00:00 UTC, January 1, 2004).	This is out of scope since it defines EE's behavior. • If no pseudonym certificates are available on the OBE for the current i_period (week), the OBE is allowed to make a download attempt at any time. • If no pseudonym certificates are available on the OBE for the next i_period (week), the OBE is allowed to make a download attempt at any time. • If no identification certificate is available on the OBE for the current	On-board Equipment (OBE)

Key	Status	Summary	Description	Justification	Notes	Component/s
					or next time period, the OBE is allowed to make a download attempt at any time.	
SCMS-1167	EE REQUIREMENT	Expired Certificate Batches	The OBE shall only download pseudonym certificate batches for the current and future i_period.	Only download certificates that are valid at the current time or in the future. Certificates that are already expired should not be downloaded.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE)
SCMS-1168	EE REQUIREMENT	OBE pseudonym certificate duplicate downloads	OBE shall not download pseudonym certificate batches that are already verified and stored on the device.	During top-up downloads, the OBE shall only download pseudonym certificate batches that are not currently verified and stored on the device. This is to prevent repeated downloads of the same content.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE)
SCMS-1171	EE REQUIREMENT	EE revoked	EEs that are revoked shall not attempt to download LCCF, LPF, pseudonym certificates, identification certificates or file misbehavior reports. Exceptions to this are: • EE is unable to determine its revocation status	To avoid unnecessary load at the RA.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
			• EE has no pseudonym or identification certificates available in local storage • EE is attempting to perform a re-enrollment operation			
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-1201	EE REQUIREMENT	EE certificate download via HTTPS over TCP/IP	EE shall use HTTPS (TLS) over TCP/IP to download files from the SCMS.	In order to use standard internet technology.	This is out of scope as it defines EE 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	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
					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.	
SCMS-1214	EE REQUIREMENT	OBE downloads .info file	OBE shall download the .info file each time OBE downloaded pseudonym or identification certificates.	EE requires the information to learn when certificates will be available for download.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE)
SCMS-1215	EE REQUIREMENT	EE contacts RA for certificate download	EE shall try to download certificates any time after the time provided by the time-stamp in the .info file that has been recovered last time EE tried to download, or downloaded, certificates.	To avoid wasting resources by trying to download certificates before they are available.	This is out of scope since it defines EE behavior. The timestamp shall be in the IEEE 1609.2 Time32 format (the number of (TAI) seconds since 00:00:00 UTC, January 1, 2004).	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-1263	EE REQUIREMENT	EE download resume	EE shall try byte-wise resume of CRL downloads from the CRL store, certificate batches, certificate files, or policy files from RA in case a previous download failed.	This will improve reliability of the download process and reduce communication cost.		On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1270	EE REQUIREMENT	Network connection	EEs shall use TCP/IP to communicate with the SCMS.	SCMS components (server) are only reachable by standard TCP/IP networking methods.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1282	EE REQUIREMENT	Error code: eeDecompressionError	EE shall log "Error code: eeDecompressionError", if it is not able to decompress the received certificate.	To allow error reaction and investigation.	Out of scope as it defines EE behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
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-1356	EE REQUIREMENT	EE uses internal certificate store	The EE shall use its internal certificate store to validate received SCMS certificates and respond to P2P certificate requests.	EEs need to be able to validate received SCMS certificates based on their certificate chain up	EE does not need to store all certificate chains, the LCCF provides the minimum	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
				to the SCMS root CA. EEs need to respond to P2P certificate requests to enable receiving EEs to validate the certificate chain.	set and EEs can learn additional chains via P2P certificate request. This is out of scope as it defines EE's behavior.	
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-1397	TESTS FAILED	Error reporting to EE	The SCMS Components shall return error code "HTTP 500" to EEs in response to all application level errors at RA.	Specific error codes should be hidden from EEs to prevent useful information from being provided to malicious actors	• Standard TCP (https://jira.campllc.org/browse/SCMS-1090~~SCMS-1090~~) and TLS (https://jira.campllc.org/browse/SCMS-977~~SCMS-977~~) errors shall be reported to EEs • All errors at the HTTP and higher levels shall be HTTP 500 for RA & ECA	CRL Store, RA

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-1404	EE REQUIREMENT	EE send data via HTTP post over TCP/IP	EE shall use HTTP post to send data towards the RA	To allow the SCMS endpoint to serve everything based on HTTP protocol	RA - Services View will document the actual HTTP post details. This is out of scope as it defines EE behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1405	CLOSED	RA accept authenticated HTTP post requests	RA shall accept HTTP post requests only from authenticated EEs.	To allow the SCMS endpoint to serve everything based on HTTP protocol	RA - Services View will document the actual HTTP post details.	RA
SCMS-1420	SCMS POC OUT OF SCOPE	Keep track of which authorization (pseudonym, ID, application) certificates are downloaded	The RA shall keep track of how far into the future each device has downloaded its certificates.	This allows revoked devices to be removed from the CRL (or deprioritized for inclusion on the CRL) once they exhaust the set of certificates that they have downloaded.	This is an optimization for CRL handling and therefore out of scope for PoC implementation.	RA
SCMS-1421	EE REQUIREMENT	LCCF validation in EE	The EE shall verify the LCCF and then update the internal certificate store each time it receives a new LCCF.	To have the latest certificate chain update available for validating certificates and answering P2P certificate requests.	This is out of scope as it defines EEs behavior	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-1454	CLOSED	Pseudonym certificate batch filename	RA shall name pseudonym certificate batch files according to the following format: • X_Y.zip • Where X is the lower 8-bytes of the SHA-256 hash of device request in hexadecimal in uppercase • Where Y is the i-value in hexadecimal in uppercase • Where the extension is .zip in lowercase	File names must be predefined to allow OBEs to make valid download requests.	Example file name: 2AFC55B22CFDBE3E_3C.zip	RA
SCMS-1456	CLOSED	Certificate file content	RA shall organize individual certificates contained within the certificate batch according to the following format: • X_Y • Where X is the i-value in hexadecimal in uppercase • Where Y is a sequence of "j" values from j = 0 to j = j_max-1 in hexadecimal in uppercase • Where there is no extension	File content must be predefined to allow EEs to process the contents.	For example: • 0_0 • 0_1 • … • 0_<*j_max-1*>	*RA*
SCMS-1639	EE REQUIREMENT	Download certificate batches	OBE shall not attempt to download certificate batches for i-value periods more than max_available_cert_supply in the future	To reduce resource usage by not attempting to download certificate batches that do not exist.	• This is out of scope as it defines EE behavior. • This is the OBE counterpart ofhttps://jira.campllc.	~~On-board Equipment (OBE)~~

Key	Status	Summary	Description	Justification	Notes	Component/s
					org/browse/SCMS-547~~SCMS-547~~	
SCMS-2463	EE REQUIREMENT	EE transactions per TLS session	EE shall perform as many SCMS transactions as possible using a single TLS session.	To minimize the number of separate TLS sessions to the SCMS. This will reduce the resources required and improve throughput.	This is out of scope as it defines EE behavior.	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)

72 issues

5.2.7.8.7 Design Notes

- See Step 3.3: Initial Download of Pseudonym Certificates for full details of the batch download process. Differences are documented in this section.
- From the SCMS point of view, the basic process for "top-up" certificate downloads is the same as that used for initial provisioning as detailed in Step 3.3: Initial Download of Pseudonym Certificates. However, this is an incremental download, not a full download of all available certificate files. The number of files downloaded shall be factored in system sizing requirements.
- From the OBE's point of view, the process is slightly different from the process for initial provisioning
- See Step 3.4: Schedule Generation of Subsequent Batch of Pseudonym Certificates for full details of the process to schedule certificate pre-generation
- The RA will record the last time an OBE established a connection. This last connection time will be used to stop pre-generating pseudonym certificates if there is no activity for a period of time.
- The RA will automatically resume pre-generating pseudonym certificates when an OBE reestablishes a connection. The new certificates will be available for download at the time specified in the .info file.

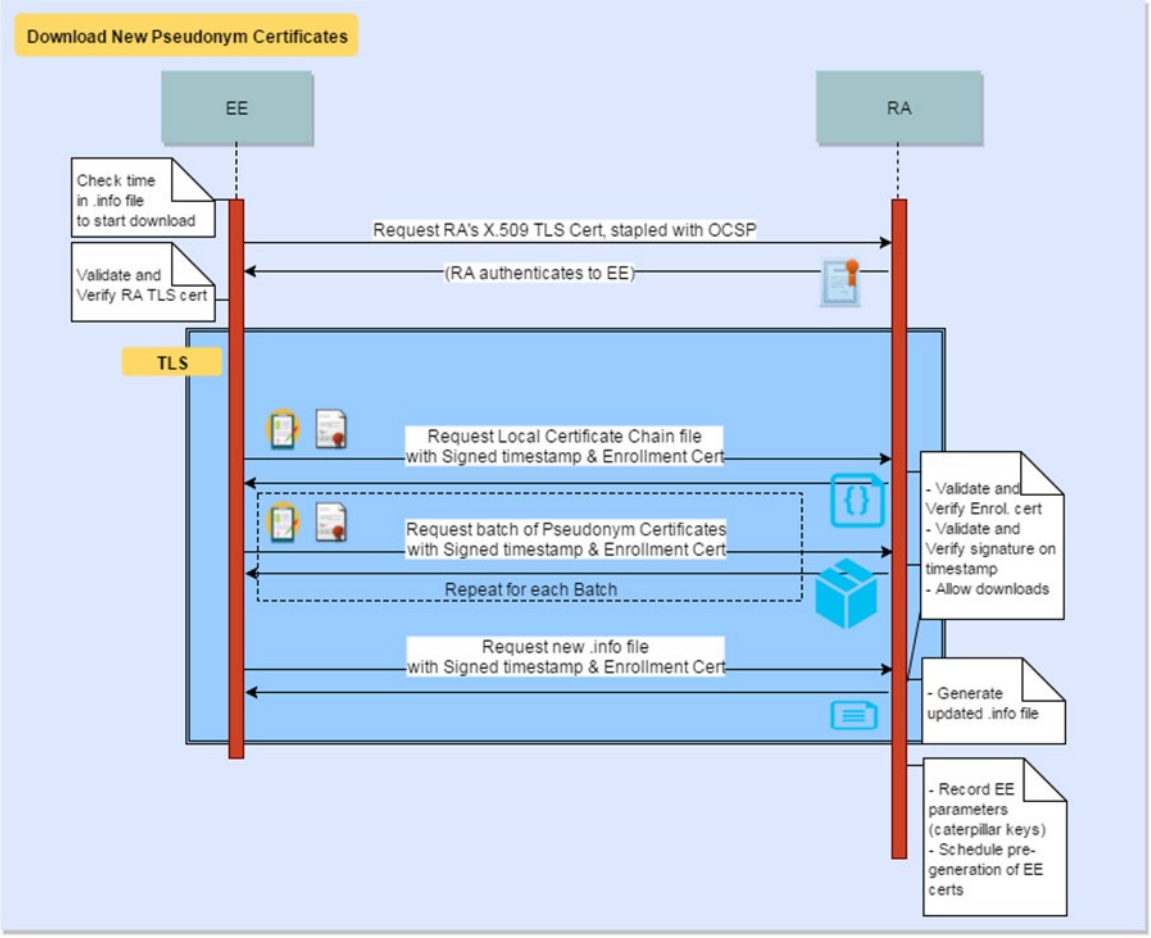


Figure 52 Download New Pseudonym Certificates

5.2.7.8.8 Not Doing

- Stopping of pre-generation of pseudonym certificates if an OBE has not contacted the RA for a period of time

5.2.8 Use Case 5: Misbehavior Reporting

Misbehavior Reporting will be integrated with the ongoing "Misbehavior Authority Integration" sub project as SCMS PoC release 2.0. Until then misbehavior reports will not be received and the previous misbehavior report format as described further down can and will change.

5.2.8.1 Goals

- Maintain the trust in the system

- Identify and remove bad actors

5.2.8.2 Background and Strategic Fit

EEs send misbehavior reports to the MA via the RA. The format of a misbehavior report is not defined yet but a report potentially includes reported BSMs as well as the reporter's pseudonym certificate and the reporter's signature. Reports may include random BSMs (casual report), suspicious BSMs, and alert-related BSMs. The report is encrypted by the EE for the MA. Note: The EEs' misbehavior detection algorithms (also called local misbehavior detection) are not defined yet.

5.2.8.3 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</td><td>RFC5289</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>
</table>

Key	Status	Summary	Description	Justification	Notes	Component/s
			_256_GCM_SHA384			
			0xC0,0xAC TLS_ECDHE_ECDSA_WITH_AES_128_CCM RFC7251			
			0xC0,0xAD TLS_ECDHE_ECDSA_WITH_AES_256_CCM RFC7251			
SCMS-411	EE REQUIREMENT	EE Authentication to RA for Request	The EE shall authenticate its requests with its enrollment certificate and signed timestamp to avoid replay attacks on the RA.	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.	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.	On-board Equipment (OBE), Road-side Equipment (RSE)
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	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
					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.	
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 (comparehttps://jira.campllc.org/browse/SCMS-859~~SCMS-859~~, SCMS-504) and the X.509 CRL (https://jira.campllc.org/bro	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
					wse/SCMS-405~~SCMS-405~~).	
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-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	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)

Key	Status	Summary	Description	Justification	Notes	Component/s
			amount of time, currently set to be 10 sec from the time of request.			
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-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-684	EE REQUIREMENT	Encryption	EE shall encrypt misbehavior reports with the Misbehavior Authority's public key before sending.	To avoid unauthorized parties getting access to the misbehaving report.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-685	CLOSED	Privacy	LOP shall remove all information in the IP layer that can be used to identify the location of the OBE before forwarding the misbehavior report to the RA.	to protect the identity of the sending OBE.	This does not apply to misbehavior reports send by RSEs.	LOP, RA

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-686	TESTS PASSED	Shuffle	RA shall shuffle misbehavior reports before sending them to MA.	Shuffling ensures MA cannot be sure that two misbehavior reports coming at the same time are from same OBE.	Amount of shuffle and/or maximum delay decided by SCMS manager.	RA
SCMS-765	TESTS PASSED	Shuffle Threshold	RA shall use a shuffle_threshold of 10,000 misbehavior reports or one day whichever is reached first.	Shuffling ensures MA cannot be sure that two misbehavior reports coming at the same time are from same RSE.		RA
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		RA

Key	Status	Summary	Description	Justification	Notes	Component/s
				will include a newer LCCF if available.		
SCMS-1171	EE REQUIREMENT	EE revoked	EEs that are revoked shall not attempt to download LCCF, LPF, pseudonym certificates, identification certificates or file misbehavior reports. Exceptions to this are: • EE is unable to determine its revocation status • EE has no pseudonym or identification certificates available in local storage • EE is attempting to perform a re-enrollment operation	To avoid unnecessary load at the RA.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1270	EE REQUIREMENT	Network connection	EEs shall use TCP/IP to communicate with the SCMS.	SCMS components (server) are only reachable by standard TCP/IP networking methods.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
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.	On-board Equipment (OBE), RA, Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
					This is out of scope since it defines EE behavior	
SCMS-1397	TESTS FAILED	Error reporting to EE	The SCMS Components shall return error code "HTTP 500" to EEs in response to all application level errors at RA.	Specific error codes should be hidden from EEs to prevent useful information from being provided to malicious actors	• Standard TCP (https://jira.campllc.org/browse/SCMS-1090~~SCMS-1090~~) and TLS (https://jira.campllc.org/browse/SCMS-977~~SCMS-977~~) errors shall be reported to EEs • All errors at the HTTP and higher levels shall be HTTP 500 for RA & ECA	CRL Store, RA
SCMS-1404	EE REQUIREMENT	EE send data via HTTP post over TCP/IP	EE shall use HTTP post to send data towards the RA	To allow the SCMS endpoint to serve everything based on HTTP protocol	RA - Services View will document the actual HTTP post details. This is out of scope as it defines EE behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1405	CLOSED	RA accept authenticated HTTP post requests	RA shall accept HTTP post requests only from authenticated EEs.	To allow the SCMS endpoint to serve everything based on HTTP protocol	RA - Services View will document the actual HTTP post details.	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-2463	EE REQUIREMENT	EE transactions per TLS session	EE shall perform as many SCMS transactions as possible using a single TLS session.	To minimize the number of separate TLS sessions to the SCMS. This will reduce the resources required and improve throughput.	This is out of scope as it defines EE behavior.	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)

Table 22 Use Case 5 - Requirements

22 issues

5.2.8.4 Design

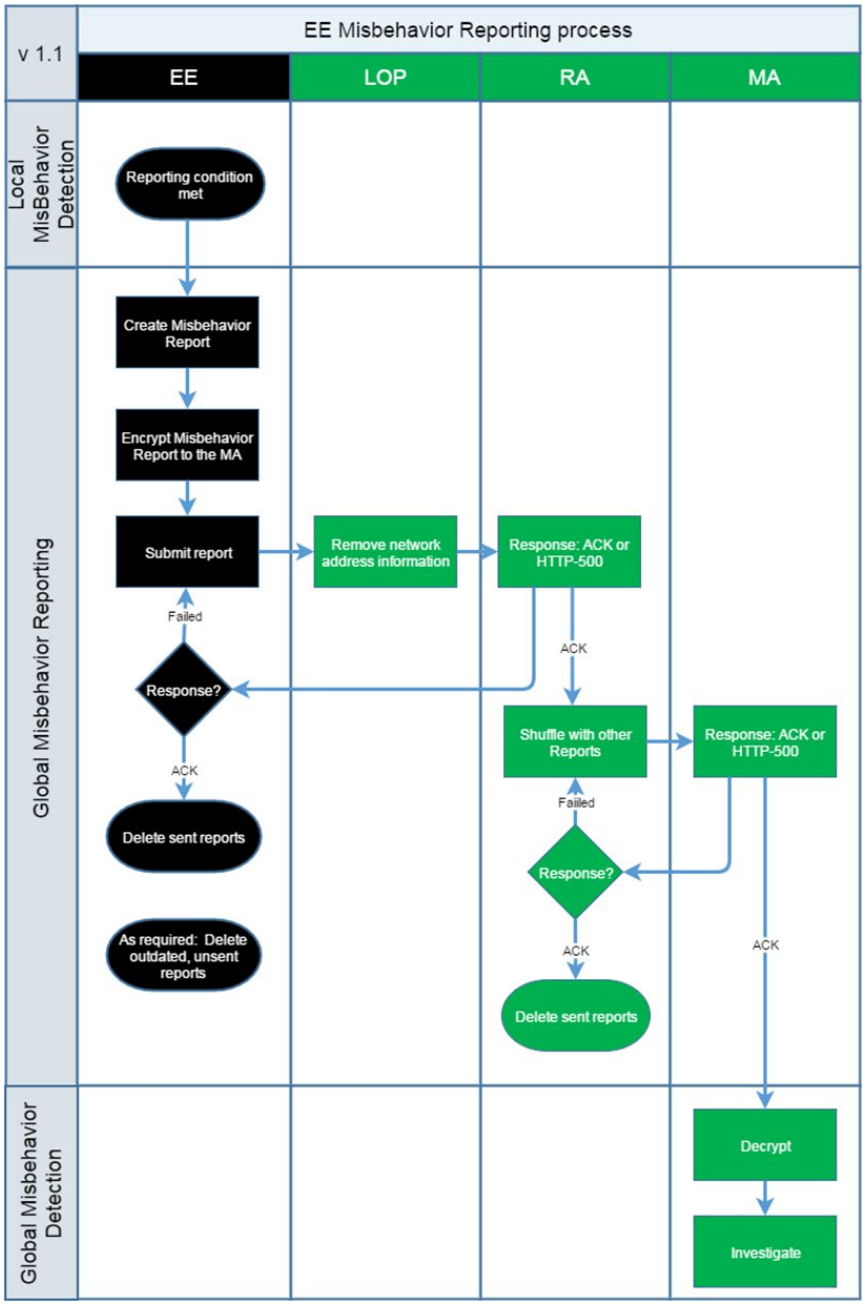


Figure 53 EE Misbehavior Reporting Process

The following steps are executed:

- Step 1: Reporting condition met
- Step 2: EE creates a misbehavior report and signs with a pseudonym certificate

- Step 3: EE encrypts report to the MA
- Step 4: EE submits it to the RA
    - Step 4.1: The LOP removes any identifiers from the encrypted misbehavior report (e.g., MAC address and IP address) and forwards the encrypted report to RA
    - Step 4.2: RA shuffles misbehavior reports and sends to MA individually. Shuffle threshold is 10,000 misbehavior reports or one day whichever is reached first. (Note: This shuffle threshold is for POC only, needs to be re-evaluated by SCMS manager for production)
- Step 5: Unsent misbehavior reports older than one week may be deleted by the EE if insufficient memory exists

5.2.8.5 ASN.1 Specification

ASN.1 interface specifications for misbehavior reports will be finalized with the to-be-awarded "Misbehavior Authority Integration" sub project. Until then the interface given is to be handled as draft.

- ee-ma.asn

5.2.9 Use Case 6: CRL Download

5.2.9.1 Goals

The goal is to provide the CRL file from the CRL Store (a component of the MA) to the EE when requested.

5.2.9.2 Background and Strategic Fit

The EE must be aware of revoked entities.

5.2.9.3 Assumptions

- One or more CRLs have been generated, signed by the CRL Generator, put into a CRL file, and has been made available to the CRL Store
- The CRL Store is able to validate cryptographically the signature on the CRL file prior to making it available for download
  The EE is able to download the CRL by issuing a CRL HTTP get request to the CRL Store.
- The CRL Store will not authenticate the EE, i.e., CRL Store will not require that EE sends its enrollment certificate for authentication purposes
- OBE has successfully executed Use Case 2: OBE Bootstrapping (Manual)

5.2.9.4 Process Steps

1. OBE downloads the CRL using the API documented in MA - Download CRL

5.2.9.5 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-335</td><td>EE REQUIREMENT</td><td>EE issues a CRL Request</td><td>An EE shall issue a HTTP get to the CRL Store to obtain the latest CRL.</td><td>EE needs to be provided with current CRL so that the EE can be informed of revoked components.</td><td>This is out of scope since it defines EE's behavior.</td><td>On-board Equipment (OBE), Road-side Equipment (RSE)</td></tr>
<tr><td>SCMS-340</td><td>CLOSED</td><td>CRL availability</td><td>The CRL Store shall provide a CRL for download at any given time.</td><td>To ensure that an EE can always download a CRL.</td><td></td><td>CRL Store</td></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></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>
</table>

Key	Status	Summary	Description	Justification	Notes	Component/s
			0xC0, 0x2B TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 RFC5289 0xC0, 0x2C TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 RFC5289 0xC0, 0xAC TLS_ECDHE_ECDSA_WITH_AES_128_CCM RFC7251 0xC0, 0xAD TLS_ECDHE_ECDSA_WITH_AES_256_CCM RFC7251			
SCMS-342	EE REQUIREMENT	CRL Store Authentication	The EE shall authenticate the CRL Store through usual SSL/TLS means.	This will provide a level of trust for the CRL Store. An impostor CRL Store might distribute only old CRLs (which would be valid).	The CRL Store does not authenticate EE before download of the CRL starts, i.e., EE does not authenticate by using its enrollment	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
					certificate to CRL Store but EE can download the CRL without authentication to CRL Store. This is out of scope as it defines EE behavior.	
SCMS-786	CLOSED	CRL download	CRLG shall provide CRL via CRL store.	so that EEs can check revocation status	CRL entries may be dependent on the type of certificate	CRLG
SCMS-991	EE REQUIREMENT	Error code: eeCRLStoreAuthenticationFailed	EE shall log "Error code: eeCRLStoreAuthenticationFailed", if it cannot authenticate the CRL Store.	EE cannot authenticate the CRL Store.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-994	EE REQUIREMENT	Error code: eeCRLDownloadFailed	EE shall log "Error code: eeCRLDownloadFailed", if EE is not able to download the CRL file.	EE cannot download CRL file.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-995	EE REQUIREMENT	Error code: eeCRLVerificationFailed	EE shall log "Error code: eeCRLVerificationFailed", if verification of the CRL signature fails.	In order to enable client side error handling.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1263	EE REQUIREMENT	EE download resume	EE shall try byte-wise resume of CRL downloads from the CRL store,	This will improve reliability of the download process		On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
			certificate batches, certificate files, or policy files from RA in case a previous download failed.	and reduce communication cost.		
SCMS-1264	CLOSED	CRL Store download resume	CRL Store shall support byte-wise resume of CRLs by EE.	This will improve reliability of the download process and reduce communication cost.		CRL Store
SCMS-1270	EE REQUIREMENT	Network connection	EEs shall use TCP/IP to communicate with the SCMS.	SCMS components (server) are only reachable by standard TCP/IP networking methods.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-2523	EE REQUIREMENT	EE TLS version	The EE shall at minimum support TLS version 1.2 as defined in RFC5246 for all communications to SCMS components.	To avoid known security issues in older versions of the protocol.	This is out of scope as it defines EE behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

Table 23 Use Case 6 - Requirements

12 issues

5.2.9.6 ASN.1 Specification

IEEE 1609.2 specifies CRLs in: https://github.com/wwhyte-si/1609dot2-asn/blob/master/crl-protocol.asn

5.2.10 Use Case 8: OBE Pseudonym Certificate Revocation

> OBE Revocation will be integrated with the ongoing "Misbehavior Authority Integration" sub project as SCMS PoC release 2.0. Until then every reported pseudonym certificate leads automatically to a revocation of all pseudonym certificates belonging to this OBE for testing purposes.

5.2.10.1 Goals

Perform misbehavior investigation and eventually revocation of OBEs.

5.2.10.2 Step 8.4: OBE CRL Check

5.2.10.2.1 Goals

The OBE needs to perform several computational steps to check whether a received Basic Safety Message (BSM) has been sent by a revoked EE. This document lists the corresponding requirements.

5.2.10.2.2 Assumptions

The OBE received a CRL as defined in Use Case 6: CRL Download.

5.2.10.2.3 Process Steps

1. The OBE expands the CRL and calculates the linkage values for the current i-period based on the CRL entries (linkage seeds) of the CRL pseudonym certificate section
2. Whenever the OBE receives a new, unknown pseudonym certificate, it checks whether the linkage value of that unknown certificate is listed in the OBE's expanded CRL (from Step 1)
    a. If yes, then the OBE discards the received certificate
    b. Otherwise, the OBE accepts the received certificate as verified
3. Whenever the OBE receives a new, unknown OBE identification certificate, the OBE will calculate the certificate digest of that unknown certificate and will check whether the CRL lists it
    a. If yes, then the OBE discards the received certificate

b. Otherwise, the OBE accepts the received certificate as verified

4. Before the end of each i-period, the OBE will:
    a. Update its expanded CRL and calculate the linkage value for the next i-period
    b. Remove entries from the expanded CRL that belong to revoked devices that ran out of certificates, if a CRL entry indicated that the revoked device does not have any more valid certificates. Note that the OBE may not immediately remove such entries, but add a safety buffer.
5. If the OBE recognizes itself on the CRL, the OBE will stop sending over-the-air DSRC messages related to the indicated PSID/SSP. This also applies if the OBE recognizes that the Enrollment CA that issued the OBE's enrollment certificate, the Pseudonym CA that issued the OBE's certificates, any Intermediate CA that is in the chain between its ECA or PCA up to the Root CA, or the Root CA itself has been revoked.

5.2.10.2.4 Requirements

Table 24 Use Case 8.4 - Requirements

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-786	Closed	CRL download	CRLG shall provide CRL via CRL store.	so that EEs can check revocation status	CRL entries may be dependent on the type of certificate	CRLG
SCMS-1217	EE requirement	OBE compares linkage values	OBE shall compare the linkage value in each received sender certificate against the list of revoked linkage values.	OBE receives BSMs with attached certificate and validates whether the certificate belongs to a revoked OBE by checking the linkage value of the pseudonym certificate against the revoked linkage value list.	This is out of scope since it defines OBE's behavior.	On-board Equipment (OBE)
SCMS-1219	EE requirement	OBE updates linkage value list	OBE shall update the list of revoked linkage values for each i-period. OBE shall either update the	OBE is able to update the linkage values for each i-period. It is left to the OEM/supplier, when the values are updated.	Linkage values are updated by hashing the linkage seed value (which is	On-board Equipment (OBE)

Key	Status	Summary	Description	Justification	Notes	Component/s
			linkage value or remove the linkage value.	The updated values are needed when a new i-period starts.	a CRL entry, a hash or a repeated hash of the CRL entry) and then recalculating the linkage value. This is out of scope since it defines OBE's behavior.	
SCMS-1220	EE requirement	OBE removes linkage values from its list	OBE shall remove linkage values from its list if a CRL entry indicated that the misbehaving OBE did not have any more valid pseudonym certificates for more than one i-period.	OBE can remove linkage values from its internal list once the misbehaving OBE does not have access to valid pseudonym certificates. That time is described on the CRL. We include one i-period of buffer.	This is out of scope since it defines OBE's behavior.	On-board Equipment (OBE)
SCMS-1221	EE requirement	EE processes CRL	EE shall process the updated CRL/CRL chunk and update its CRL within 1 minute	CRLs/CRL chunks are updated daily and EE must always update its	This is out of scope since it	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
			after receiving the update CRL or CRL chunk.	stored CRL in a timely fashion.	defines EE's behavior.	
SCMS-1222	EE requirement	Removed CRL entry	EE shall apply a missing CRL entry (from a previous CRL) for at least one more week, in case that an updated CRL misses this CRL entry.	This avoids a faulty CRL, e.g., due to a CRL generator misbehavior or mistake. This also conforms with requirement https://jira.campllc.org/browse/SCMS-1220~~SCMS-1220~~.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1223	EE requirement	EE checks against CRL for all certificate types	EEs shall check all received relevant sender certificates, i.e., certificates of received messages that are processed, against the most recent CRL. If the sender certificate is listed, EE shall discard the received message.	EEs also check all relevant certificates, i.e., certificates of received messages that are processed, against the CRL. This includes OBE pseudonym, OBE identification, and RSE application certificates. It is up to EE whether it checks non-relevant certificates, i.e. certificates or received	These checks are specified in IEEE 1609.2. Clause 5.1.3.4 describes how an EE checks whether a pseudonym certificate has been revoked by calculating the linkage values from the	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
			EE shall perform this check using the mechanism described in IEEE 1609.2-2016.	messages that are not processed, against the CRL.	linkage seeds listed in the CRL, and comparing the calculated linkage value against the linkage value in the inspected certificate. Clause 6.4.10 and 6.4.11 contain additional information about linkage values. Clause 5.1.3.5 describes how an EE checks whether an OBE identification and RSE application certificate has	

Key	Status	Summary	Description	Justification	Notes	Component/s
					been revoked by calculating the hash value of the inspected certificate, and comparing it against a CRL entry. Clause 7 contains comprehensive information about CRLs. This is out of scope since it defines EE's behavior.	
SCMS-1224	EE requirement	EE stops sending	EE shall stop sending over-the-air DSRC messages, if it detects that itself has been listed on the CRL. This is limited to the certificates of the	If certificates of a particular PSID/SSP have been revoked, EE stops sending all messages related to that PSID/SSP. EE might still receive DSRC messages, and	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
			PSID/SSP that was revoked.	send messages related to other non-revoked PSID/SSPs.		
SCMS-1285	EE requirement	EE stops sending: revoked ECA for EE's enrollment certificate	EE shall stop sending over-the-air messages, if it detects (via CRL) that its ECA, any ICA between its ECA and the root CA, or the root CA has been revoked.	In this case, EE's enrollment certificate also has been revoked.	This is out of scope since it defines EE behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1286	EE requirement	EE stops sending: revoked PCA for EE's certificates	EE shall stop using all pseudonym/identification/application certificates issued by a certain PCA, if EE detects (via CRL) that this PCA, any ICA between PCA and root CA, or root CA has been revoked.	If the PCA was revoked, all pseudonym/identification/application certificates are also revoked.	This is out of scope since it defines EE behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

No issues found

5.2.11 Use Case 11: Backend Management

5.2.11.1 Goals

- The goal of backend management is the addition and removal of SCMS components
- The provisioning and initial setup requirements for all backend components is defined in Use Case 1: SCMS Component Setup

5.2.11.2 Background and Strategic Fit

As the SCMS system evolves, it is necessary that SCMS components can be added and removed.

This includes Root CAs. For the PoC, there will be only one Root CA. To manage Roots CAs, (e.g., to add and remove them) the SCMS will employ a multi-Elector system. In this scheme, there are a number of electors. These entities are trust anchors but also vote to manage Root CAs, i.e., to remove or add a new Root CA. The SCMS Manager coordinates the electors. An operation on a Root CA (addition or revocation) will require a message signed by some given number of electors. The exact number of electors needed to perform addition or revocation is a fixed quorum *m*. The public keys of the electors will be installed into the trust stores of every SCMS component, including the OBEs. In the PoC, electors will be implemented to be manual processes, and the Root Management messages signed by electors will be generated by manual means for testing the management of the Roots CAs.

5.2.11.3 Assumptions

- SCMS components need to be added and revoked but not removed and rolled-over
- More requirements specific to each operation and component will occur in the subsections

-

5.2.11.4 Requirements

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-406	CLOSED	TLS Cipher Suite	All TLS communication between SCMS components shall employ a cipher suite that uses cryptographic mechanisms and key lengths that are at least as strong as the following cipher suite for each individual cryptographic mechanism of the suite: TLS_ECDHE_ECDSA_WITH_AES_128_CCM (as defined in RFC7251)	Forward security, ECC with defined security level as minimum, or better.	Refer to NIST recommendations to evaluate whether a selected cryptographic mechanism is stronger than the defined minimum security level. A proper starting point is "NIST, Recommendation for Key Management, Special Publication 800-57 Part 1 Rev. 3, 07/2012."	CRL Store, CRLG, DCM, ECA, IBLM, LA, MA, PCA, PG, RA
SCMS-407	IMPLEMENTED	TLS Mutual Authentication	Communication transactions between SCMS components shall be client-server mutually authenticated and encrypted with TLS (except EE-RA).	Authentication between servers with mutual TLS is an additional security layer.	For POC, TLS shall be used for inter component communication with mutual authentication, and an OCSP service at the technical component of the SCMS manager shall be deployed for	CRL Store, CRLG, DCM, ECA, IBLM, LA, MA, PCA, PG, RA

Key	Status	Summary	Description	Justification	Notes	Component/s
					revocation. Seehttps://jira.campllc.org/browse/SCMS-406~~SCMS-406~~ for information about the cipher suite, SCMS-1016 for information about OCSP, andhttps://jira.campllc.org/browse/SCMS-938~~SCMS-938~~ for TLS certificate management.	
SCMS-1017	SCMS POC OUT OF SCOPE	Robustness against catastrophic failure of the components	SCMS components shall be robust against catastrophic failure.	The SCMS must be robust enough to handle trials, and to build the basis of the robustness of the eventual production system.	For PoC only minimal robustness is required. This requirement is for the production system.	
SCMS-1018	SCMS POC OUT OF SCOPE	Data encryption in geographically diverse locations	Databases should be encrypted and authenticated before sent to geographically diverse locations.	so that no unauthorized entity can gain access to the data.	For PoC only minimal robustness is required. This requirement is for the production system.	
SCMS-1019	SCMS POC OUT OF SCOPE	HSM replication	HSMs holding private keys shall be replicated and stored securely, to be able to recover encrypted and	so that backups can be used for recovery when necessary.	For PoC only minimal robustness is required. This requirement is for the production system.	

Key	Status	Summary	Description	Justification	Notes	Component/s
			authenticated backups, as well as any operational secrets.			
SCMS-1020	SCMS POC OUT OF SCOPE	Replicated HSM storage	Replicated HSMs shall be stored securely, with protections at least at the same level as are provided to the production system.	to avoid security breaches via replicated HSMs.	For PoC only minimal robustness is required. This requirement is for the production system.	
SCMS-1021	SCMS POC OUT OF SCOPE	Hot standby	Hot standbys in geographically diverse locations shall be provisioned, and cold standbys similarly created to be able to accept replicated HSMs and reconstruct production materials from backup.	so that a failing SCMS component can be replaced immediately and without operational interruption of the overall system.	For PoC only minimal robustness is required. This requirement is for the production system.	
SCMS-1022	SCMS POC OUT OF SCOPE	Redundancy	The system hardware components, such as servers, switches, UPSs, etc. shall be deployed redundantly	so that failure of a single such component does not take the system offline; even more redundancy can be considered where multiple such components can fail and the system remains operational.	For PoC only minimal robustness is required. This requirement is for the production system. PoC system will have some sort of redundancy - compare the PoC hardware design.	
SCMS-1023	CLOSED	Root CA Trust Store	The SCMS Component shall be provisioned with the self-signed SCMS certificates of the Root CAs.	Every SCMS component will need to manage Root CA update automatically. To authenticate the Root		CRL Store, CRLG, DCM, ECA, IBLM, ICA, LA, MA, PCA, PG, RA

Key	Status	Summary	Description	Justification	Notes	Component/s
				CA management messages, the Root CA must be trusted, and therefore require that their Certificates be in the SCMS component trust stores.		
SCMS-1314	MANUAL PROCESS	SCMS component certificate types (implicit vs. explicit)	The SCMS component shall have a certificate of explicit type.	Implicit: OBE Enrollment, RSE Enrollment, Pseudonym, Application, Identification Explicit (Self Signed): RootCA, Elector Explicit: Everything else PCA, ICA, Root CA, and elector certificates need to be of explicit type in order to support P2P distribution. All the EE certificates are of implicit type to save storage space and over-the-air bytes, and all the SCMS Component certificates are of explicit type.	Details discussed in certificate types	CRL Store, CRLG, DCM, IBLM, ICA, LA, PCA, PG, RA, RCA

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-1315	MANUAL PROCESS	Only 1 certificate valid at a time	Each SCMS component shall have only 1 valid and in-use certificate at a time.	There are no privacy concerns for SCMS components that would justify more than one certificate valid at a given time. At the same time, it is desirable to keep complexity low and have maximum control over components, hence allowing exactly one certificate at a given time.		CRL Store, CRLG, DCM, ECA, IBLM, ICA, LA, PCA, PG, RA
SCMS-1316	SCMS POC OUT OF SCOPE	Additional SCMS component certificate for the next time period	Each SCMS component shall be allowed to request and receive a certificate that is valid for the next time period at a time defined by the certificate policy given by the SCMS Manager.	To allow continuity of secure communication between SCMS components.	The additional certificate is likely requested by the SCMS component towards the end of the current time period.	CRL Store, CRLG, DCM, ECA, IBLM, ICA, LA, PCA, PG, RA
SCMS-2522	CLOSED	TLS version	All TLS communication shall use TLS version 1.2 as specified in RFC5246 or higher	to avoid known security issues in older versions of the protocol.		CRL Store, CRLG, DCM, ECA, IBLM, LA, MA, PCA, PG, RA

Table 25 Use Case 11 - Requirements

13 issues

5.2.11.5 Design

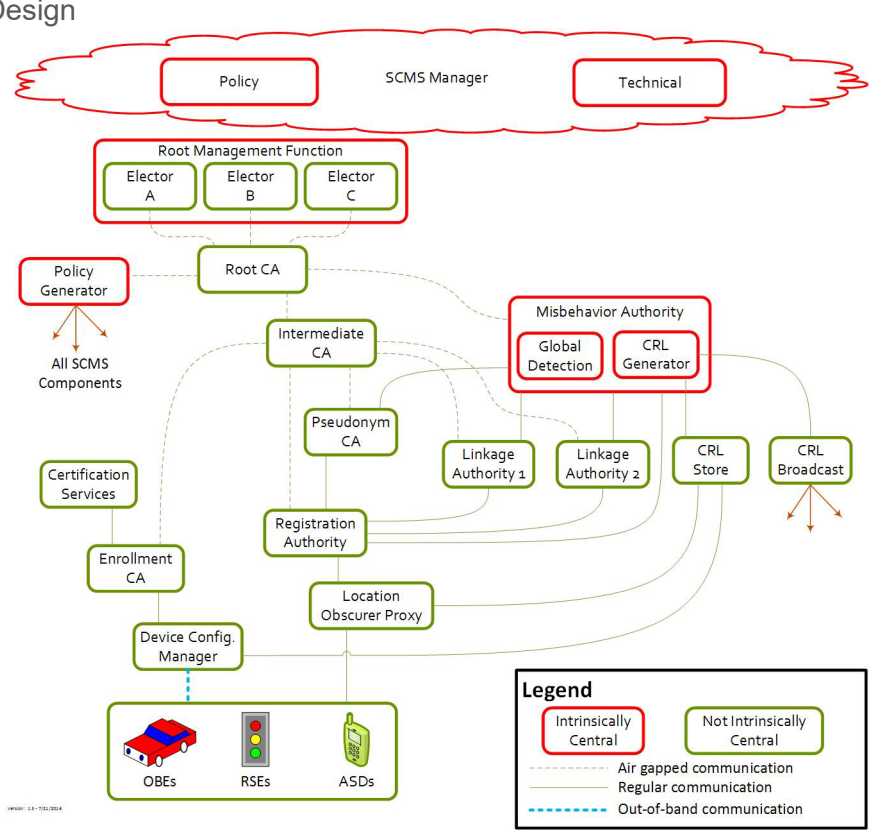


Figure 54 SCMS Architecture

5.2.11.6 Summary Showing Trust Anchor Relationships Only

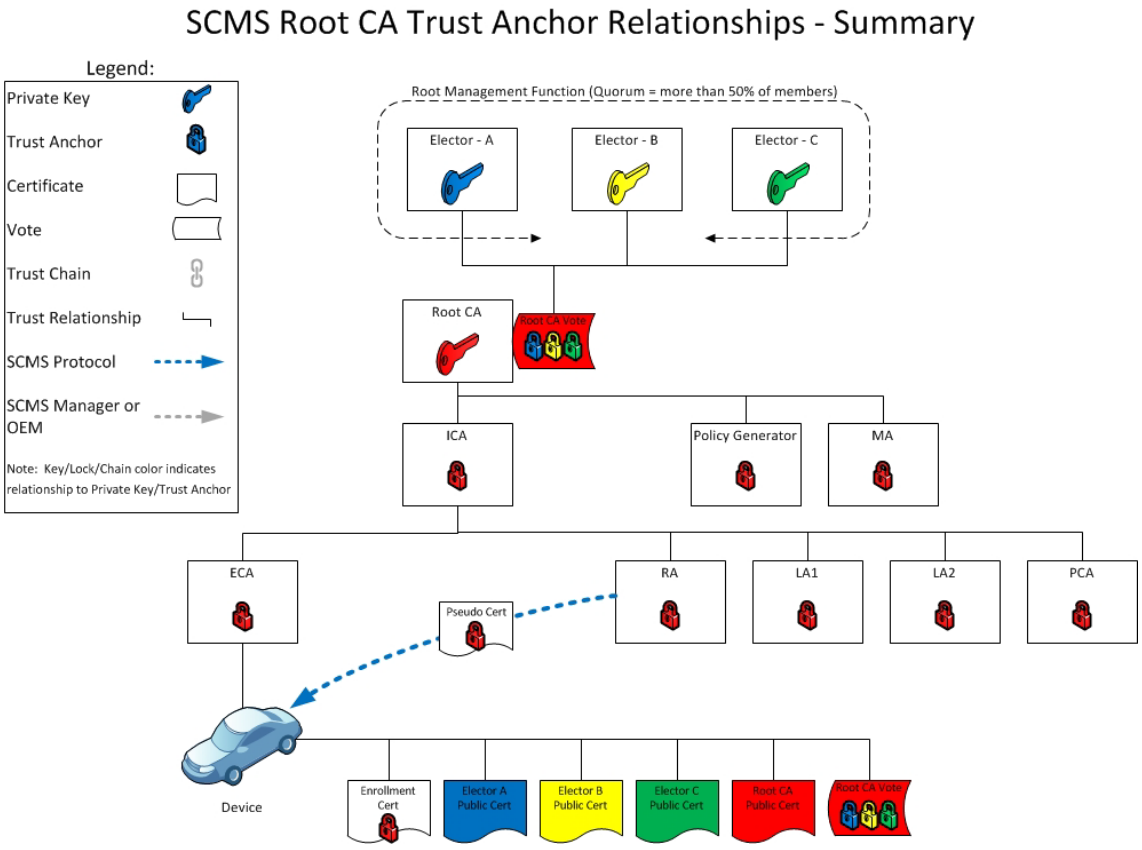


Figure 55 SCMS Root CA Trust Anchor Relationships - Overview

5.2.11.7 Typical SCMS Operations

5.2.11.7.1 Day 1: Typical SCMS System Operations

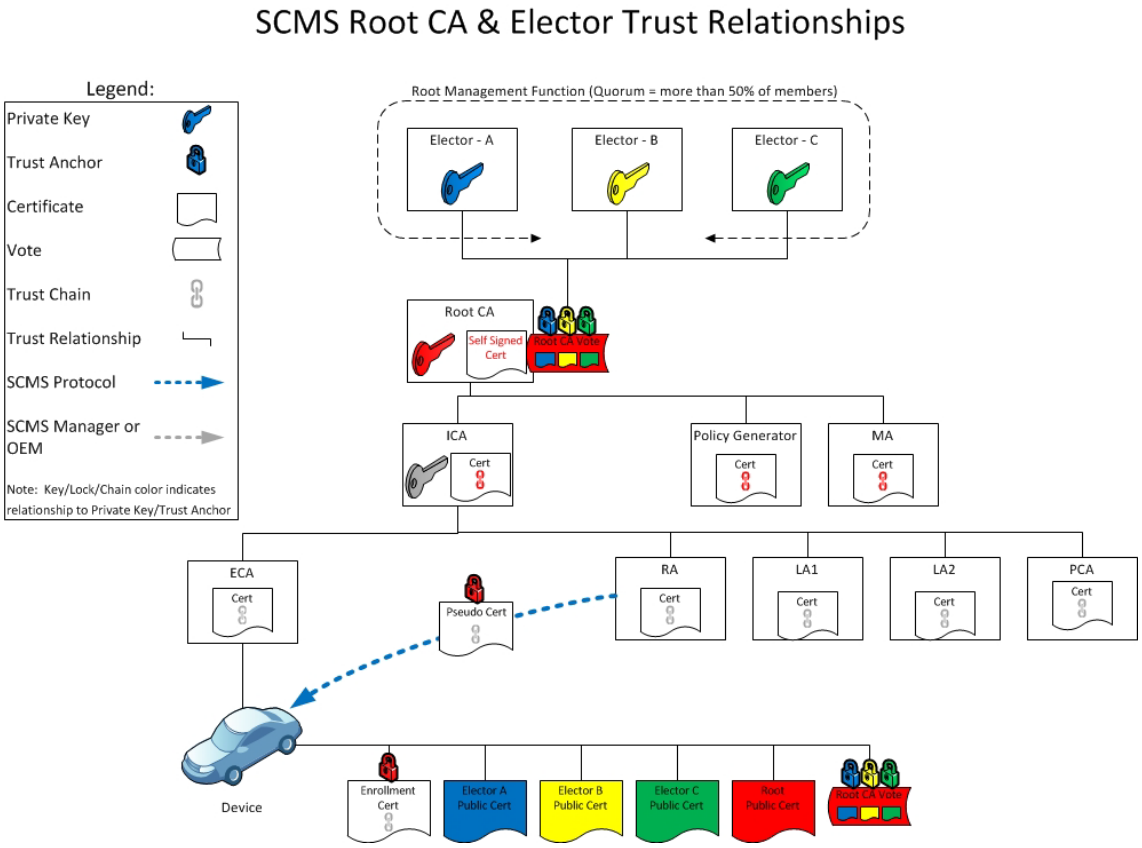


Figure 56 SCMS Root CA & Elector Trust Relationships

5.2.11.7.2 Scenario 1: Life Cycle of Elector (Level 0) Revocation and Replacement

Scenario 1, Day 2: Process to Revoke an Elector while Maintaining Functionality

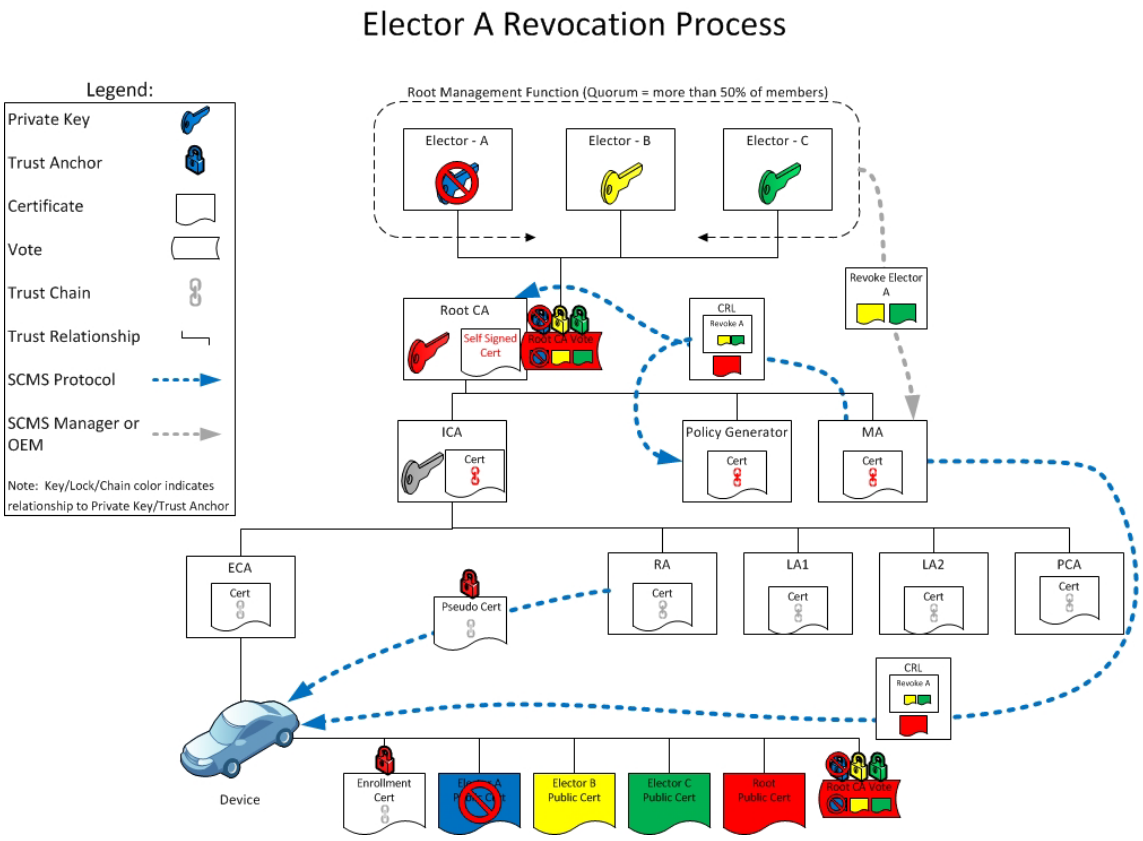


Figure 57 Elector A Revocation Process

Scenario 1, Day 3: System Functional for Period of Time with Two Root Endorsers

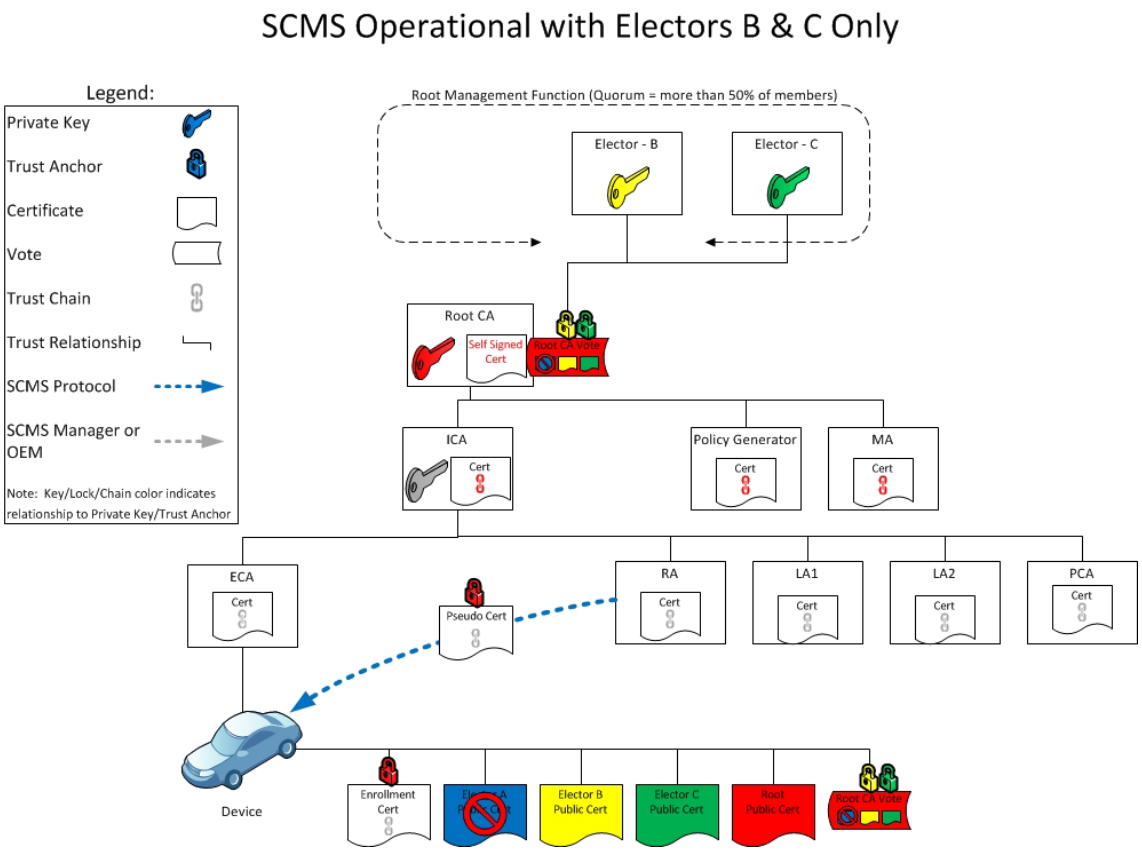


Figure 58 SCMS Operational with Electors B & C Only

Scenario 1, Day 4: Introduction of Replacement Elector

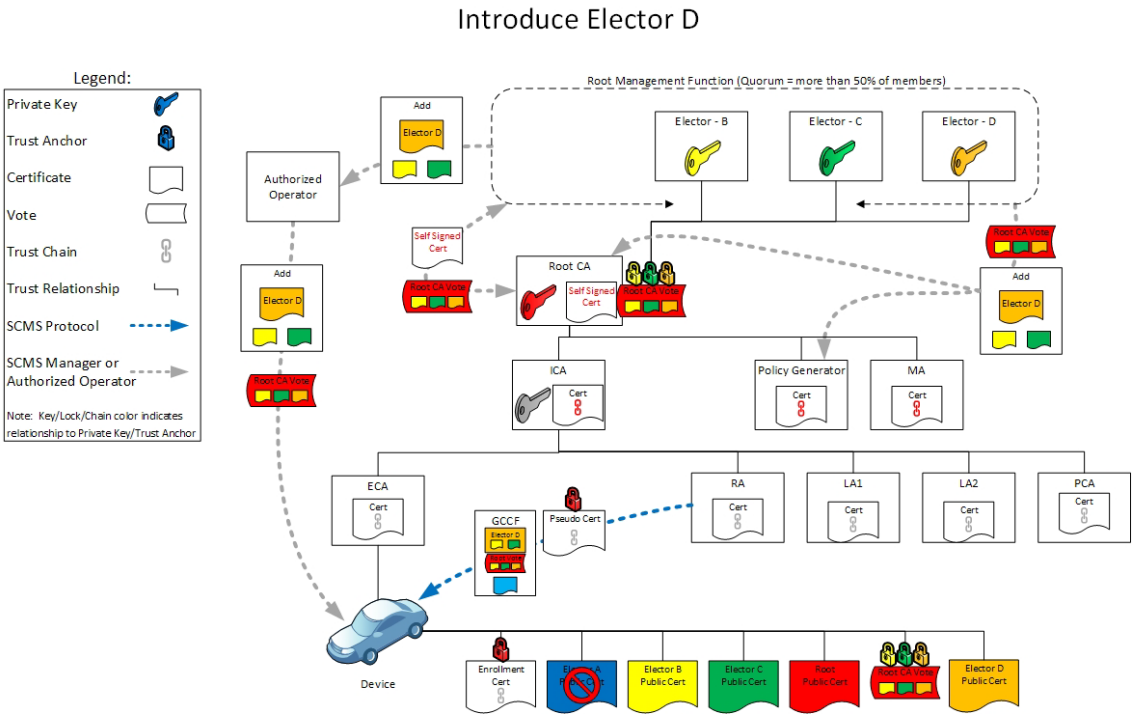


Figure 59 Introduce Elector D

Scenario 1, Day 5: Steady State Operations after the Introduction of Replacement Elector

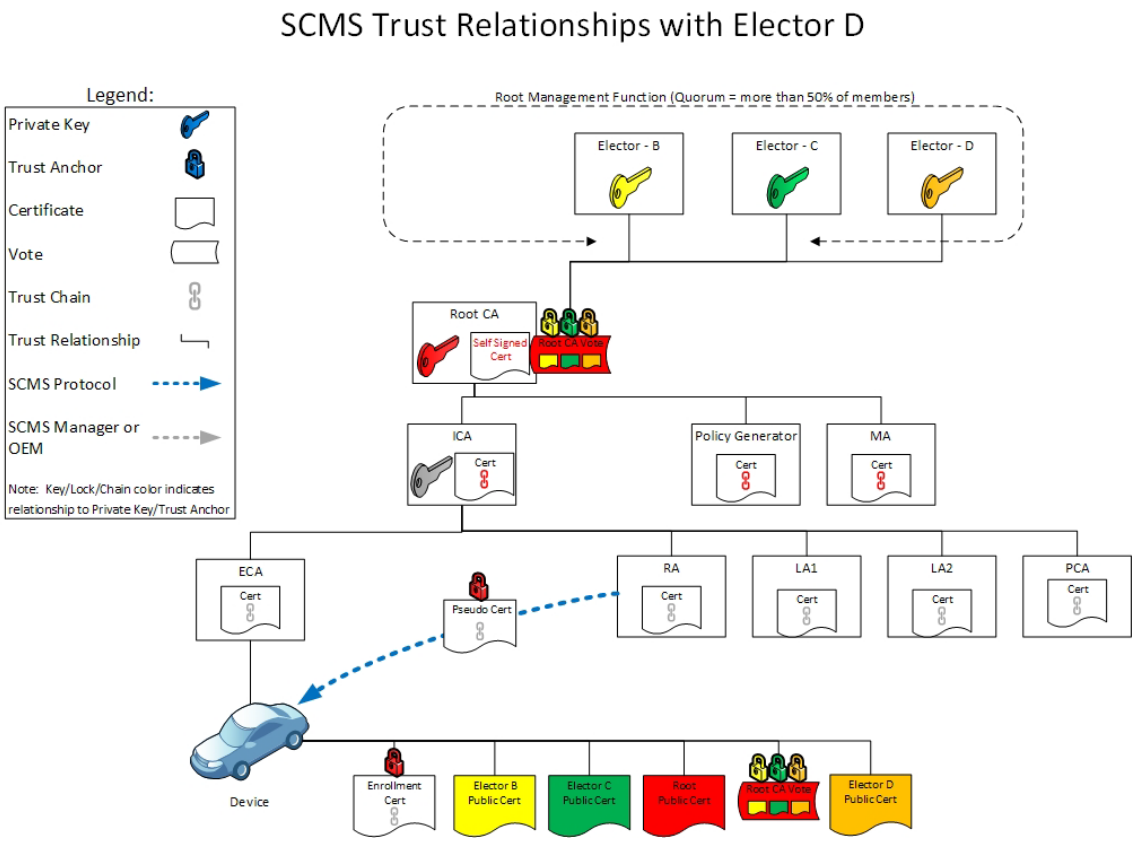


Figure 60 SCMS Trust Relationships with Elector D

5.2.11.7.3 Scenario 2: Life Cycle of Root CA (Level 1) Revocation and Replacement

Scenario 2, Day 2: Prepare New Root CA

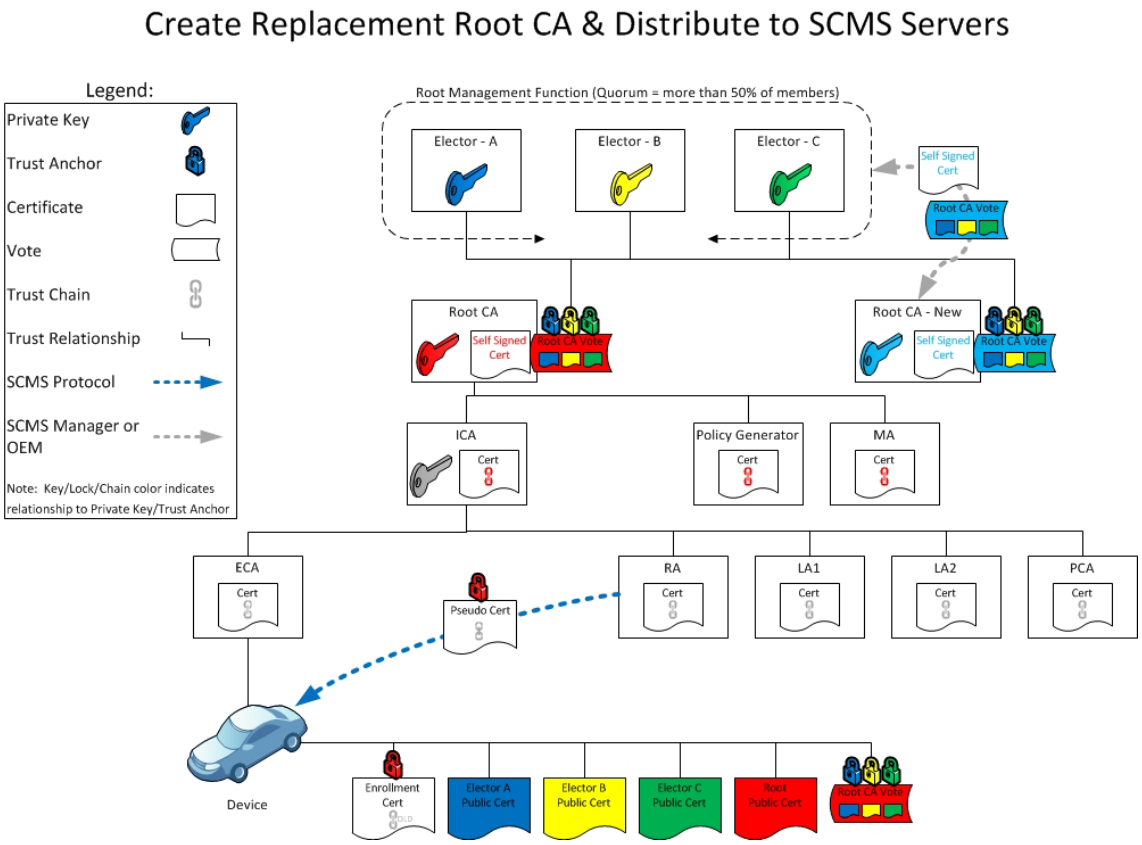


Figure 61 Create Replacement Root CA & Distribute to SCMS Servers

Scenario 2, Day 3: Generate New Certificates for all SCMS Components & Distribute

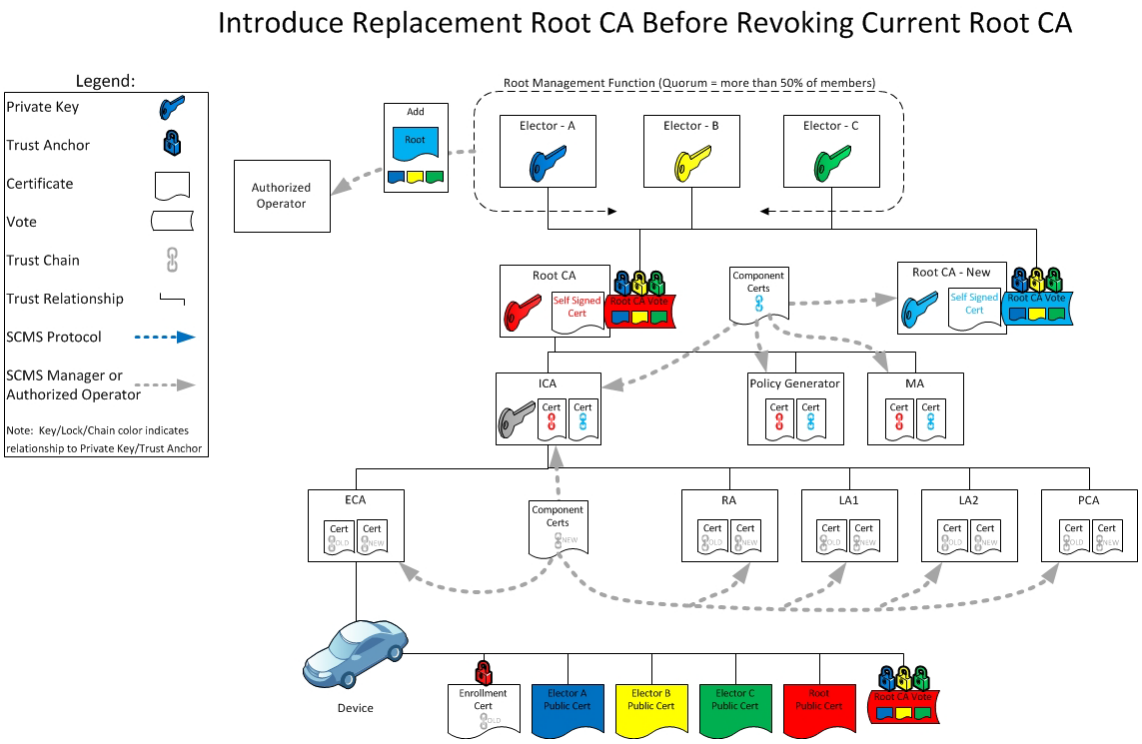


Figure 62 Introduce Replacement Root CA before Revoking Current Root CA

Scenario 2, Day 4: Revoke Root CA

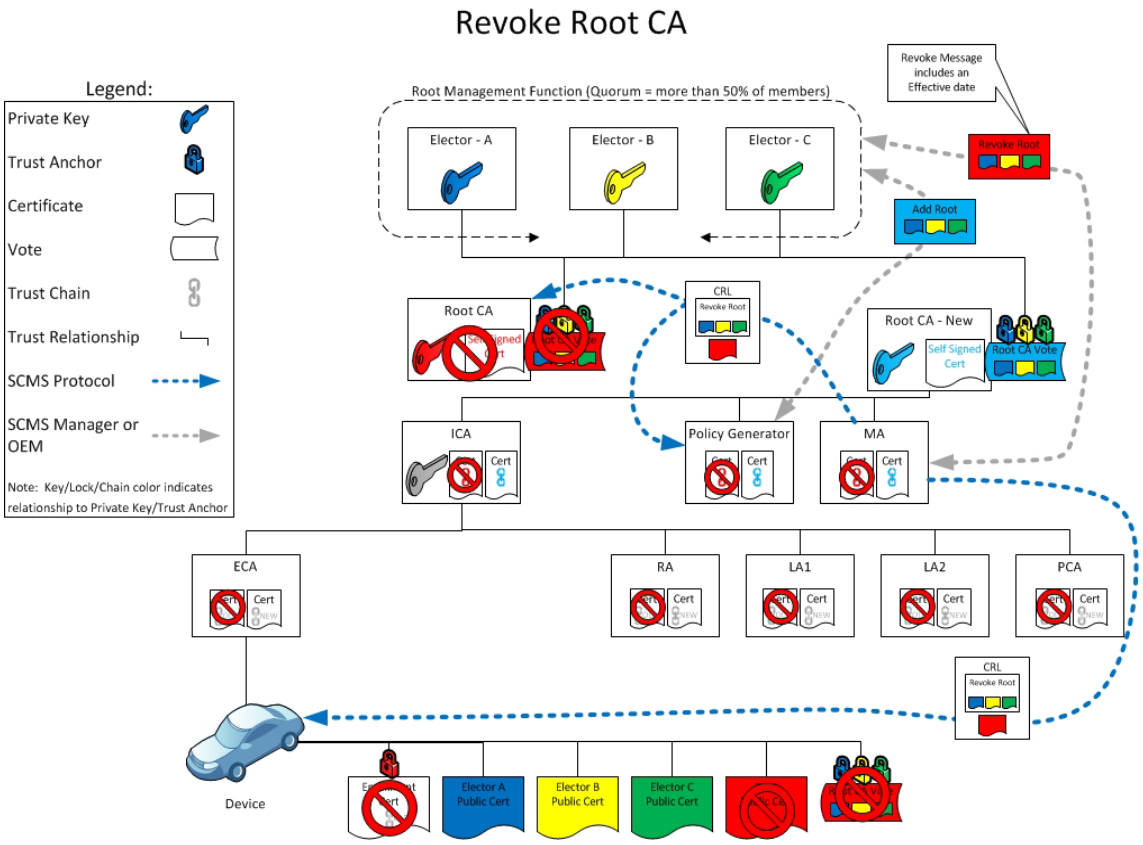


Figure 63 Revoke Root CA

Scenario 2, Day 5: Condition of SCMS while Root CA is Revoked

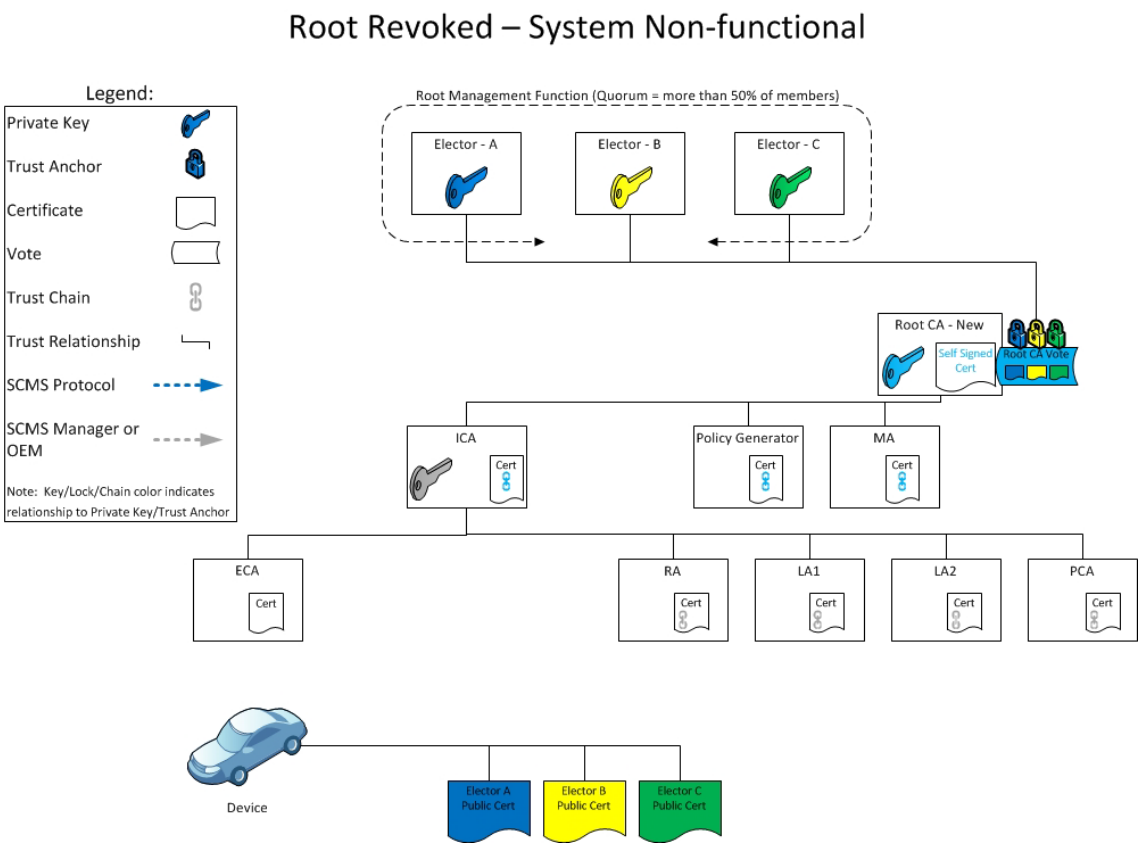


Figure 64 Root Revoked - System Non-functional

Scenario 2, Day 6: EEs Updated with New Root Certificate, New Enrollment Certificate and New Pseudonym Certificates

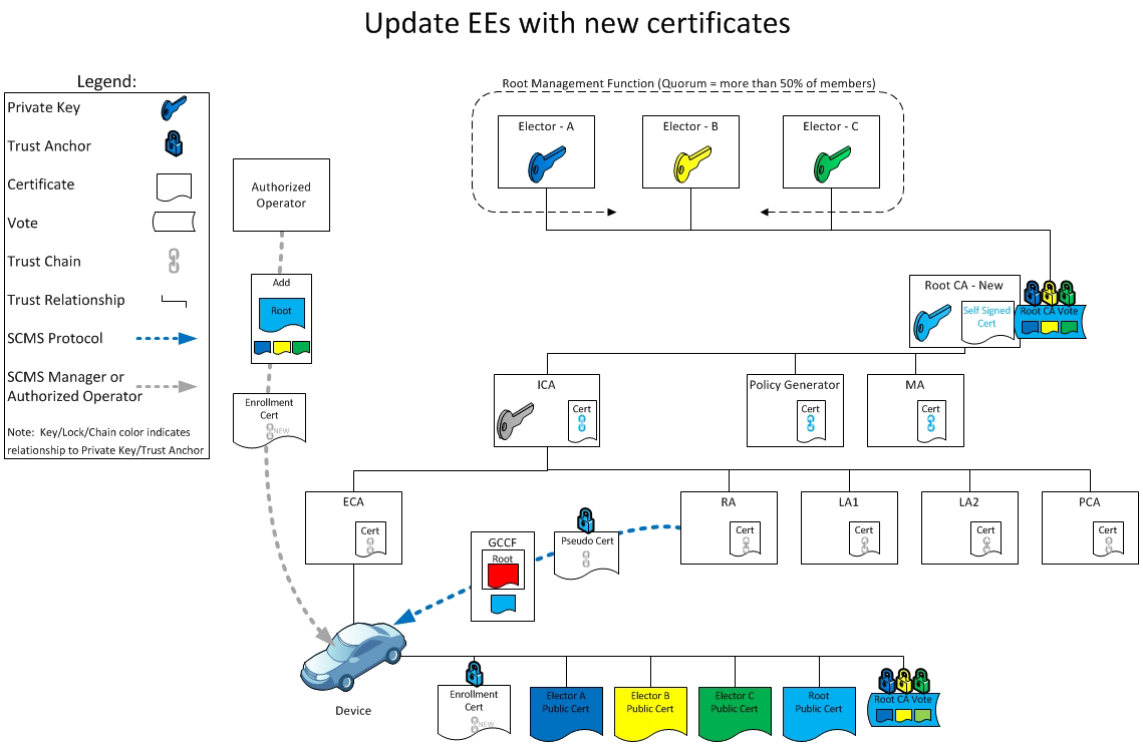


Figure 65 Update EEs with New Certificates

5.2.11.8 Step 11.1: Add SCMS Component

5.2.11.8.1 Goals

The goal of this use case with its collection of subsequent steps is to describe the procedures for adding backend SCMS components to the system. In all cases, before a component can be added it must first be setup correctly using the appropriate Component Setup use case.

5.2.11.8.2 Assumptions

- All components that will be added to the SCMS have already been configured using the appropriate Component Setup use case
- All components that will be added to the SCMS have been certified and approved through a process defined by the SCMS Manager
- The addition of any new SCMS component is coordinated and managed by an authorized agent of the SCMS Manage or local ICA Manager
- Many of the steps in the component add procedure are defined as "manual" and are not fully specified or defined in SCMS requirements. The details for these procedures will be defined by individual implementations. The goal of the SCMS requirements and these use cases are to preserve the security and integrity of the

SCMS system and ensure compatibility among individual SCMS components while granting significant latitude for diverse implementations.

5.2.11.8.3 Conditions

A new SCMS component may be added under five conditions. In many cases, these conditions require the same add procedure, but there are situations where the procedure is very different. The five conditions are defined here. Individual component use cases will describe the procedure for adding the new component or managing the transition to the component's parameters.

1. Net New
    a. This is the case where a net-new component is being added to the SCMS. This new component will be configured to receive and process messages from other components.
    b. New components are assumed to have internal storage that is prepared to store new data, but that is in a state that is initially cleared.
2. SCMS Certificate Retired and Re-Issued
    a. Most SCMS components have an SCMS certificate that has a useful life that is shorter than the expiration time for the certificate. At the end of this useful life, the old certificate is retired and an ICA or root CA will issue a new certificate.
    b. When a certificate is retired, previous signatures issued by that component may still be trusted, so normal operation may resume without the need to re-certify any sub-components.
3. Component Decommissioned and Replaced
    a. An SCMS component may be securely decommissioned and replaced. At a high level, this implies that the private key is securely destroyed or the physical device is put into secure storage. When this happens, the SCMS Manager or local ICA Manager may determine that the component's SCMS certificate does not need to be revoked.
    b. In this situation, a replacement component may share the same network address as the original component and it may be possible to transfer securely the internal storage of the original component to the new device. However, the replacement component will have a new SCMS certificate.
    c. Note that this condition is very similar to a retired SCMS certificate, but in this case, the component is being replaced with a new device and it may happen prior to the planned end of useful life for the original SMCS certificate.
4. SCMS Certificate Revoked, Component Replaced or Re-Certified
    a. When a component's certificate is revoked, it may be necessary to replace or re-certify the component.

b. In this situation, the replacement (or re-certified) component is assumed to have the same network address (but it will require a new TLS certificate) as the original component but it will have a new key pair, new SCMS certificate, and the component's internal memory will be cleared.

5. Certifying SCMS Certificate Revoked, Component Re-Certified
    a. When any higher level CA in the chain that issued a component's SCMS certificate is revoked, then the component' SCMS certificate shall also be treated as untrusted and implicitly revoked.
    b. When this happens, the SCMS Manager or local ICA Manager may determine that the impacted components can be re-certified and re-used.
    c. As in the case where the device itself is revoked, the component may retain the same network address (and possibly the same TLS certificate), but it will have a new SCMS certificate and the internal storage may be cleared.
    d. Note that this condition is very similar to the case where the SCMS certificate of the component is revoked and is treated as equivalent in most of the component add use cases.

5.2.11.8.4 Step 11.1.1: Add Non-Root SCMS Component

5.2.11.8.4.1 Goals

Provide a process for adding an SCMS component other than root CA, e.g., intermediate CA, PCA, RA, etc.

5.2.11.8.4.2 Assumptions

Use cases and more specific requirements are in the subsections under this heading.

5.2.11.8.4.3 Requirements

Table 26 Use Case 11.1.1 – Requirements

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-2842	REVIEW	Estimated project expiration	Certificates shall expire on or before 12:00:00 UTC January 3, 2025.	To ensure no certificates are valid beyond the defined project period.	Due to the 1609.2 sixtyHours unit of time, the actual certificate expiration may be up to 60 hours after the estimated project expiration of 00:00:00 UTC January 1, 2025. This is for CV-Pilot only.	CRLG, DCM, ICA, LA, MA, PG, RA
SCMS-1422	SCMS POC OUT OF SCOPE	Renewal of component certificate	A SCMS component shall request rollover IEEE 1609.2 certificates no sooner than 3 months prior to the end of the In-use life of the current certificate. A SCMS component shall not issue rollover IEEE 1609.2 certificates prior 3 months to the end of the In-use life of the current certificate.	To prevent the existence of certificates that are not valid until a significant time in the future.	Does not apply to component compromise/revoked situations. For the PoC & CV-Pilot, 3 months is being used. This should be re-evaluated for other deployments.	CRL Store, CRLG, DCM, ECA, ICA, LA, MA, PCA, PG, RA, RCA
SCMS-1386	MANUAL PROCESS	Add component's certificate to GCCF	The TCotSCMSM shall forward required information to the Policy Generator in order to add the certificate of the newly created SCMS component to the Global Certificate Chain File (GCCF).	For a newly added component to be a valid SCMS component, its certificate must chain back to the SCMS root CA and its chain must be available to any other component via GCCF.	In the PoC, this will occur by a manual process.	TCotSCMSM

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-1319	MANUAL PROCESS	Component certificate expiration	The component shall request a certificate with a validity of 3 years and 1 week.	Use 3 years for standard SCMS components	This is for POC & CV-Pilot only.	CRLG, DCM, LA, MA, PG, RA
SCMS-1035	SCMS POC OUT OF SCOPE	Error code: tcIssuedCertComponentPublishFailed	TCotSCMSM shall log "Error code: tcIssuedCertComponentPublishFailed", if the certificate issued to the new component could not be published to another SCMS component (e.g. DCM).	Issued certificate can not be published can be tracked		TCotSCMSM
SCMS-1032	SCMS POC OUT OF SCOPE	Error code: tcComponentUnreachable	TCotSCMSM shall log "Error code: tcComponentUnreachable", if testing the addressing info of the new component resulted in a failure.	Unreachable components can be tracked		TCotSCMSM
SCMS-1031	SCMS POC OUT OF SCOPE	Error code: tcComponentAddressingInfoInvalid	TCotSCMSM shall log "Error code: tcComponentAddressingInfoInvalid", if the addressing info required to locate the new component on the network supplied by the new component is invalid.	Invalid component address can be tracked		TCotSCMSM
SCMS-1027	SCMS POC OUT OF SCOPE	Error Code: authCAUnauthorizedAdd	A SCMS component shall log "Error Code: authCAUnauthorizedAdd", if the authorizing Root CA or ICA has refused to issue a certificate to the	So unauthorized add can be logged		

Key	Status	Summary	Description	Justification	Notes	Component/s
			new component due to it being unauthorized.			
SCMS-1026	MANUAL PROCESS	Error code: authCAAuthenticationFailed	A SCMS component shall log "Error code: authCAAuthenticationFailed", if the authorizing Root CA or ICA designated by the TCotSCMSM to the new component can not be authenticated.	Authentication failure error		CRL Store, CRLG, ECA, IBLM, ICA, LA, MA, PCA, PG, RA
SCMS-784	MANUAL PROCESS	TCotSCMSM inform ECA of DCMs	The local ICA Manager shall update the ECA when a DCM is added and provide the DCM's SCMS certificate and TLS certificate.	The ECA will need to authenticate with DCMs, and hence will need to be aware of their identity	In the PoC this will occur by a manual process.	TCotSCMSM
SCMS-774	CLOSED	Distribute the new component certificate	The TCotSCMSM shall forward signed certificates to the component that generated the corresponding CSR.	The result of the CSR is the new components identity in the system. This will be used to authenticate itself to other entities in the system.	After the authorizing root CA or ICA signs and returns a 1609.2 certificate to the TCotSCMSM, the new certificate must be delivered to the new component. In the PoC, this will occur by a manual process.	TCotSCMSM

11 issues

5.2.11.8.4.4 Step 11.1.1 - Add CRLG

5.2.11.8.4.4.1 Goals

The CRL Generator (CRLG) is an SCMS component that signs and publishes updated Certificate Revocation Lists (CRLs). In normal operation, the CRLG receives commands from the Misbehavior Authority (MA) or the TCotSCMSM to add revoked certificates to the current CRL. The CRLG adds revocation information of the certificates to the current CRL file, signs the new file, and publishes the new CRL. The CRLG does not directly receive messages from any other SCMS back-end components. The updated CRL is published to the CRL Store.

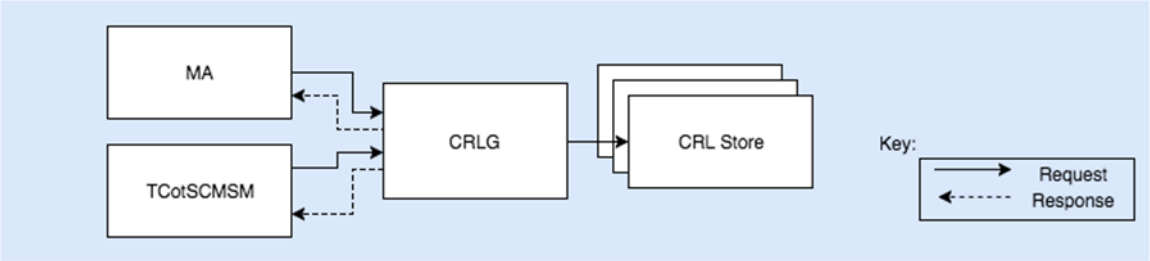


Figure 66 CRLG Messaging Diagram

The figure shows that the CRLG will receive messages from the MA and from the TCotSCMSM. It must also be able to publish a new CRL to one or more CRL Stores.

5.2.11.8.4.4.2 Process

To add a new CRLG to the SCMS, the TCotSCMSM must enable communication from the MA to the CRLG. It must also enable the CRLG to publish updated CRLs to one or more CRL Stores.

Specifically, the new CRLG must be configured with the following information:

1. The FQDN and TLS certificate of one or more CRL Store
2. The TLS certificate of the MA
3. Security credentials needed to authenticate the TCotSCMSM (this may be certificate based, user name and password, or secured through privileged access to the CRLG internal storage)

When a new CRLG is added, the MA must be updated with the following information:

1. The FQDN and TLS certificate of the CRLG

When a new CRLG is added, all CRL stores must be updated with the following information:

1. The TLS certificate of the CRLG

5.2.11.8.4.4.2.1 End State

After completing this use case, the CRLG will be configured with the following connection information:

Table 27 CRLG Values

CRLG Value	Notes
CRL Store FQDN and TLS certificate	The CRLG requires the network address of one (or more) CRL Store. For the PoC, there will be only one CRL Store.
MA TLS Certificate	The CRLG requires the MA's TLS certificate for authentication.

After completing this use case, the MA will be configured with the following connection information:

Table 28 MA Values

MA Value	Notes
CRLG FQDN and TLS certificate	The MA requires the network address of one CRLG. For the PoC, there will only be one active CRLG.

After completing this use case, the CRL store will be configured with the following connection information:

Table 29 CRL Store Values

CRL Store Value	Notes
CRLG TLS certificate	CRL store requires the TLS certificate of one or more CRLG. For the PoC, there will only be one active CRLG.

5.2.11.8.4.4.2.2 Special Cases

The procedure described above shall be used when configuring a new CRLG. The following details define how to deal with special cases of replacing a previous CRLG component.

- If the CRLG's SCMS certificate has retired and a new certificate is issued, there is no need for a special procedure to add the new certificate. It will be learned by all SCMS components when they load the latest CRL and validate the CRLG signature. The CRLG can continue to use the same network address and TLS certificate as before.
- If the CRLG has decommissioned and replaced, it will be necessary to update the internal memory of the replacement component with the last known state of the CRL. This may be done through secure transfer to the new component or by loading and validating the last published CRL. No other configuration changes are needed (provided that the replacement component has the same network address and TLS certificate as the prior CRLG).

- If the CRLG's SCMS certificate has been revoked, or if the root CA's certificate has been revoked, then the SCMS Manager will have to perform an investigation to validate the contents of the latest CRL state prior to re-certifying a replacement CRLG. Note that once a CRL is published, none of the contents can be removed from the list, even if they were added incorrectly (i.e., you cannot un-revoke a component even if you realize that the component was never compromised).

5.2.11.8.4.4.3 Assumptions

- The CRLG has been set up as described in the Setup CRL Generator use case
- The root CA issues the CRLG's SCMS certificate
- SCMS components and EEs can learn and validate the SCMS certificate when they download the latest CRL. There is no need to distribute the CRLG certificate to all components.
- The CRLG periodically publishes updated CRLs to the CRL Store
- The TCotSCMSM can trigger an immediate CRL update if necessary
- The CRLG will provide an interface to allow the addition or removal of CRL Stores from the list of sites that receive new CRL updates. This interface will require that there is always at least one active CRL Store. The mechanism for adding and removing CRL Store addresses in the CRLG is implementation specific and is not defined here.
- For the PoC there will be only one CRLG in the SCMS
- The CRLG will need to incorporate root and elector revocation commands on the CRL. These commands will be assembled by the TCotSCMSM and delivered to the CRLG through the communications mechanism established in this use case.

5.2.11.8.4.4.4 Requirements

Table 30 Step 11.1.1 Add CRLG - Requirements

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-774	CLOSED	Distribute the new component certificate	The TCotSCMSM shall forward signed certificates to the component that generated the corresponding CSR.	The result of the CSR is the new components identity in the system. This will be used to authenticate itself to other entities in the system.	After the authorizing root CA or ICA signs and returns a 1609.2 certificate to the TCotSCMSM, the new certificate must be delivered to the new component. In the PoC, this will occur by a manual process.	TCotSCMSM
SCMS-1412	MANUAL PROCESS	Destroy certificate's private key	The certificate's private key shall be destroyed at the end of the "In-use" life of a certificate. The in-use lifetime of certificates shall be defined either by SCMS policy and/or based on the expiration and In-use lifetime of subordinate certificates.	To prevent the usage of certificates that have reached the end of defined In-use lifetime.	Out of scope as this needs to be implemented as operational policy.	CRL Store, CRLG, DCM, ECA, ICA, LA, MA, PCA, PG, RA
SCMS-1581	SCMS POC OUT OF SCOPE	Component certificate in-use period	The SCMS component shall use its certificate for an in-use period of 3 years.	Use 3 years for standard SCMS components	Out of scope as this needs to be implemented as operational policy. This is for POC & CV-Pilot only.	CRLG, DCM, LA, MA, PG, RA

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-1725	MANUAL PROCESS	Component certificate FQDN match	The SCMS component shall have a certificate with a certificateId field that matches the FQDN of the component.	FQDN of each component must match the official ID of the component.		CRLG, DCM, ECA, LA, MA, PCA, PG, RA

4 issues

5.2.11.8.4.5 Step 11.1.1 - Add ECA

5.2.11.8.4.5.1 Goals

The Enrollment Certificate Authority (ECA) is an SCMS backend component that signs enrollment certificates for End Entity (EE) devices. In normal operation, the ECA receives and responds to requests from one or more Device Configuration Managers (DCMs). The addition of an ECA to the SCMS requires that the ECA is informed of the DCMs that will be sending requests and that the network is set up to enable those requests to reach the ECA.

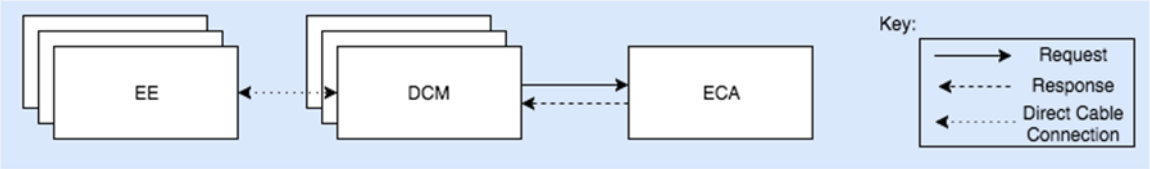


Figure 67 ECA Messaging Diagram

The figure shows that the ECA will receive messages initiated by one or more DCM. It is recommended, but not required, that each DCM work with a single ECA.

The SCMS PoC design requires that each ECA maintain a list of DCMs that are authorized to send it enrollment requests. It does this by maintaining a list of authorized DCM TLS certificates.

Each ECA will be assigned to one RA, which will only trust this ECA’s enrollment certificates.

5.2.11.8.4.5.2 Process

To add an ECA to the SCMS, the local ICA Manager must provide a list of TLS certificates to the ECA for all DCMs that are authorized to send it requests. The ECA must also configure its network to allow communication from the DCMs to the ECA.

In order to access the new ECA, each DCM that will send it requests must be provided with the following:

1. The FQDN of the new ECA
2. The ECA's TLS certificate

The local ICA Manager must inform the designated RA of the newly added ECA's SCMS certificate.

5.2.11.8.4.5.2.1 End State

After completing this use case, the ECA will be configured with the following values:

Table 31 ECA Values

ECA Value	Notes
One or more DCM TLS certificates	The ECA requires a list of authorized DCMs that can send it signature requests. The ECA shall maintain a table of allowed DCM TLS certificates.

After completion of this use case, each DCM that is authorized to communicate with the newly added ECA will be configured with the following values:

Table 32 DCM Values

DCM Value	Notes
FQDN and TLS certificate of the ECA	Each DCM requires the FQDN and TLS Certificate of one (or more) ECA to process enrollment requests.

After completion of this use case, the designated RA will have the following information:

Table 33 RA Values

RA Value	Notes
SCMS certificate of the newly added ECA	One RA must be configured to accept enrollment certificates from the new ECA.

5.2.11.8.4.5.2.2 Special Cases

The procedure described here can be used when adding a net-new ECA to the SCMS.

Other conditions must be managed as follows:

- ECA SCMS Certificate Retired and Re-Issued - When this happens, the RA that the ECA is assigned to must be informed of the new ECA certificate. The local ICA Manager will perform this update.
- ECA Decommissioned and Replaced - If an ECA is securely decommissioned, enrollment certificates that were previously issued may continue to be trusted. The local ICA Manager must instruct all DCMs that they can no longer send requests to the decommissioned ECA. A new replacement ECA may be added using the procedure described here as if it were a net-new ECA to the SCMS.
- ECA Revoked: see Step 11.2.1 - Revoke ECA

5.2.11.8.4.5.3 Assumptions

- The ECA must be configured using the Setup ECA use case before it can be added
- The ECA will support a mechanism for adding and removing authorized DCM certificates from its internal table. The method of updating this table is implementation specific and is not part of the SCMS design.
- Each DCM will maintain a list of one (or more) active ECAs that it may use for signing enrollment certificates

- Each RA will maintain a list of ECAs whose enrollment certificates it may trust
- Each ECA will be assigned to a single RA

5.2.11.8.4.5.4 Requirements

Table 34 Use Case 11.1. Add ECA - Requirements

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-770	MANUAL PROCESS	Create CSR	The to-be-added component shall create a CSR, which shall be forwarded to the authorizing root CA or ICA in order to obtain its SCMS identity certificate.	Most communications in the system are authenticated. A root CA or ICA must authorize the new component.	In the PoC, this will occur by a manual process.	CRL Store, CRLG, DCM, ECA, IBLM, ICA, LA, PCA, PG, RA
SCMS-774	CLOSED	Distribute the new component certificate	The TCotSCMSM shall forward signed certificates to the component that generated the corresponding CSR.	The result of the CSR is the new components identity in the system. This will be used to authenticate itself to other entities in the system.	After the authorizing root CA or ICA signs and returns a 1609.2 certificate to the TCotSCMSM, the new certificate must be delivered to the new component. In the PoC, this will occur by a manual process.	TCotSCMSM
SCMS-784	MANUAL PROCESS	TCotSCMSM inform ECA of DCMs	The local ICA Manager shall update the ECA when a DCM is added and provide the DCM's SCMS certificate and TLS certificate.	The ECA will need to authenticate with DCMs, and hence will need to be aware of their identity	In the PoC this will occur by a manual process.	TCotSCMSM
SCMS-1039	SCMS POC OUT OF SCOPE	Error Code: tcNotifyECAofDCMFailure	TCotSCMSM shall log "Error Code: tcNotifyECAofDCMFailure", if the TCotSCMSM cannot notify			TCotSCMSM

Key	Status	Summary	Description	Justification	Notes	Component/s
			the ECA of the DCMs with which it will communicate.			
SCMS-1386	MANUAL PROCESS	Add component's certificate to GCCF	The TCotSCMSM shall forward required information to the Policy Generator in order to add the certificate of the newly created SCMS component to the Global Certificate Chain File (GCCF).	For a newly added component to be a valid SCMS component, its certificate must chain back to the SCMS root CA and its chain must be available to any other component via GCCF.	In the PoC, this will occur by a manual process.	TCotSCMSM
SCMS-1412	MANUAL PROCESS	Destroy certificate's private key	The certificate's private key shall be destroyed at the end of the "In-use" life of a certificate. The in-use lifetime of certificates shall be defined either by SCMS policy and/or based on the expiration and In-use lifetime of subordinate certificates.	To prevent the usage of certificates that have reached the end of defined In-use lifetime.	Out of scope as this needs to be implemented as operational policy.	CRL Store, CRLG, DCM, ECA, ICA, LA, MA, PCA, PG, RA
SCMS-1591	CLOSED	ECA certificate validity	ECA shall request an ECA certificate with a validity of 11 years.	To support issuing of subordinate certificates.	This is for POC only.	ECA
SCMS-1602	SCMS POC OUT OF SCOPE	ECA certificate in-use period	ECA shall use its ECA certificate for an in-use period of 3 years.	Use 3 years for Enrollment SCMS components	Out of scope as this needs to be implemented as operational	ECA

Key	Status	Summary	Description	Justification	Notes	Component/s
					policy. This is for CV-Pilot only.	
SCMS-1605	MANUAL PROCESS	ECA certificate validity	ECA shall request an ECA certificate with a maximum validity of 8 years +/- 1 week.	To support issuing of subordinate certificates.	1st generation: Start = 428,630,405, Duration = 1,084 sixtyHours This is for CV-Pilot only.	ECA

9 issues

5.2.11.8.4.6 Step 11.1.1 - Add ICA

5.2.11.8.4.6.1 Goals

The Intermediate Certificate Authority (ICA) is a non-central, backend component of the SCMS. There may be many instances of ICAs within the system. The ICA authorizes all other non-central components including ECAs, PCAs, RAs, LAs, or additional ICAs. Adding a new ICA to the system makes the new ICA available to authorize new components.

An ICA is intended to be an offline component, meaning that it should be configured with no direct network access or address. A local ICA Manager operates the ICA manually. The specific details of how the operator presents messages to the ICA is implementation-specific and subject to review by a certification procedure approved by the SCMS Manager.

5.2.11.8.4.6.2 Procedure

The procedure required for adding an ICA to the system depends on whether the new ICA is replacing a previously revoked or removed ICA or if it is a net-new component.

5.2.11.8.4.6.2.1 New ICA

A new ICA must be properly set-up using the process described in the Setup ICA use case. Since the ICA operates offline, there are no network addresses or other parameters to configure when adding the ICA.

Note that if the new ICA issues a certificate for a PCA or RA, then the Add PCA use case will cause the ICA to be registered with the Policy Generator (PG) for inclusion in future updates to the Global Certificate Chain File (GCCF). There is no need to register the ICA with the PG until a new PCA or RA is added. All other components that are issued certificates by the ICA will make the ICA certificate available to recipients of their messages when required.

5.2.11.8.4.6.2.2 Re-Certified ICA

An ICA certificate has a limited useful life that is shorter than the expiration period of the certificate. When an ICA certificate is retired, the current private key must be deleted, a new key pair must be generated, and a new certificate must be issued. There are no additional actions needed to add or enable the new ICA certificate. As with the procedure for adding a new ICA (above), there is no need to communicate the new ICA certificate to the PG or any other components.

5.2.11.8.4.6.2.3 Replacement ICA

When replacing an ICA that was previously removed or revoked, the new component must first be set up using the Setup ICA use case. The local ICA Manager must then use the new component to re-issue certificates to all of the components that were previously authorized under the ICA that was removed or revoked, see Step 11.2.1 - Revoke ICA

5.2.11.8.4.6.3 Requirements

Table 35 Use Case 11.1.1 Add ICA - Requirements

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-715	CLOSED	Provide Elector Certificates	The TCotSCMSM shall provision all SMCMS components with the self-signed certificates of all electors that are valid at the time of the component setup.	Root Management messages require signatures from the Electors to be validated, so authentic root CA Certificates are also required.	When receiving Root Management messages through the GCCF or LCCF, the authenticity of the messages will be validated by counting valid Elector signatures on the message and ensuring that at least that number (quorum) required in the Global Policy is present, after which the Root Management message can be processed.	TCotSCMSM
SCMS-770	MANUAL PROCESS	Create CSR	The to-be-added component shall create a CSR, which shall be forwarded to the authorizing root CA or ICA in order to obtain its SCMS identity certificate.	Most communications in the system are authenticated. A root CA or ICA must authorize the new component.	In the PoC, this will occur by a manual process.	CRL Store, CRLG, DCM, ECA, IBLM, ICA, LA, PCA, PG, RA
SCMS-774	CLOSED	Distribute the new component certificate	The TCotSCMSM shall forward signed certificates to the component that generated the corresponding CSR.	The result of the CSR is the new components identity in the system. This will be used to	After the authorizing root CA or ICA signs and returns a 1609.2 certificate to the TCotSCMSM, the new	TCotSCMSM

Key	Status	Summary	Description	Justification	Notes	Component/s
				authenticate itself to other entities in the system.	certificate must be delivered to the new component. In the PoC, this will occur by a manual process.	
SCMS-1386	MANUAL PROCESS	Add component's certificate to GCCF	The TCotSCMSM shall forward required information to the Policy Generator in order to add the certificate of the newly created SCMS component to the Global Certificate Chain File (GCCF).	For a newly added component to be a valid SCMS component, its certificate must chain back to the SCMS root CA and its chain must be available to any other component via GCCF.	In the PoC, this will occur by a manual process.	TCotSCMSM
SCMS-1412	MANUAL PROCESS	Destroy certificate's private key	The certificate's private key shall be destroyed at the end of the "In-use" life of a certificate. The in-use lifetime of certificates shall be defined either by SCMS policy and/or based on the expiration and In-use lifetime of subordinate certificates.	To prevent the usage of certificates that have reached the end of defined In-use lifetime.	Out of scope as this needs to be implemented as operational policy.	CRL Store, CRLG, DCM, ECA, ICA, LA, MA, PCA, PG, RA
SCMS-1596	CLOSED	ICA certificate validity	ICA shall request an ICA certificate with a validity of 13 years.	To support issuing of subordinate certificates.	This is for POC only.	ICA
SCMS-1597	SCMS POC OUT OF SCOPE	ICA certificate in-use period	ICA shall use its ICA certificate for an in-use period of 4 years.	The in-use period shall be short to minimize	Out of scope as this needs to be implemented as operational	ICA

Key	Status	Summary	Description	Justification	Notes	Component/s
				impact, if revocation is required.	policy. This is for POC only.	
SCMS-1603	MANUAL PROCESS	ICA certificate validity	ICA shall request an ICA certificate with a maximum validity of 8 years +/- 1 week.	To support issuing of subordinate certificates.	Start = 410,313,605 Duration = 1,169 sixtyHours This is for CV-Pilot only.	ICA
SCMS-1604	SCMS POC OUT OF SCOPE	ICA certificate in-use period	ICA shall use its ICA certificate for the entire validity period of the certificate.	The In-use period shall be short to minimize impact if revocation is required.	Out of scope as this needs to be implemented as operational policy. This is for CV-Pilot only.	ICA

9 issues

5.2.11.8.4.7 Step 11.1.1 - Add MA

5.2.11.8.4.7.1 Goals

The Misbehavior Authority (MA) is an intrinsically central SCMS component that performs multiple functions to manage risk in the SCMS like receiving misbehavior reports from EEs, investigating potential misbehavior, and blacklisting or revoking components. As a central component, there will only be one MA instance.

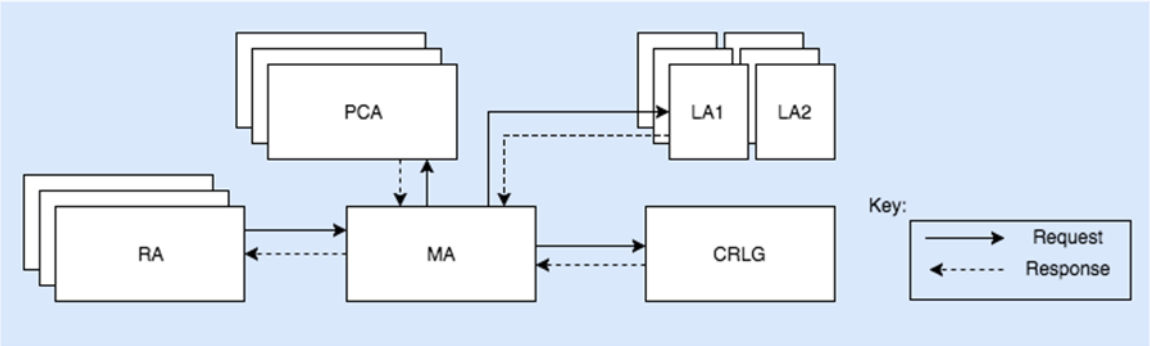


Figure 68 MA Messaging Diagram

The figure shows that the MA receives requests from one or more RAs and it sends out requests to PCAs, pairs of LAs, and the CRLG.

EEs must encrypt misbehavior reports to be sent to the MA. Therefore, all EEs will need the current MA certificate, which they obtain during enrollment from the DCM or during operation from their assigned RA.

5.2.11.8.4.7.2 Procedure

Components that communicate with an added MA must be properly configured.

5.2.11.8.4.7.2.1 End States

After completing this use case, the MA will be configured with the following values:

Table 36 MA Values

MA Value	Notes
List of RA TLS certificates	The MA must maintain a list of TLS certificates for all RA's that will forward misbehavior reports on behalf of EEs.
List of PCA FQDN and TLS certificates	The MA must maintain a list of all PCA network addresses and TLS certificates.
List of LA FQDN and TLS certificates	The MA must maintain a list of all LA's and their TLS certificates.
CRLG FQDN and TLS certificate	The MA must be able to send revocation requests to the CRLG.

After completing this use case, RAs will be configured with the following values:

Table 37 RA Values

RA Value	Notes
MA FQDN and TLS certificate	Each RA must be able to establish a secure connection to the MA.
MA's SCMS certificate	Each RA must provide MA's certificate to its EEs.

After completing this use case, DCMs will be configured with the following values:

Table 38 DCM Values

DCM Value	Notes
MA's SCMS certificate	Each DCM must provide the current MA's certificate to EEs during enrollment.

All RAs, PCAs, LAs, and the CRLG will need a copy of the new MA's TLS certificate so that they can establish secure communication. These components can learn the MA's SCMS certificate by validating any signed message from the MA and chaining it up to the SCMS root certificate (which they already have).

5.2.11.8.4.7.3 Requirements

Table 39 Use Case 11.1.1 Add MA - Requirements

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-715	CLOSED	Provide Elector Certificates	The TCotSCMSM shall provision all SMCMS components with the self-signed certificates of all electors that are valid at the time of the component setup.	Root Management messages require signatures from the Electors to be validated, so authentic root CA Certificates are also required.	When receiving Root Management messages through the GCCF or LCCF, the authenticity of the messages will be validated by counting valid Elector signatures on the message and ensuring that at least that number (quorum) required in the Global Policy is present, after which the Root Management message can be processed.	TCotSCMSM
SCMS-770	MANUAL PROCESS	Create CSR	The to-be-added component shall create a CSR, which shall be forwarded to the authorizing root CA or ICA in order to obtain its SCMS identity certificate.	Most communications in the system are authenticated. A root CA or ICA must authorize the new component.	In the PoC, this will occur by a manual process.	CRL Store, CRLG, DCM, ECA, IBLM, ICA, LA, PCA, PG, RA
SCMS-774	CLOSED	Distribute the new component certificate	The TCotSCMSM shall forward signed certificates to the component that generated the corresponding CSR.	The result of the CSR is the new components identity in the system. This will be used to authenticate itself to	After the authorizing root CA or ICA signs and returns a 1609.2 certificate to the TCotSCMSM, the new certificate must be delivered to the new component.	TCotSCMSM

Key	Status	Summary	Description	Justification	Notes	Component/s
				other entities in the system.	In the PoC, this will occur by a manual process.	
SCMS-1386	MANUAL PROCESS	Add component's certificate to GCCF	The TCotSCMSM shall forward required information to the Policy Generator in order to add the certificate of the newly created SCMS component to the Global Certificate Chain File (GCCF).	For a newly added component to be a valid SCMS component, its certificate must chain back to the SCMS root CA and its chain must be available to any other component via GCCF.	In the PoC, this will occur by a manual process.	TCotSCMSM
SCMS-1412	MANUAL PROCESS	Destroy certificate's private key	The certificate's private key shall be destroyed at the end of the "In-use" life of a certificate. The in-use lifetime of certificates shall be defined either by SCMS policy and/or based on the expiration and In-use lifetime of subordinate certificates.	To prevent the usage of certificates that have reached the end of defined In-use lifetime.	Out of scope as this needs to be implemented as operational policy.	CRL Store, CRLG, DCM, ECA, ICA, LA, MA, PCA, PG, RA
SCMS-1581	SCMS POC OUT OF SCOPE	Component certificate in-use period	The SCMS component shall use its certificate for an in-use period of 3 years.	Use 3 years for standard SCMS components	Out of scope as this needs to be implemented as operational policy. This is for POC & CV-Pilot only.	CRLG, DCM, LA, MA, PG, RA
SCMS-1725	MANUAL PROCESS	Component certificate FQDN match	The SCMS component shall have a certificate with a certificateId field that matches the FQDN of the component.	FQDN of each component must match		CRLG, DCM, ECA, LA, MA, PCA, PG, RA

Key	Status	Summary	Description	Justification	Notes	Component/s
				the official ID of the component.		

7 issues

5.2.11.8.4.8 Step 11.1.1 - Add PCA

5.2.11.8.4.8.1 Goals

The Pseudonym Certificate Authority (PCA) is an intrinsically non-central component of the SCMS. It issues pseudonym, identification, and application certificates for End Entities (EEs). There may be multiple PCAs in the SCMS. Each PCA is associated with a single RA and a pair of LAs to perform its core functions. The PCA responds to requests from the MA to investigate potential misbehavior.

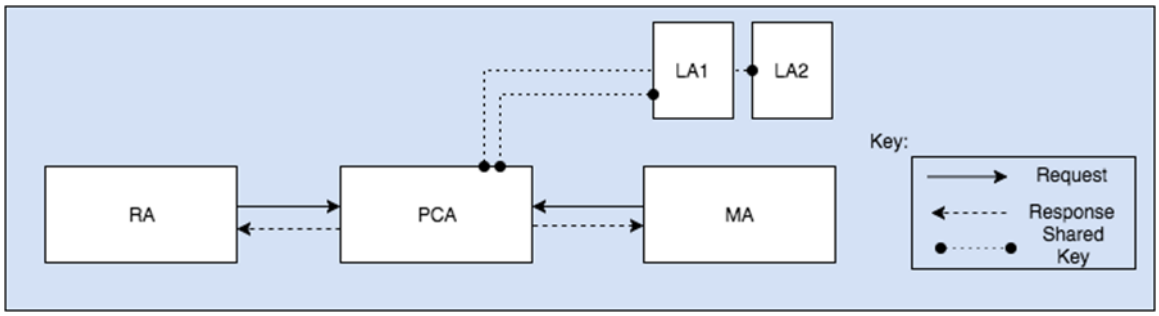


Figure 69 PCA Messaging Diagram

The figure shows that the PCA responds to requests from both the RA and the MA. It also requires shared symmetric encryption/decryption between the LAs and the PCA, although, there is no direct communication between them. The PCA also maintains a secure database containing all pre-linkage values, certificates, and a hash of the certificate request that it received from the RA.

5.2.11.8.4.8.2 Procedure

To add a new PCA to the SCMS, the local ICA Manager will select an RA and a pair of LAs to associate with the new PCA. It must then coordinate the generation and installation of the shared symmetric encryption/decryption key between the PCA and each of the LAs. It will also inform the RA and the central MA of the PCA's FQDN.

5.2.11.8.4.8.2.1 End States

After completing this use case, the PCA will be configured with the following values:

Table 40 PCA Values

PCA Value	Notes
LA1-PCA shared key	Symmetric encryption key shared with LA1
LA1 ID	A globally unique identifier associated with LA1
LA2-PCA shared key	Symmetric encryption key shared with LA2
LA2 ID	A globally unique identifier associated with LA2

After completion of this use case, the designated RA will have the following information:

Table 41 RA Values

RA Value	Notes
PCA FQDN	RA will use this address to send certificate signing requests to the PCA. RA signs each request.

After completion of this use case, the MA will have the following information:

Table 42 MA Values

MA Value	Notes
PCA FQDN	The MA must be able to contact the PCA to retrieve linkage values to support misbehavior investigation and blacklisting or revocation.

After completion of this use case, the designated LAs will have the following information:

Table 43 LA Values

LA1/2 Value	Notes
LA1/2-PCA shared key	Each LA (i.e., LA1 and LA2) stores the shared key that was exchanged with the PCA.

5.2.11.8.4.8.2.2 Special Cases

The procedure described above shall be used when adding a new PCA to the SCMS. The following details define how to deal with special cases of replacing a previous PCA component.

- If the PCA's SCMS certificate has been retired and a new certificate is issued, there is no need for a special procedure to add the new certificate. The PCA can continue to use the same FQDN and TLS certificate as before. The RA and MA should be able to learn the new PCA certificate.
- If the PCA has been securely decommissioned and replaced, the local ICA Manager may transfer the contents of the PCA database to the new component. The replacement PCA may use the same network address as the decommissioned device. The RA and MA should be able to learn the new PCA certificate.
- If the PCA's SCMS certificate has been revoked, then in addition to adding the new PCA, all certificates that were previously issued by that PCA will need to be removed by the EEs to which they were issued. This process will be triggered by the presence of the PCA's certificate on the CRL, which is distributed to all EEs (see the Revoke PCA use case for details on how to revoke a PCA). EEs that become inoperative or are at risk of jeopardizing their privacy because of this action will need to contact their RA to request new certificates or take OEM specific action to recover.
- If an ICA in the PCA's certificate chain or the root CA has been revoked and replaced, then the PCA must generate a new key pair and receive a new SCMS certificate from a re-certified or replaced ICA. As in the case of PCA revocation,

affected EEs will need to request new certificates or follow an OEM specified procedure to recover.

5.2.11.8.4.8.3 Requirements

Table 44 Use Case 11.1.1 Add PCA - Requirements

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-244	CLOSED	PCA Availability	The Local ICA Manager shall make the new PCA's certificate and information to locate it on the network available to any RAs that will forward certificate requests to it.	The PCA must be integrated correctly into the SCMS system.	In the PoC, this will occur by a manual process.	TCotSCMSM
SCMS-715	CLOSED	Provide Elector Certificates	The TCotSCMSM shall provision all SMCMS components with the self-signed certificates of all electors that are valid at the time of the component setup.	Root Management messages require signatures from the Electors to be validated, so authentic root CA Certificates are also required.	When receiving Root Management messages through the GCCF or LCCF, the authenticity of the messages will be validated by counting valid Elector signatures on the message and ensuring that at least that number (quorum) required in the Global Policy is present, after which the Root Management message can be processed.	TCotSCMSM
SCMS-770	MANUAL PROCESS	Create CSR	The to-be-added component shall create a CSR, which shall be	Most communications in the system are authenticated. A	In the PoC, this will occur by a manual process.	CRL Store, CRLG, DCM, ECA, IBLM,

Key	Status	Summary	Description	Justification	Notes	Component/s
			forwarded to the authorizing root CA or ICA in order to obtain its SCMS identity certificate.	root CA or ICA must authorize the new component.		ICA, LA, PCA, PG, RA
SCMS-774	CLOSED	Distribute the new component certificate	The TCotSCMSM shall forward signed certificates to the component that generated the corresponding CSR.	The result of the CSR is the new components identity in the system. This will be used to authenticate itself to other entities in the system.	After the authorizing root CA or ICA signs and returns a 1609.2 certificate to the TCotSCMSM, the new certificate must be delivered to the new component. In the PoC, this will occur by a manual process.	TCotSCMSM
SCMS-1386	MANUAL PROCESS	Add component's certificate to GCCF	The TCotSCMSM shall forward required information to the Policy Generator in order to add the certificate of the newly created SCMS component to the Global Certificate Chain File (GCCF).	For a newly added component to be a valid SCMS component, its certificate must chain back to the SCMS root CA and its chain must be available to any other component via GCCF.	In the PoC, this will occur by a manual process.	TCotSCMSM
SCMS-1412	MANUAL PROCESS	Destroy certificate's private key	The certificate's private key shall be destroyed at the end of the "In-use" life of a certificate. The	To prevent the usage of certificates that have reached the end of defined In-use lifetime.	Out of scope as this needs to be implemented as operational policy.	CRL Store, CRLG, DCM, ECA, ICA, LA,

Key	Status	Summary	Description	Justification	Notes	Component/s
			in-use lifetime of certificates shall be defined either by SCMS policy and/or based on the expiration and In-use lifetime of subordinate certificates.			MA, PCA, PG, RA
SCMS-1594	CLOSED	PCA certificate expiration	PCA shall request a certificate with a validity of 4 years.	The expiration must be sufficiently long to issue pseudonym certificates for 3 years in the future.	This is for POC only.	PCA
SCMS-1595	SCMS POC OUT OF SCOPE	PCA certificate in-use period	PCA shall use its certificate for an in-use period of 1 years.	The In-use period shall be short to minimize impact if revocation is required.	Out of scope as this needs to be implemented as operational policy. This is for POC & CV-Pilot only.	PCA
SCMS-1806	MANUAL PROCESS	Register non-central component with the central MA	The Local ICA Manager shall update the MA with the FQDN, TLS certificate, and SCMS certificate of any newly added PCA, LA, or RA.	The MA must know about all PCAs, LAs, and RAs in the system so that it can execute misbehavior investigations and revocation procedures.	In PoC, this will occur by a manual process. When a new PCA, LA, or RA is added, the local ICA manager will notify the TCotSCMSM about the newly added component (this is a manual process). The TCotSCMSM will then update the central MA with the	TCotSCMSM

Key	Status	Summary	Description	Justification	Notes	Component/s
					necessary information about the newly added component. It is expected (but not required) that a PCA, RA, and pair of LAs will typically be added as a complete set.	
SCMS-2608	MANUAL PROCESS	Map PCA IssuerIdentifier to PCA FQDN	The TCotSCMSM shall associate each PCA IssuerIdentifier (the HashId8 of the PCA signing certificate) with the FQDN of the PCA that has the certificate.	A mapping between PCAs' IssuerIdentifier and PCA hostname is needed. During an investigation, the MA (GMBD) will receive a cert, extract linkage value, extract IssuerIdentifier, and then ask the PCA that issued the cert for the linkage value. For that step, MA must be able to map the IssuerIdentifer to the PCA hostname. This mapping is maintained by the TCotSCMSM and configured in the MA as needed, or this mapping may be maintained as a built-in feature of the MA.	For the PoC, the SCMS operator will manually configure the mapping of PCA IssuerIdentifiers with the FQDN of the corresponding PCA.	TCotSCMSM

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-2843	MANUAL PROCESS	PCA certificate expiration	PCA shall request a certificate with a maximum validity of 4 years +/- 2 weeks.	The expiration must be sufficiently long to issue pseudonym certificates for 3 years in the future.	1st generation: Start = 428,630,405, Duration = 1,084 sixtyHours This is for CV-Pilot only.	PCA

11 issues

5.2.11.8.4.9 Step 11.1.1 - Add PG

5.2.11.8.4.9.1 Goals

The Policy Generator (PG) is an intrinsically central SCMS component that maintains and signs updates to the Global Policy File (GPF) and the Global Certificate Chain File (GCCF). In addition, the PG is required to sign Local Policy Files (LPFs) at the request of RAs who want to set local policy values or reduce the volume of information that they distribute to their EEs. When signing LPFs, the PG is responsible for validating that critical global information has not been removed and that all local policy adjustments comply with the global policy.

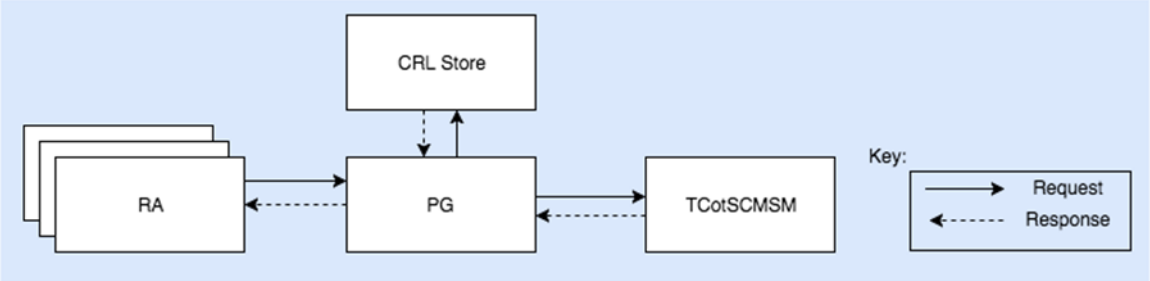


Figure 70 PG Messaging Diagram

The figure shows the request-response relationships of the PG. This diagram explicitly includes the TCotSCMSM, which is the only authority that is able to define changes to global policy, which in turn will be distributed through the GPF. The TCotSCMSM is also the conduit through which new PCA certificate chains can be communicated for addition to the GCCF. Updates to the CRL downloaded from the CRL store might trigger updates to the GCCF in case it contains a revoked certificate.

5.2.11.8.4.9.2 Procedure

The PG is an intrinsically central component, so there will only be one instance of the PG in the SCMS. When adding or replacing the PG, the TCotSCMSM must ensure that all RAs are aware of the FQDN of the PG and that they are allowed to access to the PG. This will likely be done in cooperation with local ICA Managers who operate each RA.

Prior to initiating this process, the new PG must be set up according to the Setup Policy Generator use case.

5.2.11.8.4.9.2.1 End State

After completing this use case, the PG will be configured with the following values:

Table 45 PG Values

PG Value	Notes
CRL Store FQDN	The PG needs to download the latest CRL on a regular basis in order to remove revoked certificates from the GCCF.

After completing this use case, RAs will be configured with the following values:

Table 46 RA Values

RA Value	Notes
PG FQDN	Every RA in the SCMS must be able to contact the PG to request signatures on LPFs and to download the latest GPF and GCCF.

5.2.11.8.4.9.2.2 Special Cases

The procedure defined above applies when a new PG is initially added to the SCMS. Changes required for replacing a PG are required based on the reason for the replacement.

- The PG's SCMS certificate has a useful life that is shorter than the certificate expiration date. When the PG's SCMS certificate is retired, the current private key must be deleted, a new key pair must be generated, and a new SCMS certificate can be installed in the PG. Other SCMS components can learn the new certificate by reading it from the signed updates to the GPF or GCCF and validating that the Root CA signed it. There is no need to communicate the new SCMS certificate directly to any other SCMS components.
- If the PG is securely decommissioned and replaced, the new component must be issued a new SCMS certificate, which can be learned as described above. The current state of the Global Policy and the current GCCF can be securely copied to the replacement component or it can load these files from the last signed copies that were published.
- If a PG is revoked, then it must be re-certified or replaced. The TCotSCMSM must determine if the latest published version of the GPF is reliable for loading into the new component or it can re-create a current Global Policy definition. Similarly, the TCotSCMSM can import a reliable copy of the GCCF or it can collect PCA cert chains and reproduce the GCCF.
- If the root CA is revoked causing implicit revocation of the PG, the TCotSCMSM must re-create the Global Policy and replace or re-certify the PG. In this situation, the GCCF should be re-created by collecting PCA certificate chains to ensure consistency with all newly issued root CA or ICA certificates (if an ICA has been revoked, validated certificate chains for PCAs that were not impacted may be copied from the previous GCCF).

5.2.11.8.4.9.3 Assumptions

- A new PG must be setup using the Setup Policy Generator use case
- The interface between the TCotSCMSM and the PG is not defined. It is assumed that updates to the GPF or GCCF will be encoded using the same format as the published files (i.e., using the same ASN.1 message structure up to the "to be signed" structure).
- The method for the TCotSCMSM to authenticate to the PG is not defined. It is assumed that a secure process will manage and log updates to global policy and certificate chain files.

5.2.11.8.4.9.4 Requirements

Table 47 Use Case 11.1.1 Add PG - Requirements

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-715	CLOSED	Provide Elector Certificates	The TCotSCMSM shall provision all SMCMS components with the self-signed certificates of all electors that are valid at the time of the component setup.	Root Management messages require signatures from the Electors to be validated, so authentic root CA Certificates are also required.	When receiving Root Management messages through the GCCF or LCCF, the authenticity of the messages will be validated by counting valid Elector signatures on the message and ensuring that at least that number (quorum) required in the Global Policy is present, after which the Root Management message can be processed.	TCotSCMSM
SCMS-770	MANUAL PROCESS	Create CSR	The to-be-added component shall create a CSR, which shall be forwarded to the authorizing root CA or ICA in order to obtain its SCMS identity certificate.	Most communications in the system are authenticated. A root CA or ICA must authorize the new component.	In the PoC, this will occur by a manual process.	CRL Store, CRLG, DCM, ECA, IBLM, ICA, LA, PCA, PG, RA
SCMS-774	CLOSED	Distribute the new component certificate	The TCotSCMSM shall forward signed certificates to the component that generated the corresponding CSR.	The result of the CSR is the new components identity in the system. This will be used to	After the authorizing root CA or ICA signs and returns a 1609.2 certificate to the TCotSCMSM, the new certificate must be delivered to the new component.	TCotSCMSM

Key	Status	Summary	Description	Justification	Notes	Component/s
				authenticate itself to other entities in the system.	In the PoC, this will occur by a manual process.	
SCMS-1386	MANUAL PROCESS	Add component's certificate to GCCF	The TCotSCMSM shall forward required information to the Policy Generator in order to add the certificate of the newly created SCMS component to the Global Certificate Chain File (GCCF).	For a newly added component to be a valid SCMS component, its certificate must chain back to the SCMS root CA and its chain must be available to any other component via GCCF.	In the PoC, this will occur by a manual process.	TCotSCMSM
SCMS-1412	MANUAL PROCESS	Destroy certificate's private key	The certificate's private key shall be destroyed at the end of the "In-use" life of a certificate. The in-use lifetime of certificates shall be defined either by SCMS policy and/or based on the expiration and In-use lifetime of subordinate certificates.	To prevent the usage of certificates that have reached the end of defined In-use lifetime.	Out of scope as this needs to be implemented as operational policy.	CRL Store, CRLG, DCM, ECA, ICA, LA, MA, PCA, PG, RA
SCMS-1581	SCMS POC OUT OF SCOPE	Component certificate in-use period	The SCMS component shall use its certificate for an in-use period of 3 years.	Use 3 years for standard SCMS components	Out of scope as this needs to be implemented as operational policy. This is for POC & CV-Pilot only.	CRLG, DCM, LA, MA, PG, RA

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-1725	MANUAL PROCESS	Component certificate FQDN match	The SCMS component shall have a certificate with a certificateId field that matches the FQDN of the component.	FQDN of each component must match the official ID of the component.		CRLG, DCM, ECA, LA, MA, PCA, PG, RA

7 issues

5.2.11.8.4.10 Step 11.1.1 - Add RA

5.2.11.8.4.10.1 Goals

The Registration Authority (RA) is an intrinsically, non-central component of the SCMS. There may be multiple RAs active at any given time in the SCMS.

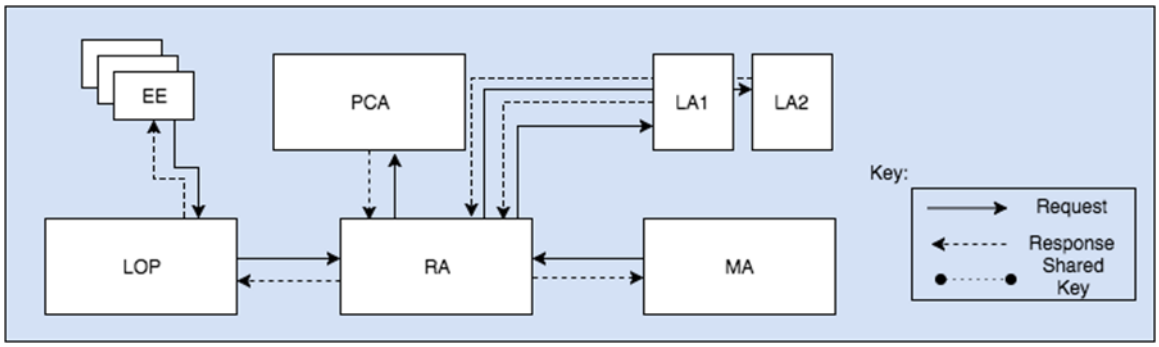


Figure 71 RA Messaging Diagram

The figure shows that each RA supports the following connections:

- The RA can receive and respond to requests from EEs through the LOP which masks the source IP address and route of the EE from the RA. Only EEs that have enrollment certificates from ECAs that are authorized to use the RA will be accepted. Each EE is configured to contact only one RA.
- The RA can initiate certificate requests to a PCA to generate certificates. Each PCA is associated with a pair of LAs (LA1 and LA2) that generate pre-linkage values for pseudonym certificates, which are used in EE revocation.
- The RA initiate requests to both LAs to obtain pre-linkage values
- The RA must respond to requests from the central MA to add EEs to its internal blacklist and to support misbehavior investigation

Not shown in Figure 1 is the association of the RA with one or more ECA. While there is no direct communication between an ECA and the RA, the RA must maintain a white list of ECA certificates such that only EEs with enrollment certificates signed by authorized ECAs can access the RA. In addition, the RA maintains extensive logs of transaction history and an internal blacklist, which identifies EEs that are disallowed to request or download new certificates.

5.2.11.8.4.10.2 Procedure

The addition of a new RA to the SCMS must begin with a certified RA component that has been setup according to the Setup RA use case.

The following actions are required to add the new RA:

- The MA must be updated with the Fully Qualified Domain Name (FQDN) of the new RA. This requires the local ICA Manager to inform the TCotSCMSM and request that the new RA be added to the MA.

- The RA must receive the FQDN of the PCA
- The RA must receive the FQDNs of both LAs and their LA IDs
- The RA must receive least one ECA certificate, which will be added to the RA's white list of authorized ECAs

All of these steps are manual processes that are carried out by the local ICA Manager.

5.2.11.8.4.10.2.1 End State

After completing this use case, the RA will be configured with the following values:

Table 48 RA Values

RA Value	Notes
PCA FQDN	The RA must initiate communication with the PCA to request certificates.
LA1/2 FQDN	The RA requires the network address of LA1 and LA2.
LA1/2 ID	The RA requires the globally unique LA ID for LA1 and LA2.
ECA certificate	The RA must have a valid SCMS certificate from at least one active ECA which will configure EEs to contact the RA for certificates.

After completing this use case, the DCM will be configured with the following values:

Table 49 DCM Values

DCM Value	Notes
RA FQDN	The DCM requires the network address of the RA that it is authorized to use when configuring new EEs.

After completing this use case, the MA will be configured with the following values:

Table 50 MA Values

MA Value	Notes
RA FQDN	The MA must be able to contact the RA to update the RA's internal blacklist or to support misbehavior investigation.

5.2.11.8.4.10.2.2 Special Cases

The general procedure described above applies when adding a new RA to the SCMS. There are variations to the process when a replacement RA is introduced.

- If the RA certificate has been retired and the same RA now has a new certificate, the RA may continue to operate using the same network address and internal storage status. All DCMs that are authorized to use the RA shall obtain the new RA certificate for use in configuring new EEs.

- If the RA hardware were securely decommissioned, the internal memory of the prior RA may be transferred to a new device. As in the previous case, all DCMs that are authorized to configure EEs for the RA shall receive the new RA certificate.
- If the RA has been revoked and replaced, the local ICA Manager must decide if any pre-existing state information can be securely transferred to the replacement component.
- If a component in the RA's certificate chain (an ICA or the Root CA) is revoked and replaced, the RA will be implicitly revoked and need to be replaced. Here too, the local ICA manager may decide if any pre-linkage values from prior transactions can be saved. If not, then past values shall be purged.

5.2.11.8.4.10.3 Requirements

Table 51 Use Case 11.1.1 Add RA - Requirements

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-264	CLOSED	SCMS Notify RA Add	The TCotSCMSM shall inform the new RA of PCAs available to receive certificate requests, making available those PCAs' certificates and necessary information for locating them on the network.	The RA must be integrated correctly into the SCMS system.	In the PoC, this will occur by a manual process.	TCotSCMSM
SCMS-266	MANUAL PROCESS	DCM configure RA	The Technical Component of the SCMS Manager shall communicate the FQDN of RA to the DCM.	The RA must be integrated correctly into the SCMS system. Logical RA.	The relevant DCMs configure their end-entity devices to communicate with an RA to request pseudonym certificates. In the PoC, this will occur by a manual process.	TCotSCMSM
SCMS-715	CLOSED	Provide Elector Certificates	The TCotSCMSM shall provision all SMCMS components with the self-signed certificates of all electors that are valid at the time of the component setup.	Root Management messages require signatures from the Electors to be validated, so authentic root CA Certificates are also required.	When receiving Root Management messages through the GCCF or LCCF, the authenticity of the messages will be validated by counting	TCotSCMSM

Key	Status	Summary	Description	Justification	Notes	Component/s
					valid Elector signatures on the message and ensuring that at least that number (quorum) required in the Global Policy is present, after which the Root Management message can be processed.	
SCMS-770	MANUAL PROCESS	Create CSR	The to-be-added component shall create a CSR, which shall be forwarded to the authorizing root CA or ICA in order to obtain its SCMS identity certificate.	Most communications in the system are authenticated. A root CA or ICA must authorize the new component.	In the PoC, this will occur by a manual process.	CRL Store, CRLG, DCM, ECA, IBLM, ICA, LA, PCA, PG, RA
SCMS-774	CLOSED	Distribute the new component certificate	The TCotSCMSM shall forward signed certificates to the component that generated the corresponding CSR.	The result of the CSR is the new components identity in the system. This will be used to authenticate itself to other entities in the system.	After the authorizing root CA or ICA signs and returns a 1609.2 certificate to the TCotSCMSM, the new certificate must be delivered to the new component. In the PoC, this will occur by a manual process.	TCotSCMSM

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-1049	MANUAL PROCESS	Error code: tcNotifyRAofPCAListFailure	The TCotSCMSM shall log "Error code: tcNotifyRAofPCAListFailure", if the TCotSCMSM cannot notify the new RA of the list of available PCAs			TCotSCMSM
SCMS-1050	SCMS POC OUT OF SCOPE	Error code: tcNotifyDCMFailure	The TCotSCMSM shall log "Error code: tcNotifyDCMFailure", if it cannot notify the DCM of a newly added RA.			TCotSCMSM
SCMS-1386	MANUAL PROCESS	Add component's certificate to GCCF	The TCotSCMSM shall forward required information to the Policy Generator in order to add the certificate of the newly created SCMS component to the Global Certificate Chain File (GCCF).	For a newly added component to be a valid SCMS component, its certificate must chain back to the SCMS root CA and its chain must be available to any other component via GCCF.	In the PoC, this will occur by a manual process.	TCotSCMSM
SCMS-1412	MANUAL PROCESS	Destroy certificate's private key	The certificate's private key shall be destroyed at the end of the "In-use" life of a certificate. The in-use lifetime of certificates shall be defined either by SCMS policy and/or based on the	To prevent the usage of certificates that have reached the end of defined In-use lifetime.	Out of scope as this needs to be implemented as operational policy.	CRL Store, CRLG, DCM, ECA, ICA, LA, MA, PCA, PG, RA

Key	Status	Summary	Description	Justification	Notes	Component/s
			expiration and In-use lifetime of subordinate certificates.			
SCMS-1581	SCMS POC OUT OF SCOPE	Component certificate in-use period	The SCMS component shall use its certificate for an in-use period of 3 years.	Use 3 years for standard SCMS components	Out of scope as this needs to be implemented as operational policy. This is for POC & CV-Pilot only.	CRLG, DCM, LA, MA, PG, RA
SCMS-1725	MANUAL PROCESS	Component certificate FQDN match	The SCMS component shall have a certificate with a certificateId field that matches the FQDN of the component.	FQDN of each component must match the official ID of the component.		CRLG, DCM, ECA, LA, MA, PCA, PG, RA
SCMS-1806	MANUAL PROCESS	Register non-central component with the central MA	The Local ICA Manager shall update the MA with the FQDN, TLS certificate, and SCMS certificate of any newly added PCA, LA, or RA.	The MA must know about all PCAs, LAs, and RAs in the system so that it can execute misbehavior investigations and revocation procedures.	In PoC, this will occur by a manual process. When a new PCA, LA, or RA is added, the local ICA manager will notify the TCotSCMSM about the newly added component (this is a manual process). The TCotSCMSM will then update the central MA with the necessary information about the newly added	TCotSCMSM

Key	Status	Summary	Description	Justification	Notes	Component/s
					component. It is expected (but not required) that a PCA, RA, and pair of LAs will typically be added as a complete set.	

12 issues

5.2.11.8.5 Step 11.1.2: Add Root CA

5.2.11.8.5.1 Goals

The goal is to define the procedures and requirements to add and manage root CA certificates in the SCMS.

5.2.11.8.5.2 Background and Strategic Fit

The SCMS root CA is the root of trust for all SCMS certificates and digital signatures. The root CA private key is stored in a high-integrity component that is accessed through offline messages and that are managed by the Technical Component of the SCMS Manager (TCotSCMSM). Adding a new root CA to the SCMS and distributing the CA's certificate is necessary to maintain the integrity of the SCMS certificate hierarchy when a previous root CA certificate expires or when a previous root CA is revoked or securely decommissioned.

There shall be only one active root CA in the SCMS at any time. Specifically, it is the responsibility of the TCotSCMSM to ensure that only one root CA can be used to sign new messages. However, the design allows SCMS components to continue to trust certificates signed by previous root CAs until their certificates expire. This mechanism allows older root CAs to be retired (i.e., cease to be used for signing new certificates) without invalidating or revoking all of the component certificates that they signed in the past. This use case describes the mechanism for introducing a new root CA to all SCMS components.

5.2.11.8.5.3 Procedure

Before a new root CA can be added to the SCMS, it must first be setup using the process defined in the Setup Root CA use case. The new root CA must then be endorsed by a quorum of existing electors and the signed root endorsement must be distributed to all SMCS components. The message will be distributed through inclusion in the Global Certificate Chain File (GCCF) and any local copies (LCCFs) that are created and distributed by an RA.

To implement this process, an authorized agent of the SCMS manager will perform the following actions:

1. In a secure environment, command the root CA to create a self-signed certificate. See the Setup Root CA use case for details on the certificate parameters.
2. Present the root CA certificate to all existing, valid SCMS electors and request that they produce a digitally signed copy of the certificate. The collection of all independent signatures from existing electors is then assembled into one root endorsement message with the sequence of elector signatures attached (note that each elector's signature contains a copy of the original message that was signed). The number of elector signatures must be greater than or equal to the value of 'quorum' defined in the current GPF. This is a manual process to be implemented by the TCotSCMSM.
3. The complete root endorsement message with signatures is then delivered to the PG for inclusion in future updates to the GCCF. Note that the PG signature is not

necessary for the root endorsement to be validated by SCMS components. The role of the PG in this case is to assemble updates to the GCCF with all active root endorsement messages included. The RAs will be required to include all root endorsement messages in any LCCF files that they derive from the GCCF.

4. SCMS components (including EEs) that receive a GCCF or LCCF with one or more root endorsement messages attached must check to see if they have already added the new root to their trust store. If they have not, they must validate the message by checking the attached signatures and confirming it has non-expired certificates for at least a 'quorum' of the existing electors that signed the message. Once the message is validated, the SCMS component must add the new root CA certificate to their trust store. When validating a message to add a root, an entity must check that the signed data is identical in each elector signature and that the 'type' element of the signed data has the value "addRoot."

5.2.11.8.5.4 Special Cases

The procedure described above is sufficient to establish a new root CA distribute its certificate to SCMS components. The following special considerations must be applied based on the reason for adding a new root.

- If the current root CA certificate is due to be retired, then the defined procedure is sufficient to distribute a new replacement root. The activation time for the new root should be set such that it does not overlap with the active life of the current root's useful life. The private key associated with the current root certificate shall be securely deleted or destroyed when the new root certificate becomes active. There is no need to remove the previous root certificate or to re-certify components.
- If the current root CA is to be securely decommissioned and replaced, the same procedure can be used as described for root certificate retirement. There is no need to remove the previous root certificate or to re-certify components.
- If the current root CA has been compromised or otherwise needs to be revoked, then the TCotSCMSM may follow the procedure described above with the activation time for the new root, set the current time, or the activation time, defined in the current root removal message. In addition, the TCotSCMSM must initiate the process of re-certifying all components in the SCMS with the new root CA. Specifically, the MA, CRGL, PG, and all ICAs that were certified with the previous root, must be re-certified. See the component "add" use cases for details on how to cascade the impact of re-certification throughout all other SCMS components.

5.2.11.8.5.5 Assumptions

- The SCMS Manager has the power to set policies for what conditions a new root CA must fulfill in order to be an accredited part of the system
- The root CA went through the setup process defined in Step 1.8: Setup Root CA
- Root Management is performed according to the elector scheme outlined in: Elector-based Root Management

- The Global Policy File (GPF) will define the current value for root management quorum, which is the minimum number of valid electors that need to endorse a root management message for it to be accepted by SCMS components. The value of quorum may be set independent of the current number of electors defined. (For the PoC, the value of quorum will be set to 2, meaning that a minimum of two elector signatures are needed for a root management command to take effect.)
- When the PG receives a valid "add root" message, it will continue to include that message on all future GCCF files that it produces until one of the following conditions occur:
    - The certificate of the root CA that is added in the message expires
    - The certificates of the endorsing electors expire resulting in fewer than 'quorum' valid signatures on the message
    - The value of 'quorum' is increased and distributed through an update to the GPF causing the "add elector" message to be invalid
    - The PG receives a valid "remove root" message that removes the endorsed root (effectively revoking the root that was added in the original message)
    - The PG receives a valid "remove elector" message that removes one of the endorsing electors reducing the number of valid electors to be less than the current value of quorum defined in the GPF, thereby rendering the message invalid

5.2.11.8.5.6 Requirements

Table 52 Use Case 11.1.2 Add Root CA - Requirements

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-178	MANUAL PROCESS	Add a Root	The TCotSCMSM shall access each of the Electors to sign an "Add Root CA" message for the new Root CA.	New Root CAs must be authenticated with multiple signatures.	In the PoC, a manual process will produce the “Add Root CA” message. In the PoC, n is set to 3, and m is set to 2. The add root message will be distributed to all SCMS components and EEs as part of the GCCF/LCCF files.	TCotSCMSM
SCMS-1024	CLOSED	Root CA Trust Store Messaging Processing	The SCMS Component shall be able to process the "Add Root CA" and "Revoke Root CA" messages, which will be signed by Electors, and shall ensure that the number of valid signatures is at least a quorum of non-revoked Electors in its trust store.	Every SCMS component will need to manage root CA updates automatically, so therefore, every SCMS component will need to be able to process Root Management messages signed by the Electors.	For the PoC, the number of Electors will be 3 and the number of Electors required to authorize any Root Management message will be 2. Elector signatures will be produced in a manual process for the PoC.	CRL Store, CRLG, DCM, ECA, IBLM, ICA, LA, MA, PCA, PG, RA
SCMS-1055	EE REQUIREMENT	EE verify "Add Root CA" message	The EE shall add the new root CA certificate to its trust store only after verifying the validity of the	A quorum of Electors must authorize a new root CA	This is out of scope as it defines EE behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
			"Add Root CA" message. The validation of this message shall be carried out securely in the EE's secure execution environment or HSM.			
SCMS-1094	CLOSED	Verify "Add Root CA" message	All SCMS Backend Components shall add the new root CA certificate to their trust stores only after verifying the validity of the "Add Root CA" message. The validation of this message shall be carried out securely in the component's HSM.	A quorum of Electors must authorize a new root CA		CRL Store, CRLG, DCM, ECA, IBLM, ICA, LA, MA, PCA, PG, RA
SCMS-1200	MANUAL PROCESS	Distribute "Add Root CA" messages	The Technical Component of the SCMS Manager (TCotSCMSM) shall communicate the multi-signed "Add Root CA" message to the Policy Generator to be included in a new Global Certificate Chain File (GCCF) which will be distributed to SCMS components and EEs to	SCMS components and EEs need to be aware of a newly added root CA. They get this information through an update to the Global Certificate Chain File (GCCF), respectively, the Local Certificate Chain File (LCCF) which contains a section for trust management messages		TCotSCMSM

Key	Status	Summary	Description	Justification	Notes	Component/s
			inform them of the new root CA.	(add a root or elector). The generation and distribution to the PG of this message is done manually whereas the distribution to other SCMS components and EEs is done automatically via GCCF/LCCF available at the RA.		
SCMS-1318	CLOSED	Root CA certificate validity	The root CA certificate validity period shall be set to 17 years.	Root CA certificates must have an expiration date. The root CA certificate must be valid at least as long as the longest issued enrollment certificate.	Certificate types and expiration periods are defined in the Certificate Types common requirements section. This is for PoC only.	RCA
SCMS-1332	MANUAL PROCESS	Root CA certificate overlap	Root CA certificates shall have an overlap of 9 years (an in-use period of 8 years).	The overlap is necessary to allow rollover.	This is for POC & CV-Pilot only.	RCA
SCMS-1409	CLOSED	Elector Trust Store Messaging Processing	The SCMS Component shall be able to process the "Add Elector" and "Revoke Elector" messages, which will be signed by Electors and shall ensure that the	Every SCMS component will need to manage Elector updates automatically, so therefore, every SCMS component will need to be	For the PoC, the number of Electors will be 3 and the number of Electors required to authorize any Root Management message will be 2. Elector signatures will	CRL Store, CRLG, DCM, ECA, IBLM, ICA, LA, MA, PCA, PG, RA

Key	Status	Summary	Description	Justification	Notes	Component/s
			number of valid signatures is at least a quorum of non-revoked Electors in its trust store.	able to process Root Management messages signed by the Electors.	be produced in a manual process for the PoC.	
SCMS-1422	SCMS POC OUT OF SCOPE	Renewal of component certificate	A SCMS component shall request rollover IEEE 1609.2 certificates no sooner than 3 months prior to the end of the In-use life of the current certificate. A SCMS component shall not issue rollover IEEE 1609.2 certificates prior 3 months to the end of the In-use life of the current certificate.	To prevent the existence of certificates that are not valid until a significant time in the future.	Does not apply to component compromise/revoked situations. For the PoC & CV-Pilot, 3 months is being used. This should be re-evaluated for other deployments.	CRL Store, CRLG, DCM, ECA, ICA, LA, MA, PCA, PG, RA, RCA

9 issues

5.2.11.8.5.7 Design

The detailed design for the elector-based root management process is described in the Elector-based Root Management section.

5.2.11.8.5.8 Diagrams

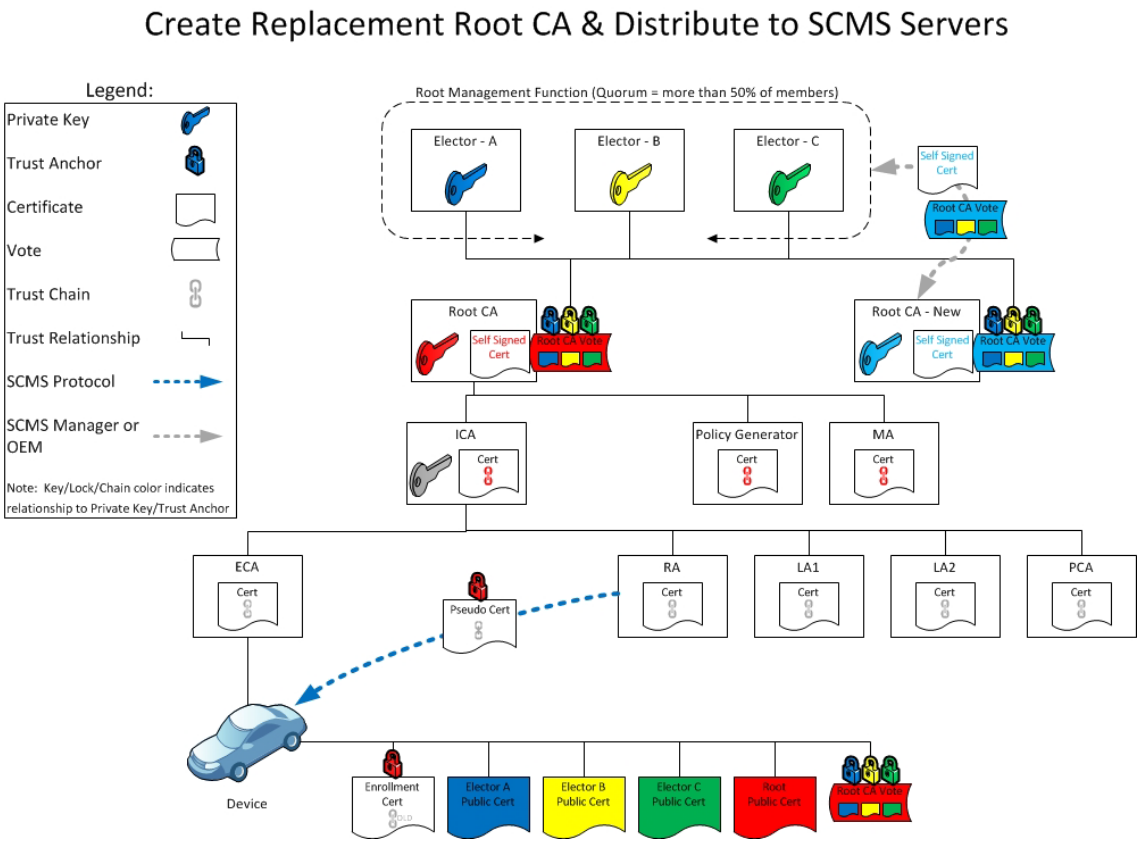


Figure 72 Create Replacement Root CA & Distribute to SCMS Servers

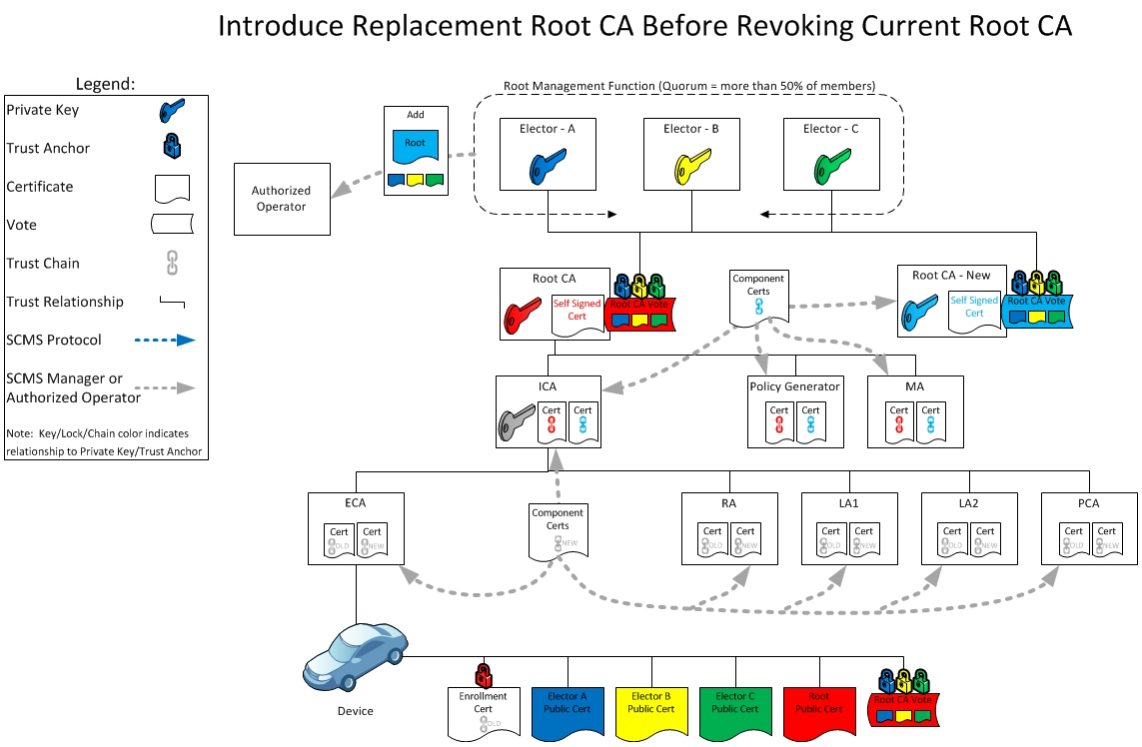


Figure 73 Introduce Replacement Root CA Before Revoking Current Root CA

5.2.11.8.6 Step 11.1.3: Add Elector

5.2.11.8.6.1 Goals

The goal is to define the procedures and requirements to add and manage root management electors in the SCMS.

5.2.11.8.6.2 Background and Strategic Fit

Electors are a collection of highly trusted backend components in the SCMS, which are used to certify root management messages. Specifically, a message that commands all SCMS components to add or remove a root CA certificate from their trust store will be trusted only if it is signed by a quorum of electors. The value of quorum is defined in the Global Policy File (GPF). Root management messages are distributed as part of the Global Certificate Chain File (GCCF) or a local copy of the chain file (an LCCF).

5.2.11.8.6.3 Procedure

Before a new elector can be added to the SCMS, it must first be setup using the process defined in the Setup Elector use case. The new elector must then be endorsed by a quorum of existing electors and the signed "add elector" message must be distributed to all SCMS components. The message will be distributed through inclusion in the Global Certificate Chain File (GCCF) and any local copies (LCCFs) that are created and distributed by an RA.

To implement this process, an authorized agent of the SCMS manager will perform the following actions:

1. Command the new elector to create a self-signed certificate of the new elector (the elector certificate is created in the Setup Elector use case) in a secure environment.
2. Present the new elector certificate to all existing, valid SCMS electors and request that they produce a digitally signed copy of the certificate. The collection of all independent signatures from existing electors is then assembled into one elector endorsement message with the sequence of existing elector signatures attached. The number of elector signatures must be greater than or equal to the value of 'quorum' defined in the current GPF. This is a manual process to be implemented by the TCotSCMSM.
3. Deliver the complete elector endorsement message with signatures to the PG for inclusion in future updates to the GCCF. Note that the PG signature is not necessary for the elector endorsement to be validated by SCMS components. The role of the PG in this case is to assemble updates to the GCCF with all active elector endorsement messages included. RAs will be required to include all elector endorsement messages in any LCCF files that they derive from the GCCF.

SCMS components (including EEs) that receive a GCCF or LCCF with one or more elector endorsement message attached must validate the message by checking the attached signatures and confirming it has non-expired certificates for at least a 'quorum' of the existing electors that signed the message. Once the message is validated, the SCMS component must add the new elector certificate to their trust store. When validating an elector endorsement message, an entity must check that the signed data is identical in each elector signature and that the ballotType element of the signed data has the value "addElector."

5.2.11.8.6.4 Assumptions

- An initial set of electors and self-signed elector certificates will be created as part of ceremony (or sequence of ceremonies) at the launch of an SCMS infrastructure. The SCMS Manager will define policies and procedures to ensure the integrity of this initial set of electors.
- Once an SCMS is in operation and the initial set of electors has been installed in all existing SCMS components, new electors may be added using the process defined here.
- The existing electors that sign an "add elector" message must have valid, non-expired SCMS certificates at the time when they sign the message. SCMS components that process an "add elector" message must confirm that the endorsing elector certificates are not expired at the time when the message is being processed. Once the message is validated, the SCMS components will add the new elector to their trust store and it will remain there even if one or more of the endorsing elector certificates expire. As long as that expiration happens after the message was validated and processed, the new elector remains trusted.

- When the PG receives a valid, "add elector" message, it will continue to include that message on all future GCCF files that it produces until one of the following conditions occur:
    - The certificate of the elector that is added in the message expires
    - The certificates of the endorsing electors expire resulting in fewer than 'quorum' valid signatures on the message
    - The value of 'quorum' is increased and distributed through an update to the GPF causing the "add elector" message to be invalid
    - The PG receives a "remove elector" message that removes the endorsed elector or removes the endorsing electors rendering the message invalid

5.2.11.8.6.5 Requirements

Table 53 Use Case 11.1.3: Add Elector - Requirements

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-1024	CLOSED	Root CA Trust Store Messaging Processing	The SCMS Component shall be able to process the "Add Root CA" and "Revoke Root CA" messages, which will be signed by Electors, and shall ensure that the number of valid signatures is at least a quorum of non-revoked Electors in its trust store.	Every SCMS component will need to manage root CA updates automatically, so therefore, every SCMS component will need to be able to process Root Management messages signed by the Electors.	For the PoC, the number of Electors will be 3 and the number of Electors required to authorize any Root Management message will be 2. Elector signatures will be produced in a manual process for the PoC.	CRL Store, CRLG, DCM, ECA, IBLM, ICA, LA, MA, PCA, PG, RA
SCMS-1380	MANUAL PROCESS	Distribute "Add Elector" message	The Technical Component of the SCMS Manager (TCotSCMSM) shall communicate the multi-signed "Add Elector" message to the Policy Generator to be included in a new Global Certificate Chain File (GCCF), which will be distributed to SCMS components and EEs to inform them of the new Elector.	SCMS components and EEs need to be aware of a newly added Elector. They get this information through an update to the Global Certificate Chain File (GCCF), respectively, the Local Certificate Chain File (LCCF), which contains a section for trust management messages (add a root or elector). The generation and distribution to the PG of this message is		TCotSCMSM

Key	Status	Summary	Description	Justification	Notes	Component/s
				done manually whereas the distribution to other SCMS components and EEs is done automatically via GCCF/LCCF.		
SCMS-1382	MANUAL PROCESS	Add an Elector	The TCotSCMSM, in cooperation with the new and existing Electors, shall produce an "Add Elector" message for the new Elector.	New Electors must be authenticated with signatures of a quorum of non revoked Electors.	In the PoC, this will message will be produced by a manual process. In the PoC, the number of electors is 3, and the quorum is set to 2.	TCotSCMSM
SCMS-1384	EE REQUIREMENT	EE verify "Add Elector" message	The EE shall add the new Elector certificate to its trust store only after verifying the validity of the "Add Elector" message. The validation of this message shall be carried out securely in the EE's secure execution environment or HSM.	A quorum of electors must authorize a new elector	This is out of scope as it defines EE behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1385	CLOSED	Verify "Add Elector" message	All SCMS Backend Components shall add the new Elector certificate to their trust stores only after verifying the validity of the	A quorum of Electors must authorize a new Elector		CRL Store, CRLG, DCM, ECA, IBLM, ICA, LA, MA, PCA, PG, RA

Key	Status	Summary	Description	Justification	Notes	Component/s
			"Add Elector" message. The validation of this message shall be carried out securely in the component's HSM.			
SCMS-1409	CLOSED	Elector Trust Store Messaging Processing	The SCMS Component shall be able to process the "Add Elector" and "Revoke Elector" messages, which will be signed by Electors and shall ensure that the number of valid signatures is at least a quorum of non-revoked Electors in its trust store.	Every SCMS component will need to manage Elector updates automatically, so therefore, every SCMS component will need to be able to process Root Management messages signed by the Electors.	For the PoC, the number of Electors will be 3 and the number of Electors required to authorize any Root Management message will be 2. Elector signatures will be produced in a manual process for the PoC.	CRL Store, CRLG, DCM, ECA, IBLM, ICA, LA, MA, PCA, PG, RA
SCMS-1414	MANUAL PROCESS	Added Elector endorses current Root CAs	The added Elector shall endorse all current root CAs by signing the existing "Add root CA" message.	To avoid a situation where a revoked Elector would enforce the revocation of an existing and valid root CA.		Elector
SCMS-1422	SCMS POC OUT OF SCOPE	Renewal of component certificate	A SCMS component shall request rollover IEEE 1609.2 certificates no sooner than 3 months prior to the end of the In-	To prevent the existence of certificates that are not valid until a significant time in the future.	Does not apply to component compromise/revoked situations. For the PoC & CV-Pilot, 3	CRL Store, CRLG, DCM, ECA, ICA, LA, MA, PCA, PG, RA, RCA

Key	Status	Summary	Description	Justification	Notes	Component/s
			use life of the current certificate. A SCMS component shall not issue rollover IEEE 1609.2 certificates prior 3 months to the end of the In-use life of the current certificate.		months is being used. This should be re-evaluated for other deployments.	
SCMS-1423	MANUAL PROCESS	Elector Certificate Expiration	The Technical Component of the SCMS Manager (TCotSCMSM) shall issue Elector certificates with an expiration of 12 years.	Component 1609 certificates shall have a defined expiration.	In the case of the certificate being revoked, the new certificate may have a different expiration to align with predefined replacement schedules (if any exist). For the initial system deployment, 1 of the 3 Electors shall have a certificate expiration of 4 years, another one a certificate expiration of 8 years, to prevent multiple elector certificates from expiring at the same time. These durations are for the SCMS PoC and CV-Pilot only. For other SCMS instances, this duration should be reevaluated.	Elector

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-1590	SCMS POC OUT OF SCOPE	Elector Certificate In-Use period	The Elector certificate In-Use period shall be the same as the Expiration period.	Out of scope as this needs to be implemented as operational policy. To maintain a fixed number of valid Elector at all times.		Elector
SCMS-1809	CLOSED	Elector certificate validity	Elector certificates validity period shall be set to 12 years.	Elector certificates must have an expiration date.	Certificate types and expiration periods are defined in the Certificate Types common requirements section. This is for PoC and CV-Pilot only.	Elector

11 issues

5.2.11.8.6.6 Design

The detailed design for the elector-based, root management process is described in the Elector-based Root Management section.

5.2.11.9 Step 11.2: Revoke SCMS Component

5.2.11.9.1 Goals

Revoke procedure for each SCMS component.

5.2.11.9.2 Assumptions

- As the SCMS system evolves, it will become necessary that components be revoked in the case of compromise or obsolescence
- Actual requirements will be outlined in subsections

5.2.11.9.3 CRL Series

This is the CRL series diagram for POC / Pilot Deployments.

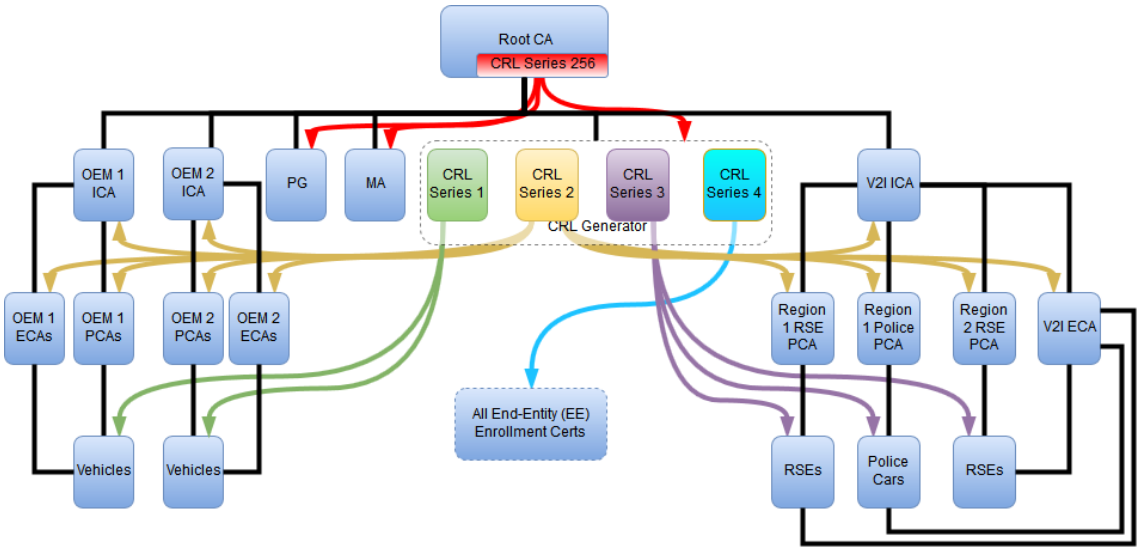


Figure 74 CRL Series Diagram

5.2.11.9.4 Step 11.2.1: Revoke non-Root SCMS Component

5.2.11.9.4.1 Goals

- Provide a mechanism for revoking an SCMS component other than root CA.
- Define procedures to enable continued SCMS operations after the revocation.

5.2.11.9.4.2 Assumptions

- The technical component of the SCMS Manager will coordinate the revocation of SCMS components to enable continued operations.

- When an SCMS component is revoked, the function that it provided will be taken over by a peer device with sufficient privileges and capabilities to continue operations. The peer device may be a pre-existing device that is taking on additional work or a newly added (i.e., replacement) device.
- This use case specifies the requirements that are common among all non-root SCMS component revocations. Individual use cases will provide specific details that are unique to each component type.

5.2.11.9.4.3 Requirements

Table 54 Requirements

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-314	CLOSED	Revocation of a Non-Root SCMS component	Root CA and CRL Generator (CRLG) shall revoke non-root SCMS components.	SCMS components that are compromised should not be trusted for operation and are revoked starting at time T, not simply removed.	Revocation of a component at a time T dictates that from this time onward all certificate chains that chain back to this component are to not be trusted. Root CA revokes PG, MA, and CRLG. CRLG revokes ICA, PCA, RA, and EE. All CRLs are available by CRLG, and CRLG shall provide the SCMS components CRL upon request.	CRLG, RCA
SCMS-772	MANUAL PROCESS	Standing up a SCMS component replacing the revoked component	The Technical Component of the SCMS Manager shall issue a replacement component certificate to the revoked certificate, if the revoked certificate belongs to a central component.	Upon revoking a component, a replacement component is needed to carry on its tasks and responsibilities.	This could be a new component or an existing one that will carry on the same tasks and responsibilities of the revoked component. In the PoC, this will occur by a manual process.	TCotSCMSM
SCMS-859	CLOSED	All relevant components cease to trust	All SCMS components receiving and validating a CRL shall remove all revoked component	The relevant components should not use the revoked component's certificate to trust it. If their chains include	Particularly, in the case of LA revocation, the RA needs to be informed in order to stop requesting encrypted PLVs from	CRL Store, CRLG, DCM, ECA, IBLM, ICA,

Key	Status	Summary	Description	Justification	Notes	Component/s
		the revoked component	certificates from their trust store. All cached certificate chains that roll up to a revoked component shall be removed.	the revoked component, they should receive new certificate chains.	the revoked LA. The MA needs to be informed in order to stop requesting linkage information (i.e., for misbehavior detection) from the revoked LA. In the case of RA revocation, the LAs need to be informed in order to stop sending encrypted PLVs to the revoked RA. All SCMS components and EEs receiving the component CRL shall mark the revoked component certificates as untrusted immediately: • In sending requests to that component • In trusting certificate chains chaining to that component's certificate • In trusting messages signed using this component's certificate	LA, MA, PCA, PG, RA
SCMS-1379	CLOSED	Provide x.509 SCMS	The Technical Component of the SCMS shall provide an OCSP service that	to ensure that SCMS components do not establish communication to other		TCotSCMSM

Key	Status	Summary	Description	Justification	Notes	Component/s
		component OCSP stapling	supports stapling for x.509 SCMS component certificates with a validity of 24 hours.	SCMS components that are revoked.		
SCMS-1387	MANUAL PROCESS	Remove revoked certificates from GCCF	The Technical Component of the SCMS Manager shall interact with the Policy Generator to remove the certificate of the revoked component and all its certificate chains from the Global Certificate Chain File.	Revoked certificates get invalid and therefore their certificate chains as well. They should not be available anymore via GCCF in order to save computational power during validation and bandwidth during transfer of the GCCF.		TCotSCMSM
SCMS-1598	CLOSED	Regenerate CRL	MA shall regenerate the CRL from internal data, if the CRLG is revoked.	Because the old CRL cannot be trusted anymore if CRLG is revoked.	Older versions of the CRL signed by the revoked CRLG would be discarded.	MA
SCMS-2461	CLOSED	SCMS components regularly pull SCMS component CRL	The SCMS component shall download the SCMS component CRL from CRLG regularly, at an interval of at least every 60 minutes	To ensure that revoked SCMS components are excluded from the system within a short time period.		DCM, ECA, LA, MA, PCA, PG, RA

7 issues

5.2.11.9.4.4 Step 11.2.1 - Revoke CRLG

5.2.11.9.4.4.1 Goals

The goal is to revoke a CRLG certificate from the SCMS System.

5.2.11.9.4.4.2 Background and Strategic Fit

A CRL Generator (CRLG) can only be revoked by a root CA. In a situation where a CRLG has been compromised or has failed, the TCotSCMSM must activate a root CA and use it to sign a Series 256 CRL listing the compromised CRLG as revoked. This file must then be copied to the CRL Store for distribution to all components.

On receipt of a CRL signed by a root CA and listing a CRLG as revoked, the CRL Store must create a new composite CRL that contains:

1. All non-expired, Elector-signed, root-management messages
2. The new root CA signed CRL listing a CRLG as revoked
3. Any other non-expired root CA signed CRLs
4. Any CRLs signed by other, no-revoked, non-expired CRLGs

This new composite CRL shall be distributed to all components.

The MA shall no longer the use revoked CRLG to sign CRLs (the procedure for adding a new CRLG will update the MA with the address and TLS certificate of the new CRLG).

5.2.11.9.4.4.3 Assumptions

- In the SCMS design, there may be more than one CRLG. However, for the Proof of Concept (PoC) deployment, there will be a single, central CRLG.
- The SCMS requires a valid CRLG in order to sustain operation. If the only active CRLG is revoked, the TCotSCMSM must initiate the process of adding a new CRLG (or re-certifying the existing CRLG) using the procedure described in the Add CRLG use case.
- After receipt of the new CRL signed by a root CA listing a CRLG as revoked, all components and EE shall cease to process any CRL signed by the revoked CRLG.
- Components will have no reliable way to know the sequence in which valid or fraudulent revocation messages were created. Therefore, there is no effective way to "un-revoke" components previously placed on the CRL by a compromised CRLG. All previously revoked components will need to be re-certified with new certificates in order to restore trust.
- The procedure for interacting with the CRL Store and assembling a new composite CRL is implementation specific. There are no standard SCMS messages or procedures for performing this function.

5.2.11.9.4.4.4 Requirements

Table 55 Use Case 11.2.1 Revoke CRLG - Requirements

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-772	MANUAL PROCESS	Standing up a SCMS component replacing the revoked component	The Technical Component of the SCMS Manager shall issue a replacement component certificate to the revoked certificate, if the revoked certificate belongs to a central component.	Upon revoking a component, a replacement component is needed to carry on its tasks and responsibilities.	This could be a new component or an existing one that will carry on the same tasks and responsibilities of the revoked component. In the PoC, this will occur by a manual process.	TCotSCMSM
SCMS-859	CLOSED	All relevant components cease to trust the revoked component	All SCMS components receiving and validating a CRL shall remove all revoked component certificates from their trust store. All cached certificate chains that roll up to a revoked component shall be removed.	The relevant components should not use the revoked component's certificate to trust it. If their chains include the revoked component, they should receive new certificate chains.	Particularly, in the case of LA revocation, the RA needs to be informed in order to stop requesting encrypted PLVs from the revoked LA. The MA needs to be informed in order to stop requesting linkage information (i.e., for misbehavior detection) from the revoked LA. In the case of RA revocation, the LAs need to be informed in order to stop sending encrypted PLVs to the revoked RA. All SCMS components and EEs receiving the component	CRL Store, CRLG, DCM, ECA, IBLM, ICA, LA, MA, PCA, PG, RA

Key	Status	Summary	Description	Justification	Notes	Component/s
					CRL shall mark the revoked component certificates as untrusted immediately: • In sending requests to that component • In trusting certificate chains chaining to that component's certificate • In trusting messages signed using this component's certificate	
SCMS-1598	CLOSED	Regenerate CRL	MA shall regenerate the CRL from internal data, if the CRLG is revoked.	Because the old CRL cannot be trusted anymore if CRLG is revoked.	Older versions of the CRL signed by the revoked CRLG would be discarded.	MA
SCMS-1606	EE REQUIREMENT	EE shall store ValidityPeriod.start of last valid CRLG Certificate	The EE shall store the ValidityPeriod.start value of the last CRLG Certificate that passes validation.	In order to prevent the following attack sequence: 1) A CRLG Certificate is compromised by attacker 2) A new valid CRLG Certificate is used to sign a CRL revoking the compromised CRLG		On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
				certificate 3) The CRL Store makes the new valid CRL available for download 4) The attacker downloads the new valid CRL 5) Attacker creates a fraudulent CRL signed by the compromised certificate which revokes the new CRLG certificate 6) Attacker distributes the new fraudulent CRL via collaborative distribution before all devices have downloaded the new valid CRL 7) Repeat steps 2-6		
SCMS-1607	EE REQUIREMENT	EE shall check CRLG Certificate Validity.start time	Upon receiving a new CRL, the EE shall reject the CRL and CRLG Certificate if the ValidityPeriod.start value of the CRLG certificate used to sign the newly received CRL is	In order to prevent the following attack sequence: 1) A CRLG Certificate is compromised by attacker		On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
			chronologically earlier then the stored ValidityPeriod.start value of the previously received valid CRLG Certificate.	2) A new valid CRLG Certificate is used to sign a CRL revoking the compromised CRLG certificate 3) The CRL Store makes the new valid CRL available for download 4) The attacker downloads the new valid CRL 5) Attacker creates a fraudulent CRL signed by the compromised certificate which revokes the new CRLG certificate 6) Attacker distributes the new fraudulent CRL via collaborative distribution before all devices have downloaded the new valid CRL 7) Repeat steps 2-6		

5 issues

5.2.11.9.4.5 Step 11.2.1 - Revoke ECA

5.2.11.9.4.5.1 Goals

The goal is to revoke an ECA certificate from the SCMS System.

5.2.11.9.4.5.2 Background and Strategic Fit

The technical component of the SCMS Manager (or a local ICA Manager in cooperation with the TCotSCMSM) determines that an Enrollment Certificate Authority (ECA) needs to be revoked. It contacts the CRLG and instructs it to add the ECA certificate to the CRL.

All components and entities that receive the updated CRL will cease to trust any enrollment certificate issued by the ECA and stop communicating with the ECA. All end-entity devices whose enrollment certificate chains back to the revoked ECA should obtain a new enrollment certificate as soon as possible (the SCMS Manager may set performance requirements for how quickly this must happen).

5.2.11.9.4.5.3 Procedure

- The local ICA Manager responsible for the revoked ECA must contact all DCMs that are configured to use the revoked component and remove it from their list of trusted ECAs for use in generating enrollment certificates. The ICA manager might reconfigure the DCMs to use a different ECA or stand up a new ECA following the procedures defined in the Add ECA use case.
- The ICA manager must also inform the RA that has the impacted ECA in its list of trusted ECAs and inform it to remove the revoked component. The RA will cease to pre-generate pseudonym certificates for any EE enrolled by that ECA and cease to accept any new requests from EEs certified by that ECA.
- EEs must have a proprietary mechanism to re-enroll in order to recover from the revocation of the ECA that signed their enrollment certificate. Once they are re-enrolled and associated with an RA, each impacted EE will have to request new pseudonym, application, or identification certificates.

5.2.11.9.4.5.4 Assumptions

- Authorized managers of EEs must provide a trusted (and certified by an agent of the SCMS Manager) method for re-enrolling EEs under their jurisdiction that are impacted by a revoked ECA
- A compromised DCM will require that all ECAs that were used with that DCM shall be revoked. All local ICA Managers will be required to record which ECAs were used in issuing enrollment certificates for every DCM.
- The procedure requires that all DCMs provide a proprietary mechanism (i.e., there are no SCMS messages defined for this step) to remove a revoked ECA from the list of ECAs that they use for enrolling new EEs. Note that a DCM should remove by default an ECA from the list of components that they use upon receipt of the updated CRL listing the ECA as revoked. However, the proprietary mechanism

described in the use case assumes that ICA Managers will want a mechanism to remove pro-actively a revoked ECA.

- The procedure requires that all RAs provide a proprietary mechanism (i.e., there are no SCMS messages defined for this step) to remove a revoked ECA from the list of ECAs whose enrollment certificates they will trust. All RAs shall remove by default an ECA from the list of components that they trust as soon as they receive the updated CRL listing the ECA as revoked. However, the proprietary mechanism described in the use case assumes that ICA Managers will want a mechanism to remove pro-actively a revoked ECA.

5.2.11.9.4.5.5 Requirements

Table 56 Use Case 11.2.1 Revoke ECA - Requirements

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-771	MANUAL PROCESS	Invoke Revocation of non-Root SCMS component	The Technical Component of the SCMS Manager shall interact with the CRLG to list the certificate of the component to be revoked in the components CRL and have the CRLG sign it.	An authenticated message from the SCMS Manager is required to revoke a component.	In the PoC, this will occur by a manual process.	TCotSCMSM
SCMS-772	MANUAL PROCESS	Standing up a SCMS component replacing the revoked component	The Technical Component of the SCMS Manager shall issue a replacement component certificate to the revoked certificate, if the revoked certificate belongs to a central component.	Upon revoking a component, a replacement component is needed to carry on its tasks and responsibilities.	This could be a new component or an existing one that will carry on the same tasks and responsibilities of the revoked component. In the PoC, this will occur by a manual process.	TCotSCMSM
SCMS-859	CLOSED	All relevant components cease to trust the revoked component	All SCMS components receiving and validating a CRL shall remove all revoked component certificates from their trust store. All cached certificate chains that roll up	The relevant components should not use the revoked component's certificate to trust it. If their chains include the revoked component, they should receive new certificate chains.	Particularly, in the case of LA revocation, the RA needs to be informed in order to stop requesting	CRL Store, CRLG, DCM, ECA, IBLM, ICA, LA, MA, PCA, PG, RA

Key	Status	Summary	Description	Justification	Notes	Component/s
			to a revoked component shall be removed.		encrypted PLVs from the revoked LA. The MA needs to be informed in order to stop requesting linkage information (i.e., for misbehavior detection) from the revoked LA. In the case of RA revocation, the LAs need to be informed in order to stop sending encrypted PLVs to the revoked RA. All SCMS components and EEs receiving the component CRL shall mark the revoked component certificates as untrusted immediately:	

Key	Status	Summary	Description	Justification	Notes	Component/s
					• In sending requests to that component • In trusting certificate chains chaining to that component's certificate • In trusting messages signed using this component's certificate	
SCMS-1387	MANUAL PROCESS	Remove revoked certificates from GCCF	The Technical Component of the SCMS Manager shall interact with the Policy Generator to remove the certificate of the revoked component and all its certificate chains from the Global Certificate Chain File.	Revoked certificates get invalid and therefore their certificate chains as well. They should not be available anymore via GCCF in order to save computational power during validation and bandwidth during transfer of the GCCF.		TCotSCMSM

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-1587	EE REQUIREMENT	EE shall cease to trust the revoked CA	EEs receiving and validating a CRL shall remove all revoked CA certificates from their trust store, remove all cached certificate chains that roll up to the revoked CA, and stop sending immediately in case EE's enrollment, pseudonym, application, or identification certificate chains up to the revoked CA.	EE should not use the revoked component's certificate to trust it. If it chains include the revoked component, they need to receive new certificates with a new certificate chain.	EEs receiving the component CRL shall mark the revoked component certificates as untrusted immediately: • In sending requests to that component • In trusting certificate chains chaining to that component's certificate • In trusting messages signed using this component's certificate • In sending messages signed with certificates that	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
					chain up to this component's certificate This is out of scope as it defines EE behavior.	
SCMS-1589	EE REQUIREMENT	EE receive new enrollment certificate after CA revocation	EE shall get back to the secure environment used during their bootstrapping process and be re-bootstrapped after its RCA, ICA or ECA was revoked.	EE should not use the revoked CA's certificate and all certificates that chain up to that CA certificate to trust it or to use it in communication. That includes enrollment certificates that chain up to the revoked CA certificate.		On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1593	EE REQUIREMENT	EE receive new pseudonym/application/identification certificates after CA revocation	EE shall request new pseudonym, application, or identification certificates after it was re-bootstrapped due to revocation of its RCA, ICA, or ECA.	EE should not use the revoked CA's certificate and all certificates that chain up to that CA certificate to trust it or to use it in communication. That includes its own pseudonym/application/identification certificates that chain up to the revoked CA certificate.		On-board Equipment (OBE), Road-side Equipment (RSE)

7 issues

5.2.11.9.4.6 Step 11.2.1 - Revoke ICA

5.2.11.9.4.6.1 Goals

The goal is to revoke an ICA certificate from the SCMS System.

5.2.11.9.4.6.2 Background and Strategic Fit

The Technical Component of the SCMS Manager (TCotSCMSM), a local ICA Manager, or the Misbehavior Authority, determines that an Intermediate Certificate Authority (ICA) needs to be revoked. The TCotSCMSM contacts the appropriate CRLG (as indicated in the ICA certificate, see the CRL Series Diagram for details) and adds the impacted ICA to the CRL. On receiving and validating the new CRL, all components will cease to trust the ICA and any certificates that chain back to the ICA.

Impacted components may include ECA, RA, PCA, LA and any EEs enrolled through an impacted ECA. All end-entity devices (EE) whose enrollment or application certificates chain back to the revoked ICA should obtain new enrollment or application certificates as soon as possible (the SCMS Manager may set performance requirements for how quickly this must happen). The SCMS will provide re-enrollment processes at a later stage.

All EEs whose pseudonym, application, or identification certificates chain back to the impacted ICA will cease to use those certificates. They shall request new certificates.

The TCotSCMSM will inform the Policy Generator (PG) to update the GCCF and remove all component certificates that chain back to the revoked ICA. The new GCCF will be distributed to all un-revoked RAs, which will incorporate the new lists in the next LCCF that they issue.

5.2.11.9.4.6.3 Assumptions

- The local ICA Manager will coordinate with the TCotSCMSM when revoking an ICA
- If the MA determines that an ICA shall be revoked, it will notify the TCotSCMSM. This will not be an automated process.
- The TCotSCMSM will inform the local ICA Manager when revoking an ICA

5.2.11.9.4.6.4 Requirements

Table 57 Use Case 11.2.1 Revoke ICA - Requirements

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-771	MANUAL PROCESS	Invoke Revocation of non-Root SCMS component	The Technical Component of the SCMS Manager shall interact with the CRLG to list the certificate of the component to be revoked in the components CRL and have the CRLG sign it.	An authenticated message from the SCMS Manager is required to revoke a component.	In the PoC, this will occur by a manual process.	TCotSCMSM
SCMS-772	MANUAL PROCESS	Standing up a SCMS component replacing the revoked component	The Technical Component of the SCMS Manager shall issue a replacement component certificate to the revoked certificate, if the revoked certificate belongs to a central component.	Upon revoking a component, a replacement component is needed to carry on its tasks and responsibilities.	This could be a new component or an existing one that will carry on the same tasks and responsibilities of the revoked component. In the PoC, this will occur by a manual process.	TCotSCMSM
SCMS-859	CLOSED	All relevant components cease to trust the revoked component	All SCMS components receiving and validating a CRL shall remove all revoked component certificates from their trust store. All cached certificate chains that roll up to a revoked component shall be removed.	The relevant components should not use the revoked component's certificate to trust it. If their chains include the revoked component, they should receive new certificate chains.	Particularly, in the case of LA revocation, the RA needs to be informed in order to stop requesting encrypted PLVs from the revoked LA. The MA needs to be informed in order to stop requesting linkage information (i.e., for misbehavior detection) from the revoked LA.	CRL Store, CRLG, DCM, ECA, IBLM, ICA, LA, MA, PCA, PG, RA

Key	Status	Summary	Description	Justification	Notes	Component/s
					In the case of RA revocation, the LAs need to be informed in order to stop sending encrypted PLVs to the revoked RA. All SCMS components and EEs receiving the component CRL shall mark the revoked component certificates as untrusted immediately: • In sending requests to that component • In trusting certificate chains chaining to that component's certificate • In trusting messages signed using this component's certificate	
SCMS-1387	MANUAL PROCESS	Remove revoked certificates from GCCF	The Technical Component of the SCMS Manager shall interact with the Policy Generator to remove the certificate of the revoked component and all its certificate chains from the Global Certificate Chain File.	Revoked certificates get invalid and therefore their certificate chains as well. They should not be available anymore via GCCF in order to save computational power during		TCotSCMSM

Key	Status	Summary	Description	Justification	Notes	Component/s
				validation and bandwidth during transfer of the GCCF.		
SCMS-1587	EE REQUIREMENT	EE shall cease to trust the revoked CA	EEs receiving and validating a CRL shall remove all revoked CA certificates from their trust store, remove all cached certificate chains that roll up to the revoked CA, and stop sending immediately in case EE's enrollment, pseudonym, application, or identification certificate chains up to the revoked CA.	EE should not use the revoked component's certificate to trust it. If it chains include the revoked component, they need to receive new certificates with a new certificate chain.	EEs receiving the component CRL shall mark the revoked component certificates as untrusted immediately: • In sending requests to that component • In trusting certificate chains chaining to that component's certificate • In trusting messages signed using this component's certificate • In sending messages signed with certificates that chain up to this component's certificate This is out of scope as it defines EE behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1589	EE REQUIREMENT	EE receive new enrollment certificate after CA revocation	EE shall get back to the secure environment used during their bootstrapping process and be re-	EE should not use the revoked CA's certificate and all certificates that chain up to that CA certificate to trust it or to		On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
			bootstrapped after its RCA, ICA or ECA was revoked.	use it in communication. That includes enrollment certificates that chain up to the revoked CA certificate.		
SCMS-1593	EE REQUIREMENT	EE receive new pseudonym/application/identification certificates after CA revocation	EE shall request new pseudonym, application, or identification certificates after it was re-bootstrapped due to revocation of its RCA, ICA, or ECA.	EE should not use the revoked CA's certificate and all certificates that chain up to that CA certificate to trust it or to use it in communication. That includes its own pseudonym/application/identification certificates that chain up to the revoked CA certificate.		On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1608	EE REQUIREMENT	EE receive new pseudonym/application/identification certificates after PCA revocation	EE shall request new pseudonym, application, or identification certificates whenever it's certificates chain up to a PCA certificate that is invalidated due to a RCA, ICA, or PCA revocation.	EE should not use the revoked CA's certificate and all certificates that chain up to that CA certificate to trust it or to use it in communication. That includes its own pseudonym/application/identification certificates that chain up to the revoked CA certificate.	EEs receiving the component CRL shall mark the revoked component certificates as untrusted immediately: • In sending requests to that component • In trusting certificate chains chaining to that component's certificate • In trusting messages signed using this component's certificate	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
					• In sending messages signed with certificates that chain up to this component's certificate This is out of scope as it defines EE behavior.	

8 issues

5.2.11.9.4.7 Step 11.2.1 - Revoke MA

5.2.11.9.4.7.1 Goals

The goal is to revoke an MA certificate from the SCMS System.

5.2.11.9.4.7.2 Background and Strategic Fit

The Technical Component of the SCMS Manager (TCotSCMSM) determines that the Misbehavior Authority (MA) needs to be revoked. It will request that the CRLG add the MA certificate to CRL and immediately issue a new CRL. The CRLG will cease to accept new requests signed by the MA. On receipt of the new CRL, all PCAs, RAs, and LAs will cease to accept new requests signed by the revoked MA.

The TCotSCMSM activates the replacement MA as described in Step 11.1.1 - Add MA.

5.2.11.9.4.7.3 Assumptions

The TCotSCMSM will recover information on any active investigations underway when the MA was revoked. Trusted data will be copied to a replacement MA and those investigations will continue.

5.2.11.9.4.7.4 Requirements

Table 58 Use Case 11.2.1 Revoke MA - Requirements

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-771	MANUAL PROCESS	Invoke Revocation of non-Root SCMS component	The Technical Component of the SCMS Manager shall interact with the CRLG to list the certificate of the component to be revoked in the components CRL and have the CRLG sign it.	An authenticated message from the SCMS Manager is required to revoke a component.	In the PoC, this will occur by a manual process.	TCotSCMSM
SCMS-772	MANUAL PROCESS	Standing up a SCMS component replacing the revoked component	The Technical Component of the SCMS Manager shall issue a replacement component certificate to the revoked certificate, if the revoked certificate belongs to a central component.	Upon revoking a component, a replacement component is needed to carry on its tasks and responsibilities.	This could be a new component or an existing one that will carry on the same tasks and responsibilities of the revoked component. In the PoC, this will occur by a manual process.	TCotSCMSM
SCMS-859	CLOSED	All relevant components cease to trust the revoked component	All SCMS components receiving and validating a CRL shall remove all revoked component certificates from their trust store. All cached	The relevant components should not use the revoked component's certificate to trust it. If their chains include the revoked component, they	Particularly, in the case of LA revocation, the RA needs to be informed in order to stop requesting encrypted PLVs from the revoked LA. The MA needs to be	CRL Store, CRLG, DCM, ECA, IBLM, ICA, LA, MA, PCA, PG, RA

Key	Status	Summary	Description	Justification	Notes	Component/s
			certificate chains that roll up to a revoked component shall be removed.	should receive new certificate chains.	informed in order to stop requesting linkage information (i.e., for misbehavior detection) from the revoked LA. In the case of RA revocation, the LAs need to be informed in order to stop sending encrypted PLVs to the revoked RA. All SCMS components and EEs receiving the component CRL shall mark the revoked component certificates as untrusted immediately: • In sending requests to that component • In trusting certificate chains chaining to that component's certificate • In trusting messages signed using this component's certificate	

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-1387	MANUAL PROCESS	Remove revoked certificates from GCCF	The Technical Component of the SCMS Manager shall interact with the Policy Generator to remove the certificate of the revoked component and all its certificate chains from the Global Certificate Chain File.	Revoked certificates get invalid and therefore their certificate chains as well. They should not be available anymore via GCCF in order to save computational power during validation and bandwidth during transfer of the GCCF.		TCotSCMSM

4 issues

5.2.11.9.4.8 Step 11.2.1 - Revoke PCA

5.2.11.9.4.8.1 Goals

The goal is to revoke a PCA certificate from the SCMS System.

5.2.11.9.4.8.2 Background and Strategic Fit

The Technical Component of the SCMS Manager (or a local ICA Manager) determines that a Pseudonym Certificate Authority (PCA) needs to be revoked.

5.2.11.9.4.8.3 Procedure

- The TCotSCMSM contacts the CRLG and adds the certificate of the impacted PCA to the CRL. On receipt of the new CRL, all components will cease to trust pseudonym certificates issued by the PCA.
- The local ICA Manager will contact any RA that was configured to use the impacted PCA and instruct it to send new pseudonym certificate requests to a different PCA or it will stand up a new PCA (see the Add PCA use case).
- The LAs that share a secret key with the impacted PCA will delete the shared key and await configuration information from the local ICA Manager to establish a key with a new PCA.
- All end-entity devices whose pseudonym certificates were signed by the revoked PCA should obtain a new batch of pseudonym certificates as soon as possible (the SCMS Manager may set performance requirements for how quickly this must happen). If they have certificates from other non-revoked PCAs for the current time period, they may continue to operate using those certificates until a replacement batch can be downloaded.

5.2.11.9.4.8.4 Assumptions

- All RAs will destroy any stored batches of pseudonym certificates proactively generated by the impacted PCA
- Any misbehavior investigations that relied on the PCA will be stopped

5.2.11.9.4.8.5 Requirements

Table 59 Use Case 11.2. Revoke PCA - Requirements

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-358	EE REQUIREMENT	Discard Certificate Batches Signed by a Revoked PCA	OBE shall discard all pseudonym certificates that were issued by a PCA upon validating that this PCA has been revoked.	PCA generates batches of pseudonym certificates and an OBE device cannot know when the pseudonym certificates were signed, therefore all such certificates from the revoked PCA must be untrusted even if the PCA's certificate was verified previously.	This is out of scope as it defines OBE behavior.	On-board Equipment (OBE)
SCMS-771	MANUAL PROCESS	Invoke Revocation of non-Root SCMS component	The Technical Component of the SCMS Manager shall interact with the CRLG to list the certificate of the component to be revoked in the components CRL and have the CRLG sign it.	An authenticated message from the SCMS Manager is required to revoke a component.	In the PoC, this will occur by a manual process.	TCotSCMSM
SCMS-772	MANUAL PROCESS	Standing up a SCMS component replacing the revoked component	The Technical Component of the SCMS Manager shall issue a replacement component certificate to the revoked certificate, if the revoked certificate belongs to a central component.	Upon revoking a component, a replacement component is needed to carry on its tasks and responsibilities.	This could be a new component or an existing one that will carry on the same tasks and responsibilities of the revoked component. In the PoC, this will	TCotSCMSM

Key	Status	Summary	Description	Justification	Notes	Component/s
					occur by a manual process.	
SCMS-859	CLOSED	All relevant components cease to trust the revoked component	All SCMS components receiving and validating a CRL shall remove all revoked component certificates from their trust store. All cached certificate chains that roll up to a revoked component shall be removed.	The relevant components should not use the revoked component's certificate to trust it. If their chains include the revoked component, they should receive new certificate chains.	Particularly, in the case of LA revocation, the RA needs to be informed in order to stop requesting encrypted PLVs from the revoked LA. The MA needs to be informed in order to stop requesting linkage information (i.e., for misbehavior detection) from the revoked LA. In the case of RA revocation, the LAs need to be informed in order to stop sending encrypted PLVs to the revoked RA. All SCMS components and EEs receiving the	CRL Store, CRLG, DCM, ECA, IBLM, ICA, LA, MA, PCA, PG, RA

Key	Status	Summary	Description	Justification	Notes	Component/s
					component CRL shall mark the revoked component certificates as untrusted immediately: • In sending requests to that component • In trusting certificate chains chaining to that component's certificate • In trusting messages signed using this component's certificate	
SCMS-1387	MANUAL PROCESS	Remove revoked certificates from GCCF	The Technical Component of the SCMS Manager shall interact with the Policy Generator to remove the certificate of the revoked component and all its certificate chains from the Global Certificate Chain File.	Revoked certificates get invalid and therefore their certificate chains as well. They should not be available anymore via GCCF in order to save computational power during validation and		TCotSCMSM

Key	Status	Summary	Description	Justification	Notes	Component/s
				bandwidth during transfer of the GCCF.		
SCMS-1587	EE REQUIREMENT	EE shall cease to trust the revoked CA	EEs receiving and validating a CRL shall remove all revoked CA certificates from their trust store, remove all cached certificate chains that roll up to the revoked CA, and stop sending immediately in case EE's enrollment, pseudonym, application, or identification certificate chains up to the revoked CA.	EE should not use the revoked component's certificate to trust it. If it chains include the revoked component, they need to receive new certificates with a new certificate chain.	EEs receiving the component CRL shall mark the revoked component certificates as untrusted immediately: • In sending requests to that component • In trusting certificate chains chaining to that component's certificate • In trusting messages signed using this component's certificate • In sending messages signed with certificates	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
					that chain up to this component's certificate This is out of scope as it defines EE behavior.	
SCMS-1608	EE REQUIREMENT	EE receive new pseudonym/application/identification certificates after PCA revocation	EE shall request new pseudonym, application, or identification certificates whenever it's certificates chain up to a PCA certificate that is invalidated due to a RCA, ICA, or PCA revocation.	EE should not use the revoked CA's certificate and all certificates that chain up to that CA certificate to trust it or to use it in communication. That includes its own pseudonym/application/identification certificates that chain up to the revoked CA certificate.	EEs receiving the component CRL shall mark the revoked component certificates as untrusted immediately: • In sending requests to that component • In trusting certificate chains chaining to that component's certificate • In trusting messages signed using this	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
					component's certificate • In sending messages signed with certificates that chain up to this component's certificate This is out of scope as it defines EE behavior.	
SCMS-2608	MANUAL PROCESS	Map PCA IssuerIdentifier to PCA FQDN	The TCotSCMSM shall associate each PCA IssuerIdentifier (the HashId8 of the PCA signing certificate) with the FQDN of the PCA that has the certificate.	A mapping between PCAs' IssuerIdentifier and PCA hostname is needed. During an investigation, the MA (GMBD) will receive a cert, extract linkage value, extract IssuerIdentifier, and then ask the PCA that issued the cert for the linkage value. For that step, MA must be able to map the IssuerIdentifer to the PCA hostname. This mapping is maintained by the TCotSCMSM and configured in the MA as	For the PoC, the SCMS operator will manually configure the mapping of PCA IssuerIdentifiers with the FQDN of the corresponding PCA.	TCotSCMSM

Key	Status	Summary	Description	Justification	Notes	Component/s
				needed, or this mapping may be maintained as a built-in feature of the MA.		

8 issues

5.2.11.9.4.9 Step 11.2.1 - Revoke PG

5.2.11.9.4.9.1 Goals

Revoke a Policy Generator certificate from the SCMS System.

5.2.11.9.4.9.2 Background and Strategic Fit

The Technical Component of the SCMS Manager (TCotSCMSM) determines that a Policy Generator (PG) needs to be revoked. The TCotSCMSM access the CRL generator for CRL series 256 (either the root CA or a central CRLG) and causes the PG to be added to the composite CRL, which is made available to all SCMS components and EEs. On receipt of the new CRL, all SCMS components and EEs shall mark the affected Policy Generator as untrusted. Components and EEs must request a new policy file signed by a new PG as soon as it is available.

5.2.11.9.4.9.3 Procedure

1. The TCotSCMSM contacts the series 256 CRL generator (see the CRL Series Diagram for details) and instructs it to add the current PG certificate to the CRL. The CRLG assembles and signs an updated CRL, which is made available to all components and EEs through the CRL store or via collaborative distribution.
2. The TCotSCMSM shall configure a new PG and issue a new GPF as described in the Add PG use case. The GPF will be made available to all RAs and back-end components. On receipt of the new GPF, each RA will assemble an updated LPF and submit the custom portion of the local policy to be signed by the new PG.
3. Upon receipt of the updated CRL, all SCMS components and EEs shall cease to trust the current policy or any new policy files signed by the revoked PG. They shall all resort to a set of pre-configured "default" policy values and attempt to download an updated policy file signed by a new PG as soon as it is available.
4. EEs shall contact their RA to download a new policy file signed by a replacement PG. They shall switch to a pre-defined set of "default" policy values until the new file is available.
5. SCMS components shall attempt to download a new policy file signed by a replacement PG. They will use a pre-defined set of "default" policy values until the new file is available.

5.2.11.9.4.9.4 Assumptions

- Backend components and EEs will be pre-programmed with a set of "default" policy values that can maintain some level of system operation while the new PG is established and new policy files are distributed.
- Each RA will need to receive the new GPF when it is available, assemble their own custom section of their LPF and submit it to the PG to be signed. Local ICA Managers will implement a manual process to push the new GPF out to their RAs. The TCotSCMSM may implement network management practices to limit traffic to the replacement PG.

- There may be a time delay before a new policy file is available from an RA for EEs to download. OEMs shall define an implementation specific mechanism to manage EE messaging to the RA. OEMs that have alternate mechanisms to push content out to their EEs may use these mechanisms to distribute a new signed policy file as soon as it is available.

5.2.11.9.4.9.5 Requirements

Table 60 Use Case 11.2.1 Revoke PG - Requirements

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-771	MANUAL PROCESS	Invoke Revocation of non-Root SCMS component	The Technical Component of the SCMS Manager shall interact with the CRLG to list the certificate of the component to be revoked in the components CRL and have the CRLG sign it.	An authenticated message from the SCMS Manager is required to revoke a component.	In the PoC, this will occur by a manual process.	TCotSCMSM
SCMS-772	MANUAL PROCESS	Standing up a SCMS component replacing the revoked component	The Technical Component of the SCMS Manager shall issue a replacement component certificate to the revoked certificate, if the revoked certificate belongs to a central component.	Upon revoking a component, a replacement component is needed to carry on its tasks and responsibilities.	This could be a new component or an existing one that will carry on the same tasks and responsibilities of the revoked component. In the PoC, this will occur by a manual process.	TCotSCMSM
SCMS-859	CLOSED	All relevant components cease to trust the revoked component	All SCMS components receiving and validating a CRL shall remove all revoked component certificates from their trust store. All cached certificate chains that roll up to a revoked component shall be removed.	The relevant components should not use the revoked component's certificate to trust it. If their chains include the revoked component, they should receive new certificate chains.	Particularly, in the case of LA revocation, the RA needs to be informed in order to stop requesting encrypted PLVs from the revoked LA. The MA needs to be informed in order to stop requesting linkage information (i.e., for misbehavior	CRL Store, CRLG, DCM, ECA, IBLM, ICA, LA, MA, PCA, PG, RA

Key	Status	Summary	Description	Justification	Notes	Component/s
					detection) from the revoked LA. In the case of RA revocation, the LAs need to be informed in order to stop sending encrypted PLVs to the revoked RA. All SCMS components and EEs receiving the component CRL shall mark the revoked component certificates as untrusted immediately: • In sending requests to that component • In trusting certificate chains chaining to that component's certificate • In trusting messages signed using this component's certificate	

<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-1387</td><td>MANUAL PROCESS</td><td>Remove revoked certificates from GCCF</td><td>The Technical Component of the SCMS Manager shall interact with the Policy Generator to remove the certificate of the revoked component and all its certificate chains from the Global Certificate Chain File.</td><td>Revoked certificates get invalid and therefore their certificate chains as well. They should not be available anymore via GCCF in order to save computational power during validation and bandwidth during transfer of the GCCF.</td><td></td><td>TCotSCMSM</td></tr>
<tr><td>SCMS-1685</td><td>EE REQUIREMENT</td><td>EEs shall use default policy when PG is revoked</td><td>EEs shall switch to the following set of pre-defined default policy values upon receipt of a CRL that revokes the Policy Generator (PG) that signed the most recently accepted policy update.<table><tr><th>Identifier</th><th>Poc Default Value</th></tr><tr><td>scms_version</td><td>1</td></tr><tr><td>global_cert_chain_file_id</td><td>2 bytes</td></tr><tr><td>overdue_CRL_tolerance</td><td>2 weeks</td></tr><tr><td>(OBE only) i_period</td><td>1 week</td></tr><tr><td>(OBE only) min_certs_per_i_period</td><td>20</td></tr></table></td><td>When the current PG is revoked, EEs can no longer trust the currently active policy values. Rather than operate with potentially invalid values, they shall switch to a set of pre-programmed default values that are deemed suitable to maintain safe operation.</td><td>This requires that EE software contain default values, which will be used when the current PG is revoked. It also implies that each EE keep track of the identity of the PG that signed the most recent policy update that the EE accepted.
This is out of scope as it defines EE behavior.</td><td>On-board Equipment (OBE), Road-side Equipment (RSE)</td></tr>
</table>

Key	Status	Summary	Description		Justification	Notes	Component/s
			(OBE only) cert_validity_model	concurrent			
			(OBE only) max_available_cert_supply	3 years			
			(RSE only) rse_application_cert_validity	1 week + 1 hour			
			(RSE only) rse_application_cert_overlap	1 hour			

5 issues

5.2.11.9.4.10 Step 11.2.1 - Revoke RA

5.2.11.9.4.10.1 Goals

Revoke an RA certificate from the SCMS System.

5.2.11.9.4.10.2 Background and Strategic Fit

The Technical Component of the SCMS Manager (TCotSCMSM) determines that an Registration Authority (RA) needs to be revoked, generates a certificate revocation message listing the RA certificate, and distributes it to all affected components. Relevant PCAs are instructed to mark the affected RA as untrusted.

The TCotSCMSM must ensure that those PCAs have at least one other RA from which to receive individual certificate requests for pseudonym certificates.

DCM(s) must no longer configure new end-entity devices to contact that RA to request pseudonym certificates.

All components and entities that receive the revocation notification also must cease to trust immediately any future message that was signed by the RA.

All end-entity devices that normally contact the revoked RA should obtain another RA's certificate and address from which to request pseudonym certificates as soon as possible (the SCMS Manager may set performance requirements for how quickly this must happen).

5.2.11.9.4.10.3 Assumptions

- Messages and procedures need to be defined, potentially using existing data structures defined in IEEE 1609.2 for CA revocation.
- These data structures only support the case where the CRL is signed by a single signer.
- If components use any other authentication mechanism, such as symmetric authentication or multiple signatures, the data structures, if used, would have to be redefined.

5.2.11.9.4.10.4 Requirements

Table 61 Use Case 11.2.1 Revoke RA - Requirements

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-364	MANUAL PROCESS	DCM Configuration of EEs After Component Revocation	DCM shall not configure new EEs with credentials of revoked SCMS component.	The SCMS Manager will manage the transition of devices after the revocation of a component.	In the PoC this will occur by a manual process. The DCM will provision EEs with valid certificates for SCMS components including one or more ICA and one or more RA. When the DCM learns that any component is revoked, it shall no longer provision new EEs with that revoked certificate.	DCM
SCMS-771	MANUAL PROCESS	Invoke Revocation of non-Root SCMS component	The Technical Component of the SCMS Manager shall interact with the CRLG to list the certificate of the component to be revoked in the components CRL and have the CRLG sign it.	An authenticated message from the SCMS Manager is required to revoke a component.	In the PoC, this will occur by a manual process.	TCotSCMSM
SCMS-772	MANUAL PROCESS	Standing up a SCMS component replacing the revoked component	The Technical Component of the SCMS Manager shall issue a replacement component certificate to the revoked certificate, if the revoked certificate belongs to a central component.	Upon revoking a component, a replacement component is needed to carry on its tasks and responsibilities.	This could be a new component or an existing one that will carry on the same tasks and responsibilities of the revoked component. In the PoC, this will occur by a manual process.	TCotSCMSM

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-859	CLOSED	All relevant components cease to trust the revoked component	All SCMS components receiving and validating a CRL shall remove all revoked component certificates from their trust store. All cached certificate chains that roll up to a revoked component shall be removed.	The relevant components should not use the revoked component's certificate to trust it. If their chains include the revoked component, they should receive new certificate chains.	Particularly, in the case of LA revocation, the RA needs to be informed in order to stop requesting encrypted PLVs from the revoked LA. The MA needs to be informed in order to stop requesting linkage information (i.e., for misbehavior detection) from the revoked LA. In the case of RA revocation, the LAs need to be informed in order to stop sending encrypted PLVs to the revoked RA. All SCMS components and EEs receiving the component CRL shall mark the revoked component certificates as untrusted immediately: • In sending requests to that component • In trusting certificate chains chaining to that component's certificate	CRL Store, CRLG, DCM, ECA, IBLM, ICA, LA, MA, PCA, PG, RA

Key	Status	Summary	Description	Justification	Notes	Component/s
					• In trusting messages signed using this component's certificate	
SCMS-1387	MANUAL PROCESS	Remove revoked certificates from GCCF	The Technical Component of the SCMS Manager shall interact with the Policy Generator to remove the certificate of the revoked component and all its certificate chains from the Global Certificate Chain File.	Revoked certificates get invalid and therefore their certificate chains as well. They should not be available anymore via GCCF in order to save computational power during validation and bandwidth during transfer of the GCCF.		TCotSCMSM

5 issues

5.2.11.9.5 Step 11.2.2: Revoke Root CA

5.2.11.9.5.1 Goals

To produce the "Revoke Root CA" message, signed by at least the required number (m below) of non-revoked Electors, which SCMS components and EEs must receive and act on.

5.2.11.9.5.2 Assumptions

Root Management is performed according to the Elector scheme outlined in Elector-based Root Management.

5.2.11.9.5.3 Background and Strategic Fit

The SCMS Manager determines that a root CA is to be revoked. The SCMS Manager employs the non-revoked Electors to authenticate the revocation of a root CA. The SCMS Manager forms the bare message indicating the revocation of the root CA, including the root CA's certificate and has this message signed by at least *m* non-revoked Electors. The SCMS Manager instructs each Elector that it desires to sign this message, authenticating the removal of the root CA. These signatures on the message are accumulated into a final message. In this way, the SCMS Manager controls the production of the "Revoke root CA" message, signed by at least *m* non-revoked Electors of *n*. This message is delivered to all affected SCMS Components via the CRL and by proprietary messaging. To validate the "Revoke root CA" message, components or EEs must verify at least *m* non-revoked Electors signatures.

The MA, relevant CAs, RAs, and CRLG(s) are instructed to remove the affected root CA from their list of trusted roots. The OEMs will ensure that new end-entity devices will not be provisioned with the revoked root CA certificate.

All components and entities that receive the revocation notification also cease to trust any other affected certificate.

All end-entity devices whose certificates chain back to the revoked root CA should obtain new certificates as soon as possible (the SCMS Manager may set performance requirements for how quickly this must happen, and will coordinate).

All CAs, the MA, RAs, and CRLG(s), whose certificates chain back to the revoked root CA should cease issuing certificates with their old certificates immediately and obtain new certificates as quickly as possible (the SCMS Manager may set performance requirements for how quickly this must happen and will coordinate). The SCMS Manager will manage the recovery from the root CA revocation and establishing a new trust hierarchy.

5.2.11.9.5.4 Procedure

To implement this process, an authorized agent of the SCMS manager will perform the following actions:

1. Obtain a copy of the root CA certificate that is to be revoked. The SCMS Manager shall define procedures for validating that the correct certificate is being revoked.

2. An agent of the SCMS Manager will present the root CA certificate to all existing, valid SCMS electors and request that they produce a digitally signed "removeRoot" ballot. The collection of all independent signed ballots from existing electors is then assembled into one root endorsement message with the sequence of elector signatures attached. The number of elector signatures must be greater than or equal to the value of 'quorum' defined in the current GPF. This is a manual process to be implemented by the TCotSCMSM.
3. The complete root removal message with signatures is then delivered to the CRLG for inclusion in an updated composite CRL file. Note that the CRLG signature is not necessary for the root removal to be validated by SCMS components. The role of the CRLG in this case is to assemble updates to the composite CRL with all active root removal messages included.
4. SCMS components (including EEs) that receive a composite CRL with one or more root removal message attached must check to see if they have already removed the root certificate from their trust store. If they have not, they must validate the root removal message by checking the attached signatures and confirming it has non-expired certificates for at least 'quorum' of the existing electors that signed the message. Once the message is validated, the SCMS component must remove the root certificate from their trust store. When validating a root removal message, an entity must check that the data, which is signed in each elector endorsement (specifically the *TbsElectorEndorsement* element), is identical and that the *EndorsementType* element of the data has the value *removeRoot*.
5. When a root is removed from a device's trust store, the device must then cease to trust any new certificates that chain back to that root.
6. When a root is removed from a device's trust store, the device must then cease to trust any certificates that chain back to that root. If a device finds that this action invalidates its own enrollment certificate or private key, it must cease operation.

5.2.11.9.5.5 Requirements

Table 62 Use Case 11.2.2 Revoke Root CA - Requirements

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-187	MANUAL PROCESS	Revoke a Root CA	The Technical Component of the SCMS Manager (TCotSCMSM) shall communicate the multi-signed "Revoke Root CA" message to CRL Generator to be included in the SCMS component CRL which will be distributed to SCMS components and EEs to inform them of the revoked Root CA.	Messages revoking Root CAs must be authenticated with m Elector signatures.	In the PoC this will message will be produced by a manual process, but automatically distributed via CRL	TCotSCMSM
SCMS-190	MANUAL PROCESS	Removing Root CA from Trust Store	MA, relevant CAs, RAs, and CRLG(s) shall validate the "Revoke Root CA" message, and if valid, the SCMS component shall remove the Root CA from its trust store. The Technical Component of the SCMS Manager shall place the "Revoke Root CA" on the CRL for distribution to EEs and other SCMS components.	Revoked Root CAs must be removed from the SCMS system with a secured message authenticated with multiple signatures.	In the PoC, a manual process will place the “Revoke Root CA” message on the CRL.	

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-192	MANUAL PROCESS	SCMS Components Obtain New Certificates	All CAs, the MA, RAs, and CRLG(s), whose certificates chain back to the revoked Root CA shall cease issuing certificates with their old certificates immediately and obtain new certificates as quickly as possible.	Any operation, which use the old certificates, will no longer be trusted and will not be trusted until new certificates are obtained.	SCMS Manager may set performance requirements for how quickly this must happen	CRLG, ICA, MA
SCMS-782	MANUAL PROCESS	Root CA revocation	A quorum of Electors shall sign the Root CA revocation message to be included in the CRL.	So that SCMS components are able to verify the revocation message.		Elector
SCMS-864	EE REQUIREMENT	EEs obtain a new LCCF upon Root CA revocation	EEs shall contact an RA to obtain a new Local Certificate Chain File (LCCF) when their current root CA has been revoked.	EE's require a valid certificate chain that can be used to validate their own pseudonym certificates and relevant SCMS component certificates.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-865	EE REQUIREMENT	EEs obtaining new Enrollment Certificates upon Root CA revocation	EEs shall obtain new Enrollment Certificates from their ECAs, if the root CA was revoked, through a re-enrollment request towards RA.	EEs need to obtain new enrollment certificates valid in the new PKI hierarchy.	Refreshed Enrollment Certificates are encrypted to the old Enrollment Certificate. The OEMs should keep a record of all Enrollment Certificates issued, so that no refreshed Enrollment Certificates are encrypted to any new Enrollment Certificate (restricting issuance of refreshed Enrollment Certificates to devices having a valid old Enrollment	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
					Certificate). This implies a strong link between the OEM and their ECA. This is out of scope since it defines EE's behavior.	
SCMS-866	EE REQUIREMENT	OBEs obtaining new Pseudonym/Identification Certificates upon Root CA revocation	OBEs shall use the new Enrollment Certificate (cp.https://jira.campllc.org/browse/SCMS-865~~SCMS-865~~) to obtain new Pseudonym or Identification Certificates that chain up to the new root CA.	OBEs need new batches of Pseudonym and Identification Certificates issued by PCAs in the new PKI hierarchy.	This requires a fresh request for butterfly keys. SCMS Manager may set performance requirements for how quickly this must happen This is out of scope as it defines OBE behavior.	On-board Equipment (OBE)
SCMS-1024	CLOSED	Root CA Trust Store Messaging Processing	The SCMS Component shall be able to process the "Add Root CA" and "Revoke Root CA" messages, which will be signed by Electors, and shall ensure that the number of valid signatures is at least a quorum of non-revoked Electors in its trust store.	Every SCMS component will need to manage root CA updates automatically, so therefore, every SCMS component will need to be able to process Root Management messages signed by the Electors.	For the PoC, the number of Electors will be 3 and the number of Electors required to authorize any Root Management message will be 2. Elector signatures will be produced in a manual process for the PoC.	CRL Store, CRLG, DCM, ECA, IBLM, ICA, LA, MA, PCA, PG, RA
SCMS-1062	MANUAL PROCESS	Revoke Component: PG Update Global Certificate Chain File	The Policy Generator shall update the GCCF and remove all impacted certificates as soon as it receives the notification that any back-end component has been revoked.	Having an updated certificate chain file makes verification processes at EEs more efficient.	When a back-end component is revoked, it may impact the validity of other certificates on the GCCF. Specifically, when any CA is revoked, all certificates that were issued by (i.e. signed by) that CA will become invalid and therefore must be removed from	PG

Key	Status	Summary	Description	Justification	Notes	Component/s
					the GCCF. This is particularly important if a Root CA is revoked, but it applies equally to other CA revocations.	
SCMS-1170	EE REQUIREMENT	RSEs obtain new application certificates	RSEs shall use the new Enrollment Certificate (cp.https://jira.campllc.org/browse/SCMS-865~~SCMS-865~~) to obtain new Application Certificates that chain up to the new root CA.	RSEs need new Application Certificates issued by PCAs in the new PKI hierarchy.	In the PoC, this will occur by a manual process. SCMS Manager may set performance requirements for how quickly this must happen	Road-side Equipment (RSE)
SCMS-1387	MANUAL PROCESS	Remove revoked certificates from GCCF	The Technical Component of the SCMS Manager shall interact with the Policy Generator to remove the certificate of the revoked component and all its certificate chains from the Global Certificate Chain File.	Revoked certificates get invalid and therefore their certificate chains as well. They should not be available anymore via GCCF in order to save computational power during validation and bandwidth during transfer of the GCCF.		TCotSCMSM
SCMS-1409	CLOSED	Elector Trust Store Messaging Processing	The SCMS Component shall be able to process the "Add Elector" and "Revoke Elector" messages, which will be signed by Electors and shall ensure that the number of valid signatures is at least a	Every SCMS component will need to manage Elector updates automatically, so therefore, every SCMS component will need to be able to process Root	For the PoC, the number of Electors will be 3 and the number of Electors required to authorize any Root Management message will be 2. Elector signatures will be produced in a manual process for the PoC.	CRL Store, CRLG, DCM, ECA, IBLM, ICA, LA, MA, PCA, PG, RA

Key	Status	Summary	Description	Justification	Notes	Component/s
			quorum of non-revoked Electors in its trust store.	Management messages signed by the Electors.		
SCMS-1587	EE REQUIREMENT	EE shall cease to trust the revoked CA	EEs receiving and validating a CRL shall remove all revoked CA certificates from their trust store, remove all cached certificate chains that roll up to the revoked CA, and stop sending immediately in case EE's enrollment, pseudonym, application, or identification certificate chains up to the revoked CA.	EE should not use the revoked component's certificate to trust it. If it chains include the revoked component, they need to receive new certificates with a new certificate chain.	EEs receiving the component CRL shall mark the revoked component certificates as untrusted immediately: • In sending requests to that component • In trusting certificate chains chaining to that component's certificate • In trusting messages signed using this component's certificate • In sending messages signed with certificates that chain up to this component's certificate This is out of scope as it defines EE behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1589	EE REQUIREMENT	EE receive new enrollment certificate after CA revocation	EE shall get back to the secure environment used during their bootstrapping process and be re-bootstrapped after its RCA, ICA or ECA was revoked.	EE should not use the revoked CA's certificate and all certificates that chain up to that CA certificate to trust it or to use it in communication. That includes enrollment		On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
				certificates that chain up to the revoked CA certificate.		
SCMS-1593	EE REQUIREMENT	EE receive new pseudonym/application/identification certificates after CA revocation	EE shall request new pseudonym, application, or identification certificates after it was re-bootstrapped due to revocation of its RCA, ICA, or ECA.	EE should not use the revoked CA's certificate and all certificates that chain up to that CA certificate to trust it or to use it in communication. That includes its own pseudonym/application/identification certificates that chain up to the revoked CA certificate.		On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1608	EE REQUIREMENT	EE receive new pseudonym/application/identification certificates after PCA revocation	EE shall request new pseudonym, application, or identification certificates whenever it's certificates chain up to a PCA certificate that is invalidated due to a RCA, ICA, or PCA revocation.	EE should not use the revoked CA's certificate and all certificates that chain up to that CA certificate to trust it or to use it in communication. That includes its own pseudonym/application/identification certificates that chain up to the revoked CA certificate.	EEs receiving the component CRL shall mark the revoked component certificates as untrusted immediately: • In sending requests to that component • In trusting certificate chains chaining to that component's certificate • In trusting messages signed using this component's certificate	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
					• In sending messages signed with certificates that chain up to this component's certificate This is out of scope as it defines EE behavior.	
SCMS-2461	CLOSED	SCMS components regularly pull SCMS component CRL	The SCMS component shall download the SCMS component CRL from CRLG regularly, at an interval of at least every 60 minutes	To ensure that revoked SCMS components are excluded from the system within a short time period.		DCM, ECA, LA, MA, PCA, PG, RA

17 issues

5.2.11.9.5.6 Design

The design for the elector-based management system is described in the Elector-based Root Management section.

5.2.11.9.5.7 Diagrams

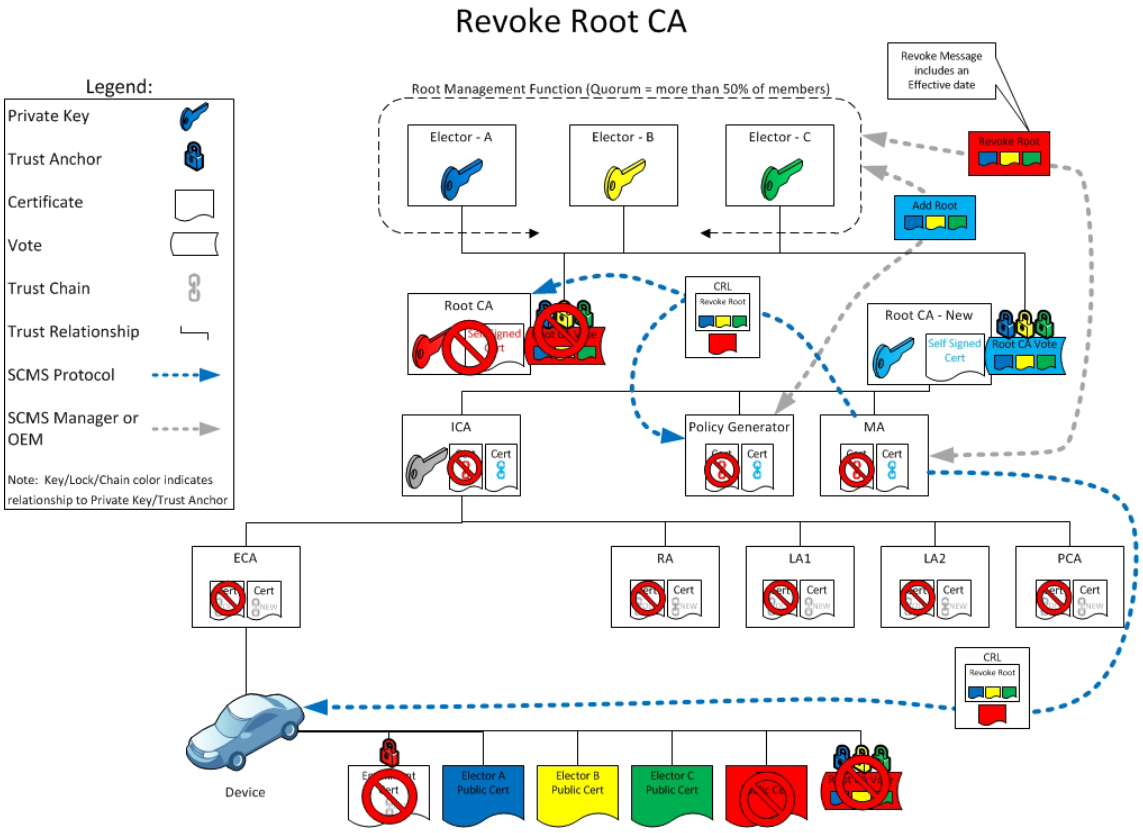


Figure 75 Revoke Root CA

5.2.11.9.6 Step 11.2.3: Revoke Elector

5.2.11.9.6.1 Goals

To produce the "Revoke Elector" message, signed by at least the required number (a quorum as defined in the Global Policy File) of non-revoked Electors, which SCMS Components and EEs must receive through updates to the composite CRL and act on.

5.2.11.9.6.2 Background and Strategic Fit

The SCMS Manager determines that an elector is to be revoked. The SCMS Manager employs the non-revoked electors to authenticate the revocation of the impacted elector. The SCMS Manager creates the message indicating the revocation of the elector, including the elector's certificate and has this message signed by at least "quorum" (as defined in the GPF) of non-revoked electors. The SCMS Manager instructs each elector that it desires to sign this message, authenticating the removal of the impacted elector. These signatures on the message are accumulated into a final message. In this way the SCMS Manager controls the production of the "Revoke

Elector" message, signed by at least *m* non-revoked electors. This message is delivered to all affected SCMS Components via the CRL (proprietary messaging may also be used for faster distribution). To validate the "Revoke Elector" message, components or EEs must verify at least *"quorum"* non-revoked electors signatures.

The TCotSCMSM will inform the PG to create a new GCCF, removing the impacted elector signature from the root endorsement. If this causes the Root CA to be endorsed by fewer than "quorum" electors, then the TCotSCMSM must establish a new elector and have it endorse the existing root CA. The only alternative is to publish a GCCF with an un-endorsed root, which would implicitly revoke the root and cause all operations to cease.

5.2.11.9.6.3 Assumptions

- Root Management is performed according to the Elector scheme outlined in Root Management and Revocation Recovery
- Elector revocation is communicated to all SCMS components through updates to the CRL

5.2.11.9.6.4 Procedure

To implement this process, an authorized agent of the SCMS manager will perform the following actions:

1. Obtain a copy of the elector certificate that is to be revoked. The SCMS Manager shall define procedures for validating that the correct certificate is being revoked.
2. An agent of the SCMS Manager will present the elector certificate to all existing, valid SCMS electors and request that they produce a digitally signed "removeElector" ballot. The collection of all independent signed ballots from existing electors is then assembled into one elector removal message with the sequence of elector signatures attached. The number of elector signatures must be greater than or equal to the value of 'quorum' defined in the current GPF. This is a manual process to be implemented by the TCotSCMSM.
3. The complete elector removal message with signatures is then delivered to the CRLG for inclusion in an updated composite CRL file. Note that the CRLG signature is not necessary for the root removal to be validated by SCMS components. The role of the CRLG in this case is to assemble updates to the composite CRL with all active elector removal messages included.
4. SCMS components (including EEs) that receive a composite CRL with one or more elector removal messages attached must check to see if they have already removed the elector from their trust store. If they have not, they must validate the elector removal message by checking the attached signatures and confirming it has non-expired certificates for at least 'quorum' of the existing electors that signed the message. Once the message is validated, the SCMS component must remove the elector certificate from their trust store. When validating an elector removal message, an entity must check that the data, which is signed in each elector

endorsement (specifically the *TbsElectorEndorsement* element) is identical and that the *EndorsementType* element of the data has the value *removeElector*.

5. When an elector is removed from a device's trust store, the device must then cease to trust any new messages endorsed by that elector.

5.2.11.9.6.5 Requirements

Table 63 Use Case 11.2.3 Revoke Elector - Requirements

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-1024	CLOSED	Root CA Trust Store Messaging Processing	The SCMS Component shall be able to process the "Add Root CA" and "Revoke Root CA" messages, which will be signed by Electors, and shall ensure that the number of valid signatures is at least a quorum of non-revoked Electors in its trust store.	Every SCMS component will need to manage root CA updates automatically, so therefore, every SCMS component will need to be able to process Root Management messages signed by the Electors.	For the PoC, the number of Electors will be 3 and the number of Electors required to authorize any Root Management message will be 2. Elector signatures will be produced in a manual process for the PoC.	CRL Store, CRLG, DCM, ECA, IBLM, ICA, LA, MA, PCA, PG, RA
SCMS-1408	CLOSED	Elector revocation	A quorum of Electors shall sign the Elector revocation message to be included in the CRL.	So that SCMS components are able to verify the revocation message.		Elector
SCMS-1409	CLOSED	Elector Trust Store Messaging Processing	The SCMS Component shall be able to process the "Add Elector" and "Revoke Elector" messages, which will be signed by Electors and shall ensure that the number of valid signatures is at least a quorum of non-revoked Electors in its trust store.	Every SCMS component will need to manage Elector updates automatically, so therefore, every SCMS component will need to be able to process Root Management messages signed by the Electors.	For the PoC, the number of Electors will be 3 and the number of Electors required to authorize any Root Management message will be 2. Elector signatures will be produced in a manual process for the PoC.	CRL Store, CRLG, DCM, ECA, IBLM, ICA, LA, MA, PCA, PG, RA
SCMS-1413	MANUAL PROCESS	Revoke Elector: PG	The Policy Generator shall update the GCCF as soon as it	Having an updated certificate chain file makes verification		PG

Key	Status	Summary	Description	Justification	Notes	Component/s
		Update Global Certificate Chain File	receives the "Revoke Elector" message and remove the "Add Elector" message of the revoked Elector.	processes at EEs more efficient.		

4 issues

5.2.11.9.6.6 Design

The design for the elector-based management system is described in the Elector-based Root Management section.

5.2.12 Use Case 12: RSE Bootstrapping (Manual)

The manual process for RSE bootstrapping is exactly the same as Use Case 2: OBE Bootstrapping (Manual) for at least the first year of CV pilot SCMS POC operations.

5.2.13 Use Case 13: RSE Application Certificate Provisioning

5.2.13.1 Goals

Provide a bootstrapped RSE with an application certificate that it can use in relevant applications.

5.2.13.2 Background and Strategic Fit

The application certificate provisioning is the process by which a bootstrapped RSE receives an application certificate. As there are no location privacy or tracking concerns for RSEs, the RA is not required to shuffle the requests (unlike the case of OBEs).

This use case involves the following SCMS components:

- Pseudonym Certificate Authority (PCA)
- Registration Authority (RA)

The validity duration of application certificate is short due to the assumption that RSEs have frequent online connectivity.

5.2.13.3 Assumptions

In order to facilitate the certificate request process, a RSE must meet the following prerequisites:

- RSE has a valid enrollment certificate
- RSE has root CA, RA and PCA certificates installed
- RSE knows the FQDN of the RA

5.2.13.4 Design

The following flow chart documents the general flow of steps an RSE needs to carry out in the given order to obtain application certificates. It is not a 100% accurate description of the process. Please refer to the use case's steps and their requirements for a complete description of the process.

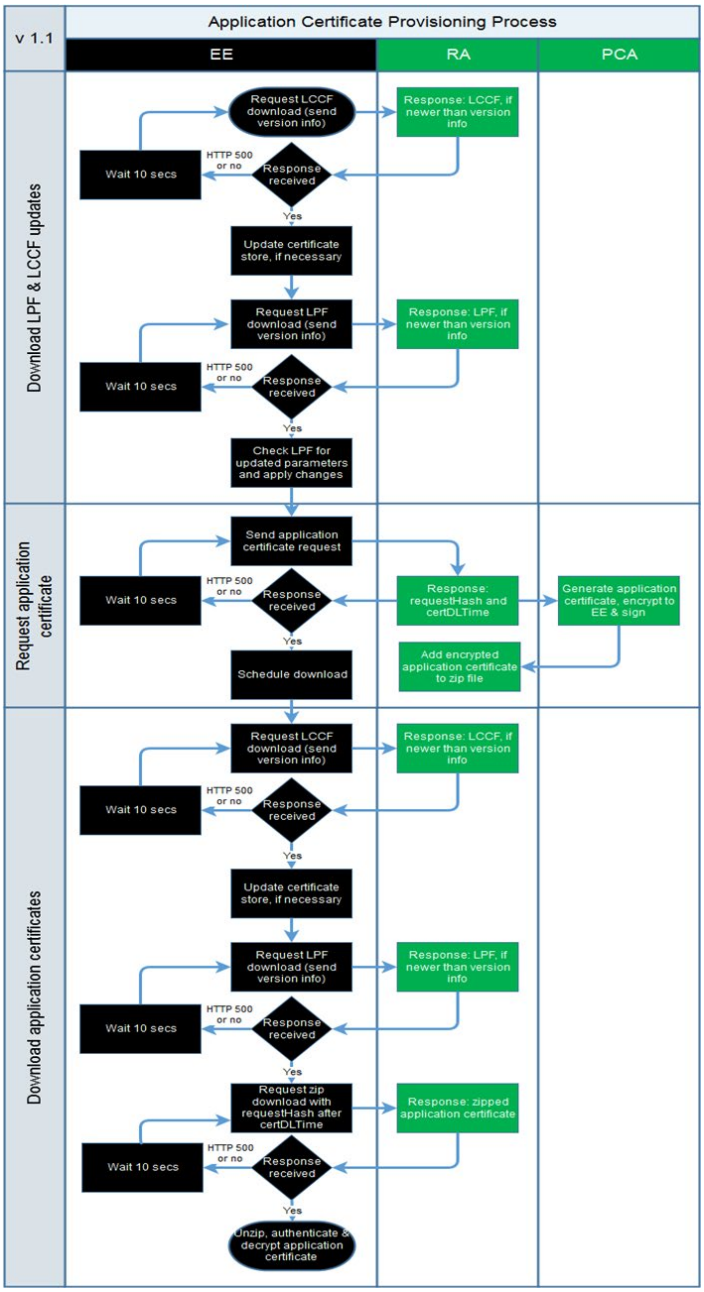


Figure 76 Application Certificate Provisioning Process

At a high level, two steps are relevant towards a RSE:

1. Request RSE Application Certificate
2. Download RSE Application Certificate

Having determined which RA to submit the request to, the RSE creates a request, signs it with the enrollment certificate, encrypts the signed request for the RA and sends it to the LOP/RA. The RA checks to make sure that the certificate request is correct and authorized, then sends back a download location (*requestHash*) and time (*certDLTime*). The RA then forwards the certificate request to the PCA. The PCA signs

the application certificate, encrypts them for the RSE, signs the encrypted version of the certificate, and returns the encrypted and signed application certificate to the RA. The RA does not remove any of the named signatures or encryptions, adds them to a zip file and stores them for download by the RSE. The RSE starts downloading the zip files at *certDLTime.*

5.2.13.5 Step 13.1: Request RSE Application Certificate

5.2.13.5.1 Goals

The goal is to define messages and other requirements for an RSE to request an application certificate.

5.2.13.5.2 Background and Strategic Fit

The RSE decides to request an application certificate from its preconfigured RA.

Having determined which RA to submit the request to, the RSE creates a request, signs it with the enrollment certificate, encrypts the signed request for the RA and sends it to the RA. The RA checks to make sure that the request is correct and authorized.

RSE will attempt to download the local certificate chain file (LCCF) and the local policy file (LPF) before submitting the request. Note that any EE should download the local policy file and local certificate chain file each time it connects to RA.

5.2.13.5.3 Assumptions

The RSE has successfully completed Use Case 12: RSE Bootstrapping (Manual).

5.2.13.5.4 Process Steps

1. The RSE downloads the Local Policy File (LPF) and the Local Certificate Chain File (LCCF) using the API documented in RA - Download local policy file and RA - Download Local Certificate Chain File
    a. If there is an updated LCCF, the RSE applies all changes to its trust-store (necessary for PCA Certificate Validations)
    b. If there is an updated LPF, the RSE applies those changes
2. The RSE creates the request, signs it with the enrollment certificate, encrypts the signed request to the RA and sends it to the RA using the API documented in RA - Request Application Certificate Provisioning
3. The RA ensures that the certificate batch request is correct and authorized, before it starts Step 13.2: Generate RSE Application Certificate

5.2.13.5.5 Error Handling

1. The RSE will abandon further interactions with the RA after a certain number of failed communication attempts result in errors.

5.2.13.5.6 Requirements

Table 64 Use Case 13.1 - 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></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>
</table>

Key	Status	Summary	Description	Justification	Notes	Component/s
			0xC0,0x2C TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 RFC5289 0xC0,0xAC TLS_ECDHE_ECDSA_WITH_AES_128_CCM RFC7251 0xC0,0xAD TLS_ECDHE_ECDSA_WITH_AES_256_CCM RFC7251			
SCMS-411	EE REQUIREMENT	EE Authentication to RA for Request	The EE shall authenticate its requests with its enrollment certificate and signed timestamp to avoid replay attacks on the RA.	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.	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.	On-board Equipment (OBE), Road-side Equipment (RSE)
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	OCSP stapling provides improved performance compared to CRLs. OCSP stapling is specified in	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
				RA must provide an OCSP stapled response so that the OBE can validate the RA's TLS certificate.	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.	
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	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
					(comparehttps://jira.campllc.org/browse/SCMS-859~~SCMS-859~~, SCMS-504) and the X.509 CRL (https://jira.campllc.org/browse/SCMS-405~~SCMS-405~~).	
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-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	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
					Communications - General Guidance	
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-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	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
					not EE's private key). OCSP stapling is specified in RFC 6066, Section 8.	
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		RA

Key	Status	Summary	Description	Justification	Notes	Component/s
				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.		
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-954	EE REQUIREMENT	Error code: eePolicyVerificationFailed	EE shall log this error code in EE's error log file, if EE is not able to verify the digital signature of the local policy file.	To enable EE side diagnostics.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-956	EE REQUIREMENT	Error code: eePolicyFileParsingFailed	EE shall log this error code in EE's error log file, if EE is not able to parse the successfully downloaded local policy file (e.g., because 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 read 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-958	EE REQUIREMENT	Error code: eeConnectionFailed	EE shall log this error code, if it cannot connect to RA because there is a connection timeout.	To enable EE side diagnostics.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-978	CLOSED	Error code: raAuthenticationFailed	RA shall log "Error code: raAuthenticationFailed", if EE-to-RA authentication fails.	To enable server side diagnostics and to avoid giving potential attackers relevant information.		RA
SCMS-981	CLOSED	Error code: raNoPcaCertificateChainFileAvailable	RA shall return status code HTTP 500, if Local Certificate Chain File is not available and log "Error code: raNoPcaCertificateChainFileAvailable".	To enable client side error handling.		RA
SCMS-987	TESTS FAILED	Error code: raWrongParameters	RA shall log "Error code: raWrongParameters", if a device sends request with wrong parameters.	To enable server side diagnostics and to avoid giving potential attackers relevant information		RA
SCMS-988	TESTS FAILED	Error code: raRetries	RA shall log "Error code: raRetries", if the EE retries within the time specified in SCMS-522.	To enable server side diagnostics and to avoid giving potential attackers relevant information. Retry not allowed within 2 seconds.		RA
SCMS-990	TESTS FAILED	Error code: raMoreThanAllowedTries	RA shall return status code HTTP 500, if the EE violates SCMS-523, and log "Error code: raMoreThanAllowedTries".	To avoid DoS attacks		RA

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-1065	CLOSED	Error code: raBlacklisted	RA shall log "Error code: raBlacklisted" if the requesting EE has been blacklisted.	Error's produced by an EE should always be logged for diagnostic purposes and never returned to the EE to avoid giving a potential attacker sensitive information.	RA response to EE shall follow SCMS-1397	RA
SCMS-1066	CLOSED	RSE duplicate request check	RA shall not issue an RSE application certificates, if a request for the same PSID and an overlapping time period beyond a configurable tolerated overlap has been requested by an RSE before (identified by its enrollment certificate).	Stop misbehaving RSEs that request multiple certificates per time period.	Consider this for MA integration at a later stage.	RA
SCMS-1068	CLOSED	Error code: raRequestForMultipleCerts	The RA shall log "Error code: raRequestForMultipleCerts" as well as identifying information of the RSE, if the RSE requested more than one certificate for the same PSID for a time period that goes beyond the tolerated overlap period.	This error code catches requests that are not duplicate but request more than one certificate per time period.		RA
SCMS-1070	CLOSED	Error code: raDuplicateRequestReceived	The RA shall log "Error code: raDuplicateRequestReceived" as well as identifying information of	This error code catches duplicate requests.	Consider this for MA integration at a later stage.	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
			the EE, if EE sent a duplicate request.			
SCMS-1082	CLOSED	Error code: raInvalidSignature	The RA shall log "Error code: raInvalidSignature", if the EE does not sign the certificate request with its enrollment certificate or if the signature is invalid.	To enable server side diagnostics and to avoid giving potential attackers relevant information	An unsigned request might be an indication for misbehavior.	RA
SCMS-1083	CLOSED	Error code: raRequestNotEncrypted	The RA shall log "Error code: raRequestNotEncrypted", if the EE does not encrypt the certificate request using the RA's 1609 certificate.	To enable server side diagnostics and to avoid giving potential attackers relevant information	An unencrypted certificate request might be an indication for misbehavior.	RA
SCMS-1084	CLOSED	Error code: raInvalidCredentials	The RA shall log "Error code: raInvalidCredentials", if the EE has invalid credentials (blacklisted, expired, unauthorized)	To enable server side diagnostics and to avoid giving potential attackers relevant information	A request with invalid credentials might be an indication for misbehavior.	RA
SCMS-1085	TESTS FAILED	Error code: raUnauthorizedRequest	RA shall log "Error code: raUnauthorizedRequest", if an EE makes an unauthorized request (invalid permissions)	To enable server side diagnostics and to avoid giving potential attackers relevant information	An unauthorized request might be an indication for misbehavior.	RA
SCMS-1086	TESTS FAILED	Error code: raMalformedRequest	RA shall log "Error code: raMalformedRequest", if an EE makes a malformed request not captured inhttps://jira.campllc.org/browse/S	To enable server side diagnostics and to avoid giving potential attackers relevant information.	A malformed request might be an indication for misbehavior.	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
			CMS-1082~~SCMS-1082~~,https://jira.campllc.org/browse/SCMS-1083~~SCMS-1083~~,https://jira.campllc.org/browse/SCMS-1084~~SCMS-1084~~, SCMS-1085.			
SCMS-1087	CLOSED	Error code: raMismatch	The RA shall log "Error code: raMismatch", if this RA does not service the requesting EE.	To enable server side diagnostics and to avoid giving potential attackers relevant information.	A request from an EE that is not serviced by the requested RA might be an indication for misbehavior.	RA
SCMS-1088	CLOSED	Error code: raInvalidTimeReceived	The RA shall return status code HTTP 500, if the EE has send an invalid system time, and log "Error code: raInvalidTimeReceived".	To avoid EEs using the invalid certificates		RA
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)

Key	Status	Summary	Description	Justification	Notes	Component/s
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

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-1210	EE REQUIREMENT	EE Secure Key Storing	EE shall store the following keys in tamper-resistant (or equivalent) storage: • Private enrollment key • Butterfly key parameters (seed + expansion function parameter) • All private keys (e.g., of OBE application certificates and private keys calculated from the Butterfly key parameters)	To avoid extraction of private keys via software-based attacks.	This is out of scope since it defines EE's behavior. It is highly recommended to protect the content encryption key by a TPM-like mechanism that offers secure boot and that protects the keys against software-based attacks. Additional details are listed in Hardware, Software and OS Security	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1270	EE REQUIREMENT	Network connection	EEs shall use TCP/IP to communicate with the SCMS.	SCMS components (server) are only reachable by standard TCP/IP networking methods.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
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)

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-1356	EE REQUIREMENT	EE uses internal certificate store	The EE shall use its internal certificate store to validate received SCMS certificates and respond to P2P certificate requests.	EEs need to be able to validate received SCMS certificates based on their certificate chain up to the SCMS root CA. EEs need to respond to P2P certificate requests to enable receiving EEs to validate the certificate chain.	EE does not need to store all certificate chains, the LCCF provides the minimum set and EEs can learn additional chains via P2P certificate request. This is out of scope as it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1397	TESTS FAILED	Error reporting to EE	The SCMS Components shall return error code "HTTP 500" to EEs in response to all application level errors at RA.	Specific error codes should be hidden from EEs to prevent useful information from being provided to malicious actors	• Standard TCP (https://jira.campllc.org/browse/SCMS-1090~~SCMS-1090~~) and TLS (https://jira.campllc.org/browse/SCMS-977~~SCMS-977~~) errors shall be reported to EEs • All errors at the HTTP and higher levels shall be HTTP 500 for RA & ECA	CRL Store, RA
SCMS-1404	EE REQUIREMENT	EE send data via HTTP post over TCP/IP	EE shall use HTTP post to send data towards the RA	To allow the SCMS endpoint to serve everything based on HTTP protocol	RA - Services View will document the actual HTTP post details.	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
					This is out of scope as it defines EE behavior.	
SCMS-1405	CLOSED	RA accept authenticated HTTP post requests	RA shall accept HTTP post requests only from authenticated EEs.	To allow the SCMS endpoint to serve everything based on HTTP protocol	RA - Services View will document the actual HTTP post details.	RA
SCMS-1421	EE REQUIREMENT	LCCF validation in EE	The EE shall verify the LCCF and then update the internal certificate store each time it receives a new LCCF.	To have the latest certificate chain update available for validating certificates and answering P2P certificate requests.	This is out of scope as it defines EEs behavior	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1625	TESTS FAILED	RA-EE Certificate Request Ack Message	RA-EE Certificate Request Ack Message shall contain the following information: Case: Certificate Provisioning Request Accept • Version • Low order 8-bytes of the SHA-256 hash of the encoded "ToBeSigned" certificate request from the device • Time at which the first certificate batches will be available for download	As the EE needs to know, when and where it can go to download certificates.		RA

Key	Status	Summary	Description	Justification	Notes	Component/s
			(represented by IEEE 1609.2 Time32) • URL of the certificate repository (common for all devices serviced by a specific RA) Case: Certificate Provisioning Request Reject • HTTP 500 error code			
SCMS-2463	EE REQUIREMENT	EE transactions per TLS session	EE shall perform as many SCMS transactions as possible using a single TLS session.	To minimize the number of separate TLS sessions to the SCMS. This will reduce the resources required and improve throughput.	This is out of scope as it defines EE behavior.	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)

47 issues

5.2.13.5.7 Design

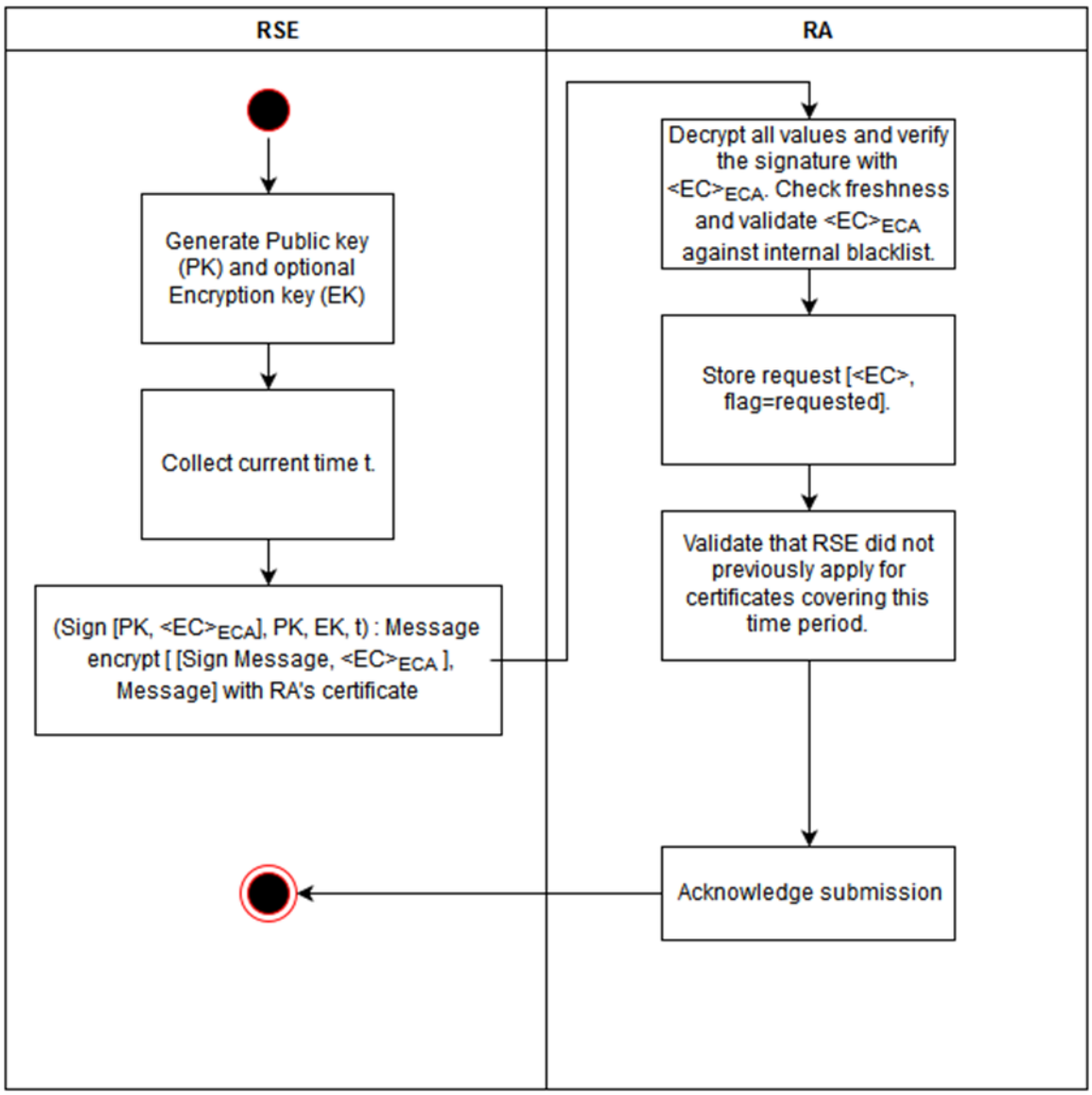


Figure 77 RSE-RA Communication

5.2.13.5.7.1 EE Request

The EE initiates the certificate request message in order to provide the RA with critical information (key parameters, current time, etc.) necessary for RSE application certificate generation. EE will send a certificate request message each time it requires a new certificate.

5.2.13.5.7.1.1 Security / Privacy

The Certificate Provisioning Request message shall use signing and encryption to ensure:

- The request has not been modified in transit
- The RA can verify the message came from the device
- The request is shared confidentially between the device and RA

The EE shall sign the request with the enrollment certificate. The EE shall also encrypt the request using the RA certificate and encapsulate in a 1609.2 frame of type encrypted.

5.2.13.5.7.1.2 Message Contents

The EE shall use the ASN.1 defined for creating the request certificate message, details can be found at RA - Request Application Certificate Provisioning. In order for a request to be validated by the RA, the EE shall include the following information in the certificate provisioning request message:

- Version
- EE enrollment certificate
- A signed certificate signature key (signed with enrollment certificate)
- A response encryption key that PCA would use to encrypt the issued certificate to EE
- Optionally: a certificate encryption key that PCA would include in the issued certificate
- Current device time: 32-bit denoting number of seconds since the Epoch (as defined in 1609.2)
- Requested certificate start time: 32-bit denoting number of seconds since the Epoch (as defined in 1609.2)

5.2.13.5.7.2 RA Response

The RA response to the certificate provisioning request message may be *accept* (indicated by a request acknowledgement) or *reject* (indicated by a HTTP 500). In case of reject, RA shall return error code "HTTP 500" to EEs. Specific error codes should be hidden from EEs and not provide useful information to malicious actors. The RA shall log the specific error for future investigation.

5.2.13.5.7.2.1 RA - EE Request Acknowledgement

The request acknowledge message is initiated by the RA in response to a certificate provisioning request message successfully received from the EE. If the EE request is received and processed without triggering an error (invalid signature, blacklisted, etc.), the RA processes the certificate request and begins certificate pre-generation. The request acknowledge message provides the EE with an URL and the time where and at which the first certificate batches will be available for download.

5.2.13.5.7.2.2 Security / Privacy

The request acknowledge message shall use signing and encryption to ensure:

- The request has not been modified in transit
- The device can verify that the message came from the RA
- The request is shared confidentially between the device and RA

The RA shall sign and encrypt the request acknowledge message using the RA certificate and encapsulate in a 1609.2 frame of type encrypted.

5.2.13.5.7.2.3 Message Contents

The RA shall use the ASN.1 defined for creating the request acknowledge message in RA - Request Application Certificate Provisioning and shall include the following information:

- Case: Certificate Provisioning Request *Accept*
    - Version
    - Low order 8-bytes of the SHA-256 hash of the encoded "ToBeSigned" certificate request from the device. Returns 0 if RA cannot calculate hash of the original request
    - Time at which the first certificate file will be available for download (represented by IEEE 1609.2 Time32)
    - URL of the certificate repository (common for all devices serviced by an specific RA)
- Case: Certificate Provisioning Request *Reject*
    - HTTP-500 Error Code

5.2.13.5.7.3 EE Response

If the RA provides a positive acknowledgement (*accept)* to a certificate provisioning request, the EE moves forward with the certificate download process using the provided URL given in the acknowledge message.

If the EE does not receive an acknowledgement from the RA in response to the request within defined time, EE should retry. Several conditions may necessitate the EE sending the request more than once. This may be due to:

- Request lost in transit (no TCP ack)
- RA offline, unavailable or RA network address has changed (EE must query DNS for latest RA network information)
- EE possesses an invalid RA certificate and cannot establish secure communications
- EE received HTTP-500 Error Code

The EE should not attempt to transmit the Request Certificate message without completing the prerequisites.

5.2.13.5.8 ASN.1 Specification

ee-ra.asn

5.2.13.6 Step 13.3: Download RSE Application Certificate

5.2.13.6.1 Goals

The goal is to provide a reliable, secure and timely method for RSEs to download certificates.

5.2.13.6.2 Background and Strategic Fit

The download will include the RSE application certificate, a local certificate chain file (LCCF), and a local policy file (LPF). The RSE will first attempt to download a LCCF (containing the PCA certificate chain required to validate the application certificate) and a LPF and process both LCCF and LPF to ensure that it is able to interpret certificates generated by the SCMS correctly. The RSE will then attempt to download the RSE application certificate.

5.2.13.6.3 Assumptions

- RSE has successfully executed Step 13.1: Request RSE Application Certificate
- RA retrieved the issued certificate from PCA, zipped, and stored it in a folder for RSE to download

5.2.13.6.4 Process Steps

1. RSE downloads the Local Policy File (LPF) and the Local Certificate Chain File (LCCF), as before in Step 13.1: Request RSE Application Certificate
    a. If there is an updated LCCF, RSE applies all changes to its trust-store (necessary for PCA Certificate Validations)
    b. If there is an updated LPF, RSE applies those changes. If those changes include changes to request parameters, RSE must skip this use case and follow Step 13.1: Request RSE Application Certificate.
2. RSE downloads application certificates using the API documented in RA - Download Application Certificate

5.2.13.6.5 Error Handling

The RSE will abandon further interactions with the RA after a certain number of failed communication attempts resulted in errors.

5.2.13.6.6 Requirements

Table 65 Use Case 13.3 - 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_A</td><td>RFC5289</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>
</table>

Key	Status	Summary	Description	Justification	Notes	Component/s
			ES_256_GCM_SHA384			
			0xC0,0xAC TLS_ECDHE_ECDSA_WITH_AES_128_CCM RFC7251			
			0xC0,0xAD TLS_ECDHE_ECDSA_WITH_AES_256_CCM RFC7251			
SCMS-411	EE REQUIREMENT	EE Authentication to RA for Request	The EE shall authenticate its requests with its enrollment certificate and signed timestamp to avoid replay attacks on the RA.	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.	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.	On-board Equipment (OBE), Road-side Equipment (RSE)
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	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	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
				OBE can validate the RA's TLS certificate.	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.	
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 (comparehttps://jira.campllc.org/browse/SCMS-859~~SCMS-859~~, SCMS-504) and the X.509 CRL (https://jira.campllc.org/bro	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
					wse/SCMS-405~~SCMS-405~~).	
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 (https://jira.campllc.org/browse/SCMS-537~~SCMS-537~~) and RA-EE authentication (https://jira.campllc.org/browse/SCMS-539~~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	It is not cost effective to provide OBEs with TLS certificates currently.	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
				requests, download certificates or files.	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	
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)

Key	Status	Summary	Description	Justification	Notes	Component/s
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-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	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
				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		
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-544	CLOSED	Download resume	RA shall support byte-wise resume of certificate batch, certificate file, or policy file, downloads, even if EE switches the IP address.	To improve reliability of the download protocol.		RA

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-590	CLOSED	Certificate availability	RA shall make application certificates available for download by the RSE.	So that proper RSEs can participate in V2I applications.		RA
SCMS-599	CLOSED	Keep valid application certificates	RA shall allow the RSE to download the application certificate that has previously been downloaded, so long as the RSE's credentials are still valid and the certificate is not expired.	This feature helps RSEs recover from a loss of certificates at the RSE level (e.g., disk corruption).		RA
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-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		RA

Key	Status	Summary	Description	Justification	Notes	Component/s
				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.		
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)

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-958	EE REQUIREMENT	Error code: eeConnectionFailed	EE shall log this error code, if it cannot connect to RA because there is a connection timeout.	To enable EE side diagnostics.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-964	CLOSED	Error code: raCertFileUnavailable	RA shall return status code HTTP 500 to EE, if certificate batch is not available and log "Error code: raCertFileUnavailable.	to enable EE side error handling.		RA
SCMS-967	EE REQUIREMENT	Error code: eeCertFileVerificationFailed	EE shall log this error code, if EE is not able to verify the digital signature of an encrypted certificate.	To enable EE side diagnostics.	This is out of scope since it defines EE behavior. This is for a single-issue certificate that has been encrypted and digitally signed by PCA.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-969	EE REQUIREMENT	Error code: eeCertificateFileDecryptionFailed	EE shall log this error code, if EE is not able to decrypt an encrypted certificate.	To enable EE side diagnostics.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-971	EE REQUIREMENT	Error code: eeCertificateVerificationFailed	EE shall log this error code, if EE is not able to verify a certificate.	This is to verify the issued certificate.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-973	EE REQUIREMENT	Error code: eeCertContentFalse	EE shall log this error code, if EE is not able to parse a certificate, or if the certificate has wrong content.	To enable EE side diagnostics.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-976	CLOSED	Error code: raInvalidURL	RA shall log "Error code: raInvalidURL", if EE requests invalid URL.	To enable server side diagnostics and to avoid giving potential attackers relevant information	This is not in ASN.1 but http 404	RA
SCMS-977	CLOSED	TLS error codes	RA shall return standard TLS error codes if TLS errors occur.	In order to enable client side error handling.		RA
SCMS-978	CLOSED	Error code: raAuthenticationFailed	RA shall log "Error code: raAuthenticationFailed", if EE-to-RA authentication fails.	To enable server side diagnostics and to avoid giving potential attackers relevant information.		RA
SCMS-979	EE REQUIREMENT	Error code: eeAuthenticationFailed	EE shall log "Error code: eeAuthenticationFailed", if RA-to-EE authentication fails.	To enable EE side diagnostics.	This is out of scope since it defines EE's behavior. This is part of TLS handshake. OEM defines EE error handling.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-981	CLOSED	Error code: raNoPcaCertificateChainFileAvailable	RA shall return status code HTTP 500, if Local Certificate Chain File is not available and log "Error code: raNoPcaCertificateChainFileAvailable".	To enable client side error handling.		RA

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-1065	CLOSED	Error code: raBlacklisted	RA shall log "Error code: raBlacklisted" if the requesting EE has been blacklisted.	Error's produced by an EE should always be logged for diagnostic purposes and never returned to the EE to avoid giving a potential attacker sensitive information.	RA response to EE shall follow SCMS-1397	RA
SCMS-1076	EE REQUIREMENT	Error code: eePolicyVerificationFailed	EE shall log this error code, if EE is not able to verify the digital signature of the local policy file.	As the local policy file contains security relevant configuration, it is essential to verify if a recently downloaded version of that file is coming from a trustworthy source.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1090	CLOSED	Error code: raTcpErrors	RA shall return standard TCP error codes if TCP errors occur and log "Error code: raTcpErrors" and the encountered TCP error.	in order to enable client side error handling.		RA
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	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)

Key	Status	Summary	Description	Justification	Notes	Component/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.			
SCMS-1201	EE REQUIREMENT	EE certificate download via HTTPS over TCP/IP	EE shall use HTTPS (TLS) over TCP/IP to download files from the SCMS.	In order to use standard internet technology.	This is out of scope as it defines EE 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	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
					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.	
SCMS-1263	EE REQUIREMENT	EE download resume	EE shall try byte-wise resume of CRL downloads from the CRL store, certificate batches, certificate files, or policy files from RA in case a previous download failed.	This will improve reliability of the download process and reduce communication cost.		On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1270	EE REQUIREMENT	Network connection	EEs shall use TCP/IP to communicate with the SCMS.	SCMS components (server) are only reachable by standard TCP/IP networking methods.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1279	EE REQUIREMENT	Error code: eeCertificateDecryptionFailed	EE shall log this error if certificate decryption failed at EE.	To allow error reaction and investigation.	Out of scope as it defines EE behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1280	EE REQUIREMENT	Error code: eeCertificateNotReadable	EE shall log this error if any certificate is not readable.	To enable error reaction and investigation.		On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-1282	EE REQUIREMENT	Error code: eeDecompressionError	EE shall log "Error code: eeDecompressionError", if it is not able to decompress the received certificate.	To allow error reaction and investigation.	Out of scope as it defines EE behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1303	EE REQUIREMENT	Verification of certificate validity	EE shall verify the validity of a received certificate against IEEE 1609.2-v3-D12, clause 5.1 and 5.3.	To verify if the certificate is issued by a trustworthy source and therefore messages signed by this certificate can be trusted.	This is for testing that SCMS issued valid and proper certificates. This is out of scope since it defines EE behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
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-1397	TESTS FAILED	Error reporting to EE	The SCMS Components shall return error code "HTTP 500" to EEs in	Specific error codes should be hidden from EEs to prevent useful information from being	• Standard TCP (https://jira.campllc.org/browse/SCMS-1090~~SCMS-1090~~) and	CRL Store, RA

Key	Status	Summary	Description	Justification	Notes	Component/s
			response to all application level errors at RA.	provided to malicious actors	TLS (https://jira.campllc.org/browse/SCMS-977~~SCMS-977~~) errors shall be reported to EEs • All errors at the HTTP and higher levels shall be HTTP 500 for RA & ECA	
SCMS-1404	EE REQUIREMENT	EE send data via HTTP post over TCP/IP	EE shall use HTTP post to send data towards the RA	To allow the SCMS endpoint to serve everything based on HTTP protocol	RA - Services View will document the actual HTTP post details. This is out of scope as it defines EE behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1405	CLOSED	RA accept authenticated HTTP post requests	RA shall accept HTTP post requests only from authenticated EEs.	To allow the SCMS endpoint to serve everything based on HTTP protocol	RA - Services View will document the actual HTTP post details.	RA
SCMS-1420	SCMS POC OUT OF SCOPE	Keep track of which authorization (pseudonym, ID, application) certificates are downloaded	The RA shall keep track of how far into the future each device has downloaded its certificates.	This allows revoked devices to be removed from the CRL (or deprioritized for inclusion on the CRL) once they exhaust the	This is an optimization for CRL handling and therefore out of scope for PoC implementation.	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
				set of certificates that they have downloaded.		
SCMS-1421	EE REQUIREMENT	LCCF validation in EE	The EE shall verify the LCCF and then update the internal certificate store each time it receives a new LCCF.	To have the latest certificate chain update available for validating certificates and answering P2P certificate requests.	This is out of scope as it defines EEs behavior	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1691	CLOSED	One RSE Application certificate file per zip file	RA shall zip exactly one application certificate file per certificate download file. The content of the certificate file is the binary representation of the application certificate. • X • X shall be the lower 8-bytes of the SHA-256 hash of the device request in hexadecimal (case insensitive) • Where there is no extension	There is only one RSE application certificate allowed at any given time (except for overlap) and therefore there should only be one certificate per zip file.	The device's request hash is different for each download, as application certificates need to be requested each time and are not pre-generated.	RA
SCMS-1692	CLOSED	RSE application certificate files	RA shall provide each application certificate to be downloaded by EE as a X.zip file in the folder provided in the ack message to the provisioning request.	This convention gives the RSE the ability to locate the file at the RA.		RA

Key	Status	Summary	Description	Justification	Notes	Component/s
			• X.zip • Where X shall be the lower 8-bytes of the SHA-256 hash of the device request in hexadecimal (case insensitive) • Where the extension is .zip in lowercase			
SCMS-2463	EE REQUIREMENT	EE transactions per TLS session	EE shall perform as many SCMS transactions as possible using a single TLS session.	To minimize the number of separate TLS sessions to the SCMS. This will reduce the resources required and improve throughput.	This is out of scope as it defines EE behavior.	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)

54 issues

5.2.14 Use Case 16: RSE Application and OBE Identification Certificate Revocation

RSE Application and OBE Identification certificate revocation will be integrated with the to-be-awarded "Misbehavior Authority Integration" Project as SCMS PoC release 2.0.

5.2.14.1 Background and Strategic Fit

5.2.14.1.1 Misbehavior Investigation

Misbehavior investigation works as follows for RSE application certificates and OBE identification certificates (non-pseudonymous certificates without linkage values). Misbehavior investigation is further described in 16.2. RSE Application and OBE Identification Certificate Misbehavior Investigation.

Since MA can link certificates based on the revocation identifier field (RIF), MA now inputs the information to its global misbehavior detection algorithm. Note that misbehavior reports involving these types of certificates can be identified and directed (within the MA) to particular misbehavior investigation algorithms, based upon the PSIDs associated with the certificate information included in the misbehavior reports. Note that the considered certificates are not covered by pseudonymous considerations, such that providing the digest of the enrollment certificate does not pose a privacy concern.

5.2.14.1.2 Revocation

Revocation works as follows for the RSE application certificates and OBE identification certificates (non-pseudonymous certificates without linkage values). Revocation is further described in 16.3. RSE Application and OBE Identification Certificate Revocation (CRL, blacklist).

1. MA-RA:
    a. Using the RIF, the MA instructs the RA to add the enrollment certificate to the blacklist. Further, the MA requests a list of further valid certificates that were issued to the same enrollment certificate (e.g., all non-expired predecessors or successors).
    b. RA adds enrollment certificate to internal blacklist
    c. RA returns a list of all non-expired certificates that were issued to the identified enrollment certificate
2. The MA adds CertIDs (e.g., CertID8) of all non-expired certificates to the CRL

Note that revocation will be performed for all PSIDs in the reported certificate. Therefore, the CRL does not have to specify PSIDs. Further, certificates will carry all PSIDs associated with the enrollment certificate that was used to request those certificates. This implies that blacklists are not PSID-specific either.

5.2.14.2 Assumptions

Non-pseudonymous certificate types - OBE identification certificates and RSE application certificates - integrate an 8-byte revocation identifier field (RIF) that is calculated as follows:

- [LSB0-7] of RIF: the eight least significant bytes [LSB0-7] of the SHA-256 hash of the EE's enrollment certificate, i.e., RIF_[LSB0] = hash_of_enrollment_cert[LSB0], RIF_[LSB7] = hash_of_enrollment_cert[LSB7], etc.

5.2.14.3 Step 16.4: RSE CRL Check

5.2.14.3.1 Goals

- The RSE needs to perform several computational steps to check whether a received Basic Safety Message (BSM) has been sent by a revoked EE
- This document lists the corresponding requirements

5.2.14.3.2 Assumptions

The RSE received a CRL as defined in Use Case 6: CRL Download.

5.2.14.3.3 Process Steps

1. Optional: RSE expands the CRL and calculates the linkage values for the current i-period based on the CRL entries (linkage seeds) of the CRL pseudonym certificate section. This only applies if the RSE wants to verify received BSMs.
2. Whenever RSE receives a new unknown OBE identification certificate, RSE will calculate the certificate digest of that unknown certificate and check whether the CRL lists it
    a. If yes, then RSE discards the received certificate
    b. Otherwise, RSE accepts the received certificate as verified
3. Optional: Whenever RSE receives a new unknown certificate, it checks whether the linkage value of that unknown certificate is listed in RSE's expanded CRL (from Step 1)
    a. If yes, then RSE discards the received certificate
    b. Otherwise, RSE accepts the received certificate as verified
4. Optional: Before the end of each i-period, RSE will:
    a. Update its expanded CRL and calculate the linkage value for the next i-period

b. Remove entries from the expanded CRL that belong to revoked devices that ran out of certificates, if a CRL entry indicated that the revoked device does not have any more valid certificates. Note that the RSE may not immediately remove such entries but add a safety buffer.

5.2.14.3.4 Requirements

Table 66 Use Case 16.4 - Requirements

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-786	CLOSED	CRL download	CRLG shall provide CRL via CRL store.	so that EEs can check revocation status	CRL entries may be dependent on the type of certificate	CRLG
SCMS-1171	EE REQUIREMENT	EE revoked	EEs that are revoked shall not attempt to download LCCF, LPF, pseudonym certificates, identification certificates or file misbehavior reports. Exceptions to this are: • EE is unable to determine its revocation status • EE has no pseudonym or identification certificates available in local storage • EE is attempting to perform a re-enrollment operation	To avoid unnecessary load at the RA.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1221	EE REQUIREMENT	EE processes CRL	EE shall process the updated CRL/CRL chunk and update its CRL within 1 minute after receiving the update CRL or CRL chunk.	CRLs/CRL chunks are updated daily and EE must always update its stored CRL in a timely fashion.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-1223	EE REQUIREMENT	EE checks against CRL for all certificate types	EEs shall check all received relevant sender certificates, i.e., certificates of received messages that are processed, against the most recent CRL. If the sender certificate is listed, EE shall discard the received message. EE shall perform this check using the mechanism described in IEEE 1609.2-2016.	EEs also check all relevant certificates, i.e., certificates of received messages that are processed, against the CRL. This includes OBE pseudonym, OBE identification, and RSE application certificates. It is up to EE whether it checks non-relevant certificates, i.e. certificates or received messages that are not processed, against the CRL.	These checks are specified in IEEE 1609.2. Clause 5.1.3.4 describes how an EE checks whether a pseudonym certificate has been revoked by calculating the linkage values from the linkage seeds listed in the CRL, and comparing the calculated linkage value against the linkage value in the inspected certificate. Clause 6.4.10 and 6.4.11 contain additional information about linkage values. Clause 5.1.3.5 describes how an EE checks whether an OBE identification and RSE application certificate has been revoked by calculating the hash value of the inspected certificate,	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
					and comparing it against a CRL entry. Clause 7 contains comprehensive information about CRLs. This is out of scope since it defines EE's behavior.	
SCMS-1224	EE REQUIREMENT	EE stops sending	EE shall stop sending over-the-air DSRC messages, if it detects that itself has been listed on the CRL. This is limited to the certificates of the PSID/SSP that was revoked.	If certificates of a particular PSID/SSP have been revoked, EE stops sending all messages related to that PSID/SSP. EE might still receive DSRC messages, and send messages related to other non-revoked PSID/SSPs.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1263	EE REQUIREMENT	EE download resume	EE shall try byte-wise resume of CRL downloads from the CRL store, certificate batches, certificate files, or policy files from RA in case a previous download failed.	This will improve reliability of the download process and reduce communication cost.		On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1285	EE REQUIREMENT	EE stops sending: revoked ECA for EE's	EE shall stop sending over-the-air messages, if it detects (via CRL) that its ECA, any ICA between its ECA and the root CA, or the root CA has been revoked.	In this case, EE's enrollment certificate also has been revoked.	This is out of scope since it defines EE behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
		enrollment certificate				
SCMS-1286	EE REQUIREMENT	EE stops sending: revoked PCA for EE's certificates	EE shall stop using all pseudonym/identification/application certificates issued by a certain PCA, if EE detects (via CRL) that anything on the pseudonym certificate chain, including PCA, ICA, or Root CA has been revoked.	If the PCA or anything in its chain was revoked, all pseudonym/identification/application certificates are also revoked.	This is out of scope since it defines EE behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

8 issues

5.2.14.3.5 Not Doing

- For POC and CV Pilots, RSE application certificates are not listed on CRLs but revocation is enforced by not renewing certificates. At a later stage, this might be changed.
- In that case, the following requirement needs to be added: If RSE recognizes itself on the CRL, the RSE will stop sending over-the-air DSRC messages related to the indicated PSID/SSP. This also applies if RSE recognizes that the ECA, that issued RSE's enrollment certificate, or the PCA that issued RSE's certificates, has been revoked.

5.2.15 Use Case 18: Provide and Enforce Technical Policies

5.2.15.1 Goals

- Provide mechanisms to create an SCMS manager configuration policy
- Provide mechanisms to create policy settings and then distribute those policy settings to all SCMS components and EEs
- Provide mechanisms for individual SCMS operators to define and distribute local policies to EEs
- Provide mechanisms to distribute IEEE 1609.2 certificates to SCMS components and EEs

5.2.15.2 Background and Strategic Fit

The SCMS manager needs to set up a list of SCMS manager, technical, configuration choices and, therefore, will design technical, global policy files that are signed by the policy generator. The policy generator is an inherently centralized component.

There are local policy files affecting configurations for various SCMS components, as well as local policy files specifically for EEs. These local policy files may be signed by the appropriate SCMS component or secured through proprietary means approved by the SCMS manager. The global and local policy configuration options are displayed in Step 18.1: Policy Configuration Options.

Any changes in technical global policies will result in an updated global policy file. Global policies are categorized based on if they are relevant to EEs or non-relevant to EEs. All EE relevant policies are compiled and signed by the Policy Generator (PG). Non-EE relevant policies are then appended and the entire policy file is signed again. This structure allows global limits (signed by the central PG) to be securely communicated to EEs while allowing individual RAs to assign customized values. This is described in Step 18.3: Generate Global Policy file.

The local policy file is constructed by combining the complete, signed EE relevant section of the global policy file and RA specific custom policy values and/or local policies. Any of these changes in the technical policies, which directly affect the EEs operating under the jurisdiction of a particular RA, may also result in an updated local

policy file. Changes to customized global policies or locally defined policies may also result in an updated local policy file. The local policy file is then signed by the RA. The EEs being operated by that RA should then download that RA's specific, updated, local policy file whenever the EE next communicates with the SCMS. This is described in Step 18.2: Generate Local Policies for EEs.

There are also global certificate chain files, each version of which contains a copy of all SCMS component certificates. When any of these certificate chains change due to additions, revocations, and other revisions, the PG generates a new version of this file and distributes it to other SCMS components. In addition, each RA will create a local certificate chain file that contains (at a minimum) all of the PCA certificate chains that are used to issue pseudonym certificates for the EEs under that RAs authority. These are described in Step 18.5: Generate Global and Local Chain File.

5.2.15.3 Assumptions

- The SCMS manager develops and documents global policies
- Technical global policies may include acceptable ranges within which technical local policy options may be set

5.2.15.4 Design

There are three types of policies:

- Global policies
    - Are mandatory policies that are defined by the SCMS Manager and their values set by the SCMS Manager
    - The values can be a single value, a list or a range
    - Global policies are further categorized as EE relevant and non-EE (or component) relevant
    - Are signed by the PG
- Custom policies
    - Are global polices where a specific RA has modified the values
    - Only global policies that are list or range types my have custom values
    - The custom values can be single values, a list or a range
    - All custom values must be within the limits defined by the global values
    - Are signed by an RA
- Local policies
    - Are operator-specific and not defined by the SCMS manager
    - Local policies shall not override or be substituted for policies/limits defined by the SCMS manager
    - Are signed by an RA

There are two types of certificate chain files

- Global certificate chain file
    - Contains IEEE 1609.2 certificates of all SCMS components
    - Contains elector endorsements
    - Contains root CA endorsements
- Local certificate file
    - Contains all IEEE 1609.2 certificates that are required by a specific EE(s) to validate certificates issued to the EE
    - Contains elector endorsements
    - Contains root CA endorsements
    - Optionally, contains other SCMS component IEEE 1609.2 certificates that may be useful to the EE (to validate messages from other EEs)
- There is a global PG which is operated by the SCMS manager
- PG's certificate is signed by the top-level certificate (top-level ICA, if available, and root CA otherwise)
- PG signs the technical global policy files using its complete security chain
- The technical global policy files are mandatory sets of policies applicable to SCMS components and EEs
- A repository includes technical global policies for all the different SCMS components and EEs
- PG creates a technical global policy file containing global technical policies that are applicable to RAs and EEs and provides this file to all RAs
- The respective RA conveys local policies, which are pertinent to EEs, and to the EEs through local policy files constructed by each RA
- For the PoC, the technical global policy files can be transferred manually
- PG creates a Global Certificate Chain File (GCCF) containing all certificate chains of the overall SCMS and provides this file to all RAs

5.2.15.5 Step 18.1: Policy Configuration Options

5.2.15.5.1 Configuration Options

Configuration options are available for global and local policy parameters.

5.2.15.5.1.1 List of Global Configuration Options

Table 67 List of Global Configuration Options

Identifier	Affected Component	Configuration Option	Description	Required for PoC	Option Value for PoC	Comment
scms_version	(all)	SCMS Version	Version number of the SCMS	Y	1	
global_cert_chain_file_id	RA, PCA, EE	The Global Certificate Chain File (GCCF) version	This identifier is used to determine if the EE's version of the LCCF is up-to-date. The identifier for the LCCF is mirrored from the GCCF identifier by the RA and included in the LCCF file name. If the GCCF and related LCCF identifier in the LCCF file name indicate that a newer LCCF version is available, the RA will download the updated LCCF to the EE.	Y	2 bytes	Additional information on the GCCF File can be found in: Global Certificate Chain File.
overdue_CRL_tolerance	EE	Maximum time to maintain trust past next CRL date	How long an EE can continue to operate without a CRL update past a next CRL date before deciding that messages are not trustworthy and rejecting all of them (and turning on an	Y	2 weeks	This is not expected to be implemented in the EEs for PoC, but should be included in the global file for PoC. There must be some point at which this transition occurs, or CRLs

Identifier	Affected Component	Configuration Option	Description	Required for PoC	Option Value for PoC	Comment
			appropriate driver warning indicator).			are greatly weakened; and it makes sense for the tolerance to change as CRL distribution technology improves.
i_period	RA, EE	The length of the certificate's i-period in minutes	Currently the i-value is defined as one week (or 10080 minutes) but this might change with more connectivity.	Y	1 week	Global parameter
min_certs_per_i_period	RA, EE	Minimum certificates per i-period	The minimum number of certificates an EE receives per i-value (currently i-value = week). This number is also the j-value. Currently that is 20 per week and this might change over time.	Y	20	No maximum number capabilities. Note that CRL plan means that this can be set no higher than 255.
cert_validity_model	RA, EE	Certificate validity model	Pseudonym certificates are either "concurrently" or "non-concurrently" valid.	Y	concurrent	This setting means that the 20 certs per week are all concurrently valid during that week, also affects CRL.

Identifier	Affected Component	Configuration Option	Description	Required for PoC	Option Value for PoC	Comment
max_available_cert_supply	RA, PCA, EE	Maximum time with which to provision OBEs with pseudonym certificates	How many years worth of pseudo certs should be provided during the initial provisioning, and then maintained by top-off. For PoC, it is currently 3 years.	Y	3 years	Affects ability to make major changes in the overall system; also affects size of CRL.
max_cert_request_age	RA	Maximum Individual Certificate Request Age	Controls maximum amount of time an Individual Certificate Request can stay in the aggregator waiting to be shuffled.	Y	2 days	NOTE: this is only for certificate requests (not for top-offs) - minimum number or timing minimum, whichever comes first. In deployment, this will be an infinite number. Use of this option in deployment, if allowed, will require permission from the SCMS Manager.
shuffle_threshold	RA	Shuffle Threshold	Specifies the minimum number of Individual Certificate Requests to accumulate before shuffling and sending to PCA.	Y	1000	This is being considered as the minimum number for full privacy mode. Global sets acceptable option value limits. Local sets option value within Global limits.

Identifier	Affected Component	Configuration Option	Description	Required for PoC	Option Value for PoC	Comment
hash_of_request_size	RA, PCA	The length in bytes of the "hash of request"	The length in bytes of the "hash of request" that PCA and RA use to identify individual requests.	Y	32 bytes	Full hash for PoC
max_gpf_gccf_retrieval_interval	RA, PCA, LA	Maximum time interval between requesting GPF and GCCF updates	SCMS Components need to know when the contents of the Global Policy File (GPF) or Global Certificate Chain File (GCCF) change.	Y	1 day	Under current procedures, SCMS Components need to request the GPF and GCCF.
rse_application_cert_validity	RA, PCA, RSE	Validity period of RSE application certificates		Y	1 week + rse_application_cert_overlap	The value of this parameter shall be the total validity period, including the overlap interval. The initial PoC value should be 169 hours (1 week + 1 hour of overlap)
rse_application_cert_overlap	RA, PCA, RSE	Overlap period of RSE application certificates		Y	1 hour	

5.2.15.5.1.2 List of local configuration options

Table 68 List of Local Configuration Options

Identifier	Affected Component	Configuration Option	Description	Required for PoC	Option Value for PoC	Comment
shuffle_threshold	RA	Shuffle Threshold	Controls how many Individual Certificate Requests to accumulate before shuffling and sending to PCA.	Y	1000	This is being considered as the minimum number for full privacy mode; Global sets acceptable option value limits; Local sets option value within Global limits.
certs_per_i_period	RA, LA, EE	The actual number of certificates per i-value. certs_per_i_value must be equal or larger than min_certs_per_i_value.	This is the actual number of certificates an EE receives. For POC, this is an RA setting (i.e., the setting is per RA, or possibly sub-RA, not necessarily per EE).	Y	20/40	Current plan is to use 20 as the main PoC value, but to test that 40 would also work. Note that CRL plan means that this can be set no higher than 255. All affected components and/or EEs do not necessarily need to be notified separately from the results of cert update requests.
address_la1	RA	Addresses of LA_1	Used to communicate with Linkage Authority 1.	Y		Local configuration to be approved by SCMS Manager?
address_la2	RA	Addresses of LA_2	Used to communicate with Linkage Authority 2.	Y		Local configuration to be approved by SCMS Manager?

Identifier	Affected Component	Configuration Option	Description	Required for PoC	Option Value for PoC	Comment
address_pca	RA	Address of PCA	Used to communicate with the Pseudonym Certificate Authority.	Y		Local configuration to be approved by SCMS Manager?
tls_cert_ra	RA	TLS Certificate for RA	X.509 certificate used for transport layer security.	Y		Local configuration
shared_key_update_interval	PCA, LA	Shared symmetric key between LA and PCA	Maximum time between changes to pre-linkage value encryption/decryption key.	Y		Local configuration to be approved by SCMS Manager?
tls_cert_pca	PCA	TLS Certificate for PCA	X.509 certificate used for transport layer security.	Y		Local configuration
tls_cert_la	LA	TLS Certificate for LA	X.509 certificate used for transport layer security.	Y		Local configuration

5.2.15.5.2 Time Limited Configuration Options

It is valuable to define a time validity for options. This capability is very useful when the value of a configuration option changes. For instance, if i_period changes from one week to one day on January 1st, 2030, it is necessary to inform all EEs ahead of time about the change.

5.2.15.5.2.1 Format

This is done by including a time validity for each configuration option. Each configuration option entry can take the following time validity options:

1. N/A: there is no timely limitation for this configuration parameter
2. Sequence of configuration option value and time validity - There is a sequence of the following per configuration option entry
    a. The configuration option value
    b. Start time: The start-time when the configuration option value starts being valid. This is 'N/A' if the start-time was in the past. The current/first entry is always 'N/A.'
    c. End time: The end-time until the configuration option value ends being valid. This is 'N/A' if there is no defined end-time. The last entry is always 'N/A' (open ended).

5.2.15.5.2.2 Example

The following example provides two time dependent options for the parameter la_identifier_size:

```
la_identifier_size, {[2, N/A, 12/31/2015], [4, 1/1/2016, N/A]}
```

Here the text in [] is one option, and there are two options. The first option indicates a byte size of 2 bytes for la_identifier_size, valid until 12/31/2015 without any start date. The second option indicates a byte size of 4 bytes for la_identifier_size, valid from 1/1/2016 without any end date.

5.2.15.5.2.3 PoC

PoC will test the format and delivery of this extended policy configuration, but each identifier entry will have a single open-ended time span.

5.2.15.5.3 Requirements

1. *Uniqueness of global policy file*: Each global policy file shall be unique in the sense that it supersedes a previous global policy file, and there is exactly one valid technical global policy file
2. *Completeness of configuration option entry*: Each configuration option entry shall be complete in the sense that it provides a configuration option value for any time in

the future. This implies that the first time entry and the last time entry are always open ended ('N/A').

3. *Uniqueness of configuration option entry:* Each configuration option entry shall be unique and unambiguous, and at no point in time shall there be two valid entries
4. Minimum options: Each configuration option entry shall be minimal, and two subsequent time periods shall not use the same option value.

Table 69 Use Case 18.1 - Requirements

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-630	MANUAL PROCESS	Global policy file options	The global policy files shall include global configuration options from the list of configuration options listed in 18.1 - Policy Configuration Options	These values must be consistent throughout the SCMS in order to maintain nationwide interoperability	For PoC, these configuration options may be implemented manually.	
SCMS-631	MANUAL PROCESS	Local policy	Local policies shall include local configuration options from the list of configuration options listed in 18.1 - Policy Configuration Options	shuffle_threshold and certs_per_i_period must be consistent throughout the SCMS in order to maintain nationwide interoperability; remaining local policies may be unique for particular components and might be considered part of component configuration options, subject to SCMS Manager approval in most cases	For PoC, these configuration options will be implemented manually.	
SCMS-1226	EE REQUIREMENT	EE Timely Limited Configuration Options	EE shall support the use of timely limited configuration options.	It must be possible to define a time at which configuration option values change.		On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1227	EE REQUIREMENT	EE Timely Limited	For POC, EE shall support the parsing of a timely	For POC, this feature will not be tested; however, the final policy file format will be used.	EE does not need to parse, process, and handle more than one choice though. If there	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
		Configuration Options: POC	limited configuration option policy file.		is more than one choice, EE will only consider the first choice and assume that this first choice is always valid.	
SCMS-1349	SCMS POC OUT OF SCOPE	RA Timely Limited Configuration Options	RA shall support the use of timely limited configuration options.	It must be possible to define a time at which configuration option values change.		RA
SCMS-1350	SCMS POC OUT OF SCOPE	RA Timely Limited Configuration Options: POC	For POC, RA shall support the parsing of a timely limited configuration option policy file. RA does not need to parse, process and handle more than one choice though. If there is more than one choice, RA will only consider the first choice and assume that this first choice is always valid.	For POC, this feature will not be tested, however, the final policy file format will be used.		RA

6 issues

5.2.15.5.3.1 ASN.1 Specification

scms-policy.asn

5.2.15.6 Step 18.2: Generate Local Policies for EEs

5.2.15.6.1 Background and Strategic Fit

It is the responsibility of the authorized managers of EE operations to configure EEs properly. The RA, therefore, needs to provide its own appropriate, RA-specific local policy file to the EEs under its jurisdiction. Local EE policies are defined by OEMs, or other authorized managers of EE operations, for particular EE devices or EE device groups. The local EE policies must be consistent with relevant global policies. The RA needs to construct its own local policy file, within any restrictions imposed by global policies, and include all fields in the global policy file that are relevant to the EEs within that RA's jurisdiction.

5.2.15.6.2 Design

The Local Policy File (LPF) has one section of interest: Custom Policy. This section is a local representation of the Global Policy File with custom changes requested by the RA that issues the file. The RA has the option to remove any GPF values that are not relevant for any of the EE's that is services. The RA may also modify some global default values and replace them with local settings. The data elements for the Custom Policy section of the LPF are identical to the data elements for the GPF (listed here: Step 18.1: Policy Configuration Options). The Policy Generator (PG) must validate and sign the custom policy.

In creating the Custom Policy section of the LPF, it is assumed that the RA will start with the latest version of the Global Policy File (GPF) and make adjustments or delete specific data elements based on the needs of the EEs that it services. If the RA chooses to make no changes to the GPF, it must copy the content of the GPF into the Custom Policy section of the LPF. This allows the EEs to download a single policy file (the complete LPF) which contains all relevant policies.

Once the Custom Policy is created, the RA shall send a copy of the data structure to the PG to be validated and signed. Since the Custom Policy shares the same structure as the GPF, the RA's host ID is added to the Custom Policy to identify clearly which RA created the content. If the PG approves the Custom Policy, it will sign the complete structure (including the RA Host ID) and send it back to the RA. Note that if the RA Host ID changes, it will need to request a new Custom Policy signature to match the new Host ID.

Specific details on which GPF parameters may be modified or eliminated when translating the GPF into the Custom Policy section of the LPF must be defined by the SCMS Manager and implemented by the Policy Generator in validating signature requests.

5.2.15.6.3 Access & Download

To download the LPF, the EE will retrieve it from an URL defined in RA - Services View.

The EE will download the files via a HTTP get request, analogous with the mechanism used to download the pseudonym certificate batch files.

5.2.15.6.4 Requirements

Table 70 Use Case 18.2 - Requirements

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-1513	MANUAL PROCESS	RA to submit local policy file to PG for signature	RA shall submit the local policy file (LPF) to the PG for approval and signing prior to delivering the file to any EEs.	The LPF needs to be approved by the PG to ensure that it conforms to the limits set by the SCMS manager.	This is not in scope for the POC. The PG will check all values in the LPF to make sure that all required properties are included and that they do not exceed the limits defined by the SCMS Manager. If the PG approves of the LPF contents, it will sign the file and return it to the RA for distribution to EEs. The RA and PG will both add their signatures to the "signatures" list in the LPF data structure. EEs will check that both signatures are present and valid before applying the LPF values.	PG, RA
SCMS-1583	EE REQUIREMENT	EE parses LPF	EE shall parse the local policy file (LPF) and react to changed parameters accordingly.	EE must be able to understand the LPF. For each parameter, EE will either updates its configuration, or ignore that parameter (e.g., for new parameters).	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1687	MANUAL PROCESS	RA constructs its local policy file	The RA shall construct its own local policy file (LPF), within any restrictions imposed by	It is the responsibility of the authorized managers of EE operations to configure EEs properly. The RA therefore needs		RA

Key	Status	Summary	Description	Justification	Notes	Component/s
			global policies, and include all fields in the global policy file (GPF) that are relevant to the EEs within that RA's jurisdiction.	to provide its own appropriate, RA-specific local policy file to the EEs under its jurisdiction.		

SCMS-1726	CLOSED	File name format LPF and LCCF	RA shall name LPF and LCCF using the following scheme:
			`local_policy_<lpfglobalversion>_<lpflocalversion>.abc`
			`local_certificate_chains_<lccfglobalversion>_<lccflocalversion>.abc`
			where:
			<*globalversion> is the version id of the file.
			Both <*globalversion> and <*localversion> is 4 hex digit counter starting
				to have a defined naming scheme for files to be downloaded by EEs.	abc could e.g. be zip or tar.
					Version number is required to maintain re-freshness of LPF and LCCF
					The local policy file is expected to be updated at intervals; the unique identifier supports version control
					File naming format needs to be re-evaluated for full deployment.
						RA

Key	Status	Summary	Description	Justification	Notes	Component/s
			at 0000. abc is the file extension identifying the encoding format. The only file extension support for POC is oer that is indicated that file is encoded using OER. For each file, the counter value shall be unique to that file. The value shall be incremented each time the file's content changes.			

4 issues

5.2.15.6.5 Not Doing

The current Design foresees two sections in the LPF, whereas the second section is not used in the current version of the SCMS but might be utilized in future versions:

1. Custom Policy - This section is a local representation of the Global Policy File with custom changes requested by the RA that issues the file. The RA has the option to remove any GPF values that are not relevant to any of the EE's that is services. The RA may also modify some global default values and replace them with local settings. The data elements for the Custom Policy section of the LPF are identical to the data elements for the GPF (listed here: Step 18.1: Policy Configuration Options). The Policy Generator (PG) must validate and sign the custom policy.
2. Local Policy - This section contains local parameters that are not included in the Global Policy File but helps manage the EEs under RA's jurisdiction through additional configuration parameters. This section is signed by the RA only and added to the LPF after the Custom Policy was added.

5.2.15.7 Step 18.3: Generate Global Policies for EEs

5.2.15.7.1 Goals

The goal is to provide global policies that are valid for all EEs.

5.2.15.7.2 Background and Strategic Fit

The Policy Generator (PG) prepares a Global Policy File (GPF) that includes all global policies that are relevant to the EEs. The PG makes the GPF available to all SCMS components. The RA decides which of the global policies in the GPF are relevant for the EEs under that RA’s jurisdiction, determines specific values within option ranges allowed in the GPF, and creates an RA-specific Local Policy File (LPF) containing this information. The RA sends its LPF to the PG for approval and signature. The RA updates its LPF whenever there is a change in the GPF that affects the information in its LPF, and subsequently makes its current LPF available to all EEs within its jurisdiction.

5.2.15.7.3 Assumptions

- The PG will generate a Global Policy File (GPF), which includes global policies relevant for EEs, as listed in Step 18.1: Policy Configuration Options
- The PG will make the GPF available to all RAs
- The RA will combine policy fields in the GPF that are relevant to the EEs under its jurisdiction with its particular local policy fields relevant to those EEs
- The RA will send its combined local policy file to PG for assessment of compliance with all relevant global policies

- If approved, the PG will sign the RA-specific integrated policy file (local policy file - LPF) and send it back to the appropriate RA
- The RA will make the RA-specific integrated policy file (local policy file - LPF) available to all EEs within its jurisdiction
- The RA will convey changes to the global policies that affect EEs to all EEs within its jurisdiction through an updated LPF

5.2.15.7.4 Requirements

Table 71 Use Case 18.3 - Requirements

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-629	SCMS POC OUT OF SCOPE	SCMS Version	The global policy shall be capable of changing the SCMS version (see global policy parameters in 18.1 - Policy Configuration Options)	Major changes in the SCMS over time may be require; this SCMS version designation would indicate such a major change in the system	Out-of-scope for PoC as it is not intended to change version during PoC deployment	PG
SCMS-633	MANUAL PROCESS	Global Policy File Distribution	RA shall have mechanisms to receive the signed Global Policy File from the Policy Generator (PG).	The SCMS Manager develops and documents global policies, prepares appropriate global policy files for EEs and signs them within its Policy Generator function; RAs need to have these files to convey them to the EEs	Other authorized EE managers (such as OEMs) may also need to have mechanisms to receive signed global policy files from the PG in order to provide these files to EEs using for out-of-band communication. This might be a manual process for PoC.	RA

Key	Status	Summary	Description	Justification	Notes	Component/s

SCMS-634	CLOSED	File name format GPF and GCCF	PG shall name GPF and GCCF using the following scheme:
			`global_policy_<gpfglobal version>.abc`
			`global_certificate_chains_<gccfglobalversion>.abc`
			where:
			<*globalversion> is the version id of the GPF or GCCF.
			<*globalversion> is 4 hex digit counter starting at 0000.
			abc is the file extension identifying the encoding format. The only file extension support for POC is oer that is indicated that file is encoded using OER.
			For each file, the counter value shall be unique to that file. The value shall be incremented each time the file's content changes.
				The global policy file is expected to be updated at intervals; the unique identifier supports version control	File naming format needs to be re-evaluated for full deployment.	PG

SCMS-635	CLOSED	Generation time	The global policy shall have a generation time	In addition to the identifier, the generation time helps to establish	A generation time confirmation would	PG

Key	Status	Summary	Description	Justification	Notes	Component/s
				and confirm the precedence order of the global policy file	help with version control mechanisms	
SCMS-636	CLOSED	Activation time	The global policy shall have an activation time	The activation time determines at what point in time any changes in the global policy file should be implemented	This helps to provide an orderly implementation of changes to global policies. Having multiple global policy files concurrently valid should be avoided. The SCMS Manager should use global policy ID as a sequential versioning device, with only the most recent release being valid, whether its activation is before or after previously valid versions.	PG
SCMS-637	CLOSED	Signed Global Policy	The global policy file shall be signed by the PG.	The SCMS Manager has the responsibility to set global policies, so the PG function within the SCMS Manager	This file preparation and signing may be a manual process in PoC, since the SCMS Manager	PG

Key	Status	Summary	Description	Justification	Notes	Component/s
				needs to sign the global policy files to ensure authenticity	function is not being implemented	
SCMS-638	MANUAL PROCESS	Duplicate Entries	The RA shall ensure that the field entries in the local policy files that it provides to the EEs within its jurisdiction (e.g., OEM proprietary) are within the ranges and restrictions for those data fields in the current Global Policy File. If there is a duplicate field entry in both local and global policies, the global policy field entry, if more restrictive, shall take precedence.	Local policies need to be set within the allowable global policy range	For OBE, will not be tested in POC; likely to be implemented as a manual process in PoC on RA side.	RA
SCMS-640	SCMS POC OUT OF SCOPE	Field sizes for SCMS protocols and SCMS datatypes	The global policy shall be capable of changing the field sizes for SCMS protocols and SCMS data types (see global policy parameters in 18.1 - Policy Configuration Options)	Technological evolution may require longer field sizes for global policy parameters listed in 18.1 in the future; capability to change these allows for evolutionary change within the system	Out-of-scope for PoC	PG
SCMS-641	SCMS POC OUT OF SCOPE	Identifier sizes for SCMS protocols and SCMS datatypes	The global policy shall be capable of changing the identifier sizes (e.g. LA identifier) for SCMS protocols and SCMS data types.	Expansion of the number of components in the SCMS may require longer identifier	Out-of-scope for PoC	PG

Key	Status	Summary	Description	Justification	Notes	Component/s
				sizes in the future for global policy parameters; capability to change these allows for evolutionary change within the system		
SCMS-642	MANUAL PROCESS	Overdue CRL tolerance	The global policy shall be capable of specifying overdue_CRL_tolerance as a time period.	Overdue CRL tolerance is expected to vary as the numbers of deployed devices increases; this parameter therefore needs to be adjustable	Automated process is out-of-scope for PoC; likely to be implemented as a manual process in PoC	PG

10 issues

5.2.15.7.5 Design

Whenever there is a change in global policies that affect EEs, the RA constructs an updated version of its own LPF, gets its LPF approved (and signed) by the PG, and then makes the LPF available to the EEs within that RA's jurisdiction, i.e., whenever the EE submits a new certificate request, or otherwise contacts the RA, as appropriate. In the cases where the EE software and hardware can still support the global changes in the system, the EE will implement the changes upon receipt of the LPF containing those changes. If the policy changes are too significant for the EE to continue being functional, the EE may need to be updated or else possibly operate in a legacy mode. This could likely be managed by the relevant RA within the restrictions of global policies but is out-of-scope for PoC.

5.2.15.8 Step 18.4: Generate Global and Local Certificate Chain File

5.2.15.8.1 Goals

The intended use of the Global Certificate Chain File (GCCF) and Local Certificate Chain File (LCCF) is to facilitate the distribution of certificates among SCMS components and EEs. Collecting certificate chains into these files will significantly reduce the need for collaborative distribution of certificates. These files will be the primary mechanism to inform components and EEs about new certificates in the system including replacements for components that have been revoked or whose certificates have expired or retired.

5.2.15.8.2 Structure

The GCCF shall contain a copy of all SCMS component certificates. It will also contain the root certificate endorsement signed by electors and any elector endorsements for newly added electors. Specifically, it will contain endorsements for all electors' certificates that have been added since the launch of the SCMS and are still valid.

Each RA will create an LCCF that contains, at a minimum, all of the PCA certificate chains that are used to issue pseudonym certificates for its EEs (this is to support P2P certificate distribution) and the SCMS certificates of all components that the EE must interact with or trust (RA, MA, CRLG, Root CA and elector endorsements). Optionally, an RA may choose to provide other PCA certificate chains in the LCCF. Any EE connecting to its associated RA shall get the current LCCF if the RA has a later version than the EE. For the POC, all content in GCCF will be contained in the required section of LCCF and these files will be created manually. The GCCF and LCCF are not signed as each certificate within the file has a signature. The recipient of a GCCF or LCCF must validate all signatures up to a trusted CA prior to trusting certificates in these files.

Example: Let us say for a particular EE, RA uses PCA1 and PCA2 for generating its pseudonym certificates. RA must provide full certificate chains for PCA1 and PCA2 in the LCCF. The RA may choose to provide certificate chains for other PCAs as well.

Using this LCCF, EEs will be able to:

- Validate certificates generated by their PCA
- Respond to a certificate request in P2P certificate distribution protocol
- Validate certificates signed by any other PCA that the RA included in the LCCF

In order to validate certificates signed by PCAs that were not included in the LCCF, the EE must request the PCA certificate chains from other EEs via collaborative distribution. The EE must validate all PCA certificate chains obtained via collaborative distribution.

5.2.15.8.3 Access & Download

To download the LCCF, the EE will retrieve it from an URL defined in RA - Services View.

The EE will download the files via a HTTP get request, analogous with the mechanism used to download the pseudonym certificate batch files.

5.2.15.8.4 Format

The following diagram shows the relationship between GCCF and LCCF. Note that GCCF and LCCF do not contain initial elector or root CA certificates. However, they contain subsequent ballots endorsing elector and root CA certificates, as well as those new certificates themselves.

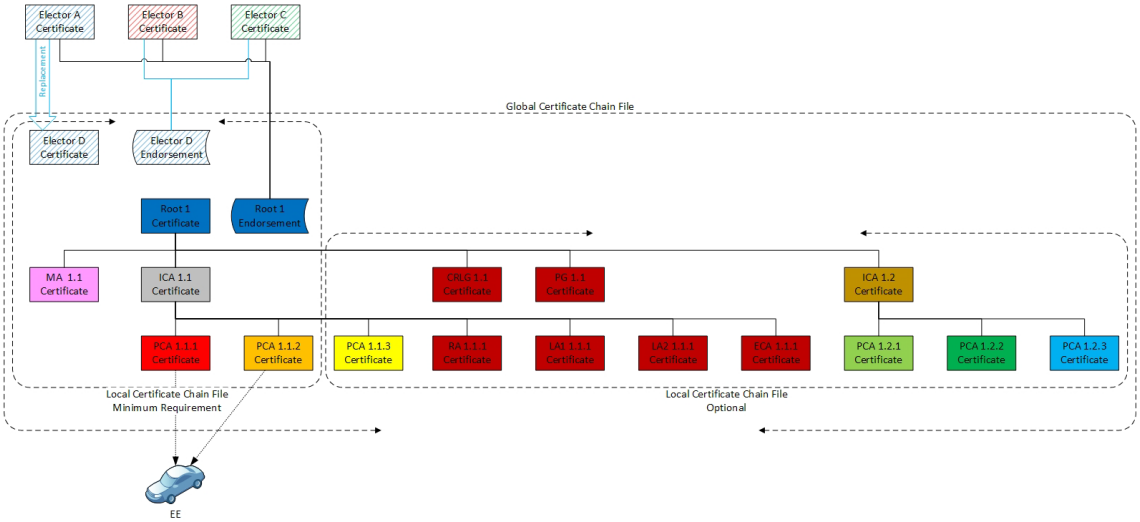


Figure 78 Relationship GCCF-LCCF

The following diagram shows the structure of GCCF and LCCF.

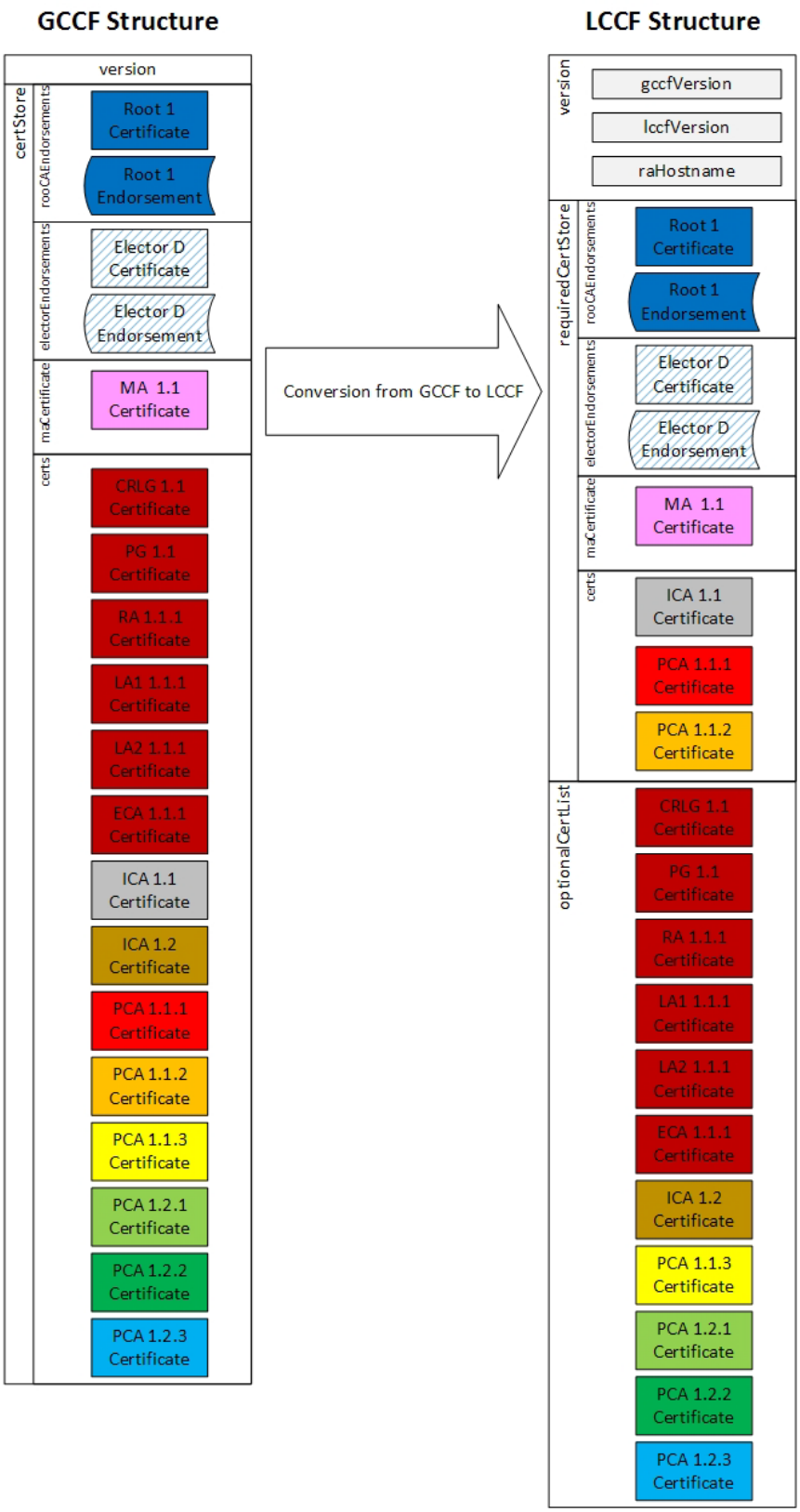


Figure 79 GCCF/LCCF Structure

5.2.15.8.4.1 Global Certificate Chain File (GCCF) Generation:

PG creates the GCCF and makes it available to all RAs whenever there is an update. It shall have the version number for updating purposes. Note that the version numbers are for management purposes only and do not serve any security purpose. The version number is the indicator that the content of the file has changed and is not an indicator of the validity of the content of the file. For the POC, the creation of GCCF is a manual process.

The GCCF structure shall contain the following elements:

Table 72 GCCF Structure Elements

Element	Notes
version	This is a 16 bit unsigned integer that represents a unique identifier for this GCCF. It is generated by the PG when the GCCF is published (note that this value is not signed by the PG, it is for informational purposes only).
certStore	This is a structure that holds the following values:

Element	Notes
rootCAEndorsements	One or more root certificate with signatures from at least 'n' valid electors where n >= the value of quorum defined in the GPF
electorEndorsements	List of electors that have been added since the launch of this instance of the SCMS (initial electors are not listed in the GCCF) with signatures from at least 'n' valid electors (not including the one endorsed) where n >= the value of quorum defined in the GPF
maCertificate	MA certificate
certs	List of certificates - Note that it is the responsibility of the generator of this file (the PG in the case of GCCF) to ensure that the list contains a complete chain with all signers required to validate any certificate on the chain all the way up to the root CA

Note that for the PoC, the GCCF will contain all certificates for all SCMS components.

5.2.15.8.4.2 Creation of Local Certificate Chain File (LCCF)

The RA creates the LCCF and makes it available to all EEs whenever there is an update. For the POC, the creation of LCCF is a manual process. It is up to OEMs or other authorized RA operators to decide whether they want to use the complete GCCF as their LCCF, or create only a specific, proprietary LCCF using limited, pertinent information from the GCCF.

The LCCF structure shall contain the following elements:

Table 73 LCCF Structure Elements

<table>
<tr><th>Element</th><th>Notes</th></tr>
<tr><td>version</td><td>This is a structure that holds the following values:<table><tr><th>Element</th><th>Notes</th></tr><tr><td>gccfVersion</td><td>This is the version number of the GCCF that was used to generate this LCCF</td></tr><tr><td>lccfVersion</td><td>This 16-bit, unsigned integer is a unique ID for this version of the LCCF that was derived from the specific GCCF on which it is based. The RA that issued this LCCF assigns this value.</td></tr><tr><td>raHostname</td><td>The fully qualified domain name (FQDN) of the RA that generated this file</td></tr></table></td></tr>
<tr><td>requiredCertStore</td><td>This is a structure that holds the following values:<table><tr><th>Element</th><th>Notes</th></tr><tr><td>rootCAEndorsements</td><td>The content of this field MUST be identical to the root CA endorsement list contained in the GCCF on which this file is based</td></tr><tr><td>electorEndorsements</td><td>The content of this field MUST be identical to the elector endorsement list contained in the GCCF on which this file is based</td></tr><tr><td>maCertificate</td><td>MA certificate</td></tr><tr><td>certs</td><td>List of certificates - This must include the full certificate chain for the root itself and for all ECAs and PCAs that it services. There may be other required content based on current SCMS policy.</td></tr></table></td></tr>
<tr><td>optionalCertList</td><td>This is a list of certificates. This list may include any additional certificates that the generating RA chooses to include. It should not duplicate any certificates already contained in the requiredCertStore.</td></tr>
</table>

Note that for PoC, the requiredCertStore will contain the full certificate chains for all PCAs and the optionalCertList will be empty.

5.2.15.8.4.3 Use Cases Affected

1. Use Case 1: SCMS Component Setup
2. Use Case 2: OBE Bootstrapping (Manual) and Use Case 12: RSE Bootstrapping (Manual)
    a. During bootstrap the device gets all the necessary certificates, ECA, RA, MA and LCCF
3. Step 3.3: Initial Download of Pseudonym Certificates, Step 3.5: Top-off Pseudonym Certificates, Step 13.3: Download RSE Application Certificate, Step 19.3: Initial

Download of OBE Identification Certificates, and Step 19.5: Top-off OBE Identification Certificates

a. RA provides the updated LCCF

4. Use Case 11: Backend Management

5.2.15.8.5 Requirements

Table 74 Use Case 18.4 - Requirements

Key	Status	Summary	Description	Justification	Notes	Component/s

SCMS-634	CLOSED	File name format GPF and GCCF	PG shall name GPF and GCCF using the following scheme:
			`global_policy_<gpfglobalversion>.abc`
			`global_certificate_chains_<gccflobalversion>.abc`
			where:
			<*globalversion> is the version id of the GPF or GCCF.
			<*globalversion> is 4 hex digit counter starting at 0000.
			abc is the file extension identifying the encoding format. The only file extension support for POC is oer that is indicated that file is encoded using OER.
			For each file, the counter value shall be unique to that file. The value shall be incremented each time the file's content changes.
				The global policy file is expected to be updated at intervals; the unique identifier supports version control	File naming format needs to be re-evaluated for full deployment.	PG

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-711	CLOSED	Global Certificate Chain List File	The Policy Generator shall create the Global Certificate Chain File (GCCF) with all valid certificate chains and a unique identifier encoded in the file name.	EEs need to know all valid certificate chains in order to validate messages from other EEs and communicate with the SCMS	For PoC, this file may be implemented manually (and is expected to be very small for PoC).	PG
SCMS-1062	MANUAL PROCESS	Revoke Component: PG Update Global Certificate Chain File	The Policy Generator shall update the GCCF and remove all impacted certificates as soon as it receives the notification that any back-end component has been revoked.	Having an updated certificate chain file makes verification processes at EEs more efficient.	When a back-end component is revoked, it may impact the validity of other certificates on the GCCF. Specifically, when any CA is revoked, all certificates that were issued by (i.e. signed by) that CA will become invalid and therefore must be removed from the GCCF. This is particularly important if a Root CA is revoked, but it applies equally to other CA revocations.	PG

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-1352	CLOSED	Local Certificate Chain File (LCCF) generation	RA shall use appropriate information from the Global Certificate Chain File to create a Local Certificate Chain File for EEs within its jurisdiction that contains at least all the PCA certificate chains that are used to issue pseudonym certificates for those EEs (this is to support P2P certificate distribution) and the GCCF/LCCF version ID per SCMS-1354.	to support P2P certificate distribution.	Based upon the current GCCF, each RA creates its own LCCF that contains, as a minimum, all the PCA certificate chains that are used to issue pseudonym certificates for the EEs within its jurisdiction and the GCCF/LCCF version ID per SCMS-1354. Optionally, RA could choose to provide additional PCA certificate chains in the LCCF.	RA
SCMS-1355	CLOSED	GCCF and LCCF generation in POC	RA shall put all content of GCCF in the required section of LCCF.	as there is only one single PCA in PoC	"PoC only" requirement. For POC these files will be created manually. GCCF and LCCF are not signed.	RA
SCMS-1413	MANUAL PROCESS	Revoke Elector: PG Update Global	The Policy Generator shall update the GCCF as soon as it receives the "Revoke Elector"	Having an updated certificate chain file makes verification		PG

Key	Status	Summary	Description	Justification	Notes	Component/s
		Certificate Chain File	message and remove the "Add Elector" message of the revoked Elector.	processes at EEs more efficient.		
SCMS-1626	CLOSED	Global Certificate Chain File Distribution	RA shall retrieve the Global Certificate Chain File (GCCF) from the Policy Generator (PG) at a regular interval - at least as frequently as specified in max_gpf_gccf_retrieval_interval.	The SCMS Manager develops policy about how often RA should retrieve GCCF and indicates this requirement in max_gpf_gccf_retrieval_interval in the GPF. For POC RA retrieves GCCF daily.	OEM may also need to have mechanisms to retrieve GCCF from policy generator. For PoC this interval is daily. This might be a manual process for PoC.	RA
SCMS-1632	EE REQUIREMENT	EE parse LCCF	EE shall parse the local certificate chain file (LCCF) and adjust its store of trusted certificate chains accordingly.	The EE needs to be able to understand the certificate chains included in the LCCF and to maintain its own list of trusted certificate chains based upon the input from the LCCF.	This is out of scope as it defines EE behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1726	CLOSED	File name format LPF and LCCF	RA shall name LPF and LCCF using the following scheme:	to have a defined naming scheme for files to be downloaded by EEs.	abc could e.g. be zip or tar. Version number is required to maintain re-freshness of LPF	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
			local_policy_<lpfglobalversion>_<lpflocalversion>.abc local_certificate_chains_<lccfglobalversion>_<lccflocalversion>.abc where: <*globalversion> is the version id of the file. Both <*globalversion> and <*localversion> is 4 hex digit counter starting at 0000. abc is the file extension identifying the encoding format. The only file extension support for POC is oer that is indicated that file is encoded using OER. For each file, the counter value shall be unique to that file. The value shall be incremented each time the file's content changes.		and LCCF The local policy file is expected to be updated at intervals; the unique identifier supports version control File naming format needs to be re-evaluated for full deployment.	

9 issues

5.2.15.8.6 ASN.1 Definition

cert-chain-files.asn

5.2.16 Use Case 19: OBE Identification Certificate Provisioning

5.2.16.1 Goals

The goal is the initial request of OBE identification certificates and then subsequent top-up.

5.2.16.2 Background and Strategic Fit

The OBE identification certificate provisioning is the process by which a bootstrapped OBE receives an identification certificate. As there are no location privacy or tracking concerns for identification certificates (but anonymity concerns), the RA is not required to shuffle the requests (unlike the case of pseudonym certificates). Butterfly keys are still used to allow easy top-up. Revocation is enabled by adding individual identification certificates to the CRL, but OBE Identification certificates do not use linkage values. Each OBE only receives one identification certificate per time period, except for a minimal overlap period to account for critical events.

This use case involves the following SCMS components:

- Pseudonym Certificate Authority (PCA)
- Registration Authority (RA)

The validity duration of identification certificate is dependent on the connectivity of the OBE. Smaller validity durations will potentially reduce the number of CRL entries but require more connectivity of the OBE to RA.

5.2.16.3 Assumptions

- The OBE is assumed to have a valid enrollment certificate that empowers it to request OBE identification certificates; specifically related to its SSID and SSP combination in the enrollment certificate. Some applications may require additional enrollment certificates to be added to the OBE, such as first responder vehicles. The addition of another enrollment certificate would occur in a secure environment.
- The OBE is assumed to have Root CA, RA and PCA certificates
- The OBE is assumed to have relevant address(s) to communicate with the RA
- The identification certificate that is issued has a validity period consistent with an associated application

5.2.16.4 Design

The following flow chart documents the general flow of steps an OBE needs to carry out in the given order to obtain identification certificates. It is not a 100% accurate description of the process. Please refer to the use case's steps and their requirements for a complete description of the process.

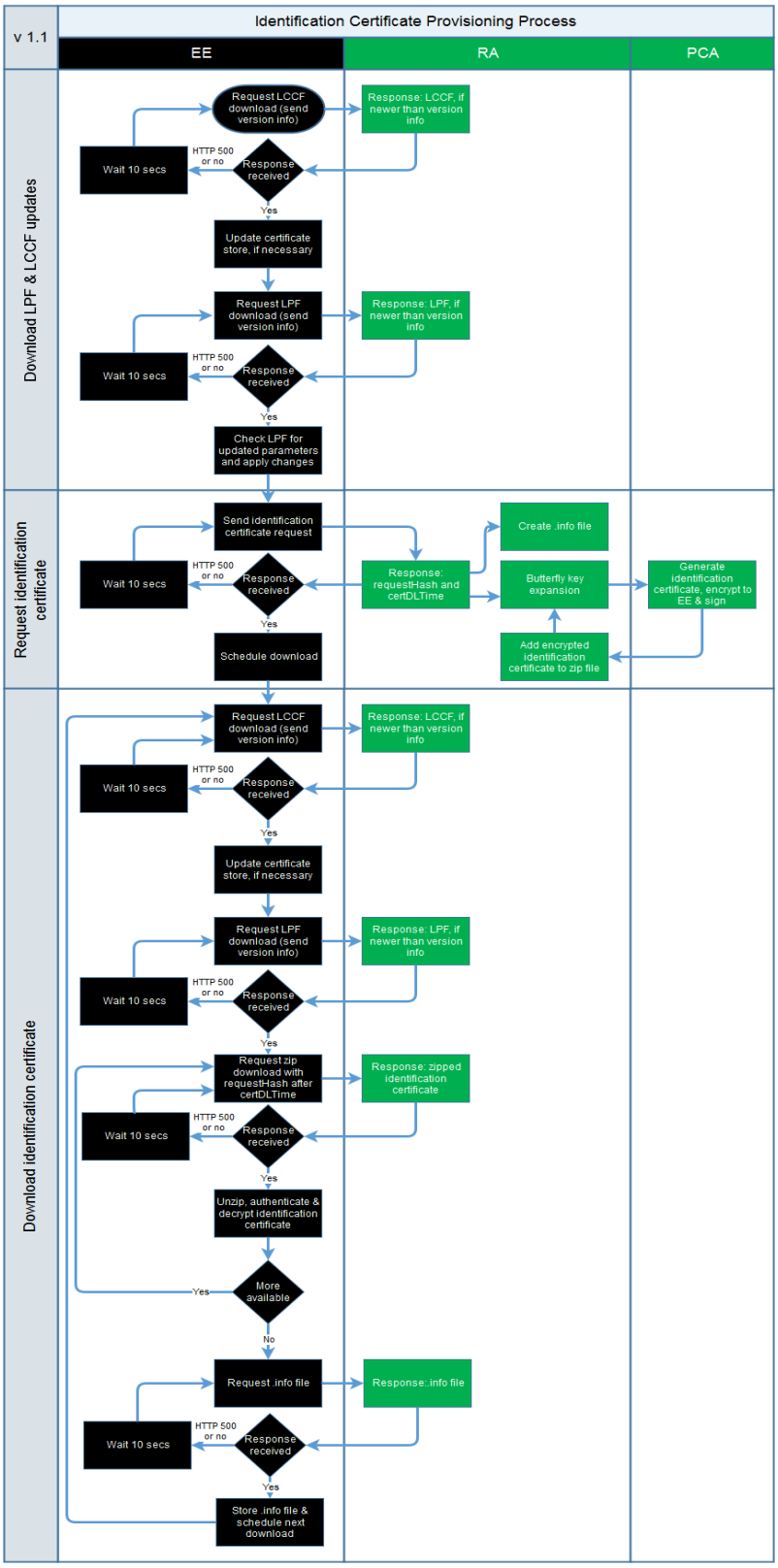


Figure 80 Identification Certificate Provisioning Process

OBE Identification certificates use Butterfly Keys for the certificate signature key (mandatory), butterfly keys for the certificate encryption key (optional), and butterfly keys for a response encryption key (mandatory). The use-case works as follows:

- Initial Request
    - EE creates a random, signature, butterfly key public seed (elliptic curve point) and a random, expansion, function parameter. EE signs those with its enrollment certificate.
    - Optional: EE creates a random, encryption, butterfly key public seed (elliptic curve point) and a random, expansion, function parameter. The resulting encryption keys are optionally used as encryption key in a certificate.
    - EE creates a response, encryption, butterfly key public seed (elliptic curve point) and a random, expansion, function parameter. The resulting encryption keys are used by PCA to encrypt the issued certificate to EE.
    - EE provides the signed (with enrollment certificate) signature, butterfly key public seed and expansion function parameter and a response, encryption, butterfly key public seed and expansion function parameter to RA. EE optionally provides the encryption butterfly key public seed and expansion function parameter. All parameters are signed with EE's enrollment certificate, and encrypted to RA.
    - RA verifies all received parameters
    - RA creates butterfly keys based on the policy (either policy linked to EE and/or PSID; e.g., one certificate per month for month, one hour of overlap between certificates). RA creates Butterfly keys for the certificate signature key, for the response encryption key, and optionally for the certificate encryption key.
    - RA creates a revocation identifier (RIF) for EE
    - RA does not shuffle nor wait on purpose before forwarding to PCA
    - RA forwards to PCA the certificate signature butterfly key (B_i), RIF, response encryption key (H_i), and optionally the certificate encryption key (E_i)
    - PCA issues the certificate using B_i and RIF and, if available, E_i. PCA then encrypts the issued certificate with H_i and signs the encrypted certificate
    - RA collects PCA's responses, bundles them in file(s), and stores it in a folder
    - EE can now download the file(s)
- Top-up
    - RA regularly checks and will initiate a generation of certificates as needed and defined in the policy

- RA will look-up RIF and calculate the proper Butterfly key(s) and send butterfly keys B_i, H_i, and RIF to PCA. If available, RA will also include E_i.
- PCA issues certificates, encrypts to EE, and sign the encrypted certificate
- RA collects PCA's responses, bundles them in file(s), and stores the file(s) in a folder
- EE can now download the file

At a high level, two steps are relevant towards an OBE:

1. Step 19.1: Request for OBE Identification Certificates
2. Step 19.3: Initial Download of OBE Identification Certificates
3. Step 19.5: Top-off OBE Identification Certificates

5.2.16.5 Step 19.1: Request for OBE Identification Certificates

5.2.16.5.1 Goals

The goal of this use case is to define the messages and actions that allow a device to request new identification certificates from the RA.

5.2.16.5.2 Background and Strategic Fit

The OBE decides to request an identification certificate from its preconfigured RA.

Having determined which RA to submit the request to, the OBE creates a request, signs it with the enrollment certificate, encrypts the signed request for the RA and sends it to the RA. The RA checks to make sure that the request is correct and authorized.

5.2.16.5.3 Assumptions

In order to facilitate the certificate request process, the following prerequisites should be met:

- The OBE has successfully completed Use Case 2: Bootstrapping

5.2.16.5.4 Process Steps

1. The OBE downloads the Local Policy File (LPF) and the Local Certificate Chain File (LCCF) by using the API documented in RA - Download local policy file and RA - Download Local Certificate Chain File
    a. If there is an updated LCCF, the OBE applies all changes to its trust-store (necessary for PCA Certificate Validations)
    b. If there is an updated LPF, the OBE applies those changes

2. The OBE creates the request, signs it with the enrollment certificate, encrypts the signed request for the RA and sends it to the RA using the API documented RA - Request Identification Certificate Provisioning.
3. The RA ensures that the request is correct and authorized before it starts with Step 19.2: OBE Identification Certificate Generation

5.2.16.5.5 Error Handling

1. The OBE will abandon further interactions with the RA after a certain number of failed communication attempts resulted in errors
2. The OBE will not attempt to execute the certificate provisioning process if it finds itself on the latest CRL (assumes that a willful violator has not compromised the device). The OBE will need to execute the certification/bootstrap process again to exit a revoked state.

5.2.16.5.6 Requirements

Table 75 Use Case 19.1 - 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_A</td><td>RFC5289</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>
</table>

Key	Status	Summary	Description	Justification	Notes	Component/s
			ES_256_GCM_SHA384 0xC0, 0xAC — TLS_ECDHE_ECDSA_WITH_AES_128_CCM — RFC7251 0xC0, 0xAD — TLS_ECDHE_ECDSA_WITH_AES_256_CCM — RFC7251			
SCMS-411	EE REQUIREMENT	EE Authentication to RA for Request	The EE shall authenticate its requests with its enrollment certificate and signed timestamp to avoid replay attacks on the RA.	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.	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.	On-board Equipment (OBE), Road-side Equipment (RSE)
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	OCSP stapling provides improved performance compared to CRLs. OCSP stapling is specified in RFC	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
				response so that the OBE can validate the RA's TLS certificate.	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.	
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	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
					compromised components to speak with the RA, the RA needs to validate against the SCMS component CRL (comparehttps://jira.campllc.org/browse/SCMS-859~~SCMS-859~~, SCMS-504) and the X.509 CRL (https://jira.campllc.org/browse/SCMS-405~~SCMS-405~~).	
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-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	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
					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	
SCMS-520	EE REQUIREMENT	Request only initial set	OBE shall make a certificate provisioning request only for the initial set of pseudonym and application certificates or when the certificate parameters change	Because top-up certificates are generated automatically by the RA.	This is out of scope as it defines OBE behavior.	On-board Equipment (OBE)
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	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)

Key	Status	Summary	Description	Justification	Notes	Component/s
			set to be 10 sec from the time of request.			
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-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	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
					EE's enrollment certificate (but not EE's private key). OCSP stapling is specified in RFC 6066, Section 8.	
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		RA

Key	Status	Summary	Description	Justification	Notes	Component/s
				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.		
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	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
				the latest version of that file.		
SCMS-954	EE REQUIREMENT	Error code: eePolicyVerificationFailed	EE shall log this error code in EE's error log file, if EE is not able to verify the digital signature of the local policy file.	To enable EE side diagnostics.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-956	EE REQUIREMENT	Error code: eePolicyFileParsingFailed	EE shall log this error code in EE's error log file, if EE is not able to parse the successfully downloaded local policy file (e.g., because 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 read 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-978	CLOSED	Error code: raAuthenticationFailed	RA shall log "Error code: raAuthenticationFailed", if EE-to-RA authentication fails.	To enable server side diagnostics and to avoid giving potential attackers relevant information.		RA
SCMS-987	TESTS FAILED	Error code: raWrongParameters	RA shall log "Error code: raWrongParameters", if a device sends request with wrong parameters.	To enable server side diagnostics and to avoid giving potential attackers relevant information		RA

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-988	TESTS FAILED	Error code: raRetries	RA shall log "Error code: raRetries", if the EE retries within the time specified in SCMS-522.	To enable server side diagnostics and to avoid giving potential attackers relevant information. Retry not allowed within 2 seconds.		RA
SCMS-990	TESTS FAILED	Error code: raMoreThanAllowedTries	RA shall return status code HTTP 500, if the EE violates SCMS-523, and log "Error code: raMoreThanAllowedTries".	To avoid DoS attacks		RA
SCMS-1065	CLOSED	Error code: raBlacklisted	RA shall log "Error code: raBlacklisted" if the requesting EE has been blacklisted.	Error's produced by an EE should always be logged for diagnostic purposes and never returned to the EE to avoid giving a potential attacker sensitive information.	RA response to EE shall follow SCMS-1397	RA
SCMS-1076	EE REQUIREMENT	Error code: eePolicyVerificationFailed	EE shall log this error code, if EE is not able to verify the digital signature of the local policy file.	As the local policy file contains security relevant configuration, it is essential to verify if a recently downloaded version of that file is coming from a trustworthy source.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-1082	CLOSED	Error code: raInvalidSignature	The RA shall log "Error code: raInvalidSignature", if the EE does not sign the certificate request with its enrollment certificate or if the signature is invalid.	To enable server side diagnostics and to avoid giving potential attackers relevant information	An unsigned request might be an indication for misbehavior.	RA
SCMS-1083	CLOSED	Error code: raRequestNotEncrypted	The RA shall log "Error code: raRequestNotEncrypted", if the EE does not encrypt the certificate request using the RA's 1609 certificate.	To enable server side diagnostics and to avoid giving potential attackers relevant information	An unencrypted certificate request might be an indication for misbehavior.	RA
SCMS-1084	CLOSED	Error code: raInvalidCredentials	The RA shall log "Error code: raInvalidCredentials", if the EE has invalid credentials (blacklisted, expired, unauthorized)	To enable server side diagnostics and to avoid giving potential attackers relevant information	A request with invalid credentials might be an indication for misbehavior.	RA
SCMS-1085	TESTS FAILED	Error code: raUnauthorizedRequest	RA shall log "Error code: raUnauthorizedRequest", if an EE makes an unauthorized request (invalid permissions)	To enable server side diagnostics and to avoid giving potential attackers relevant information	An unauthorized request might be an indication for misbehavior.	RA
SCMS-1086	TESTS FAILED	Error code: raMalformedRequest	RA shall log "Error code: raMalformedRequest", if an EE makes a malformed request not captured inhttps://jira.campllc.org/browse/SCMS-1082~~SCMS-1082~~,https://jira.campllc.org/browse/SCMS-1083~~SCMS-~~	To enable server side diagnostics and to avoid giving potential attackers relevant information.	A malformed request might be an indication for misbehavior.	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
			~~1083~~,https://jira.campllc.org/browse/SCMS-1084~~SCMS-1084~~, SCMS-1085.			
SCMS-1087	CLOSED	Error code: raMismatch	The RA shall log "Error code: raMismatch", if this RA does not service the requesting EE.	To enable server side diagnostics and to avoid giving potential attackers relevant information.	A request from an EE that is not serviced by the requested RA might be an indication for misbehavior.	RA
SCMS-1088	CLOSED	Error code: raInvalidTimeReceived	The RA shall return status code HTTP 500, if the EE has send an invalid system time, and log "Error code: raInvalidTimeReceived".	To avoid EEs using the invalid certificates		RA
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)

Key	Status	Summary	Description	Justification	Notes	Component/s
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	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
					the internal blacklist. The RA does not send out enrollment certificates to the IBLM.	
SCMS-1210	EE REQUIREMENT	EE Secure Key Storing	EE shall store the following keys in tamper-resistant (or equivalent) storage: • Private enrollment key • Butterfly key parameters (seed + expansion function parameter) • All private keys (e.g., of OBE application certificates and private keys calculated from the Butterfly key parameters)	To avoid extraction of private keys via software-based attacks.	This is out of scope since it defines EE's behavior. It is highly recommended to protect the content encryption key by a TPM-like mechanism that offers secure boot and that protects the keys against software-based attacks. Additional details are listed in Hardware, Software and OS Security	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1263	EE REQUIREMENT	EE download resume	EE shall try byte-wise resume of CRL downloads from the CRL store, certificate batches, certificate files,	This will improve reliability of the download process and reduce communication cost.		On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
			or policy files from RA in case a previous download failed.			
SCMS-1270	EE REQUIREMENT	Network connection	EEs shall use TCP/IP to communicate with the SCMS.	SCMS components (server) are only reachable by standard TCP/IP networking methods.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
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-1356	EE REQUIREMENT	EE uses internal certificate store	The EE shall use its internal certificate store to validate received SCMS certificates and respond to P2P certificate requests.	EEs need to be able to validate received SCMS certificates based on their certificate chain up to the SCMS root CA. EEs need to respond to P2P certificate requests to enable receiving EEs	EE does not need to store all certificate chains, the LCCF provides the minimum set and EEs can learn additional chains via P2P certificate request.	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
				to validate the certificate chain.	This is out of scope as it defines EE's behavior.	
SCMS-1397	TESTS FAILED	Error reporting to EE	The SCMS Components shall return error code "HTTP 500" to EEs in response to all application level errors at RA.	Specific error codes should be hidden from EEs to prevent useful information from being provided to malicious actors	• Standard TCP (https://jira.campllc.org/browse/SCMS-1090~~SCMS-1090~~) and TLS (https://jira.campllc.org/browse/SCMS-977~~SCMS-977~~) errors shall be reported to EEs • All errors at the HTTP and higher levels shall be HTTP 500 for RA & ECA	CRL Store, RA
SCMS-1404	EE REQUIREMENT	EE send data via HTTP post over TCP/IP	EE shall use HTTP post to send data towards the RA	To allow the SCMS endpoint to serve everything based on HTTP protocol	RA - Services View will document the actual HTTP post details. This is out of scope as it defines EE behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-1405	CLOSED	RA accept authenticated HTTP post requests	RA shall accept HTTP post requests only from authenticated EEs.	To allow the SCMS endpoint to serve everything based on HTTP protocol	RA - Services View will document the actual HTTP post details.	RA
SCMS-1421	EE REQUIREMENT	LCCF validation in EE	The EE shall verify the LCCF and then update the internal certificate store each time it receives a new LCCF.	To have the latest certificate chain update available for validating certificates and answering P2P certificate requests.	This is out of scope as it defines EEs behavior	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1512	EE REQUIREMENT	Generating Butterfly Key seeds and expansion function	The EE shall generate butterfly key seeds and expansion function.	Protect privacy of data during transfer by not extracting the keys.	For OBE pseudonym certificates, OBE will generate Butterfly key parameters for the certificate signature keys and the response encryption key. For OBE identification certificates, OBE will generate Butterfly key parameters for the certificate signature keys, and optionally for certificate encryption	On-board Equipment (OBE)

Key	Status	Summary	Description	Justification	Notes	Component/s
					keys and response encryption keys.	
SCMS-1625	TESTS FAILED	RA-EE Certificate Request Ack Message	RA-EE Certificate Request Ack Message shall contain the following information: Case: Certificate Provisioning Request Accept • Version • Low order 8-bytes of the SHA-256 hash of the encoded "ToBeSigned" certificate request from the device • Time at which the first certificate batches will be available for download (represented by IEEE 1609.2 Time32) • URL of the certificate repository (common for all devices serviced by a specific RA) Case: Certificate Provisioning Request Reject • HTTP 500 error code	As the EE needs to know, when and where it can go to download certificates.		RA

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-2463	EE REQUIREMENT	EE transactions per TLS session	EE shall perform as many SCMS transactions as possible using a single TLS session.	To minimize the number of separate TLS sessions to the SCMS. This will reduce the resources required and improve throughput.	This is out of scope as it defines EE behavior.	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-2612	REVIEW	Store butterfly parameters	RA shall store butterfly parameters for each OBE for the estimated functional lifetime of the OBE.	So that the certificate pre-generation and revocation can function 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.		RA

49 issues

5.2.16.5.7 Design

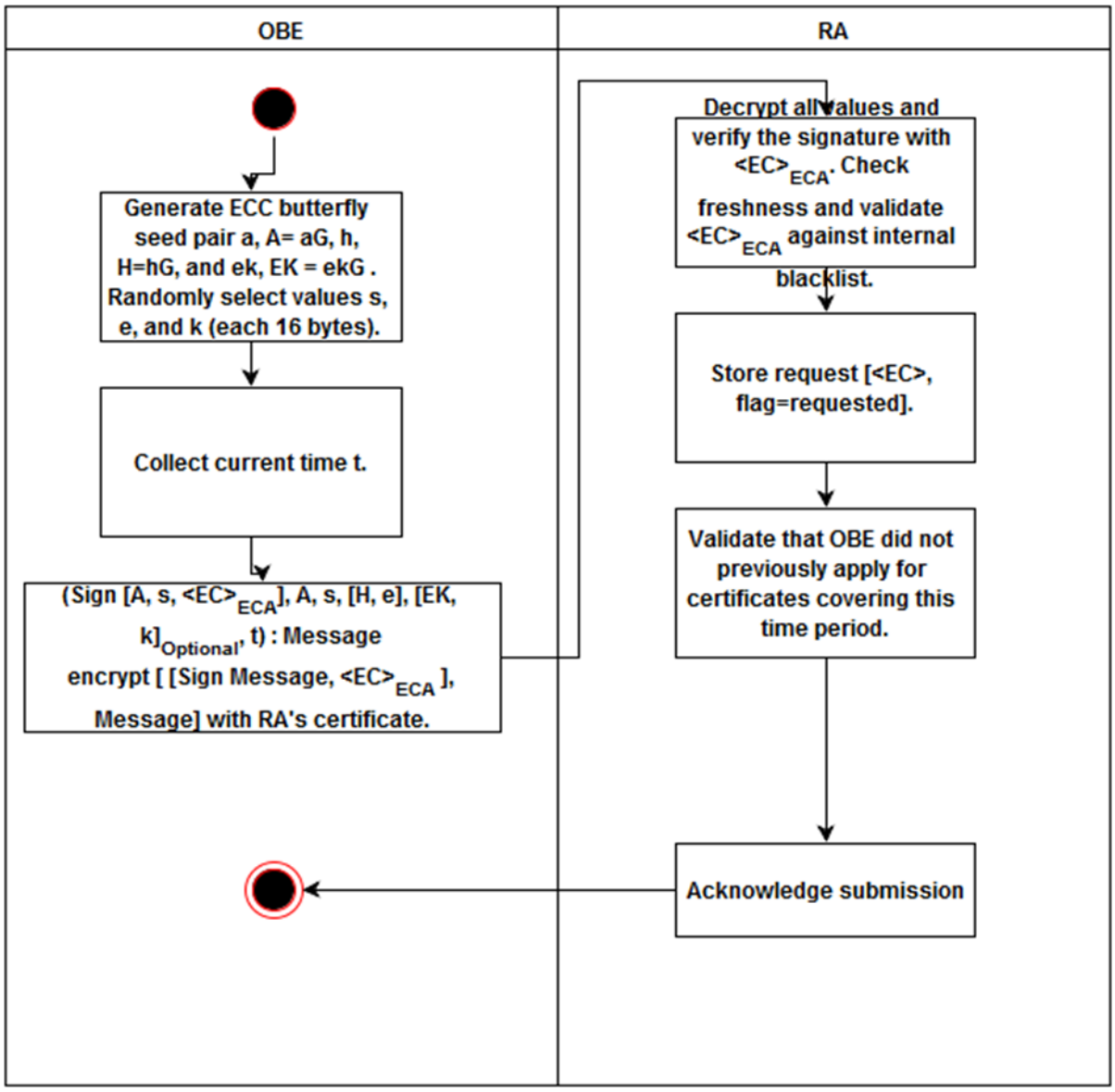


Figure 81 OBE-RA Communication

5.2.16.5.7.1 EE Request

The EE initiates the Certificate Provisioning Request message in order to provide the RA with critical information (key parameters, current time, etc.) necessary for the OBE identification certificate generation. New devices may experience some delay between the initial request and the time the first certificate is available for download to accommodate provisioning processes such as certificate generation and certificate encryption. The RA will store information from the initial Certificate Provisioning Request message and use for ongoing certificate pre-generation until:

- The device provides new parameters in a subsequent Certificate Provisioning Request
- The device is blacklisted at the RA due to misbehavior or malfunction

The Certificate Provisioning Request message shall be sent once for each unique request. No subsequent Certificate Provisioning Request is necessary to acquire new certificates.

5.2.16.5.7.1.1 Security / Privacy

The Certificate Provisioning Request message shall use signing and encryption to ensure:

- The request has not been modified in transit
- The RA can verify the message came from the device
- The request is shared confidentially between the device and RA

The EE shall sign the request with the Enrollment Certificate. The EE shall also encrypt the request using the RA certificate and encapsulate in a 1609.2 frame of type encrypted.

5.2.16.5.7.1.2 Message Contents

The EE shall use the ASN.1 defined for creating the Request Certificate message, details can be found at RA - Identification Certificate Provisioning Request . In order for a request to be validated by the RA, the EE shall include the following information in the Certificate Provisioning Request message:

- Version
- EE enrollment certificate
- Butterfly public seed / expansion function (see Butterfly key for details) parameters for:
    - Certificate signing key (signed with enrollment certificate)
    - Response encryption key (to encrypt the created certificate towards EE)
    - Optionally certificate encryption key
- Current device time: 32-bit denoting number of seconds since the Epoch (as defined in 1609.2)
- Requested certificate start time: 32-bit denoting number of seconds since the Epoch (as defined in 1609.2)

5.2.16.5.7.2 RA Response

The RA response to the Certificate Provisioning Request message may be *accept* (indicated by a Request Acknowledgement) or *reject* (indicated by a HTTP 500). Specific error codes should be hidden from EEs to avoid providing useful information to malicious actors. RA shall log the specific error for future investigation.

5.2.16.5.7.2.1 RA - EE Request Acknowledgement

The Request Acknowledge message is initiated by the RA in response to a Certificate Provisioning Request message successfully received from the EE. If the EE request is received and processed without triggering an error (invalid signature, blacklisted, etc.) the RA processes the certificate request and begins certificate pre-generation. The Request Acknowledge message provides the EE with the URL and the time where and at which the first certificates batches will be available for download.

5.2.16.5.7.2.2 Security / Privacy

The Request Acknowledge message shall use signing and encryption to ensure:

- The request has not been modified in transit
- The device can verify the message came from the RA
- The request is shared confidentially between the device and RA

The RA shall sign and encrypt the Request Acknowledge message using the RA certificate and encapsulate in a 1609.2 frame of type encrypted.

5.2.16.5.7.2.3 Message Contents

The RA shall use the ASN.1 defined for creating the Request Acknowledge message, which can be found at RA - Identification Certificate Provisioning Request and shall include the following information:

- Case: Certificate Provisioning Request *Accept*
    - Version
    - Low order 8-bytes of the SHA-256 hash of the encoded "ToBeSigned" certificate request from the device. Returns 0 if RA cannot calculate hash of the original request.
    - Time at which the first certificate batches will be available for download (represented by IEEE 1609.2 Time32)
    - URL of the certificate repository (common for all devices serviced by an specific RA)
- Case: Certificate Provisioning Request *Reject*
    - HTTP-500 Error Code

5.2.16.5.7.3 EE Response

If the RA provides a positive acknowledgement (*accept)* to a Certificate Provisioning Request, the EE moves forward with the certificate batch download process using the provided URL and time both given in the acknowledge message.

If the EE does not receive an acknowledgement from the RA in response to the request within the defined time, the EE should retry. Several conditions may necessitate the EE sending the request more than once. This may be due to:

- Request lost in transit (no TCP ack)

- RA offline, unavailable or the RA network address has changed (EE must query DNS for latest RA network information)
- The EE possesses an invalid RA certificate and cannot establish secure communications
- The EE received HTTP-500 Error Code

The EE should not attempt to transmit the Request Certificate message without having completed the prerequisites.

5.2.16.5.8 ASN.1 Specification

- ee-ra.asn
- scms-protocol.asn
- scms-base-types.asn
- scms-error.asn
- scms-policy.asn
- scms-common-errors.asn
- 1609dot2-schema.asn
- 1609dot2-base-types.asn

5.2.16.6 Step 19.3: Initial Download of OBE Identification Certificates

5.2.16.6.1 Goals

The goal is to provide a reliable, secure, and timely method for certified devices to download OBE identification certificates.

5.2.16.6.2 Background and Strategic Fit

The purpose of this use-case is to provide a defined method that a certified OBE can use to download OBE identification certificates. The download will include:

1. File(s) X_i.zip that each include one file X_i with a certificate
2. A .info file that includes the time when new certificates will be available
3. A local certificate chain file containing all PCA certificate chains required to validate the identification certificates, but not the policy file

5.2.16.6.3 Assumptions

- The OBE has successfully completed Step 19.1: Request for OBE Identification Certificates
- The RA retrieved the issued certificates from the PCA, zipped, and stored them in a folder for OBE to download

5.2.16.6.4 Process Steps

1. The OBE downloads the Local Policy File (LPF) and the Local Certificate Chain File (LCCF), as done before in Step 19.1: Request for OBE Identification Certificates
    a. If there is an updated LCCF, the EE applies all changes to its trust-store (necessary for the PCA Certificate Validations)
    b. If there is an updated LPF, the EE applies those changes
2. The OBE downloads the new OBE identification certificates using the API documented in RA - Download Identification Certificate
3. The OBE downloads .info file using the API documented in RA - Download .info File

5.2.16.6.5 Error Handling

1. The OBE will abandon further interactions with the RA after a certain number of failed communication attempts resulted in critical errors
2. The OBE will not attempt to execute the certificate provisioning process if it finds itself on the latest CRL (assumes that a willful violator has not compromised the device). The device will need to execute the certification/bootstrap process again to exit a revoked state.

5.2.16.6.6 Requirements

Table 76 Use Case 19.3 - 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</td><td>RFC5289</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>
</table>

Key	Status	Summary	Description	Justification	Notes	Component/s
			_AES_256_GCM_SHA384			
			0xC0,0xAC TLS_ECDHE_ECDSA_WITH_AES_128_CCM RFC7251			
			0xC0,0xAD TLS_ECDHE_ECDSA_WITH_AES_256_CCM RFC7251			
SCMS-411	EE REQUIREMENT	EE Authentication to RA for Request	The EE shall authenticate its requests with its enrollment certificate and signed timestamp to avoid replay attacks on the RA.	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.	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.	On-board Equipment (OBE), Road-side Equipment (RSE)
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	OCSP stapling provides improved performance compared to CRLs.	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
				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 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.	
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	Every logical RA has its own internal blacklist that is not shared with anyone	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
				with the RA anymore	else. To prevent compromised components to speak with the RA, the RA needs to validate against the SCMS component CRL (comparehttps://jira.campllc.org/browse/SCMS-859~~SCMS-859~~, SCMS-504) and the X.509 CRL (https://jira.campllc.org/browse/SCMS-405~~SCMS-405~~).	
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,	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
					certificates, .info file etc.	
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 (https://jira.campllc.org/browse/SCMS-537~~SCMS-537~~) and RA-EE authentication (https://jira.campllc.org/browse/SCMS-539~~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	It is not cost effective to provide OBEs with TLS certificates currently. Instead, the OBE will use TLS to	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
				certificates or files.	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	
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	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)

Key	Status	Summary	Description	Justification	Notes	Component/s
			specified amount of time, currently set to be 10 sec from the time of request.			
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-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	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
					access to a large database of tracking data. For other certificates, this is just an add-on security layer.	
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	To avoid connecting to a revoked and	This is out of scope since it specifies EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
			stapling) to verify RA revocation status.	potentially rogue RA.	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.	
SCMS-543	CLOSED	Individual certificate downloads	RA shall support individual certificate batch, or certificate file, downloads by EEs.	The design allows download of individual certificate batches, or files, to avoid that an EE needs to download all certificates each time. This also allows easier		RA

Key	Status	Summary	Description	Justification	Notes	Component/s
				resume of a download.		
SCMS-544	CLOSED	Download resume	RA shall support byte-wise resume of certificate batch, certificate file, or policy file, downloads, even if EE switches the IP address.	To improve reliability of the download protocol.		RA
SCMS-547	CLOSED	Available certificate batches	The number of certificate batches, or certificate files, available for download shall be configurable (e.g. 3 years) as defined by the configuration option max_available_cert_supply in the global policy.	This might change during the lifetime of the SCMS. It might even vary for different EEs.		RA
SCMS-548	CLOSED	X.info file	RA shall provide an .info file for download by EE.	The .info file provides information when new pseudonym certificates, or identification certificates, can be downloaded.	In order for the EE to determine the earliest time which new certificate batches will be available for download, the RA shall maintain a file in each device specific repository. This file will contain a timestamp at which the RA is predicted to update certificate	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
					batches in the device repository. The timestamp shall be in the IEEE 1609.2 Time32 format (the number of (TAI) seconds since 00:00:00 UTC, January 1, 2004). The file shall be named according to the following format: X.info Where X is the lower 8-bytes of the SHA-256 hash of device request in hexadecimal	
SCMS-549	CLOSED	Keep Certificates	The RA shall allow the EE to download certificates that have previously been downloaded, so long as the devices credentials are still valid and the certificates are not expired.	to recover from a loss of certificates at the device level (e.g., disk corruption).		RA
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	If no policy file is available on the EE, the EE is allowed to	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
				using the latest policy for new downloaded certificates. Policy definition details are available at Use Case 18: Provide and Enforce Technical Policies.	make a download attempt at any time. This is out of scope since it defines EE behavior.	
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		RA

Key	Status	Summary	Description	Justification	Notes	Component/s
				send their current LCCF's version number in the download request to RA and the response will include a newer LCCF if available.		
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-954	EE REQUIREMENT	Error code: eePolicyVerificationFailed	EE shall log this error code in EE's error log file, if EE is not able to verify the digital signature of the local policy file.	To enable EE side diagnostics.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-956	EE REQUIREMENT	Error code: eePolicyFileParsingFailed	EE shall log this error code in EE's error log file, if EE is not able to parse the successfully downloaded local policy file (e.g., because 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 read 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-958	EE REQUIREMENT	Error code: eeConnectionFailed	EE shall log this error code, if it cannot connect to RA because there is a connection timeout.	To enable EE side diagnostics.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-964	CLOSED	Error code: raCertFileUnavailable	RA shall return status code HTTP 500 to EE, if certificate batch is not available and log "Error code: raCertFileUnavailable.	to enable EE side error handling.		RA
SCMS-965	EE REQUIREMENT	Error code: eeCertFileDownloadFailed	If OBE is not able to download pseudonym or identification certificate files (e.g., because there is none or it is corrupted), OBE shall implement OEM defined error handling and store the error code in OBE's error log file.	To enable EE side diagnostics.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE)

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-969	EE REQUIREMENT	Error code: eeCertificateFileDecryptionFailed	EE shall log this error code, if EE is not able to decrypt an encrypted certificate.	To enable EE side diagnostics.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-971	EE REQUIREMENT	Error code: eeCertificateVerificationFailed	EE shall log this error code, if EE is not able to verify a certificate.	This is to verify the issued certificate.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-973	EE REQUIREMENT	Error code: eeCertContentFalse	EE shall log this error code, if EE is not able to parse a certificate, or if the certificate has wrong content.	To enable EE side diagnostics.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-976	CLOSED	Error code: raInvalidURL	RA shall log "Error code: raInvalidURL", if EE requests invalid URL.	To enable server side diagnostics and to avoid giving potential attackers relevant information	This is not in ASN.1 but http 404	RA
SCMS-977	CLOSED	TLS error codes	RA shall return standard TLS error codes if TLS errors occur.	In order to enable client side error handling.		RA
SCMS-978	CLOSED	Error code: raAuthenticationFailed	RA shall log "Error code: raAuthenticationFailed", if EE-to-RA authentication fails.	To enable server side diagnostics and to avoid giving potential attackers relevant information.		RA

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-979	EE REQUIREMENT	Error code: eeAuthenticationFailed	EE shall log "Error code: eeAuthenticationFailed", if RA-to-EE authentication fails.	To enable EE side diagnostics.	This is out of scope since it defines EE's behavior. This is part of TLS handshake. OEM defines EE error handling.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-981	CLOSED	Error code: raNoPcaCertificateChainFileAvailable	RA shall return status code HTTP 500, if Local Certificate Chain File is not available and log "Error code: raNoPcaCertificateChainFileAvailable".	To enable client side error handling.		RA
SCMS-982	CLOSED	X.info file update period	RA shall update the .info file at least on a weekly basis.	The .info file is updated regularly to provide timely updates to EE		RA
SCMS-984	EE REQUIREMENT	Error code: obeInfoFileDownloadFailed	OBE shall log this error code, if it is not able to download the .info file (e.g. because there is none or it is corrupted).	to enable EE side diagnostics.	This is out of scope since it defines EE behavior.	On-board Equipment (OBE)
SCMS-1065	CLOSED	Error code: raBlacklisted	RA shall log "Error code: raBlacklisted" if the requesting EE has been blacklisted.	Error's produced by an EE should always be logged for diagnostic purposes and	RA response to EE shall follow SCMS-1397	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
				never returned to the EE to avoid giving a potential attacker sensitive information.		
SCMS-1090	CLOSED	Error code: raTcpErrors	RA shall return standard TCP error codes if TCP errors occur and log "Error code: raTcpErrors" and the encountered TCP error.	in order to enable client side error handling.		RA
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-1201	EE REQUIREMENT	EE certificate download via HTTPS over TCP/IP	EE shall use HTTPS (TLS) over TCP/IP to download files from the SCMS.	In order to use standard internet technology.	This is out of scope as it defines EE 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

Key	Status	Summary	Description	Justification	Notes	Component/s
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	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
					certificates to the IBLM.	
SCMS-1214	EE REQUIREMENT	OBE downloads .info file	OBE shall download the .info file each time OBE downloaded pseudonym or identification certificates.	EE requires the information to learn when certificates will be available for download.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE)
SCMS-1215	EE REQUIREMENT	EE contacts RA for certificate download	EE shall try to download certificates any time after the time provided by the time-stamp in the .info file that has been recovered last time EE tried to download, or downloaded, certificates.	To avoid wasting resources by trying to download certificates before they are available.	This is out of scope since it defines EE behavior. The timestamp shall be in the IEEE 1609.2 Time32 format (the number of (TAI) seconds since 00:00:00 UTC, January 1, 2004).	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1228	CLOSED	OBE identification certificate files	RA shall provide each identification certificate to be downloaded by EE as a X_i.zip file in the folder provided in the ack message to the provisioning request. • X_i.zip	this convention gives the OBE the ability to locate the file at the RA.	The file iterator i starts at 0 and is then incremented by 1 for each new file. The first issued certificate is stored in X_1.zip, the second certificate is stored in X_2.zip,	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
			• Where X shall be the lower 8-bytes of the SHA-256 hash of the device request in hexadecimal (case insensitive) • Where i is a file iterator in hexadecimal starting at 0 (case insensitive) • Where the extension is .zip in lowercase		the 4 billion-th certificate is stored in X_EE6B2800.zip, and so on.	
SCMS-1263	EE REQUIREMENT	EE download resume	EE shall try byte-wise resume of CRL downloads from the CRL store, certificate batches, certificate files, or policy files from RA in case a previous download failed.	This will improve reliability of the download process and reduce communication cost.		On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1270	EE REQUIREMENT	Network connection	EEs shall use TCP/IP to communicate with the SCMS.	SCMS components (server) are only reachable by standard TCP/IP networking methods.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1303	EE REQUIREMENT	Verification of certificate validity	EE shall verify the validity of a received certificate against IEEE 1609.2-v3-D12, clause 5.1 and 5.3.	To verify if the certificate is issued by a	This is for testing that SCMS issued valid and proper	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
				trustworthy source and therefore messages signed by this certificate can be trusted.	certificates. This is out of scope since it defines EE behavior.	
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-1356	EE REQUIREMENT	EE uses internal certificate store	The EE shall use its internal certificate store to validate received SCMS certificates and respond to P2P certificate requests.	EEs need to be able to validate received SCMS certificates based on their certificate chain up to the SCMS root CA. EEs need to respond to P2P certificate requests to	EE does not need to store all certificate chains, the LCCF provides the minimum set and EEs can learn additional chains via P2P certificate request. This is out of scope	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
				enable receiving EEs to validate the certificate chain.	as it defines EE's behavior.	
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-1397	TESTS FAILED	Error reporting to EE	The SCMS Components shall return error code "HTTP 500" to EEs in response to all application level errors at RA.	Specific error codes should be hidden from EEs to prevent useful information from being provided to malicious actors	• Standard TCP (https://jira.campllc.org/browse/SCMS-1090~~SCMS-1090~~) and TLS (https://jira.campllc.org/browse/SCMS-977~~SCMS-977~~) errors shall be reported to EEs • All errors at the HTTP and higher levels shall be	CRL Store, RA

Key	Status	Summary	Description	Justification	Notes	Component/s
					HTTP 500 for RA & ECA	
SCMS-1404	EE REQUIREMENT	EE send data via HTTP post over TCP/IP	EE shall use HTTP post to send data towards the RA	To allow the SCMS endpoint to serve everything based on HTTP protocol	RA - Services View will document the actual HTTP post details. This is out of scope as it defines EE behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1405	CLOSED	RA accept authenticated HTTP post requests	RA shall accept HTTP post requests only from authenticated EEs.	To allow the SCMS endpoint to serve everything based on HTTP protocol	RA - Services View will document the actual HTTP post details.	RA
SCMS-1420	SCMS POC OUT OF SCOPE	Keep track of which authorization (pseudonym, ID, application) certificates are downloaded	The RA shall keep track of how far into the future each device has downloaded its certificates.	This allows revoked devices to be removed from the CRL (or deprioritized for inclusion on the CRL) once they exhaust the set of certificates that they have downloaded.	This is an optimization for CRL handling and therefore out of scope for PoC implementation.	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-1421	EE REQUIREMENT	LCCF validation in EE	The EE shall verify the LCCF and then update the internal certificate store each time it receives a new LCCF.	To have the latest certificate chain update available for validating certificates and answering P2P certificate requests.	This is out of scope as it defines EEs behavior	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1639	EE REQUIREMENT	Download certificate batches	OBE shall not attempt to download certificate batches for i-value periods more than max_available_cert_supply in the future	To reduce resource usage by not attempting to download certificate batches that do not exist.	• This is out of scope as it defines EE behavior. • This is the OBE counterpart ofhttps://jira.campllc.org/browse/SCMS-547~~SCMS-547~~	~~On-board Equipment (OBE)~~
SCMS-2251	CLOSED	One OBE identification certificate file per zip file	RA shall zip exactly one identification certificate file per certificate download file. The content of the certificate file is the binary representation of the encrypted identification certificate. • X_i	There is only one OBE identification certificate allowed at any given time (except for overlap) and therefore there should only be	The file iterator i starts at 0 and is then incremented by 1 for each new file. The first issued certificate is stored in X_1, the second certificate is stored in X_2, the 4	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
			• X shall be the lower 8-bytes of the SHA-256 hash of the device request in hexadecimal (case insensitive) • i is a file iterator in hexadecimal starting at 0 (case insensitive) • Where there is no extension	one certificate per zip file.	billion-th certificate is stored in X_EE6B2800, and so on.	
SCMS-2463	EE REQUIREMENT	EE transactions per TLS session	EE shall perform as many SCMS transactions as possible using a single TLS session.	To minimize the number of separate TLS sessions to the SCMS. This will reduce the resources required and improve throughput.	This is out of scope as it defines EE behavior.	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)

62 issues

5.2.16.7 Step 19.5: Top-off OBE Identification Certificates

5.2.16.7.1 Goals

The goal is to provide a reliable, secure, and timely method for certified devices to download credentials.

5.2.16.7.2 Background and Strategic Fit

The purpose of this use case is to provide a defined method that a certified OBE can use to download subsequent batches of credentials. The step at hand is to top-up OBE identification certificates. It is similar to Step 19.3: Initial Download of OBE Identification Certificates. Differences are documented in this section. Also, see Step 19.4: Schedule generation of subsequent batch of OBE identification certificates for full details of the process to schedule certificate pre-generation.

5.2.16.7.3 Assumptions

- The OBE has successfully completed Step 19.1: Request for OBE Identification Certificates
- The OBE has successfully completed Step 19.3: Initial Download of OBE Identification Certificates
- The RA retrieved the issued certificates from PCA, zipped, and stored them in a folder for OBE to download

5.2.16.7.4 Process Steps

1. The OBE checks that, and if necessary waits until, the current time matches or is after the timestamp given in the .info file
2. The OBE downloads the Local Policy File (LPF) and the Local Certificate Chain File (LCCF), as done before in Step 19.3: Initial Download of OBE Identification Certificates
    a. If there is an updated LCCF, OBE applies all changes to its trust-store (necessary for PCA Certificate Validations)
    b. If there is an updated LPF, OBE applies those changes
3. The OBE downloads the new OBE identification certificates
4. The OBE downloads .info file using the API documented in RA - Download .info File

5.2.16.7.5 Error Handling

- The EE will abandon further interactions with the RA after a certain number of failed communication attempts resulted in critical errors
- The EE will not attempt to execute the certificate provisioning process if it finds itself on the latest CRL (assumes that a willful violator has not compromised the

device). The device will need to execute the certification/bootstrap process again to exit a revoked state.

- The EE may terminate the certificate batch download process if sufficient storage is not available for subsequent batches

5.2.16.7.6 Requirements

Table 77 Use Case 19.5 - 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>
</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>
</table>

Key	Status	Summary	Description	Justification	Notes	Component/s
			0xC0,0x2C TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 RFC5289 0xC0,0xAC TLS_ECDHE_ECDSA_WITH_AES_128_CCM RFC7251 0xC0,0xAD TLS_ECDHE_ECDSA_WITH_AES_256_CCM RFC7251			
SCMS-411	EE REQUIREMENT	EE Authentication to RA for Request	The EE shall authenticate its requests with its enrollment certificate and signed timestamp to avoid replay attacks on the RA.	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.	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.	On-board Equipment (OBE), Road-side Equipment (RSE)
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	OCSP stapling provides improved performance compared	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
				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.	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.	
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	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
					components to speak with the RA, the RA needs to validate against the SCMS component CRL (comparehttps://jira.campllc.org/browse/SCMS-859~~SCMS-859~~, SCMS-504) and the X.509 CRL (https://jira.campllc.org/browse/SCMS-405~~SCMS-405~~).	
SCMS-509	CLOSED	Stop pre-generating pseudonym and OBE identification certificates for revoked device	RA shall stop pre-generating pseudonym and OBE identification certificates for a device that has been revoked by the MA, i.e., for a device that appears on RA's internal blacklist.	so that computing resources are not wasted by generating certificates for revoked devices		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

Key	Status	Summary	Description	Justification	Notes	Component/s
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 (https://jira.campllc.org/browse/SCMS-537~~SCMS-537~~) and RA-EE authentication (https://jira.campllc.org/browse/SCMS-539~~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	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
					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	
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)

Key	Status	Summary	Description	Justification	Notes	Component/s
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-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	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
					DNS is able to learn EE's enrollment certificate (but not EE's private key). OCSP stapling is specified in RFC 6066, Section 8.	
SCMS-544	CLOSED	Download resume	RA shall support byte-wise resume of certificate batch, certificate file, or policy file, downloads, even if EE switches the IP address.	To improve reliability of the download protocol.		RA
SCMS-576	CLOSED	Update .info file	The RA shall update .info files for all EEs even if no new certificate batches are created.	The EE uses the .info file to determine when the the earliest the next download is allowed to happen.	Timestamp in .info file is dynamically calculated based on system load. PoC scope will be to update .info file for non-revoked EEs only.	RA
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	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)

Key	Status	Summary	Description	Justification	Notes	Component/s
				18: Provide and Enforce Technical Policies.		
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-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	As the policy file is essential for the system to work correctly and	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
			policy file (e.g., because there is none or it is corrupted).	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.		
SCMS-954	EE REQUIREMENT	Error code: eePolicyVerificationFailed	EE shall log this error code in EE's error log file, if EE is not able to verify the digital signature of the local policy file.	To enable EE side diagnostics.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-956	EE REQUIREMENT	Error code: eePolicyFileParsingFailed	EE shall log this error code in EE's error log file, if EE is not able to parse the successfully downloaded local policy file (e.g., because 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 read 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-958	EE REQUIREMENT	Error code: eeConnectionFailed	EE shall log this error code, if it cannot connect to RA because there is a connection timeout.	To enable EE side diagnostics.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-964	CLOSED	Error code: raCertFileUnavailable	RA shall return status code HTTP 500 to EE, if certificate batch is not available and log "Error code: raCertFileUnavailable.	to enable EE side error handling.		RA
SCMS-976	CLOSED	Error code: raInvalidURL	RA shall log "Error code: raInvalidURL", if EE requests invalid URL.	To enable server side diagnostics and to avoid giving potential attackers relevant information	This is not in ASN.1 but http 404	RA
SCMS-977	CLOSED	TLS error codes	RA shall return standard TLS error codes if TLS errors occur.	In order to enable client side error handling.		RA
SCMS-978	CLOSED	Error code: raAuthenticationFailed	RA shall log "Error code: raAuthenticationFailed", if EE-to-RA authentication fails.	To enable server side diagnostics and to avoid giving potential attackers relevant information.		RA
SCMS-979	EE REQUIREMENT	Error code: eeAuthenticationFailed	EE shall log "Error code: eeAuthenticationFailed", if RA-to-EE authentication fails.	To enable EE side diagnostics.	This is out of scope since it defines EE's behavior. This is part of TLS handshake. OEM defines EE error handling.	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-1065	CLOSED	Error code: raBlacklisted	RA shall log "Error code: raBlacklisted" if the requesting EE has been blacklisted.	Error's produced by an EE should always be logged for diagnostic purposes and never returned to the EE to avoid giving a potential attacker sensitive information.	RA response to EE shall follow SCMS-1397	RA
SCMS-1164	EE REQUIREMENT	OBE next download timing	OBE shall use the stored .info file to schedule the next download attempt.	The .info file contains the timestamp when the next batch of certificates (pseudonym or identification) will be available for download. This timestamp is the earliest the OBE is allowed to connect to the RA for the next download. The timestamp shall be in the IEEE 1609.2 Time32 format (the number of (TAI) seconds since 00:00:00 UTC, January 1, 2004).	This is out of scope since it defines EE's behavior. • If no pseudonym certificates are available on the OBE for the current i_period (week), the OBE is allowed to make a download attempt at any time. • If no pseudonym certificates are available on the OBE for the next i_period (week), the OBE is allowed to make a	On-board Equipment (OBE)

Key	Status	Summary	Description	Justification	Notes	Component/s
					download attempt at any time. • If no identification certificate is available on the OBE for the current or next time period, the OBE is allowed to make a download attempt at any time.	
SCMS-1171	EE REQUIREMENT	EE revoked	EEs that are revoked shall not attempt to download LCCF, LPF, pseudonym certificates, identification certificates or file misbehavior reports. Exceptions to this are: • EE is unable to determine its revocation status • EE has no pseudonym or identification certificates available in local storage • EE is attempting to perform a re-enrollment operation	To avoid unnecessary load at the RA.	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	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)

Key	Status	Summary	Description	Justification	Notes	Component/s
			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.			
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	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
					and put it on the internal blacklist. The RA does not send out enrollment certificates to the IBLM.	
SCMS-1214	EE REQUIREMENT	OBE downloads .info file	OBE shall download the .info file each time OBE downloaded pseudonym or identification certificates.	EE requires the information to learn when certificates will be available for download.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE)
SCMS-1263	EE REQUIREMENT	EE download resume	EE shall try byte-wise resume of CRL downloads from the CRL store, certificate batches, certificate files, or policy files from RA in case a previous download failed.	This will improve reliability of the download process and reduce communication cost.		On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1270	EE REQUIREMENT	Network connection	EEs shall use TCP/IP to communicate with the SCMS.	SCMS components (server) are only reachable by standard TCP/IP networking methods.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1282	EE REQUIREMENT	Error code: eeDecompression Error	EE shall log "Error code: eeDecompressionError", if it is not able to decompress the received certificate.	To allow error reaction and investigation.	Out of scope as it defines EE behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1289	EE REQUIREMENT	OBE identification certificate duplicate downloads	The OBE shall not download OBE identification certificates that are already verified and stored in OBE.	During top-up downloads, the EE shall only download		On-board Equipment (OBE)

Key	Status	Summary	Description	Justification	Notes	Component/s
				OBE identification certificates that are not currently verified and stored on the device. This is to prevent repeated downloads of the same content.		
SCMS-1291	EE REQUIREMENT	Expired Certificate Files	The OBE shall only download OBE identification certificate files for the current and future time periods.	Only download certificates that are not expired yet.		On-board Equipment (OBE)
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-1356	EE REQUIREMENT	EE uses internal certificate store	The EE shall use its internal certificate store to validate received SCMS certificates and respond to P2P certificate requests.	EEs need to be able to validate received SCMS certificates based on their certificate chain up to the SCMS root CA. EEs need to respond to	EE does not need to store all certificate chains, the LCCF provides the minimum set and EEs can learn additional chains via P2P certificate request.	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
				P2P certificate requests to enable receiving EEs to validate the certificate chain.	This is out of scope as it defines EE's behavior.	
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-1404	EE REQUIREMENT	EE send data via HTTP post over TCP/IP	EE shall use HTTP post to send data towards the RA	To allow the SCMS endpoint to serve everything based on HTTP protocol	RA - Services View will document the actual HTTP post details. This is out of scope as it defines EE behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1405	CLOSED	RA accept authenticated HTTP post requests	RA shall accept HTTP post requests only from authenticated EEs.	To allow the SCMS endpoint to serve everything based on HTTP protocol	RA - Services View will document the actual HTTP post details.	RA
SCMS-1420	SCMS POC OUT OF SCOPE	Keep track of which authorization (pseudonym, ID, application) certificates are downloaded	The RA shall keep track of how far into the future each device has downloaded its certificates.	This allows revoked devices to be removed from the CRL (or deprioritized for inclusion on the CRL) once they exhaust the set of certificates that they have downloaded.	This is an optimization for CRL handling and therefore out of scope for PoC implementation.	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-1421	EE REQUIREMENT	LCCF validation in EE	The EE shall verify the LCCF and then update the internal certificate store each time it receives a new LCCF.	To have the latest certificate chain update available for validating certificates and answering P2P certificate requests.	This is out of scope as it defines EEs behavior	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1639	EE REQUIREMENT	Download certificate batches	OBE shall not attempt to download certificate batches for i-value periods more than max_available_cert_supply in the future	To reduce resource usage by not attempting to download certificate batches that do not exist.	• This is out of scope as it defines EE behavior. • This is the OBE counterpart ofhttps://jira.campllc.org/browse/SCMS-547~~SCMS-547~~	~~On-board Equipment (OBE)~~
SCMS-2463	EE REQUIREMENT	EE transactions per TLS session	EE shall perform as many SCMS transactions as possible using a single TLS session.	To minimize the number of separate TLS sessions to the SCMS. This will reduce the resources required and improve throughput.	This is out of scope as it defines EE behavior.	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	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
				static and may change at any time.		

50 issues

5.2.16.7.7 Design Notes

- See Step 19.3: Initial Download of OBE Identification Certificates for full details of the download process
- From the SCMS point of view, the basic process for "top-up" certificate downloads is the same as that used for initial provisioning as detailed in Step 19.3: Initial Download of OBE Identification Certificates. However, this is an incremental download and not a full download of all available certificate files. The number of files downloaded shall be factored in system sizing requirements.
- From the OBE's point of view, the process is slightly different from the process for initial provisioning
- The RA will record the last time an OBE established a connection. This last connection time will be used to stop pre-generating pseudonym certificates if there is no activity for a period of time.
- The RA will automatically resume pre-generating pseudonym certificates when an OBE reestablishes a connection. The new certificates will be available for download at the time specified in the .info file.

5.2.17 Use Case 20: EE Re-Enrollment

> EE re-enrollment will be integrated with the to-be-awarded "SCMS PoC extension" project as SCMS PoC release 3.0. Until then these are preliminary concepts.

5.2.17.1 Goals

All End Entities (EEs, including OBEs and RSEs) receive an Enrollment Certificate as part of a secure initial provisioning process (see Use Case 2: OBE Bootstrapping (Manual) and Use Case 12: RSE Bootstrapping (Manual) for details). This certificate is used to authenticate the EE to an RA for all secured transactions with the SCMS. When this certificate approaches its expiration, the EE must be re-established to receive a new certificate. There are also cases where infrastructure components (such as an ICA or Root CA) may be revoked without directly impacting the EEs that have certificates that are chained back to the revoked component. The re-enrollment use cases describe secure procedures for maintaining the integrity and security of EE enrollment certificates in these situations.

5.2.17.2 Assumptions

The EE has a non-revoked, non-expired enrollment certificate and the EE has not been placed on the RA's blacklist.

5.2.17.3 Step 20.1: EE Enrollment Certificate Rollover

5.2.17.3.1 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 procedure 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).

5.2.17.3.2 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.

5.2.17.3.3 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 (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.

5.2.17.3.3.1 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 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.

5.2.17.3.3.2 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. 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.

5.2.17.3.3.3 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 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.

5.2.17.3.3.4 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.

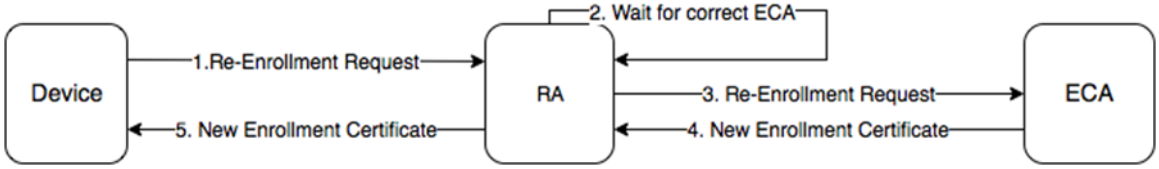


Figure 82 Role Of The RA And ECA In Re-enrollment

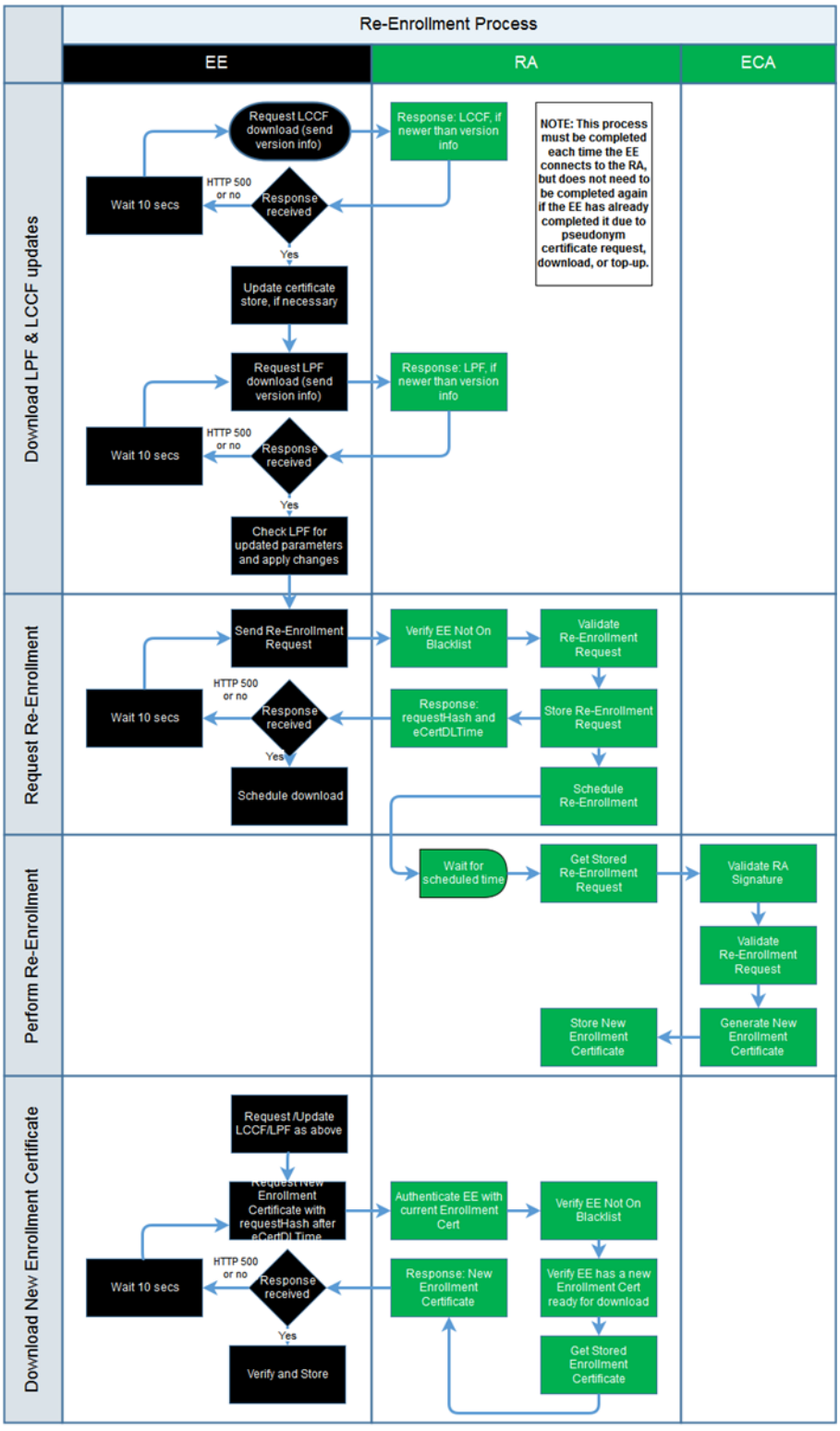


Figure 83 Re-enrollment Process Diagram

5.2.17.3.4 Requirements

Table 78 Use Case 20.1 - 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></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>
</table>

Key	Status	Summary	Description	Justification	Notes	Component/s
			0xC0, 0xAD | TLS_ECDHE_ECDSA_WITH_AES_256_CCM | RFC7251			
SCMS-411	EE REQUIREMENT	EE Authentication to RA for Request	The EE shall authenticate its requests with its enrollment certificate and signed timestamp to avoid replay attacks on the RA.	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.	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.	On-board Equipment (OBE), Road-side Equipment (RSE)
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	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
					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.	
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 (comparehttps://jira.campllc.org/browse/SCMS-859~~SCMS-859~~, SCMS-504) and the X.509 CRL (https://jira.campllc.org/browse/SCMS-405~~SCMS-405~~).	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
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 (https://jira.campllc.org/browse/SCMS-537~~SCMS-537~~) and RA-EE authentication (https://jira.campllc.org/browse/SCMS-539~~SCMS-539~~). IEEE 1609.2 certificates within a TLS session will be used for EE-RA authentication (SCMS-538).	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
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	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)

Key	Status	Summary	Description	Justification	Notes	Component/s
			a specified amount of time, currently set to be 10 sec from the time of request.			
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	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
					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.	
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	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	Justification	Notes	Component/s
					enrollment certificate (but not EE's private key). OCSP stapling is specified in RFC 6066, Section 8.	
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		RA

Key	Status	Summary	Description	Justification	Notes	Component/s
				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.		
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,	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)

Key	Status	Summary	Description	Justification	Notes	Component/s
			EE also shall not attempt to download a local policy file or local certificate chain file from RA.			
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	RA

Key	Status	Summary	Description	Justification	Notes	Component/s
					not send out enrollment certificates to the IBLM.	
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)

Key	Status	Summary	Description	Justification	Notes	Component/s
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

Key	Status	Summary	Description	Justification	Notes	Component/s
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

Key	Status	Summary	Description	Justification	Notes	Component/s
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

6 Software Design Documents

6.1 Common - Services View

The Service View shows the architecture from the perspective of the services exposed by each component. Components interact with each other via service invocation. The service is therefore the point of contact between two collaborating components. A Service is a discrete piece of functionality that is made accessible for other components to consume over the network. While there are other types of services, we chose to design our solution in the style of RESTful Web Services, which provides the following advantages:

- Relatively simple connector implementation with plenty of tooling and libraries to support development
- Easier to introduce proxies, gateways, caches, and load balancers without affecting involved components
- Wide adoption by the industry at large

However, the implementation will differ from a pure RESTful style in the following significant details:

1. Payloads are not JSON or XML (as commonly used in most RESTful services) but binary messages generated from custom ASN.1 grammars
2. Cacheability of responses may not be used due to the nature of the problem domain
3. Uniform Interface architectural constraint is not fully observed due to adherence to ASN.1-defined protocol and to keep payload sizes to the minimum possible

6.2 MA - Services View

Please refer to the Common - Services View section for an introduction of the Services View.

6.2.1 General Notes

All Misbehavior Authority Services use the same scheme (**https**) and port **8894**. That is, all the requests to MA will have URLs that look like:

`https://<SERVER>:8894/<PATH>`

Where <SERVER> is the IP or host name, and PATH is the name of the service.

For all the services, the HTTP Content-Type is set to application/octet-stream.

No information is returned in case of error, just an HTTP code of 500.

6.2.2 Services Summary for EE-MA Communications

Service Name	<PATH>
MA - Download CRL	/download-crl/

6.2.3 MA - Download CRL

EEs use this service to download the CRL File.

PORT	8894
PATH	**/download-crl/**
HTTP Method	GET
HTTP Request Body	Empty
HTTP Request Headers	Empty
HTTP Response Body	ASN.1 Serialized CRL File as defined by the CompositeCrl ASN.1 definition

6.2.3.1 Preconditions

1. CRL has been generated by the CRL Generator and stored in the CRL Store

6.2.3.2 Postconditions

1. Returned file contains ASN.1 Serialized Composite CRL File as defined by the CompositeCrl ASN.1 definition

6.2.3.3 Quality of Protection

- MA protects access with HTTPS (TLS V1.2)
- Supports at a minimum OpenSSL cipher suite ECDHE-ECDSA-AES128-SHA256
- This download service **IS NOT** protected via download authentication message as other download service. This service does not authenticate the downloading entity.

6.3 RA - Services View

Please refer to the Common - Services View section for an introduction of the Services View.

6.3.1 General Notes

All Registration Authority Services use the same scheme (**https**) and port **8892**. That is, all the requests to RA will have URLs that look like:

```
https://<SERVER>:8892/<PATH>
```

Where <SERVER> is the IP or host name and PATH is the name of the service.

For all the services, the HTTP Content-Type is set to application/octet-stream.

No information is returned in case of error, just an HTTP code of 500, in a production environment. QA environment will give back errors as outlined in Overview of Used Error Codes.

6.3.2 Services Summary for EE-RA Communications

Table 79 Services Summary For EE-RA Communications

Service Name	<PATH>
Request Application Certificate Provisioning	/provision-application-certificate
Download .info file	/download/info
Download local policy file	/download/policy/local
Download Pseudonym Certificate Batch	/download/batch
Retrieve Registration Authority Certificate	/retrieve-ra-certificate
Request Identification Certificate Provisioning	/provision-identity-certificate
Download Identification Certificate	/download/identity-certificate
Request Pseudonym Certificate Batch Provisioning	/provision-pseudonym-certificate-batch
Download Application Certificate	/download/application-certificate
Download Local Certificate Chain File	/download/local-certificate-chain
Submit Misbehavior Report	/process-misbehavior-report

6.3.3 RA - Request Pseudonym Certificate Batch Provisioning

OBEs use this service to request the initial batch of Pseudonym Certificates. After the initial batch is requested, subsequent batches are automatically provisioned.

PORT	**8892**
PATH	**/provision-pseudonym-certificate-batch**
HTTP Method	POST
HTTP Request Body	ASN.1 serialized *SecuredPseudonymCertProvisioningRequest*

PORT	8892
HTTP Response Body	*SignedPseudonymCertProvisioningAck* 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 *PseudonymCertProvisioningAck* with a *certDLTime* property containing the expected time for download of the requested batch, and a *certDLURL* property containing the URL where the batch can be downloaded.

6.3.3.1 Preconditions

1. Policy referenced in the request message is previously known
2. PLV Cache has at least one PLV chain
3. Device is not revoked

6.3.3.2 Postconditions

None.

6.3.3.3 Error Handling

See "RA-EE Errors" in Overview of Used Error Codes

6.3.3.4 Quality of Service

Estimated values are per logical unit, meaning multiple individual nodes can contribute to achieve the desired level of service. This service will be used once for each initial provisioning request for each new OBE. There may also be a very small addition of OBEs re-requesting provisioning in order to update their parameters. However, this should be a low enough volume to have no significant impact on these calculations.

Quality Metric	1 Year	3 Years	5 Years	10 Years
Throughput	(17,000,000 new vehicles) / 31,557,600 seconds/year = .5 batch requests / second	(17,000,000 new vehicles) / 31,557,600 seconds/year = .5 batch requests / second	(17,000,000 new vehicles) / 31,557,600 seconds/year = .5 batch requests / second	(17,000,000 new vehicles) / 31,557,600 seconds/year = .5 batch requests / second

6.3.3.5 Quality of Protection

- RA protects access with HTTPS (TLS V1.2)
- Supports at a minimum OpenSSL cipher suite ECDHE-ECDSA-AES128-SHA256
- Uses certificate-based client authentication of data signed by the device enrollment certificate, validated at the application layer. This is a supplement to the one-way TLS authentication, to provide two-way authentication with a TLS/1609.2 hybrid scheme.

- Incoming message is encrypted (within the ASN.1 message structure) with the RA Component certificate public key

6.3.4 RA - Download .info File

OBEs use this service to determine the earliest date on which a new batch of pseudonym certificate will become available. There will be a .info file for each device containing this information.

PORT	**8892**
PATH	**/download/info**
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 matching the regular expression *[0-9A-F]{16}\.info*. That is, the name part of the file name is the 16 hexadecimal digits Request Hash obtained during initial provisioning request of this device.
HTTP Response Body	File containing a time stamp of when the next batch is estimated to be available. Due to varying system load, an exact download time can not be provided. If the device receives error 5065 then it should reschedule the download for a later time.

6.3.4.1 Preconditions

1. Device had previously requested a certificate batch
2. Time stamp in the request *AuthenticatedDownloadRequest* is not more than 5 seconds apart from the server's time. (Controlled by the *ra.client-signature-ttl-sec* configuration setting.)

6.3.4.2 Postconditions

1. RA returned a file containing a single IEEE 1609 format Time32 time stamp that the device will use to schedule a subsequent "top-up" download

6.3.4.3 Error Handling

See "RA-EE Errors" in Overview of Used Error Codes

6.3.4.4 Quality of Service

$$f(year) = \left(\sum_{i=1}^{year-1} 17million \right) + \frac{17million}{2}$$

Estimated values are per logical unit, meaning multiple individual nodes can contribute to achieve the desired level of service. The number of vehicles that potentially invoke this service in a week is a function of the number of years in service:

Quality Metric	Rationale	1 Year	3 Years	5 Years	10 Years
Throughput	Assuming half of all new cars plus all existing vehicles need to check for notifications in the same week.	8,500,000 new vehicles / 604,800 seconds/week = **14** requests / second	(8,500,000 new vehicles + 34,000,000 existing vehicles) / 604,800 seconds/week = **70** requests / second	(8,500,000 new vehicles + 68,000,000 existing vehicles) / 604,800 seconds/week = **126** requests / second	(8,500,000 new vehicles + 153,000,000 existing vehicles) / 604,800 seconds/week = **267** requests / second

6.3.4.5 Quality of Protection

- RA protects access with HTTPS (TLS V1.2)
- Supports at a minimum OpenSSL cipher suite ECDHE-ECDSA-AES128-SHA256
- Uses certificate-based client authentication of data signed by the device enrollment certificate, validated at the application layer. This is a supplement to the one-way TLS authentication, to provide two-way authentication with a TLS/1609.2 hybrid scheme.

6.3.5 RA - Download Local Policy File

EEs use this service to download a local policy file.

PORT	**8892**
PATH	**/download/policy/local**
HTTP Method	GET
HTTP Request Body	Empty
HTTP Request Headers	Optionally, the request may include the standard HTTP Header 'If-None-Match' containing the filename of the local policy file that the EE currently possesses, **excluding any path**. For example:

PORT	8892
	If-None-Match: "local_policy_0001_0001.oer" This is used to prevent the same policy file from being downloaded by the device multiple times.
HTTP Response Body	File containing the local policy represented by an OER encoded ASN.1 serialized SignedLocalPolicyFile. The file name returned is of the form: local_policy_<X>_<Y>.<Z> Where: • X is the global version number • Y is the local policy version • Z is one of the permitted encoding formats (oer) from the file name in the request message OR An HTTP code of 304 (Not Modified), if the provided file name in the 'If-None-Match' header matches the current version available on the RA server.

6.3.5.1 Preconditions

None

6.3.5.2 Postconditions

1. Returned file contains policy that the device will use

6.3.5.3 Error Handling

See "RA-EE Errors" in Overview of Used Error Codes

6.3.5.4 Quality of Service

Estimated values are per logical unit, meaning multiple individual nodes can contribute to achieve the desired level of service. The number of vehicles that potentially invoke this service in a week is a function of the number of years in service:

$$f(year) = \left(\sum_{i=1}^{year-1} 17million \right) + \frac{17million}{2}$$

Quality Metric	Rationale	1 Year	3 Years	5 Years	10 Years
Throughput	Assuming half of all new cars plus all existing vehicles	8,500,000 new vehicles / 604,800 seconds/week	(8,500,000 new vehicles + 34,000,000 existing vehicles) /	(8,500,000 new vehicles + 68,000,000 existing vehicles) / 604,800 seconds/week	(8,500,000 new vehicles + 153,000,000 existing vehicles) / 604,800 seconds/week

Quality Metric	Rationale	1 Year	3 Years	5 Years	10 Years
	need to download local policy in the same week.	= **14** requests / second	604,800 seconds/week = **70** requests / second	= **126** requests / second	= **267** requests / second

6.3.5.5 Quality of Protection

- RA protects access with HTTPS (TLS V1.2)
- Supports at a minimum OpenSSL cipher suite ECDHE-ECDSA-AES128-SHA256

6.3.6 RA - Download Pseudonym Certificate Batch

OBEs use this service to download a batch of Pseudonym Certificates for a specific time period.

PORT	8892
PATH	**/download/batch**
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}_[0-9A-F]{1,8}.zip, where the first group of 16 hexadecimal digits is the device's request hash obtained from the initial provision pseudonym certificate batch request, and the second group of up to 8 hexadecimal digits is the i-value. Example: AB09281C9867DE53_F.zip corresponds to i value 15, for device with request hash AB09281C9867DE53. **Range (optional) as defined in RFC 2616:** To support partial downloads for resuming interrupted transfers. Examples: 1. From byte offset 500 to 700: Range : bytes=500-700 2. Starting from byte offset 1000 to the end: Range : bytes=1000-
HTTP Response Body	If no Range header is present, the entire zip file corresponding to the requested batch. If a Range header is present, the specified bytes of the referenced file.

6.3.6.1 Preconditions

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

6.3.6.2 Postconditions

1. The zip file corresponding to the batch specification in the request URL is returned.
2. The content of the zip file is organized as a flat directory containing *n* files (where 0 <= *n* <= *j_max* - 1) with the naming format:
    a. X_Y (NOTE: no file extension)
    b. Where X is the i-value representing the SCMS I period in which the certificate is valid in hexadecimal
    c. Where Y is a sequence of "j" values from j = 0 to j = j_max-1 in hexadecimal
    d. Example zip file contents for period i=55, j = 20:
        i. 37_0
        ii. 37_1
        iii. ...
        iv. 37_12
        v. 37_13
    e. The contents of each individual file within the .zip is a binary OER encoding of the appropriate SignedEncryptedCertificateResponse.

6.3.6.3 Error Handling

See "RA-EE Errors" in Overview of Used Error Codes

6.3.6.4 Quality of Service

Estimated values are per logical unit, meaning multiple individual nodes can contribute to achieve the desired level of service. The number of files downloaded in a year is a function of the number of years in service:

$$f(year) = \left(\sum_{i=1}^{year-1} (17million \times 52weeks) \right) + (17million \times 156weeks)$$

which assumes 17 million vehicles are added each year.

Quality Metric	Rationale	1 Year	3 Years	5 Years	10 Years
Throughput	Assuming 17 million new vehicles downloading	With no previous year vehicles:	With and two years' worth	With four years' worth of	At the end of the first 10 years, there will be a total of 170 million cars in the

Quality Metric	Rationale	1 Year	3 Years	5 Years	10 Years
	the initial three years' worth of certificates (156 files) plus old cars downloading one year's worth of certificates (52 files).	17m x 52 weeks * 3 years = 2,652 million files Divided by the number of seconds in a year: 2,652 million files / 31,557,600 seconds = **85 files per second**	of old vehicles (34 million): 17m (new) + 34m (old) Old cars only download one year's worth of certificates (52 files) while new cars download three years' worth of certificates (156 files) so: (17m * 156 files) + (34m * 52 files) = 2,652 million files + 1,768 million files = 4,420 million files Divided by the number of seconds in a year: 4,420 million files /31,557,600 seconds = **~141 files per second**	old vehicles (68 million): 17m (new) + 68m (old) Old cars only download one year's worth of certificates (52 files) while new cars download three years' worth of certificates (156 files) so: (17m * 156 files) + (68m * 52 files) = 2,652 million files + 3,536 million files = 6,188 million files Divided by the number of seconds in a year: 6,188 million files /31,557,600 seconds = **~197 files per second**	system out of which, 153 million will be old vehicles: 17m (new) + 153m (old) The new cars will be downloading three years' worth of certificates (156 weeks), while the rest of the vehicles will be topping up only (52 weeks). Since each file contains one week's worth of certificates, we can express this in number of files: (17m x 156 files) + (153m x 52 files) = (2,652mf + 7,956mf) = 10,608 million files Divided by the number of seconds in a year: 15,028 million files / 31,557,600 seconds = **~337 files per second**

6.3.6.5 Quality of Protection

- RA protects access with HTTPS (TLS V1.2)
- Supports at a minimum OpenSSL cipher suite ECDHE-ECDSA-AES128-SHA256
- Uses certificate-based client authentication of data signed by the device enrollment certificate, validated at the application layer. This is a supplement to the one-way

TLS authentication, to provide two-way authentication with a TLS/1609.2 hybrid scheme.

6.3.7 RA - Retrieve Registration Authority Certificate

EEs use this service to refresh its locally cached RA certificate.

PORT	8892
PATH	**/retrieve-ra-certificate**
HTTP Method	POST
HTTP Request Body	ASN.1 serialized *SecuredRACertRequest* PDU Message.
HTTP Response Body	Serialized IEEE 1609.2 certificate

6.3.7.1 Preconditions

None

6.3.7.2 Postconditions

1. The 1609 certificate is returned to the device.

6.3.7.3 Error Handling

See "RA-EE Errors" in Overview of Used Error Codes

6.3.7.4 Quality of Service

Estimated values are per logical unit, meaning multiple individual nodes can contribute to achieve the desired level of service. The number of vehicles likely to download the RA certificate is a function of the number of years in service:

$$f(year) = \left(\sum_{i=1}^{year-1} 17million \right) + \frac{17million}{2}$$

Quality Metric	Rationale	1 Year	3 Years	5 Years	10 Years
Throughput	Assuming half of all new cars plus all existing vehicles need to refresh their copy of the	8,500,000 new vehicles / 604,800 seconds/week = **14** requests / second	(8,500,000 new vehicles + 34,000,000 existing vehicles) / 604,800 seconds/week = **70** requests / second	(8,500,000 new vehicles + 68,000,000 existing vehicles) / 604,800 seconds/week = **126** requests / second	(8,500,000 new vehicles + 153,000,000 existing vehicles) / 604,800 seconds/week = **267** requests / second

Quality Metric	Rationale	1 Year	3 Years	5 Years	10 Years
	RA certificate in one week.				

6.3.7.5 Quality of Protection

- RA protects access with HTTPS (TLS V1.2)
- Supports at a minimum OpenSSL cipher suite ECDHE-ECDSA-AES128-SHA256

6.3.8 RA - Request Identification Certificate Provisioning

OBEs use this service to request the new identification certificates. After the initial batch is requested, subsequent batches are automatically provisioned.

PORT	8892
PATH	**/provision-identity-certificate**
HTTP Method	POST
HTTP Request Body	ASN.1 serialized *SecuredIdCertProvisioningRequest*
HTTP Response Body	ASN.1 serialized *SignedIdCertProvisioningAck* with a *requestHash* property containing the lower 8 bytes of the request hash. This value will identify this device from this point on, and it is to be used in subsequent download calls. The *reply* property contains a *PseudonymCertProvisioningAck* with a *certDLTime* property containing the expected time for download of the requested certificate and a *certDLURL* property containing the URL where the certificate can be downloaded.

6.3.8.1 Preconditions

1. Policy referenced in the request message is previously known
2. EE is not revoked

6.3.8.2 Postconditions

None.

6.3.8.3 Error Handling

See "RA-EE Errors" in Overview of Used Error Codes

6.3.8.4 Quality of Protection

- RA protects access with HTTPS (TLS V1.2)
- Supports at a minimum OpenSSL cipher suite ECDHE-ECDSA-AES128-SHA256

- Uses certificate-based client authentication of data signed by the device enrollment certificate, validated at the application layer. This is a supplement to the one-way TLS authentication, to provide two-way authentication with a TLS/1609.2 hybrid scheme.

6.3.9 RA - Download Identification Certificate

OBEs use this service to download a previously requested Identification Certificate.

PORT	**8892**
PATH	**/download/identity-certificate**
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}_i.zip, where the group of 16 hexadecimal digits is the device's request hash obtained from the provision identification certificate request, and i is a file iterator in hexadecimal starting at 0 (both are case insensitive). Example: AB09281C9867DE53_F.zip corresponds to i = 15, for a device with request hash AB09281C9867DE53. There shall be exactly one identification certificate per file. **Range (optional) as defined in RFC 2616:** To support partial downloads for resuming interrupted transfers. Examples: 1. From byte offset 500 to 700: Range : bytes=500-700 2. Starting from byte offset 1000 to the end: Range : bytes=1000-
HTTP Response Body	If no Range header is present, the entire tar file corresponding to the requested batch. If a Range header is present, the specified bytes of the referenced file.

6.3.9.1 Preconditions

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

6.3.9.2 Postconditions

1. The zip file corresponding to the certificate specified in the request URL is returned.
2. The content of the tar file is organized as a flat directory containing 1 file named as in:

- X_i
- X shall be the lower 8-bytes of the SHA-256 hash (16 hexadecimal digits) of the device request in hexadecimal (case insensitive)
- Where there is no extension

6.3.9.3 Error Handling

See "RA-EE Errors" in Overview of Used Error Codes

6.3.9.4 Quality of Service

For PoC the volume for this interface is still TBD but is not expected to have significant impact on system throughput requirements.

6.3.9.5 Quality of Protection

- RA protects access with HTTPS (TLS V1.2)
- Supports at a minimum OpenSSL cipher suite ECDHE-ECDSA-AES128-SHA256
- Uses certificate-based client authentication of data signed by the device enrollment certificate, validated at the application layer. This is a supplement to the one-way TLS authentication, to provide two-way authentication with a TLS/1609.2 hybrid scheme.

6.3.10 RA - Request Application Certificate Provisioning

RSEs use this service to request new application certificates. After the initial certificate is requested, subsequent certificates are **NOT** automatically provisioned.

PORT	**8892**
PATH	**/provision-application-certificate**
HTTP Method	POST
HTTP Request Body	ASN.1 serialized *SecuredAppCertProvisioningRequest*
HTTP Response Body	ASN.1 serialized *SignedAppCertProvisioningAck* 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 *PseudonymCertProvisioningAck* with a *certDLTime* property containing the expected time for download of the requested certificate and a *certDLURL* property containing the URL where the certificate can be downloaded.

6.3.10.1 Preconditions

1. Policy referenced in the request message is previously known
2. EE is not revoked

6.3.10.2 Postconditions

None.

6.3.10.3 Error Handling

See "RA-EE Errors" in Overview of Used Error Codes

6.3.10.4 Quality of Service

For PoC the volume for this interface is 50,000 RSEs. This is not expected to have significant impact on system throughput requirements.

6.3.10.5 Quality of Protection

- RA protects access with HTTPS (TLS V1.2)
- Supports at a minimum OpenSSL cipher suite ECDHE-ECDSA-AES128-SHA256
- Uses certificate-based client authentication of data signed by the device enrollment certificate, validated at the application layer. This is a supplement to the one-way TLS authentication, to provide two-way authentication with a TLS/1609.2 hybrid scheme.
- Incoming message is encrypted (within the ASN.1 message structure) with the RA Component certificate public key.

6.3.11 RA - Download Application Certificate

RSEs use this service to download a previously requested Application Certificate.

PORT	**8892**
PATH	**/download/application-certificate**
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 initial provision application certificate request. There shall be exactly one application certificate per file. **Range (optional) as defined in RFC 2616:** To support partial downloads for resuming interrupted transfers. Examples: 1. From byte offset 500 to 700: Range : bytes=500-700

PORT	**8892**
	2. Starting from byte offset 1000 to the end: Range : bytes=1000-
HTTP Response Body	If no Range header is present, the entire zip file corresponding to the requested batch. If a Range header is present, the specified bytes of the referenced file.

6.3.11.1 Preconditions

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

6.3.11.2 Postconditions

1. The file corresponding to the certificate specified in the request URL is returned
2. The content of the file is exactly one application certificate file per certificate download file. The content of the certificate file is the binary representation of the application certificate named as in:
    - X
    - X shall be the lower 8-bytes of the SHA-256 hash of the device request in hexadecimal (case insensitive 16 hexadecimal digits)
    - Where there is no extension

6.3.11.3 Error Handling

See "RA-EE Errors" in Overview of Used Error Codes

6.3.11.4 Quality of Service

For PoC, the volume for this interface is still TBD but is not expected to have significant impact on system throughput requirements.

6.3.11.5 Quality of Protection

- RA protects access with HTTPS (TLS V1.2)
- Supports at a minimum OpenSSL cipher suite ECDHE-ECDSA-AES128-SHA256
- Uses certificate-based client authentication of data signed by the device enrollment certificate, validated at the application layer. This is a supplement to the one-way TLS authentication, to provide two-way authentication with a TLS/1609.2 hybrid scheme.

6.3.12 RA - Download Local Certificate Chain File

EEs use this service to download a local certificate chain file.

PORT	**8892**
PATH	**/download/local-certificate-chain**

PORT	8892
HTTP Method	GET
HTTP Request Body	Empty
HTTP Request Headers	Optionally, the request may include the standard HTTP Header 'If-None-Match' containing the file name of the local certificate chains file that the EE currently possesses, **excluding any path**. For example: If-None-Match: "local_certificate_chains_01_03.oer" This is used to prevent the same file from being downloaded by the device multiple times.
HTTP Response Body	File containing the local certificate chains represented by an OER encoded ASN.1 serialized ScopedLocalCertificateChainFile. The file name returned is of the form: local_certificate_chains_<X>_<Y>.<Z> Where: • X is the global certificate chain version, i.e., the *cert_chain_file_id* parameter found in the Global Policy File • Y is the local certificate chain version • Z is one of the permitted encoding formats (oer) from the file name in the request message OR An HTTP code of 304 (Not Modified), if the provided file name in the 'If-None-Match' header matches the current version available on the RA server.

6.3.12.1 Preconditions

None

6.3.12.2 Postconditions

1. Returned file contains SCMS certificates chains that the device will use

6.3.12.3 Error Handling

See "RA-EE Errors" in Overview of Used Error Codes

6.3.12.4 Quality of Service

Estimated values are per logical unit, meaning multiple individual nodes can contribute to achieve the desired level of service. The number of vehicles that potentially invoke this service in a week is a function of the number of years in service:

$$f(year) = \left(\sum_{i=1}^{year-1} 17million \right) + \frac{17million}{2}$$

Quality Metric	Rationale	1 Year	3 Years	5 Years	10 Years
Throughput	Assuming half of all new cars plus all existing vehicles need to download local certificate chain file in the same week.	8,500,000 new vehicles / 604,800 seconds/week = **14** requests / second	(8,500,000 new vehicles + 34,000,000 existing vehicles) / 604,800 seconds/week = **70** requests / second	(8,500,000 new vehicles + 68,000,000 existing vehicles) / 604,800 seconds/week = **126** requests / second	(8,500,000 new vehicles + 153,000,000 existing vehicles) / 604,800 seconds/week = **267** requests / second

6.3.12.5 Quality of Protection

- RA protects access with HTTPS (TLS V1.2)
- Supports at a minimum OpenSSL cipher suite ECDHE-ECDSA-AES128-SHA256

6.3.13 RA - Submit Misbehavior Report

EEs use this service to submit a Misbehavior Report (MBR) that RA will forward to the Misbehavior Authority.

PORT	**8892**
PATH	**/process-misbehavior-report**
HTTP Method	POST
HTTP Request Body	ASN.1 serialized *SecuredMisbehaviorReport*
HTTP Response Body	Empty

6.3.13.1 Preconditions

1. EE is not revoked

6.3.13.2 Postconditions

None.

6.3.13.3 Error Handling

See "RA-EE Errors" in Overview of Used Error Codes

6.3.13.4 Quality of Service

For PoC, the volume for this interface will be estimated by the currently underway V2V-CR Project (GMBD), but is not expected to have significant impact on system throughput requirements.

6.3.13.5 Quality of Protection

- RA protects access with HTTPS (TLS V1.2)
- Supports at a minimum OpenSSL cipher suite ECDHE-ECDSA-AES128-SHA256
- Uses certificate-based client authentication of data signed by the device enrollment certificate, validated at the application layer. This is a supplement to the one-way TLS authentication, to provide two-way authentication with a TLS/1609.2 hybrid scheme.
- Incoming message is encrypted (within the ASN.1 message structure) with the MA Component certificate public key

7 Test Vectors

7.1 Purpose

The purpose is to provide the implementation and testing team with:

- Input/output values for core cryptographic functions as well as intermediate values
- Python scripts outlining the mathematical steps involved in each cryptographic function along with pertinent inline documentation

The input/output values along with the Python scripts will serve in ensuring the correct implementation of the cryptographic algorithms, which are typically prone to erroneous implementation.

7.2 Test Vectors Location

Test vectors are located at http://stash.campllc.org/projects/SCMS/repos/crypto-test-vectors/ .

7.3 Overview

The following is the README in that Stash repository:**README.md**master SCMS/crypto-test-vectors

7.4 Crypto Test Vectors

This directory contains test vectors for the following functions as specified here.

Additionally there are test vectors for crypto functions needed for encryption and signing/verification.

All python scripts implement the corresponding functionality in order to depict the mathematical and cryptographic calculations involved.

7.4.1 Linkage Values lv(i,j)

- lv.txt: test vectors for i = {0,1} and j randomly chosen in [1,20]
- lv.py : Python script that generates the test vectors

7.4.2 Group Linkage Values glv(i,j,k) and Encrypted Indices ei(j,k)

- glv.txt: test vectors for i = {0,1} and j randomly chosen 32-bit value

- glv.py : Python script that generates the test vectors

7.4.3 Butterfly Expansion Function

- bfkeyexp.txt: test vectors for Butterfly Expansion Function for Certificate and Encryption key pairs
- bfkeyexp.py : Python script that generates the test vectors

7.4.4 Key Derivation Function, KDF2 [IEEE-1363a, ANSI X9.63] with SHA-256

- kdf.txt: ANSI X9.63 test vectors of KDF2 with SHA-256
- kdf.py : Python script that implements KDF2 and tests it against the test vectors included

7.4.5 Message Authentication Code, MAC1 (HMAC)[IEEE-1363a, ANSI X9.71, RFC 2104, 4231] with SHA-256

- mac1.txt: RFC 4231 test vectors of HMAC-SHA-256
- mac1.py : Python script that implements HMAC-SHA-256 and tests it against the test
  vectors included

7.4.6 AES-CCM-128 Symmetric Authenticated Encryption [IEEE-1609.2, NIST SP 800-38C]

- aesccm.txt: test vectors for AES-CCM-128 Symmetric Authenticate Encryption based on NIST SP 800-38C (and RFC 3610) with parameters defined in IEEE-1609.2
- aesccm.py : Python script that generates the test vectors

7.4.7 ECDH Key Agreement [SP800-56A Section 5.7.1.2]

- ecdh.txt: test vectors for ECDH Key Agreement Scheme as per SP800-56A Section 5.7.1.2 using NIST test vectors
- ecdh.py : Python script that implements ECDH for curve P-256 and tests it against the test
  vectors included

7.4.8 ECIES Public-Key Encryption [IEEE-1609.2]

- ecies.txt: test vectors for ECIES Encryption as per IEEE-1609.2,
  Used to wrap AES-CCM 128-bit keys

- ecies.py : Python script that generates the test vectors

7.4.9 Implicit Certificate Generation and Public/Private Keys Reconstruction [SEC-4]

- implicit.txt: test vectors for generating implicit certificates and for reconstructing the corresponding private and public keys as per [SEC-4].
- implicit.py : Python script that generates the test vectors

7.4.9.1 Other files:

- radix.py:
- array.py: utility scripts for printing the output
- ecc.py: Elliptic Curve Cryptosystems core computations

7.4.10 Hash-based Functions

7.4.10.1 Key Derivation Function, KDF2

- This function is used to expand/derive keys from shared secret and specified input parameters. The derived keys may be used in symmetric-key encryption and/or authentication.
- Based on SHA-256
- Implemented as per IEEE-1363a and ANSI X9.63
- Required in the implementation of ECIES

7.4.10.2 Message Authentication Code, MAC1 (HMAC)

- This is a symmetric-key authentication function, i.e., it takes as input an authentication key and the data to be authenticated and outputs an authentication tag that is appended to the data and ensures its integrity and authenticity
- Based on SHA-256
- Implemented as per IEEE-1363a, ANSI X9.71, RFC 2104 and 4231
- Required in the implementation of ECIES

7.4.11 AES-based Functions

7.4.11.1 AES-CCM Authenticated Encryption

- This is a symmetric-key authenticated encryption function, i.e., it takes as input a symmetric key and a plaintext and outputs a cipher text and an authentication tag. It provides confidentiality, integrity and authenticity of the data.
- Based on AES-128

- Implemented as per IEEE-1609.2 and NIST SP 800-38C
- Used in all data encryption. The symmetric key used is then wrapped with ECIES and sent along with the encrypted data.

7.4.12 ECC Functions

7.4.12.1 ECDH Key Agreement

- Elliptic Curve Diffie-Hellman is a public-key primitive where two parties can compute a shared secret by exchanging public keys and employing them and the corresponding private keys in the computation
- Based on ECC over the curve P-256
- Implemented as per NIST SP800-56A Section 5.7.1.2
- Required in the implementation of ECIES

7.4.12.2 ECIES Public-key Encryption

- Elliptic Curve Integrated Encryption Scheme is a hybrid encryption primitive composed of public-key key agreement (ECDH), a key derivation function (KDF2) and symmetric-key encryption (XOR) and authentication (MAC1). A Sender employs this scheme to encrypt a message using the public-key of the Recipient.
- The primitives in the brackets above are as per IEEE-1609.2
- Used to wrap (encrypt) AES-CCM-128 encryption keys

7.4.12.3 Implicit Certificate Generation and Public/Private Keys Reconstruction

- Implicit certificates are employed for pseudonym certificates, enrollment certificates, etc. (see Certificate Types)
  They do not contain the subject's public key and are not signed by the issuer, as is the case with explicit certificates, rather they contain a public key reconstruction point that is used to reconstruct the public key of the subject knowing the public key of the issuer. When issued, a private key reconstruction value is sent along from the issuer to the subject and only the subject can reconstruct the actual private key using this value and the private key used in the certificate request. In the case of pseudonym certificates, for example, the subject is the EE and the issuer is the PCA.
- Based on ECC over the curve P-256
- `H(CertU)` in the script is provided as an illustrative value. See IEEE 1609.2-2016, Sec. 6.4.8, under ENCODING CONSIDERATIONS: "for implicit certificates, the value H(CertU) in SEC 4, section 3, is for purposes of this standard taken to be H (H (canonicalized ToBeSignedCertificate from the subordinate certificate) || H(entirety of issuer Certificate)). See 5.3.2 for further discussion" See the cited section for details.
- **Notes**:

- CertU is a term in SEC4 standard which only deals with implicit certs and public/private keys reconstruction. It is used in the Python scripts that generate the test vectors with comments that ensure that it's understood to be only for illustrative purpose:
-
    - tbsdata was arbitrary
-
    - CertU = Hash (tbsdata || pub key recon point), just to emphasize that however the input to the hash is formulated, it should contain at least the tbs data and the public key reconstruction point for mathematical and cryptographic correctness and assurance of the algorithm
    - In 1609.2-2016, Sec 6.4.5 and 6.4.8, the public key reconstruction point is the verifyKeyIndicator and is already part of ToBeSignedCertificate, which already satisfies the cryptographic requirement in the previous item. In addition to that, there is another input, the issuer cert; as explained in Sec 6.4.8, the hash is calculated as: H (H (canonicalized ToBeSignedCertificate from the subordinate certificate) || H(entirety of issuer Certificate))
    - The hash in 1609.2 is calculated the same way for implicit and explicit certs as in Sec 5.3.1 and Sec. 6.4.8
- The operations in SEC4 that would require using the 1609.2-2016 hashing algorithm are conveniently listed in 1609.2-2016 Sec 5.3.2:

  5.3.2 Implicit Certificates

  Implicit certificates were proposed in Brown, Gallant, and Vanstone [B3] and Pintsov and Vanstone [B18] while modifications to protect against attacks were proposed in Brown, Campagna, and Vanstone [B4]. In this standard, implicit certificates are processed as specified in Standards for Efficient Cryptography (SEC) 4 except for the exceptions noted in this subclause.

  a) In this standard, an implicit certificate is encoded as an ImplicitCertificate, as defined in 6.4.5, and is encoded with the Canonical Octet Encoding Rules (COER). All references to "the certificate CertU" in SEC 4 should be taken as referring to the encoded ImplicitCertificate except when the implicit certificate is hashed to an integer modulus n. This case is addressed in item b) below.

  b) When an implicit certificate is hashed to an integer modulo n, the input is not simply the implicit certificate CertU but the information specified below. This affects the following steps in SEC 4:
  1) Section 3.4, Action 7
  2) Section 3.5, Action 4
  3) Section 3.6, Action 2

4) Section 3.7, Action 4
5) Section 3.8, Action 4

The encoded data input to the hash function is Hash (ToBeSignedCertificate from the subordinate certificate as specified in 6.4.8) || Hash (Entirety of issuer certificate as specified in 6.4.3).

7.4.13 Linkage Values and Butterfly Key Expansion Functions

- These are as specified in Special Cryptographic Primitives in SCMS

7.5 1602.2 and SCMS ASN.1 Objects

scms-protocol.asn:

```
SecuredScmsPDU ::= Ieee1609Dot2Data
```

Figure 84 SCMS-Protocol ASN.1

1609.2-schema.asn:

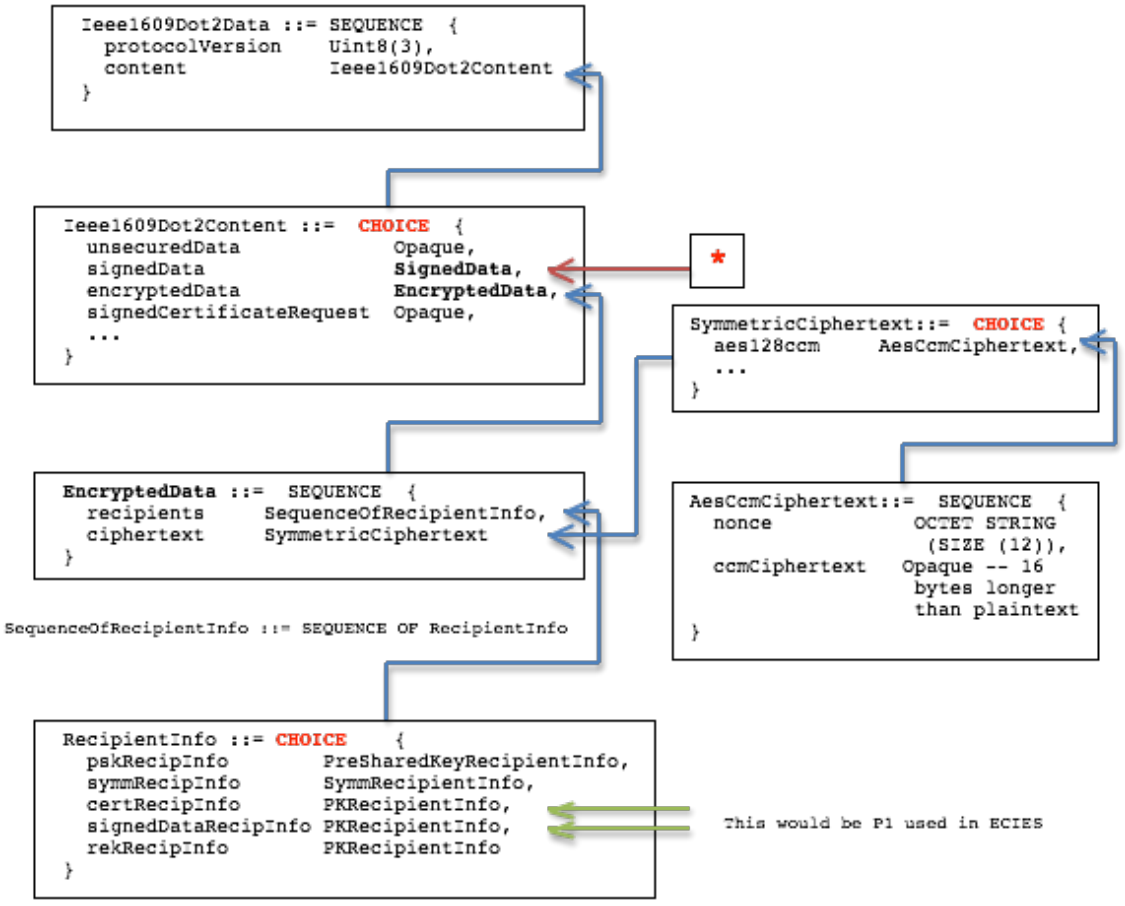


Figure 85 IEEE 1609.2 Schema ASN.1

See ECIES diagram and Notes on Encrypted Data below, as well as PKRecipientInfo and EciesP256EncryptedKey ASN.1 objects in 1609dot2-schema.asn and EciesP256EncryptedKey in 1609dot2-base-types.asn, to see how the outputs of ECIES are encoded in the RecipientInfo.

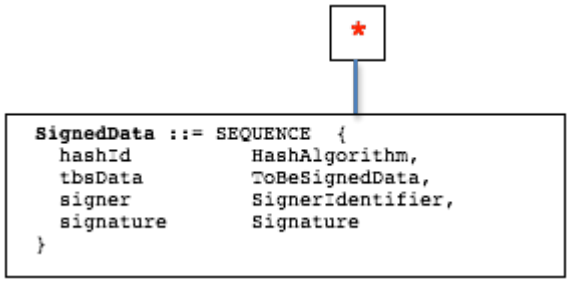


Figure 86 SignedData ASN.1

Example of SignedData from scms-protocol.asn:

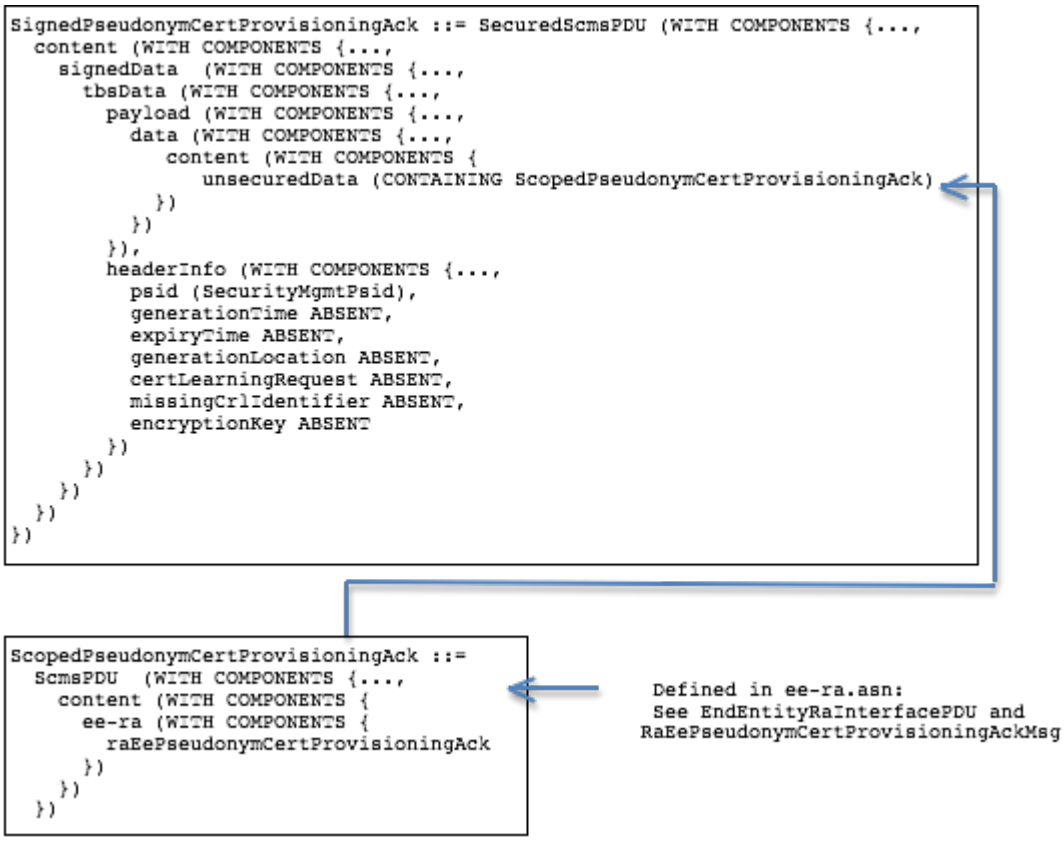


Figure 87 SignedData Example ASN.1

7.6 ECIES Encryption as in 1609.2-2016, Sec 5.3.5

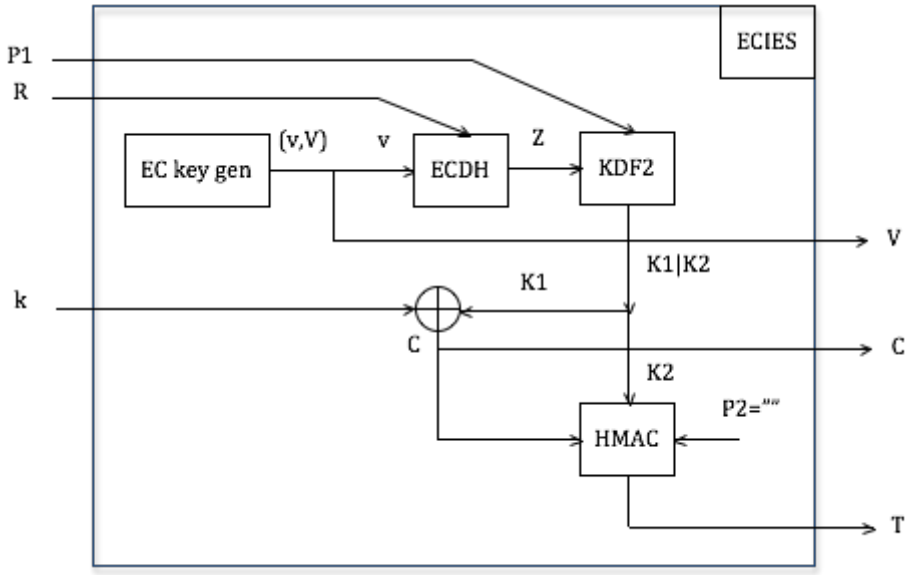


Figure 88 ECIES Encryption

Inputs:
P1: see below
R: recipient's public key
k: AES-CCM symmetric key to be encrypted with ECIES

Outputs:
V: Sender's ephemeral public key
C: Cipher text (encrypted symmetric key k)
T: Tag

Notes:

- KDF is KDF2 [in IEEE 1363a, Section 13.2]:
  KDF2(Z, P1) = Hash(Z || Counter || P1),
  where Hash is SHA-256, and the 32-bit counter increases as more output blocks are generated, the output blocks are concatenated to form the KDF output
- MAC2 is HMAC:
  HMAC(K2, C) = Hash((K2 ^ iPad) || Hash((K2 ^ oPad) || C)),
  where Hash is SHA-256, and iPad and oPad are 256-bit (32-byte) blocks formed by repeating the byte 0x36 and 0x5C, respectively
- in 1609.2-2016
  "Encryption shall use non-DHAES mode. This means that the elliptic curve points shall be converted to octet strings using LSB compressed representation."
  Regarding non-DHAES mode, in IEEE 1363a-2004:
  "The length in bits of the shared secret key K shall be l + k2 where k2 is the length in bits of the key for the message authentication code (l is the bitlength of the

message M to be encrypted). In non-DHAES mode, let K1 be the leftmost l bits of K and let K2 be the remaining k2 bits."
This means that the KDF output = ENC key | MAC Key, in a (big endian) byte array.

- From 1609.2-2016, Sec 6.3.30:
  On EncryptedData:

  This data structure encodes data that has been encrypted to one or more recipients using the recipients' public or symmetric keys as specified in 5.3.4.Sec 5.3.4.1: This section explains how the data is encrypted with a fresh symmetric key generated by the sender, and the symmetric key is then encrypted for the recipient using that recipient's encryption key and refers to Sec 5.3.5 that explains Public Key Encryption using ECIES.

- Sec 6.3.31:
  On RecipientInfo:
  - certRecipInfo: The data encryption key was encrypted using the public encryption key in a certificate. This field contains the HashedId8 of the certificate. In this case, the parameter P1 to ECIES as defined in 5.4.5 is the hash of the certificate.
  - signedDataRecipInfo: The data encryption key was encrypted using the public response encryption key from a SignedData. In this case, this field contains the HashedId8 of the1609Dot2Data containing the SignedData containing the encryption key. In this case, the parameter P1 to ECIES as defined in 5.4.5 is the SHA-256 hash of the Ieee1609Dot2Data containing the response encryption key.
  - rekRecipInfo: The data encryption key was encrypted using a public response encryption key that was not obtained from a SignedData. In this case, this field contains the HashedId8 of the response encryption key. In this case, the parameter P1 to ECIES as defined in 5.4.5 is the hash of the empty string.

8 Glossary

Acronym	Full Form / Description
3D	Three-Dimensional
AES	The **Advanced Encryption Standard** (**AES**), also known as Rijndael (its original name), is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001
APDU	The **APDU** (Application Protocol Data Unit) is the communication unit between a reader and a card. The structure of an **APDU** is defined by the ISO 7816 standards. There are two categories of APDUs: command APDUs and response APDUs
ASD	Aftermarket Safety Device
ASN.1	Abstract Syntax Notation One (**ASN**.**1**) is a standard and notation that describes rules and structures for representing, encoding, transmitting, and decoding data in telecommunications and computer networking. The formal rules enable representation of objects that are independent of machine-specific encoding techniques.
BMC	Backend Management Commands
BSM	Basic Safety Message as defined in the SAE J2735 standard
BSS	In computer networking, a service set is a set consisting of all the devices associated with a consumer or enterprise IEEE 802.11 wireless local area network (WLAN). The service set can be local, independent, extended or mesh. Service sets have an associated identifier, the Service Set Identifier (SSID), which consists of 32 octets that frequently contains a human readable identifier of the network. The **basic service set** (**BSS**) provides the basic building-block of an 802.11 wireless LAN. In infrastructure mode, a single access point (AP) together with all associated stations (STAs) is called a BSS; not to be confused with the coverage of an access point, known as the **basic service area** (**BSA**). The access point acts as a master to control the stations within that BSS; the simplest BSS consists of one access point and one station. In OCB mode there is no access point and therefore all stations within reach is called a BSS.
BSW	The **Blind Spot Warning** and Lane Change Warning (**BSW**+LCW) application is intended to warn the driver of the vehicle during a lane change attempt if the blind-spot zone into which the vehicle intends to switch is, or will soon be, occupied by another vehicle traveling in the same direction. Moreover, the application provides advisory information that is intended to inform the driver that

Acronym	Full Form / Description
	another vehicle in an adjacent lane is positioned in a blind-spot zone of the vehicle even if a lane change is not being attempted.
C2C-CC	The **CAR 2 CAR Communication Consortium** (**C2C-CC**) is a nonprofit, industry-driven organization initiated by European vehicle manufacturers and supported by equipment suppliers, research organizations and other partners. The C2C-CC is dedicated to the objective of further increasing road traffic safety and efficiency by means of cooperative intelligent transport systems (ITS) with vehicle-to-vehicle communication (V2V) supported by vehicle-to-infrastructure communication (V2I).
C2X	Car-to-X - the European version of V2X
CA	In cryptography, a **certificate authority** or certification **authority** (CA) is an entity that issues digital **certificates**. A digital **certificate** certifies the ownership of a public key by the named subject of the **certificate**.
CAMP	Crash Avoidance Metrics Partners LLC
CAN	A **Controller Area Network** (**CAN bus**) is a vehicle bus standard designed to allow microcontrollers and devices to communicate with each other in applications without a host computer. It is a message-based protocol, designed originally for multiplex electrical wiring within automobiles, but is also used in many other contexts.
CCH	In radio communication, a **control channel** (**CCH**) is a central channel that controls other constituent radios by handling data streams.
CCM	**CCM mode** (**Counter with CBC-MAC**) is a mode of operation for cryptographic block ciphers. It is an authenticated encryption algorithm designed to provide both authentication and confidentiality. CCM mode is only defined for block ciphers with a block length of 128 bits.
CFR	The **Code of Federal Regulations** (**CFR**) is the codification of the general and permanent rules and **regulations** (sometimes called administrative law) published in the **Federal** Register by the executive departments and agencies of the **federal** government of the United States
CME	Certificate Management Entity
CONVERGE	**Communication Network Vehicle Road Global Extension** (**CONVERGE**): Pioneering approaches to traffic management and vehicle safety issues are increasingly growing together. Still a holistic system architecture for flexible interaction between different service providers and communications network operators is missing in a decentralized, scalable structure. The aim of the project CONVERGE is to close this gap.
CPR	Certificate Provisioning Request

Acronym	Full Form / Description
CPU	A **Central Processing Unit** (**CPU**) is the electronic circuitry within a computer that carries out the instructions of a computer program by performing the basic arithmetic, logical, control and input/output (I/O) operations specified by the instructions. The term has been used in the computer industry at least since the early 1960s.Traditionally, the term "CPU" refers to a processor, more specifically to its processing unit and control unit (CU), distinguishing these core elements of a computer from external components such as main memory and I/O circuitry.
CRACA	Certificate Revocation Authorizing Certificate Authority
CRL	In the operation of some cryptosystems, usually public key infrastructures (PKIs), a **Certificate Revocation List (CRL)** is a list of certificates (or more specifically, a list of serial numbers for certificates) that have been revoked, and therefore, entities presenting those (revoked) certificates should no longer be trusted.
CRLG	Certificate Revocation List Generator
CS	Certificate Store
CSR	A **CSR** or **Certificate Signing Request** is a block of encrypted text that is generated by the device that will use the **certificate**. It contains information that will be included in your **certificate** such as PSID/SSP.
CTS	**RTS/CTS** (**Request to Send / Clear to Send**) is the optional mechanism used by the IEEE 802.11 wireless networking protocol to reduce frame collisions introduced by the hidden node problem. Originally the protocol fixed the exposed node problem as well, but modern RTS/CTS includes ACKs (acknowledgements) and does not solve the exposed node problem.
DCM	Device Configuration Manager.Attests to the ECA that an EE device is eligible to receive enrollment certificates, and provides all relevant configuration settings and certificates during bootstrapping.
DER	The **Distinguished Encoding Rules** for ASN.1, abbreviated DER, are a subset of the Basic Encoding Rules (BER) specification, and give exactly one way to represent any ASN.1 value as an octet string. DER is intended for applications in which a unique octet string **encoding** is needed, as is the case when a digital signature is computed on an ASN.1 value.
DF	A **data frame** (**DF**) is a digital data transmission unit in computer networking and telecommunication. A frame typically includes frame synchronization features consisting of a sequence of bits or symbols that indicate to the receiver the beginning and end of the payload data within the stream of symbols or bits it receives. If a receiver is connected to the system in the middle of a frame transmission, it ignores the data until it detects a new frame synchronization sequence.

Acronym	Full Form / Description
DNPW	The **Do Not Pass Warning (DNPW)** application is intended to warn the driver of the vehicle during a passing maneuver attempt when a slower moving vehicle, ahead and in the same lane, cannot be safely passed using a passing zone which is occupied by vehicles in the opposite direction of travel. In addition, the application provides advisory information that is intended to inform the driver of the vehicle that the passing zone is occupied when a vehicle is ahead and in the same lane even if a passing maneuver is not being attempted.
DNS	**Domain Name Servers** (**DNS**) are the Internet's equivalent of a phone book. They maintain a directory of **domain names** and translate them to Internet Protocol (IP) addresses. This is necessary because, although **domain names** are easy for people to remember, computers or machines, access websites based on IP addresses.
DSA	The **Digital Signature Algorithm** (**DSA**) is a Federal Information Processing Standard (FIPS) for digital signatures. It was proposed by the National Institute of Standards and Technology (NIST) in August 1991 for use in their Digital Signature Standard and adopted as FIPS 186 in 1993. Four revisions to the initial specification have been released: FIPS 186-1 in 1996,FIPS 186-2 in 2000, FIPS 186-3 in 2009, and FIPS 186-4 in 2013.
DSRC	**Dedicated Short-Range Communications (DSRC)** are one-way or two-way short-range to medium-range wireless communication channels specifically designed for automotive use and a corresponding set of protocols and standards.
DVI	Driver Vehicle Interface
ECA	Enrollment Certificate Authority. Issues enrollment certificates, which act as a passport for a device to authenticate against the RA, e.g., when requesting certificates. Different ECAs may issue enrollment certificates for different geographic regions, manufacturers, or device types.
ECB	In cryptography, a **mode of operation** is an algorithm that uses a block cipher to encrypt messages of arbitrary length in a way that provides confidentiality or authenticity. A block cipher by itself is only suitable for the secure cryptographic transformation (encryption or decryption) of one fixed-length group of bits called a block. A mode of operation describes how to repeatedly apply a cipher's single-block operation to securely transform amounts of data larger than a block. The simplest of the encryption modes is the **Electronic Codebook (ECB)** mode. The message is divided into blocks, and each block is encrypted separately.
ECC	**Elliptic Curve Cryptography (ECC)** is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC requires smaller keys compared to non-ECC cryptography (based on plain Galois fields) to provide equivalent security.
ECDSA	The **Elliptic Curve Digital Signature Algorithm** (**ECDSA**) offers a variant of the Digital Signature Algorithm (DSA) which uses elliptic curve cryptography.

Acronym	Full Form / Description
ECDLP	Public-key cryptography is based on the intractability of certain mathematical problems. Early public-key systems are secure assuming that it is difficult to factor a large integer composed of two or more large prime factors. For elliptic-curve-based protocols, it is assumed that finding the discrete logarithm of a random elliptic curve element with respect to a publicly known base point is infeasible: this is the "**elliptic curve discrete logarithm problem**" or **ECDLP**. The security of ECC depends on the ability to compute a point multiplication and the inability to compute the multiplicand given the original and product points. The size of the elliptic curve determines the difficulty of the problem.
ECIES	**Elliptic Curve Integrated Encryption Scheme**, or **ECIES**, is a hybrid encryption system proposed by Victor Shoup in 2001. ECIES has been standardized in ANSI X9.63, IEEE 1363a, ISO/IEC 18033-2, and SECG SEC-1. ECIES combines a Key Encapsulation Mechanism (KEM) with a Data Encapsulation Mechanism (DEM). The system independently derives a bulk encryption key and a MAC key from a common secret. Data is first encrypted under a symmetric cipher, and then the cipher text is MAC'd under an authentication scheme. Finally, the common secret is encrypted under the public part of a public/private key pair. The output of the encryption function is the tuple {K,C,T}, where K is the encrypted common secret, C is the ciphertext, and T is the authentication tag. There is some hand waiving around the "common secret" since its actually the result of applying a Key Agreement function, and it uses the static public key and an ephemeral key pair.
ECQV	In cryptography, **implicit certificates** are a variant of public key certificate, such that a public key can be reconstructed from any implicit certificate, and is said then to be *implicitly* verified, in the sense that the only party who can know the associated private key is the party identified in the implicit certificate. This does not rule out the possibility that nobody knows the private key, but this possibility is not considered a major problem. By comparison, traditional public-key certificates include a copy of the public key and the digital signature of the certificate authority. Upon verification of the digital signature, the public key is *explicitly* verified, in the sense that the party identified in the certificate knows the associated private key and is the only party who can know the private key. Unlike an implicit certificate, there is no possibility that nobody knows the private key. For the purposes of this document, such certificates will be called *explicit* certificates. **Elliptic Curve Qu-Vanstone** (**ECQV**) are one kind of implicit certificates.
ECU	In automotive electronics, **Electronic Control Unit** (**ECU**) is a generic term for any embedded system that controls one or more of the electrical system or subsystems in a transport vehicle.
EDCA	Enhanced Distributed Channel Access

Acronym	Full Form / Description
EE	An end-entity (EE) device that sends or receives messages, e.g., an OBE, an after-market safety device (ASD), an RSE, or a Traffic Management Center (TMC) backend.
EEBL	The **Emergency Electronic Brake Light** (**EEBL**) application enables a vehicle to broadcast a self-generated emergency brake event to surrounding vehicles. Upon receiving the event information, the receiving vehicle determines the relevance of the event and, if appropriate, provides a warning to the driver in order to avoid a crash. This application is particularly useful when the driver's line of sight is obstructed by other vehicles or bad weather conditions (e.g., fog, heavy rain).
EGNOS	The **European Geostationary Navigation Overlay Service** (**EGNOS**) is a satellite based augmentation system (SBAS) developed by the European Space Agency, the European Commission and EUROCONTROL. It supplements the GPS, GLONASS and Galileo systems by reporting on the reliability and accuracy of the positioning data. According to specifications, horizontal position accuracy should be better than seven metres. In practice, the horizontal position accuracy is at the metre level. The EGNOS system consists of four geostationary satellites and a network of ground stations.
EK	Encryption Key
Elector	**Electors** represent the center of trust of the SCMS. Electors sign ballots that either endorse or revoke an RCA or another elector. The SCMS Manager distributes those ballots to all SCMS components, including devices, to establish trust relationships in RCAs and electors. An elector has a self-signed certificate, and all entities of the system will implicitly trust the initial set of electors. Therefore, all entities have to protect electors against unauthorized alteration, once they installed the initial set.
EMVCo	Europay-Mastercard-Visa Consortium
ETSI	The **European Telecommunications Standards Institute** (**ETSI**) is an independent, not-for-profit, standardization organization in the telecommunications industry in Europe, headquartered in Sophia-Antipolis, France, with worldwide projection.
FCC	The **Federal Communications Commission** (**FCC**) is an independent agency of the United States government, created by Congressional statute to regulate interstate communications by radio, television, wire, satellite, and cable in all 50 states, the District of Columbia and U.S. territories. The FCC works towards six goals in the areas of broadband, competition, the spectrum, the media, public safety and homeland security, and modernizing itself.
FCW	The **Forward Collision Warning** (**FCW**) application is intended to warn the driver of the vehicle in case of an impending rear-end collision with another vehicle ahead in traffic in the same lane and direction of travel. The application

Acronym	Full Form / Description
	uses data received from other vehicles to determine if a forward collision is imminent. FCW is intended to advise drivers to take specific action in order to avoid or mitigate rear-end vehicle collisions in the forward path of travel.
FHWA	The **Federal Highway Administration** (**FHWA**) is a division of the United States Department of Transportation that specializes in highway transportation.
FIPS	**FIPS** (**Federal Information Processing Standards**) are a set of **standards** that describe document **processing**, encryption algorithms and other **information** technology **standards** for use within non-military government agencies and by government contractors and vendors who work with the agencies.
FM	In telecommunications and signal processing, **frequency modulation** (**FM**) is the encoding of information in a carrier wave by varying the instantaneous frequency of the wave. This contrasts with amplitude modulation, in which the amplitude of the carrier wave varies, while the frequency remains constant.
FMVSS	**Federal Motor Vehicle Safety Standards** (**FMVSS**) are U.S. **federal regulations** specifying design, construction, performance, and durability requirements for **motor vehicles** and regulated **automobile safety**-related components, systems, and design features.
FQDN	A **Fully Qualified Domain Name** (**FQDN**) is the complete **domain name** for a specific computer, or host, on the Internet. The **FQDN** consists of two parts: the hostname and the **domain name**. For example, an **FQDN** for a hypothetical mail server might be mymail.somecollege.edu
GCCF	Global Certificate Chain File
GD	Global Detection
GHz	Gigahertz. See Hertz
GMBD	Global Misbehavior Detection is the process to identify potential misbehavior in the system, investigate suspicious activity, and if confirmed, to revoke certificates of misbehaving devices.
GNSS	A satellite navigation system with global coverage may be termed a **global navigation satellite system** (**GNSS**). A satellite navigation or satnav system is a system that uses satellites to provide autonomous geo-spatial positioning. It allows small electronic receivers to determine their location (longitude, latitude, and altitude/elevation) to high precision (within a few metres) using time signals transmitted along a line of sight by radio from satellites. The system can be used for navigation or for tracking the position of something fitted with a receiver (satellite tracking). The signals also allow the electronic receiver to calculate the current local time to high precision, which allows time synchronisation. Satnav systems operate independently of any telephonic or internet reception, though

Acronym	Full Form / Description
	these technologies can enhance the usefulness of the positioning information generated.
GP	General Purpose
GP-CPU	General Purpose Central Processing Unit
GPF	Global Policy File
HCF	Hybrid Coordination Function
HD	Hybrid-Digital
HSM	A **hardware security module** (**HSM**) is a physical computing device that safeguards and manages digital keys for strong authentication and provides cryptoprocessing. These modules traditionally come in the form of a plug-in card or an external device that attaches directly to a computer or network server.
HTTP	The **Hypertext Transfer Protocol** (**HTTP**) is an application protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web. Hypertext is structured text that uses logical links (hyperlinks) between nodes containing text. HTTP is the protocol to exchange or transfer hypertext.
HTTPS	**HTTPS** (also called **HTTP over TLS**, **HTTP over SSL**, and **HTTP Secure**) is a protocol for secure communication over a computer network which is widely used on the Internet. HTTPS consists of communication over Hypertext Transfer Protocol (HTTP) within a connection encrypted by Transport Layer Security (TLS) or its predecessor, Secure Sockets Layer (SSL). The main motivation for HTTPS is authentication of the visited website and protection of the privacy and integrity of the exchanged data.
HV	Host Vehicle
Hz	The **hertz** (symbol **Hz**) is the unit of frequency in the International System of Units (SI) and is defined as one cycle per second. It is named for Heinrich Rudolf Hertz, the first person to provide conclusive proof of the existence of electromagnetic waves. Hertz are commonly expressed in SI multiples **kilohertz** (10^3 Hz, symbol **kHz**), **megahertz** (10^6 Hz, **MHz**), **gigahertz** (10^9 Hz, **GHz**), and **terahertz** (10^{12} Hz, **THz**).
ICA	**Intermediate certificate authority (ICA):** there are two types of certificate authorities (CAs), root CAs and intermediate CAs. The ICA serves as a

Acronym	Full Form / Description
	secondary Certificate Authority to shield the RCA from traffic and attacks. The RCA issues the Intermediate CA certificate.
ICANN	The **Internet Corporation for Assigned Names and Numbers** (**ICANN** /ˈaɪkæn/ ***EYE****-kan*) is a nonprofit organization that is responsible for coordinating the maintenance and procedures of several databases related to the namespaces of the Internet - thereby ensuring the network's stable and secure operation. ICANN performs the actual technical maintenance work of the central Internet address pools and DNS Root registries pursuant to the Internet Assigned Numbers Authority (IANA) function contract.
IEEE	The **Institute of Electrical and Electronics Engineers** (**IEEE**, pronounced "I triple E") is a professional association with its corporate office in New York City and its operations center in Piscataway, New Jersey. It was formed in 1963 from the amalgamation of the American Institute of Electrical Engineers and the Institute of Radio Engineers. Today, it is the world's largest association of technical professionals with more than 400,000 members in chapters around the world. Its objectives are the educational and technical advancement of electrical and electronic engineering, telecommunications, computer engineering and allied disciplines.
IETF	The **Internet Engineering Task Force** (**IETF**) develops and promotes voluntary Internet standards, in particular the standards that comprise the Internet protocol suite (TCP/IP). It is an open standards organization, with no formal membership or membership requirements. All participants and managers are volunteers, though their work is usually funded by their employers or sponsors.
ILS	Initial Linkage Seed
IMA	The **Intersection Movement Assist** (**IMA**) application warns the driver of a vehicle when it is not safe to enter an intersection due to high collision probability with other vehicles at stop sign controlled and uncontrolled intersections. This application can provide collision warning information to the vehicle operational systems which may perform actions to reduce the likelihood of crashes at the intersections.
IP	**The Internet Protocol (IP)** is the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries. Its routing function enables internetworking, and essentially establishes the Internet.
IPsec	**Internet Protocol Security (IPsec)** is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session.
IPv4	**Internet Protocol version 4** (**IPv4**) is the fourth version of the Internet Protocol (IP). It is one of the core protocols of standards-based internetworking methods in the Internet, and was the first version deployed for production in the ARPANET in 1983. It still routes most Internet traffic today, despite the ongoing deployment of a successor protocol, IPv6. IPv4 is described in IETF publication

Acronym	Full Form / Description
	RFC 791 (September 1981), replacing an earlier definition (RFC 760, January 1980). IPv4 is a connectionless protocol for use on packet-switched networks. It operates on a best effort delivery model, in that it does not guarantee delivery, nor does it assure proper sequencing or avoidance of duplicate delivery. These aspects, including data integrity, are addressed by an upper layer transport protocol, such as the Transmission Control Protocol (TCP).
IPv6	**Internet Protocol version 6** (**IPv6**) is the most recent version of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion. IPv6 is intended to replace IPv4.
ITS	**Intelligent transportation systems (ITS)** are advanced applications which, without embodying intelligence as such, aim to provide innovative services relating to different modes of transport and traffic management and enable various users to be better informed and make safer, more coordinated, and 'smarter' use of transport networks.
ITS JPO	The **ITS Joint Program Office** (**ITS JPO**), within the Office of the Assistant Secretary for Research and Technology (OST-R), is charged with executing Subtitle C- Intelligent Transportation System Research of Public Law 109-59 Safe Accountable, Flexible, Efficient Transportation Equity Act: A Legacy for Users, enacted August 10, 2005.
kHz	Kilohertz. See Hertz
LA	Linkage Authority. Generates pre-linkage values, which are used to form linkage values that go in the certificates and support efficient revocation. There are two LAs in the SCMS, referred to as LA1 and LA2. The splitting prevents the operator of an LA from linking certificates belonging to a particular device.
LCCF	Local Certificate Chain File
LCI	Linkage Chain Identifier
LCM	Local Certificate Management
LCW	The Blind Spot Warning and **Lane Change Warning** (BSW+**LCW**) application is intended to warn the driver of the vehicle during a lane change attempt if the blind-spot zone into which the vehicle intends to switch is, or will soon be, occupied by another vehicle traveling in the same direction. Moreover, the application provides advisory information that is intended to inform the driver that another vehicle in an adjacent lane is positioned in a blind-spot zone of the vehicle even if a lane change is not being attempted.

Acronym	Full Form / Description
LMBD	Local Misbehavior Detection
LOP	Location Obscurer Proxy. Hides the location of the requesting device by changing source addresses, and thus, prevents linking of network addresses to locations.
LPF	Local Policy File
LS	Linkage Seed
LTA	**Left Turn Assist (LTA)** is an application intended to warn the driver when there is strong probability they will collide with an oncoming vehicle when making a left turn. This is especially critical when the driver's line-of-sight is blocked by a vehicle also making a left turn from the opposite direction.
LV	Linkage Value
MA	Misbehavior Authority. Processes misbehavior reports to identify potential misbehavior or malfunctioning by devices, and revokes and adds them to the CRL, if necessary. It also initiates the process of linking a certificate identifier to the corresponding enrollment certificates and adding them to the RA's internal blacklist. The MA contains two subcomponents: Global Misbehavior Detection, which determines which devices are misbehaving; and CRL Generator, which generates, digitally signs and releases the CRL to the public.
MAC	The **Media Access Control (MAC)** Layer is one of two sublayers that make up the Data Link Layer of the Open System Interconnection (OSI) model. The MAC layer is responsible for moving data packets to and from one Network Interface Card to another across a shared channel.
MAC	In cryptography, a **Message Authentication Code (MAC)** is a short piece of information used to authenticate a message and to provide integrity and authenticity assurances on the message.
MBR	Misbehavior Report
MD	Model Deployment
MHz	Megahertz. See Hertz.
MIB	A **management information base** (**MIB**) is a database used for managing the entities in a communication network. Most often associated with the Simple Network Management Protocol (SNMP), the term is also used more generically in contexts such as in OSI/ISO Network management model. While intended to refer to the complete collection of management information available on an

Acronym	Full Form / Description
	entity, it is often used to refer to a particular subset, more correctly referred to as MIB-module.
MLME	MLME stands for Media Access Control (MAC) Sublayer Management Entity. MLME is the management entity where the Physical layer (PHY) MAC state machines reside.
MPR	Minimum Performance Requirements
NAT	**Network Address Translation** (**NAT**) is a method of remapping one IP address space into another by modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device.
NHTSA	The **National Highway Traffic Safety Administration** (**NHTSA**) is an agency of the Executive Branch of the U.S. government, part of the Department of Transportation. It describes its mission as "Save lives, prevent injuries, reduce vehicle-related crashes." As part of its activities, NHTSA is charged with writing and enforcing Federal Motor Vehicle Safety Standards as well as regulations for motor vehicle theft resistance and fuel economy, the latter under the rubric of the Corporate Average Fuel Economy (CAFE) system. NHTSA also licenses vehicle manufacturers and importers, allows or blocks the import of vehicles and safety-regulated vehicle parts, administers the vehicle identification number (VIN) system, develops the anthropomorphic dummies used in safety testing, as well as the test protocols themselves, and provides vehicle insurance cost information. The agency has asserted preemptive regulatory authority over greenhouse gas emissions, but this has been disputed by such state regulatory agencies as the California Air Resources Board.
NIST	The **National Institute of Standards and Technology** (**NIST**) is a measurement standards laboratory, and a non-regulatory agency of the United States Department of Commerce. Its mission is to promote innovation and industrial competitiveness. NIST's activities are organized into laboratory programs that include Nanoscale Science and Technology, Engineering, Information Technology, Neutron Research, Material Measurement, and Physical Measurement.
NMEA	The **National Marine Electronics Association** (**NMEA**) is a US-based marine electronics trade organization setting standards of communication between marine electronics.
Nonce	In cryptography, a **Nonce** is an arbitrary number that may only be used once. It is similar in spirit to a nonce word, hence the name. It is often a random or pseudo-random number issued in an authentication protocol to ensure that old communications cannot be reused in replay attacks. They can also be useful as initialization vectors and in cryptographic hash function.

Acronym	Full Form / Description
NTP	**Network Time Protocol** (**NTP**) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. In operation since before 1985, NTP is one of the oldest Internet protocols in current use. NTP is intended to synchronize all participating computers to within a few milliseconds of Coordinated Universal Time (UTC). It uses a modified version of Marzullo's algorithm to select accurate time servers and is designed to mitigate the effects of variable network latency. NTP can usually maintain time to within tens of milliseconds over the public Internet, and can achieve better than one millisecond accuracy in local area networks under ideal conditions. Asymmetric routes and network congestion can cause errors of 100 ms or more.
OBE	On-board Equipment
OCB	**Outside the Context of a BSS (OCB)** is a Wireless LAN mode that allows operation and data dissemination without association, avoiding signaling overhead prior to the actual data exchange. This is required to support the high dynamics of vehicular networks that can lead to extremely short contact times and thus, communication opportunities.
OEM	Original Equipment Manufacturer
OFDM	**Orthogonal Frequency Division Multiplexing (OFDM)** is a method of encoding digital data on multiple carrier frequencies. OFDM is a frequency-division multiplexing (FDM) scheme used as a digital multi-carrier modulation method. A large number of closely spaced orthogonal sub-carrier signals are used to carry data on several parallel data streams or channels. Each sub-carrier is modulated with a conventional modulation scheme (such as quadrature amplitude modulation or phase-shift keying) at a low symbol rate, maintaining total data rates similar to conventional *single-carrier* modulation schemes in the same bandwidth.
OSI	**Open Systems Interconnection** networking model
OTA	Over-the-Air
PCA	Pseudonym Certificate Authority. Issues short-term pseudonym, identification, and application certificates to devices. Individual PCAs may be, e.g., limited to a particular geographic region, a particular manufacturer, or a type of device.
PCR	TPM contains several **Platform Configuration Registers** (PCRs) that allow a secure storage and reporting of security relevant metrics.
PDU	In telecommunications, the term **protocol data unit** (**PDU**) has the following meanings:

Acronym	Full Form / Description
	• Information that is delivered as a unit among peer entities of a network and that may contain control information, such as address information, or user data. • In a layered system, a unit of data which is specified in a protocol of a given layer and which consists of protocol-control information and possibly user data of that layer.
PG	Policy Generator. Maintains and signs updates of the Global Policy File (GPF), which contains global configuration information, and the Global Certificate Chain File (GCCF), which contains all trust chains of the SCMS.
PH	Path History
PHY	**PHY** is an abbreviation for the physical layer of the OSI model and refers to the circuitry required to implement physical layer functions. A **PHY** connects a link layer device (often-called MAC as an abbreviation for media access control) to a physical medium such as an optical fiber or copper cable.
PICS	A **Protocol Implementation Conformance Statement** (**PICS**) is a structured document which asserts, which specific requirements are met by a given implementation of a protocol standard.
PKI	A **Public Key Infrastructure** (**PKI**) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.
PLME	Physical Layer management Entity
PLV	Pre-Linkage Value
PoC	Proof of Concept
PP	Path Prediction
PPS	A **pulse per second** (**PPS** or **1PPS**) is an electrical signal that has a width of less than one second and a sharply rising or abruptly falling edge that accurately repeats once per second. PPS signals are output by radio beacons, frequency standards, other types of precision oscillators and some GPS receivers.Precision clocks are sometimes manufactured by interfacing a PPS signal generator to processing equipment that aligns the PPS signal to the UTC second and converts it to a useful display. Atomic clocks usually have an external PPS output, although internally they may operate at 9,192,631,770 Hz. PPS signals have an accuracy ranging from a 12 picoseconds to a few microseconds per second, or 2.0 nanoseconds to a few milliseconds per day based on the resolution and accuracy of the device generating the signal.

Acronym	Full Form / Description
PSID	The **Provider Service Identifier (PSID)** is a four-byte numeric string used by the IEEE 1609 set of standards to identify a particular application service provider that announces that it is providing a service to potential users of an application or service.
RA	The PKI role that assures valid and correct registration is called a **registration authority** (RA). An RA validates and processes requests from devices. From those, it creates individual requests for certificates to the PCA. The RA implements mechanisms to ensure that revoked devices are not issued new certificates, and that devices are not issued more than one set of certificates for a given time period. In addition, the RA provides authenticated information about SCMS configuration changes to devices, which may include a component changing its network address or certificate, or relaying policy decisions issued by the SCMS Manager. Additionally, when sending pseudonym certificate signing requests to the PCA or forwarding information to the MA, the RA shuffles the requests/reports to prevent the PCA from taking the sequence of requests as an indication for which certificates may belong to the same batch and the MA from determining the reporters' routes.
RCA	In a PKI there are two types of certificate authorities (CAs), **root CAs** (**RCA**) and intermediate CAs. An RCA is the root at the top of a certificate chain in the SCMS and hence a trust anchor in a traditional PKI sense. It issues certificates for ICAs as well as SCMS components like PG and MA. An RCA has a self-signed certificate, and a ballot with a quorum vote of the electors establishes trust in an RCA. RCA certificates must be stored in secure storage that is usually referred to as a Trust Store. An entity verifies any certificate by verifying all certificates along the chain from the certificate at hand to the trusted RCA. This concept is called chain-validation of certificates and is the fundamental concept of any PKI. If the RCA and its private key are not secure, then the system is potentially compromised. Due to its importance, an RCA is typically off-line when not in active use.
RIF	Revocation Identifier Field
RF	**Radio frequency** (**RF**) is any of the electromagnetic wave frequencies that lie in the range extending from around 3 kHz to 300 GHz, which include those frequencies used for communications or radar signals.
RSA	**RSA** is one of the first practical public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key, which is kept secret. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers. RSA is made of the initial letters of the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who first publicly described the algorithm in 1977.
RSE	Road-side Equipment. Synonym for RSU. Equivalent to RSU definition in DSRC Roadside Unit (RSU) Specifications Document v4.1

Acronym	Full Form / Description
RSU	Roadside Unit. Synonym for RSE
RTS	**RTS/CTS** (**Request to Send / Clear to Send**) is the optional mechanism used by the IEEE 802.11 wireless networking protocol to reduce frame collisions introduced by the hidden node problem. Originally the protocol fixed the exposed node problem as well, but modern RTS/CTS includes acknowledgements (ACKs) and does not solve the exposed node problem.
RV	Remote Vehicle
SAE	**SAE International**, initially established as the **Society of Automotive Engineers (SAE)**, is a U.S.-based, globally active professional association and standards developing organization for engineering professionals in various industries. Principal emphasis is placed on transport industries such as automotive, aerospace, and commercial vehicles.
SAP	A **Service Access Point** (**SAP**) is an identifying label for network endpoints used in Open Systems Interconnection (OSI) networking.
SBAS	Augmentation of a global navigation satellite system (GNSS) is a method of improving the navigation system's attributes, such as accuracy, reliability, and availability, through the integration of external information into the calculation process. There are many such systems in place and they are generally named or described based on how the GNSS sensor receives the external information. Some systems transmit additional information about sources of error (such as clock drift, ephemeris, or ionospheric delay), others provide direct measurements of how much the signal was off in the past, while a third group provide additional vehicle information to be integrated in the calculation process. A **satellite-based augmentation system** (**SBAS**) is a system that supports wide-area or regional augmentation through the use of additional satellite-broadcast messages. Such systems are commonly composed of multiple ground stations, located at accurately-surveyed points. The ground stations take measurements of one or more of the GNSS satellites, the satellite signals, or other environmental factors which may impact the signal received by the users. Using these measurements, information messages are created and sent to one or more satellites for broadcast to the end users.
SCH	Service Channel
SCMS	The **Security Credential Management System** (**SCMS**) is the term used to identify the PKI used in the U.S. V2X system.
SCMS Manager	Intrinsically central component of the SCMS. The SCMS Manager ensures efficient and fair operation of the SCMS, defines organizational and technical

Acronym	Full Form / Description
	policies, and sets guidelines for reviewing misbehavior and revocation requests to ensure that they are correct and fair according to procedures.
SNMP	**Simple Network Management Protocol** (**SNMP**) is an Internet-standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior. Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks and more. SNMP is widely used in network management for network monitoring. SNMP exposes management data in the form of variables on the managed systems organized in a management information base which describe the system status and configuration. These variables can then be remotely queried (and, in some circumstances, manipulated) by managing applications.
SOAP	**Simple Object Access Protocol (SOAP)** is a messaging protocol that allows programs that run on disparate operating systems (such as Windows and Linux) to communicate using Hypertext Transfer Protocol (HTTP) and its Extensible Markup Language (XML).
SQL	**SQL** (**Structured Query Language**) is a standard interactive and programming language for getting information from and updating a database.
SSL	**SSL** (**Secure Sockets Layer**) is the standard security technology for establishing an encrypted link between a web server and a client. This link ensures that all data passed between the web server and clients remain private and integral.
SSP	**SSP (Service Specific Permission**) is a field that encodes permissions relevant to a particular certificate holder.
STA	In IEEE 802.11 (Wi-Fi) terminology, a **station** (**STA**) is a device that has the capability to use the 802.11 protocol. For example, a station may be a laptop, access point or Wi-Fi phone. Generally in wireless networking terminology, a station, wireless client and node are often used interchangeably, with no strict distinction existing between these terms. A station may also be referred to as a transmitter or receiver based on its transmission characteristics. IEEE 802.11-2007 formally defines station as: *Any device that contains an IEEE 802.11-conformant media access control (MAC) and physical layer (PHY) interface to the wireless medium (WM).*
TAI	**International Atomic Time** (**TAI**, from the French name ***Temps Atomique International***) is a high-precision atomic coordinate time standard based on the notional passage of proper time on Earth's geoid. It is the basis for Coordinated Universal Time (UTC), which is used for civil timekeeping all over the Earth's surface, and for Terrestrial Time, which is used for astronomical calculations. As of 30 June 2015 when another leap second was added, TAI is exactly 36 seconds ahead of UTC. The 36 seconds results from the initial difference of 10 seconds at the start of 1972, plus 26 leap seconds in UTC since 1972.

Acronym	Full Form / Description
TCP	The **Transmission Control Protocol** (**TCP**) is a core protocol of the Internet Protocol Suite. It originated in the initial network implementation in which it complemented the Internet Protocol (IP). Therefore, the entire suite is commonly referred to as TCP/IP.
TCG	The **Trusted Computing Group** is a group formed by AMD, Hewlett-Packard, IBM, Intel and Microsoft to implement Trusted Computing concepts across personal computers.TCG's original goal was the development of a Trusted Platform Module (TPM), a semiconductor intellectual property core or integrated circuit that conforms to the trusted platform module specification put forward by the Trusted Computing Group and which is to be included with computers to enable trusted computing features.
TCotSCMSM	Technical Component of the SCMS Manager
TIM	Traveler Information Message as described in SAE J2735.
TLS	**Transport Layer Security** (**TLS**) is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL).
TMC	Traffic Management Center.
TPM	**Trusted Platform Module** (**TPM**) is an international standard for a secure cryptoprocessor, which is a dedicated microcontroller designed to secure hardware by integrating cryptographic keys into devices.
TRNG	A **true random number generator** (**TRNG**) is a device that generates random numbers from a physical process, rather than a computer program. Such devices are often based on microscopic phenomena that generate low-level, statistically random "noise" signals, such as thermal noise, the photoelectric effect, involving a beam splitter, and other quantum phenomena. These processes are, in theory, completely unpredictable, and the theory's assertions of unpredictability are subject to experimental test. The main application for electronic hardware random number generators is in cryptography, where they are used to generate random cryptographic keys to transmit data securely.
TSF	**Timing Synchronization Function** (**TSF**) is specified in IEEE 802.11 wireless local area network (WLAN) standard to fulfill timing synchronization among users. A Timing Synchronization Function (TSF) keeps the timers for all stations in the same Basic Service Set (BSS) synchronized.
Tx	In telecommunications, **transmission** (abbreviation: **Tx**) is the process of sending and propagating an analogue or digital information signal over a physical point-to-point or point-to-multipoint transmission medium, either wired, optical fiber or wireless.

Acronym	Full Form / Description
USDOD	The **United States Department of Defense** (**USDOD** or **DoD**) is an executive branch department of the federal government of the United States charged with coordinating and supervising all agencies and functions of the government concerned directly with national security and the United States Armed Forces. It is headquartered at the Pentagon in Arlington, Virginia, just outside of Washington, D.C.
USDOT	The **United States Department of Transportation** (**USDOT** or **DOT**) is a federal Cabinet department of the U.S. government concerned with transportation. It was established by an act of Congress on October 15, 1966, and began operation on April 1, 1967.
UT1	**Universal Time** (**UT**) is a time standard based on Earth's rotation. It is a modern continuation of Greenwich Mean Time (GMT), i.e., the mean solar time on the Prime Meridian at Greenwich, London, UK. In fact, the expression "Universal Time" is ambiguous (when accuracy of better than a few seconds is required), as there are several versions of it, the most commonly used being Coordinated Universal Time (UTC) and UT1. All of these versions of UT, except for UTC, are based on Earth's rotation relative to distant celestial objects (stars and quasars), but with a scaling factor and other adjustments to make them closer to solar time. UTC is based on International Atomic Time, with leap seconds added to keep it within 0.9 second of UT1. **UT1** is the principal form of Universal Time. While conceptually it is mean solar time at 0° longitude, precise measurements of the Sun are difficult. Hence, it is computed from observations of distant quasars using long baseline interferometry, laser ranging of the Moon and artificial satellites, as well as the determination of GPS satellite orbits. UT1 is the same everywhere on Earth, and is proportional to the rotation angle of the Earth with respect to distant quasars, specifically, the International Celestial Reference Frame (ICRF), neglecting some small adjustments. The observations allow the determination of a measure of the Earth's angle with respect to the ICRF, called the Earth Rotation Angle (ERA, which serves as a modern replacement for Greenwich Mean Sidereal Time). UT1 is required to follow the relationship ERA = $2\pi(0.7790572732640 + 1.00273781191135448T_u)$ radians, where T_u = (Julian UT1 date - 2451545.0)
UTC	**Coordinated Universal Time** (**UTC**), is the primary time standard by which the world regulates clocks and time. It is within about 1 second of mean solar time at 0° longitude; it does not observe daylight saving time. It is one of several closely related successors to Greenwich Mean Time (GMT). For most purposes, UTC is considered interchangeable with GMT, but GMT is no longer precisely defined by the scientific community. UTC was officially formalized in 1960 by the International Radio Consultative Committee in Recommendation 374, having been initiated by several national time laboratories. The system was adjusted several times until leap seconds were adopted in 1972 to simplify future adjustments. A number of proposals

Acronym	Full Form / Description
	have been made to replace UTC with a new system that would eliminate leap seconds, but no consensus has yet been reached. The current version of UTC is defined by International Telecommunications Union Recommendation (ITU-R TF.460-6), *Standard-frequency and time-signal emissions* and is based on International Atomic Time (TAI) with leap seconds added at irregular intervals to compensate for the slowing of Earth's rotation. Leap seconds are inserted as necessary to keep UTC within 0.9 seconds of universal time, UT1.
V2I	**Vehicle-to-Infrastructure** (**V2I**). See V2X
V2V	**Vehicle-to-Vehicle** (**V2V**) is an automobile technology designed to allow automobiles to "talk" to each other. In the US the systems will use a region of the 5.9 GHz band set aside by the United States Congress in 1999. V2V is also known as VANET (vehicular ad hoc network). It is a variation of MANET (Mobile ad hoc network), with the emphasis being now the node is the vehicle.
V2V-SE	Vehicle to Vehicle System Engineering and Vehicle Integration Research for Deployment (CAMP Project)
V2X	**Vehicle-to-everything** (**V2X**) communication is the passing of information from a vehicle to any entity that may affect the vehicle, and viceversa. It is a vehicular communication system that incorporates other more specific types of communication as V2I (Vehicle-to-Infrastructure), V2V (Vehicle-to-vehicle), V2P (Vehicle-to-Pedestrian), V2D (Vehicle-to-device) and V2G (Vehicle-to-grid).
VIIC	Vehicle Infrastructure Integration Consortium
VOD	Verify on Demand
VPN	A **Virtual Private Network** (**VPN**) extends a private network across a public network, such as the Internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network, and, thus, are benefiting from the functionality, security and management policies of the private network.A VPN establishes a virtual point-to-point connection using dedicated connections, virtual tunneling protocols, or traffic encryption.
VSA	Vendor Specific Action
VSC-A	Vehicle Safety Communication - Applications (CAMP project)
VSC3	Vehicle Safety Communications 3 (CAMP Consortium)

Acronym	Full Form / Description
VSC5	Vehicle Safety Communications 5 (CAMP Consortium)
VSCS	Vehicle Safety Communications Security (Studies, CAMP projects)
WAAS	The **Wide Area Augmentation System** (**WAAS**) is an air navigation aid developed by the Federal Aviation Administration (prime contractor Raytheon Company) to augment the Global Positioning System (GPS), with the goal of improving its accuracy, integrity, and availability.
WAN	**Wide Area Network (WAN)** is a computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local-area networks (LANs).
WAVE	IEEE 802.11p is an approved amendment to the IEEE 802.11 standard to add **Wireless Access in Vehicular Environments** (**WAVE**), a vehicular communication system. It defines enhancements to IEEE 802.11 (the basis of products marketed as Wi-Fi) required to support Intelligent Transportation Systems (ITS) applications. This includes data exchange between high-speed vehicles and between the vehicles and the roadside infrastructure in the licensed ITS band of 5.9 GHz (5.85-5.925 GHz).
WBSS	To define different WAVE communication zones, think of the term **WAVE Basic Service Set** (**WBSS**) as a unique identifier for each communication zone. Vehicles must associate with only one WBSS at a time.
Wget	**GNU Wget** (or just **Wget**) is a computer program that retrieves content from web servers, and is part of the GNU Project. Its name is derived from *World Wide Web* and *get*. It supports downloading via HTTP, HTTPS, and FTP protocols.
WGS	The **World Geodetic System** (**WGS**) is a standard for use in cartography, geodesy, and navigation including by GPS. It comprises a standard coordinate system for the Earth, a standard spheroidal reference surface (the *datum* or *reference ellipsoid*) for raw altitude data, and a gravitational equipotential surface (the *geoid*) that defines the *nominal sea level*.
WME	The **WAVE Management Entity** (**WME**) represents another entity that is unique to WAVE standards and performs much of the operations unique to WAVE standards. For instance, when data frames are scheduled, the transmission channel must be defined along with QoS priorities. Those priorities must allow an emergency safety message to be transmitted at anytime with very limited latency. Management of frame queuing, priority channels and handling of safety messages are quite unique to WAVE standards. The WME handles those particular processing in coordination with other design entities.
WSM	WAVE Short Message
WSA	WAVE Service Advertisement

Acronym	Full Form / Description
WSMP	WAVE communication services provide data communications over two protocol stacks, namely; IPv6 and **WAVE Short Message Protocol** (**WSMP**). WSMP is unique to the WAVE standards and is designed for use by specialized applications like safety applications. Applications using WSMP may initiate a WBSS to configure the Service Channel (SCH) for their use. But availability of SCH is optional since WSMP can be exchanged on the Control Channel (CCH) even in the absence of WBSS (i.e., in a V2V scenario).